IT Systems
www.SystemOnLine.cz
Číslo 1–2/2022
Ročník 24
110 Kč/5 €
Leden–Únor
Január–Február

Retail v roce 2022 bude o flexibilitě
a automatickém řízení zásob

Plánování výroby a nákupu
má velké nároky na kvalitu IS

Automatizace přináší efektivitu
v každém odvětví

Budoucnost business intelligence
je v propojení kompozitní analytiky a headless BI

ITAM musí být proaktivní
a hledět do budoucnosti

Příloha IT Security 2022

9 771212 456008 01

Cesta průmyslu od automatizace k autonomii • Optimalizace logistiky
Prediktivní řízení zásobování čerstvými potravinami • Moderní řízení skladu
Nová éra e-commerce • Jak úspěšně vstoupit do světa e-commerce? • E-shop budoucnosti zná svého zákazníka • Digital Services Act

MasterDC

Udržujeme firemní IT v pohybu

master.cz

Klíčovou schopností bude flexibilita

V aktuálním vydání IT Systems jsme se zaměřili na problematiku digitalizace potravinářství, logistiky a retailu. Tato odvětví prochází bouřlivými a do značné míry vynucenými změnami. Jejich důsledkem je zmatek na všech úrovních dodavatelského řetězce a problémy, které velmi pravděpodobně potrvají i nadále. Návrat dodavatelského řetězce do stavu před pandemií totiž nelze podle odborníků čekat dříve než v horizontu několika let. K vytvoření nové rovnováhy bude třeba, aby podniky přehodnotily svá dosavadní řešení a byly ještě flexibilnější.

Podle Martina Plajnera z Logio se dodavatelské řetězce nachází ve stavu, kdy viditelně vyžadují revizi a mnohdy tvrdé zásahy, aby mohly dál efektivně fungovat. Ve svém článku pak představuje strategii optimalizace, která je založena na třech pilířích od pochopení výchozího stavu, přes quick wins až po strategické změny logistiky.

Roland Džogan z Ydistri ve svém článku popisuje, že na změny, které pandemie přinesla, byli nuceni bezprostředně reagovat nejen obchodníci a dodavatelé, ale své chování přehodnocovali také zákazníci. Spotřebitelé si v době pandemie rychle zvykli na online nakupování a vyšší podíl nákupů na internetu nezmizí ani po jejím odeznění. Je tak dál jasnější, že retail bude pod narůstajícím tlakem, aby technologicky držel krok s konkurencí v podobě dravé a rychle rostoucí e-commerce. Aby kamenné obchody zůstaly konkurenceschopné, musí se technologicky vyzbrojit. To ovšem platí i pro e-shopy. Lockdown jim přinesl výhodu, která se už doufejme nebude opakovat. Matěj Kapošváry ze Shopsysu se proto zamýšlí, jak nepromarnit šanci, kterou přinesl skokový růst e-commerce. Lásló Szabó z agentury Growww Digital na něj volně navazuje a dodává, že klíčem pro úspěch e-commerce je znát potřeby a chování nakupujících. Proto podle něj dále poroste význam personalizace, kdy se e-shop snaží poznat každého zákazníka individuálně a přizpůsobit mu nabídku i komunikaci na míru. Radoslav Revenda z E LINKX zase upozorňuje, že probíhající změny mají velký dopad na efektivitu skladů, a proto se ve svém článku věnuje modernizaci jejich řízení s využitím nových technologií.

S Vladimírem Bartošem z Minervy se podíváme na samý počátek problémů dodavatelského řetězce – na výrobní podniky, které podle něj často nedokážou nastartovat systémové plánování. Přitom proces plánování výroby a nákupu má největší přidanou hodnotu. Současně je ale závislý na dobré funkci a spolupráci všech oddělení ve firmě. Stačí jedno nefunkční a plánování přestává správně pracovat. Vladimír se proto ve svém článku zamýšlí, jak zlepšit plánování ve výrobním podniku a dosáhnout snížení zásob a rozpracovanosti při rostoucích tržbách.

Na závěr bych chtěl ještě upozornit na článek Milana Frýberta z Bootiq, který radí, jak úspěšně vstoupit do světa e-commerce, a upozorňuje, že to firmu změní od základů. Samotné otevření e-shopu je podle něj jen špičkou ledovce. Nenechte si ujít ani rozhovor s Davidem Foxenem, který má dlouholeté zkušenosti v oblasti IT Asset Managementu. Požádali jsme ho o rozhovor, ve kterém jsme hovořili o tom, proč by se ITAM měl dívat více do budoucnosti.

Výše uvedené je pouze malým zlomkem obsahu nového vydání IT Systems, a proto věřím, že v něm opět najdete inspiraci pro rozvoj vašeho podniku nebo organizace. Tak neváhejte a pusťte se do čtení!

Lukáš Grásgruber

OBSAH

Příloha IT Security 2022:

ZETOR bude řídit výrobu, prodej i servis **systémem Infor SyteLine**

Společnost ZETOR TRACTORS, výrobce legendárních traktorů ZETOR, zahájila budování nového informačního řešení. Cílem je sjednotit procesy a nástroje společnosti v Česku i všech světových pobočkách. Základem nového řešení bude ERP systém Infor SyteLine (CloudSuite Industrial) včetně pokročilého plánování APS, integrační platformy Infor OS, konfigurátoru Infor CPQ a další prvky.

Dodavatelem řešení je softwarová a konzultační společnost ITeuro, která bude v projektu kombinovat on-premise i cloudový software. ERP Infor SyteLine nasadí ZETOR klasickou formou na hostovaném nebo vyhrazeném hardwaru. Konfigurátor a portály Infor CPQ a integrační platforma Infor OS včetně nástrojů pro řízení dokumentů IDM a týmovou spolupráci Ming.le poběží v cloudu. V rámci ERP mají významnou roli pokročilé plánování výroby APS s vazbou na řízení dodavatelského řetězce a rozšiřující modul Servis a údržba jak pro informace o servisních zásazích vyrobených vozidel, tak pro potřeby interní údržby výrobního provozu. Počítá se rovněž s nasazením pevných počítačových terminálů na výrobních linkách a mobilních terminálů pro logistické procesy.

Součástí B2B portálu Enterprise Quoting pro přímý prodej i partnery a distributory bude konfigurátor Infor CPQ, samozřejmě provázaný s technologickými daty a výrobou v ERP. Prodejcům po celém světě umožní jednoduše vytvářet složité nabídky a zpřístupní katalog dílů včetně vyhledávání podle VIN kódu vozidla. Zároveň pomocí workflow urychlí řešení nestandardních požadavků, které přesahují rámec běžných smluv a obchodních podmínek, tudíž podléhají schválení příslušnou autoritou.

Ve značné míře se využijí i ostatní webové portály, které obsáhnou celý životní cyklus traktoru od poptávky po následný servis. Dodavatelé budou přes portál reagovat na poptávku komponent pro výrobu, dealeři nejen konfigurovat nové stroje, ale i objednávat náhradní díly a řešit servis vozidel.

ERP Infor SyteLine nahradí v ZETOR TRACTORS zastaralý a již nepodporovaný systém Avalon.

Společnost **eobuv nasadila** cloudové **řešení Oracle** Retail

Společnost eobuwie.pl, která na českém trhu působí pod značkou eobuv a je lídrem regionu CEE v online prodeji obuvi, tašek a doplňků, zvolila pro plánování zásob a správu zboží cloudové řešení Oracle Retail. Od nového řešení si slibuje možnost provádět integrovanější a chytřejší plánování pro všechny produktové řady napříč rostoucím sortimentem. Díky expanzi na nové trhy se totiž firmě stále rozrůstají zásoby a sortiment obuvi a doplňků. Díky volbě cloudového řešení bylo možné implementaci provést během pouhých 13 týdnů.

„Díky nové cloudové službě můžeme zlepšit plánování napříč různými kanály, trhy a segmenty zákazníků, a lépe tak podpořit naše rostoucí podnikání. Plánovači mohou proaktivně řídit proces open-to-buy pomocí nástroje Oracle Retail Merchandise Financial Planning,“ řekl k přínosům nového řešení Wiktor Miernik-Zdanowicz, vedoucí oddělení obchodních operací ve společnosti eobuwie.pl S.A, a dodal: *„Naším cílem je trávit méně času ručním shromažďováním dat a více času analýzou a identifikací příležitostí zvyšujících ziskovost.“*

„Díky investici do řešení Oracle Cloud se společnost eobuwie.pl může soustředit na své hlavní podnikání a zároveň pro vylepšení plánování a správy zboží využít zabudovanou sílu strojového učení a umělé inteligence.“ dodal Mike Webster, senior viceprezident a vrchní ředitel pro řešení Oracle Retail ve společnosti Oracle.

Společnost eobuwie.pl zvolila řešení Oracle Retail Merchandise Financial Planning Cloud Service provozované na infrastruktuře Oracle Cloud Infrastructure. Na implementaci řešení spolupracovala společnost Pronos, člen Oracle PartnerNetwork (OPN). Díky využití „štíhlého“ přístupu k projektu Pronos úspěšně implementoval novou cloudovou službu za pouhých 13 týdnů.

„Zaměstnanci z IT oddělení a obchodní týmy eobuwie.pl nyní mohou spolupracovat prostřednictvím centralizovaného plánovacího procesu. Očekáváme, že maloobchodní prodejci dokážou zvýšit marže díky optimalizaci politiky slev a zásob na konci sezóny,“ komentuje očekávané přínosy nasazeného řešení Pawel Kowalewski, viceprezident společnosti Pronos.

ČSOB šetří náklady díky zavedení voicebota

Československá obchodní banka (ČSOB) vytvořila spolu s firmou VOCALLS voicebota, tedy konverzačního hlasového asistenta s umělou inteligencí. Voicebot pomáhá ve druhé největší bance v ČR s obsluhou klientů na telefonu. Jeho vytížení postupně roste a například loni v říjnu už obsloužil více než 200 tisíc hovorů. Významně přitom šetří náklady a podle banky zvyšuje spokojenost klientů ve srovnání se starší technologií hlasového automatu IVR.

Cílem implementace voicebota bylo uvolnit ruce telefonním operátorům od rutinních hovorů a získat tak prostor pro řešení složitějších

a časově náročnějších požadavků. Pokročilý hlasový ekosystém byl v ČSOB vytvořený a plně integrovaný do bankovního IT prostředí během jednoho roku. Voicebot v podobě hlasového asistenta už zcela nahradil starší hlasový automat IVR (Interactive Voice Response). Díky tomu už zákazník neuslyší žádné „pro platby stiskněte jedničku“, ale jednou větou řekne, co potřebuje, a podle toho je odbaven nebo přepojen. Míra následného přepojování z prvního specialisty, který hovor přijme, na dalšího klesla díky voicebotovi z 23 % na 16 %. V relativním srovnání se tak zlepšila úspěšnost přepojení na správného specialistu o 35 %. Voicebot již dnes zvládá více než 130 různých klientských požadavků a tým VOCALLS s ČSOB pracuje na propojení voicebota s dalšími bankovními systémy (např. pro identifikaci a autentizaci klienta, nebo sjednání schůzky na pobočce).

„Ve srovnání s lidskou pracovní silou ušetří náš voicebot na klientském centru ČSOB až dvě třetiny nákladů,“ dodává k praktickým dopadům zavedení hlasového asistenta v klientském centru Artem Markevich, CEO VOCALLS.

Vedle správného přepojení na specialistu hlasový asistent v ČSOB postupně zvládl zcela vyřešit některé servisní požadavky. Umí klienta navést, jak si může službu změnit nebo nastavit sám. Např. odblokování přístupu do ČSOB identity nebo změna limitů platební karty. Zvládne i sám volat klientům z banky a také pomáhá při neočekávaných událostech a vysokém zatížení klientského centra (např. poskytoval informace o novince v zasílání potvrzení o platbě kartou na Internetu).

„Zážitek klienta při rozhovoru s hlasovým asistentem oproti IVR je nesrovnatelný. Obávali jsme se, jak budou klienti na voicebota reagovat, ale mnoho klientů ani nepozná, že nemluví s živým operátorem! Kvalitu řešení našeho voicebota dokazují i ocenění odborníků v několika soutěžích v ČR i v rámci Evropy,“ dodává Jan Sadil, člen představenstva ČSOB.

Joyson PlasTec vsadil na cloudové řešení

Německý výrobce plastových komponent pro automobilový průmysl, firma Joyson PlasTec, oznámila, že se rozhodla pro modernizaci svého informačního systému a bude implementovat oborové cloudové řešení Infor CloudSuite Automotive, specificky určené pro automobilový průmysl. Cílem modernizace je získat větší flexibilitu a schopnost rychle reagovat na změny na extrémně konkurenčním trhu.

Joyson PlasTec GmbH je předním dodavatelem plastových komponent pro automobilové výrobce, když jeho portfolio zahrnuje interiérové a exteriérové díly na bázi vstřikování plastů jak pro osobní, tak nákladní vozy. Společnost zaměstnává zhruba 380 lidí v bavorském Alberthausenu. Nové IT řešení, pro které se společnost rozhodla,

je přesně zacílené na potřeby automobilového průmyslu. Obsahuje široké spektrum funkčností zaměřených za řízení výroby a kvality, řízení dodavatelského řetězce, plánování i řízení vztahů se zákazníky. Řešení rovněž nabízí podporu v oblasti Internetu věcí (IoT), machine-to-machine konektivity a elektronické výměny dat (EDI) postavené na platformě Amazon Web Services (AWS). Součástí implementace bude i analytické řešení Infor Birst, od kterého Joyson PlasTec očekává výrazné zrychlení reportovacích a rozhodovacích procesů.

„Výhodou vybraného řešení je, že je navrženo přímo pro potřeby automobilového průmyslu a je vysoce škálovatelné," řekl Jörg Koch, finanční ředitel Joyson PlasTec. „Infor CloudSuite Automotive je živé softwarové řešení a díky multi-tenantnímu cloudu budeme mít k dispozici vždy nejaktuálnější technologie a budeme se moci soustředit výhradně na hlavní výzvy svého podnikání."

Během nasazení zákazník využije nejnovějšího implementačního konceptu 60-30-10, kdy bude s pomocí implementačního akcelerátoru nasazeno 60 % standardní funkčnosti a procesů a dalších 30 % s využitím konfigurátoru k zajištění hladkého přechodu na ostrý provoz. Zbylých 10 % vysoce specifických a unikátních podnikových procesů bude vyřešeno dodatečně. Takto bude zajištěna vysoká kvalita a rychlost nasazení celého systému.

ČÚZK rozšířil možnosti přihlašování do IS Katastru nemovitostí

Český úřad zeměměřický a katastrální (ČÚZK) zavedl nové řešení pro přihlašování ke službám Katastru nemovitostí. K přihlášení je možné použít eObčanku i BankID, současně se zvýšila bezpečnost systému a modernizoval jeho vzhled. Ve spolupráci se společností Ness Czech nasadil ČÚZK nový přihlašovací portál, který zastřešuje přihlašování uživatelů a umožňuje ověřit identitu uživatele pomocí externí autority NIA (Národní identitní autorita) v rámci architektury eGovernmentu ČR. ČÚZK je mezi českými úřady v tomto směru průkopníkem a napojení na NIA přinesl jako jeden z prvních.

Český úřad zeměměřický a katastrální v minulosti umožňoval přístup k externím službám buď anonymním uživatelům, nebo uživatelům registrovaným přímo v IS ČÚZK. Historicky úřad pro registraci a správu externích uživatelů provozoval dva systémy, z hlediska technologií i procesů zcela oddělené.

„Zadavatel požadoval sjednocení autentizačních a autorizačních procesů a v souladu se strategií eGovernmentu přístup i s pomocí externí autority NIA. Uživatelé se díky tomu mohou přihlašovat několika způsoby, včetně využití portálu Identita občana, který nabízí širokou

škálu autentizačních prostředků, jako jsou Mobilní klíč eGovernmentu, NIA ID, eObčanka, Bankovní identita, mojeID a další," říká Martin Silvička ze společnosti Ness Czech.

Nově se tedy uživatelé již nemusí registrovat v systémech ČÚZK a služby katastru nemovitostí mohou využívat na základě přihlášení do svého účtu v portálu Identita občana. Přístup přitom získají i k těm informacím a službám, které byly dosud anonymním uživatelům částečně či zcela nedostupné. Především jde o dálkový přístup a nahlížení do Katastru nemovitostí a návrhy na vklad. Přes Identitu občana je také možné zřídit Službu sledování změn (SSZ), která uživatele automaticky informuje prostřednictvím datové schránky, e-mailu či SMS, pokud u sledované nemovitosti dojde ke změně záznamů v katastru. Součástí strategie ČÚZK je publikovat své výstupy více externě, nicméně v souladu s GDPR.

Nové řešení přineslo také zvýšení bezpečnosti přihlašování díky zajištění vyšší dostupnosti, výkonu, robustnosti a nezávislosti aplikace Přihlašovací portál ČÚZK na ostatních systémech ČÚZK. Podstatnou novinkou z hlediska bezpečnosti je také zavedení možnosti dvoufaktorové autentizace uživatelských účtů evidovaných v ČÚZK, buď prostřednictvím jednorázového SMS kódu nebo ještě bezpečnější metody užití jednorázového kódu generovaného autentizační mobilní aplikací.

Na základě reálných zkušeností z provozu byly optimalizovány procesy Přihlašovacího portálu zejména s ohledem na zajištění provozu a administrace řešení. Byly zpřístupněny další výstupy uživatelům externích služeb ČÚZK a objednávkový systém byl modernizován z pohledu přístupnosti plně responzivního designu. Moderní vzhled a chování webových aplikací doplňuje podpora moderních prohlížečů a soulad s pravidly přístupnosti dle normy WAI-ARIA.

LOMAX nasadí nový konfigurátor pro B2B partnery

Společnost LOMAX, která je největším českým výrobcem garážových vrat, se rozhodla pro implementaci řešení Infor CPQ. Jde o konfigurátor produktů, který bude součástí nového B2B portálu pro konfiguraci sekčních, posuvných a křídlových vrat, rolovacích systémů a venkovních žaluzií. Rozšiřující modul Infor 3D Design Automation umožní po konfiguraci generování 3D výstupů v různých formátech. Vše bude napojeno na stávající ERP systém HELIOS iNuvio.

Řešení Infor CPQ dodá LOMAXu společnost ITeuro. Dokončení projektu je naplánováno na březen 2022. *„Kvalitní konfigurátor pro B2B partnery vnímáme jako nezbytnou součást zlepšování a zrychlení prodejních procesů. Vybrali jsme si Infor CPQ jako osvědčený produkt s prokazatelnými přínosy. Reference ITeuro nám jednoznačně potvrdily*

jak vhodnost řešení pro naše potřeby, tak firmy ITeuro jako dodavatele, " říká Radek Dufek, jednatel a obchodní ředitel společnosti LOMAX.

foto: Komfort.cz

Oceněné projekty digitalizace obchodních a logistických procesů

V prosinci se tradičně konalo vyhlášení soutěže portálu EDIZone.cz za projekt roku v oblasti elektronizace obchodních a logistických procesů. Do finále 11. ročníku se probojovala IT firma MoroSystems, která díky digitalizaci účetnictví šetří 60 hodin práce měsíčně, nebo maloobchodní řetězec Albert, který s digitalizací pomáhá svým dodavatelům. Vítězem se ale stal e-shop MALL.CZ, který díky komplexnímu řešení automatizace dat šetří až 4 miliony korun ročně.

Brněnská IT firma MoroSystems je příkladem toho, že automatizace prospívá i menším firmám. Do finále soutěže se dostala díky tomu, že za minimální náklady ušetřila 60 hodin práce měsíčně. A to je pro

Iva Šmerdová

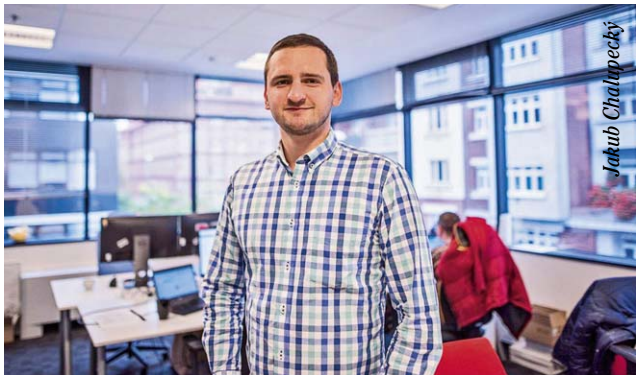
firmu o 130 lidech velký skok. „Dříve jsme jednu fakturu zpracovávali přibližně čtvrt hodiny, teď to stíháme za 5 minut," říká hlavní účetní Iva Šmerdová z firmy MoroSystems, která pro automatizaci příjmu faktur využívá řešení Invoice Flow.

Druhým finalistou byl maloobchodní řetězec Albert, který vytvořil jednoduchou webovou aplikaci pro své menší dodavatele, aby si mohli faktury či dodací listy posílat elektronicky. „S největšími dodavateli fungujeme elektronicky již od roku 2002, chtěli jsme ale zapojit také menší dodavatele,

Petr Beran

a proto jsme se společností Grit vyvinuli bezplatné řešení Albert portál. Jediné, co teď dodavatelé k bezpapírové komunikaci s námi potřebují, je přístup k internetu," říká manažer společnosti Petr Beran.

Absolutní vítěz, e-shop MALL.CZ, s digitalizací objednávek a faktur začal před sedmi lety. Jen za rok 2020 na zpracování faktur ušetřil 4 miliony korun. MALL.CZ digitalizoval také schvalování objednávek



Jakub Chalupecký

a faktur. Díky tomu šetří čas na interních procesech i na administrativě s dodavateli, čímž se jim daří dlouhodobě zlepšovat vzájemné vztahy.

„Když se na elektronizaci faktur podívám zpětně, šlo při našem vysokém množství dodavatelů a dokladů o projekt s rychlou návratností," říká finanční ředitel MALL.CZ Jakub Chalupecký. „Nový digitalizovaný proces nám navíc pomohl zajistit snadné a bezpečné fungování v době covidu, kdy většina zaměstnanců pracuje na home office," dodává. ■

Potenciál digitalizace tuzemského průmyslu je obrovský, klíčem k úspěchu je práce s velkými a relevantními daty

Martin Hummel, Teodor Škereň

Digitalizace českého a slovenského průmyslu má za vyspělými západními zeměmi stále zpoždění. Rezervy ve využití či zpracování dat z výroby směrem ke zvýšení automatizace a lepším datovým analýzám vnímá podle našeho loňského průzkumu 55 % českých firem a dokonce 70 % podniků ze Slovenska. Hledat příčiny pouze v ekonomické síle podniků či jejich technologickém a personálním zázemí by ale bylo příliš velké zjednodušení.

Důležitou roli v tempu digitalizace totiž hraje struktura ekonomiky. I když se situace postupně mění, v Česku i na Slovensku stále v průmyslu hrají velkou roli výrobní podniky s vysokým podílem lidské práce. Zahraniční matky českých firem si naopak na vlastním trhu ponechávají ty části celého výrobního a obchodního řetězce, jež nesou vysokou přidanou hodnotu a marži – výzkum a vývoj, hi-tech produkci, marketing a prodej. Administrativní a obchodní činnosti se přitom dají digitalizovat snadněji než výroba závisející do velké míry na lidech. Také mezi Českem a Slovenskem však panují v digitalizaci průmyslu rozdíly. Česko sice má řadu technologicky špičkových vysoce digitalizovaných firem, vedle nich ale stále stojí silná sféra tradičních strojírenských či montážních podniků s kvalitní a specializovanou kusovou či malosériovou výrobou. Právě tyto firmy jsou přitom s digitalizací často teprve na začátku, protože u produkce v malých sériích bývá mnohdy efektivnější a levnější dál sázet na lidskou práci.

Naopak Slovensko v oblasti digitalizace paradoxně těží z toho, že tamní průmyslové podniky se většinou rozvíjely později než ty české. Klasických výrobních firem s dlouhou historií je tam proto méně a větší váhu mají výrobní a montážní továrny zahraničních koncernů, typických například pro segment automotive, jenž se vyznačuje robotizovanou a široce digitalizovanou pásovou produkcí s velkými počty opakovaných výrobků.

Celkové výsledky průzkumu, který jsme si o digitalizaci podniků nechali zpracovat, tak pro obě země ukázaly srovnatelné výsledky, ačkoli se podoba jejich průmyslu liší – prvky digitalizace, technologie IoT a principy průmyslu 4.0 má již zavedeno, nebo je právě zavádí, celkem 58 % českých firem a 51 % slovenských podniků.

Klíčem k digitalizaci jsou data

Digitalizace průmyslových podniků postupuje ve dvou rovinách. První z nich spočívá v generování dále využitelných dat při výrobě – v tomto ohledu je většina českých i slovenských podniků obvykle již na pokročilé úrovni. I starší stroje jsou už v dnešní době řízené počítačem, který o zařízení prostřednictvím senzorů a čidel získává řadu informací. Ví, zda stroj funguje, jak má, zkontroluje výrobek a dokáže identifikovat případné zmetky. Data jsou ale přítomna pouze na lokální úrovni a jakmile výrobní cyklus skončí, bez využití mizí. Pro továrnu jako celek pak nemají žádný přínos.

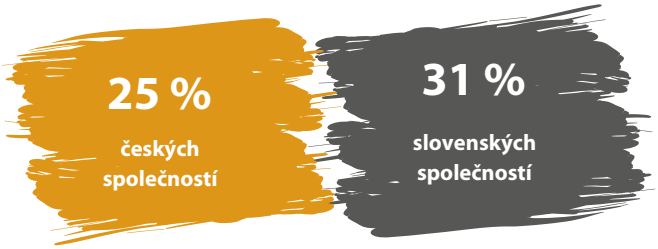
Právě na tomto místě se ukazuje potenciál druhé pokročilejší roviny digitalizace. Její jádro je ve shromažďování již dostupných dat, jejich centralizovaném zpracování, následné analýze a přeměně na dále využitelné informace. Ty pak slouží k optimalizaci výroby a vylepšení provozních postupů. Výsledkem mohou být úspory energií, snížení frekvence servisu, zvýšení životnosti strojů, předcházení odstávkám

2/3

SPOLEČNOSTÍ SBÍRÁ DIGITÁLNĚ DATA Z PRODUKCE A UKLÁDÁ JE CENTRÁLNĚ

Přičemž ve více než 3/4 společností jde hlavně o kvantitativní data využité na řízení produktivity a efektivity výroby. Tato data jsou považována za nejdůležitější až v 80 % společností. 1/3 společností sbírá data týkající se kvality produkce a i tato kvalitativní data považuje za důležité a na řízení kvality je využívá.

DENNĚ ČELÍ NEČEKANÝM VÝPADKŮM VÝROBY



Ovšem údržbu plánují hlavně podle výrobních parametrů a zkušeností (v ČR) nebo v pravidelných intervalech (v SR).

a závažným poruchám či lepší řízení kvality výroby. To s sebou přináší časové i finanční úspory a rychlejší rozvoj podnikání.

Jednoduchá řešení místo komplexních zásahů

Zástupci průmyslových firem, pro které u nás ve firmě připravujeme projekty digitalizace, zpravidla přicházejí s poptávkou na řešení konkrétního problému. Buď jde o zadání v produktivně-optimalizační oblasti, kdy je například potřeba zvýšit objem výroby či snížit náklady, kupříkladu minimalizací výpadků, nebo se jedná dodržování parametrů při výrobě, jejich sledování a dopady na kvalitu výsledného výrobku. Vždy je ale potřeba mít nad technickým řešením digitalizace nasazený ještě další proces, který dokáže získaná data ze zařízení a čidel zpracovat a zasadit do kontextu celého provozu.

Mnozí manažeři si pojem digitalizace automaticky spojují s vysokými náklady a komplexní těžkou úlohou s nejistým výsledkem. Především tak jde o to, jim představit možnosti, které poskytuje správná datová analýza a zároveň ukázat, že v konečném důsledku nemusí digitalizace představovat velký zásah do provozu podniku

Příkladem je naše konkrétní řešení opakovaných výpadků montážní linky. V první fázi byla linka osazena čidly, snímajícími odběr proudu, teplotu, náklon, a dokonce i zvuk. Možných příčin výpadků byla celá řada, ale jakmile byla k dispozici data, pomocí jednoduché analýzy se ukázalo, že pokud se teplota jednoho komponentu linky zvýší o několik stupňů oproti průměrné provozní teplotě, v relativně krátkém čase dojde k zadření. Problém, který by někteří řešili nákladným servisem či dokonce výměnou linky, se nám podařilo odstranit instalací jednoduchého systému monitorujícího teplotu. Výsledkem digitalizace tak nemusí být vždy komplexní a drahá řešení, jež se budou dlouho zavádět, nebudou spolehlivá a jejich přínos bude diskutabilní.

Začít s digitalizací nemusí být drahé

Projekty na poli digitalizace často fungují tak, že na začátku ani zákazník ani my jakožto dodavatel nevíme, zda je reálné problém vyřešit a zajistit návratnost nákladů. Proto je vhodné připravit pilotní fázi, která by měla být co nejjednodušší a nejlevnější, ale zároveň by měla poskytovat dostatečnou výpovědní hodnotu. Podle velikosti firmy se mohou počáteční náklady pohybovat v částkách od zhruba 10 tisíc eur, za něž se již dá pořídit relevantní pilotní projekt sběru reprezentativních dat a prvotní datová analýza. Na základě výsledků je pak možné navrhnout dlouhodobější a rozsáhlejší projekt digitalizace s řádově vyšší jistotou návratnosti investice.

DATA Z PROVOZU JSOU NA PREDIKCI ZÁSAHŮ ÚDRŽBY YUŽÍVÁNY JEN VE 12 AŽ 16 % SPOLEČNOSTÍ.

Klíčové je digitalizovaný systém nastavit tak, aby v něm pak uměli zaměstnanci firmy sami provádět změny. Výroba je dynamická a mění se. Není tedy možné připravit black box, se kterým pak „nikdo nehne“. Systém naopak musí být lidem přístupný a uživatelsky i procesně srozumitelný, aby ho technici uměli používat a přizpůsobovat aktuálním potřebám výroby.

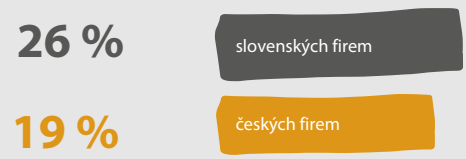
Změny s sebou ale obvykle přinášejí rizika, proto je někdy při digitalizaci průmyslu potřeba zvolit pomalejší a pozvolnější postup. Vytipovat buď jeden problém, jenž zákazníka nejvíce trápí a způsobuje značné škody, nebo se naopak zaměřit na vhodnou menší část systému či provozu. Takový přístup omezí riziko narušení výroby při zavádění změn. Fungování řešení se na těchto dílčích nebo pilotních projektech ověří v praxi. V případě úspěchu si navíc jakožto dodavatel můžeme získat důvěru zaměstnanců, kteří se často obávají, že jim digitalizace zkomplikuje práci, nebo je o ni rovnou připraví.

Technologický posun umožňuje digitalizovat všem

Zatímco ještě před několika lety bylo pro práci s velkým objemem dat nutné počítat s rozsáhlými a drahými datovými centry, dnes stojí digitalizace v průmyslu stále více na open source softwaru a nestrukturovaných databázích. Ty dokážou prakticky za cenu hardwaru absorbovat, zpracovat a analyzovat obrovské množství dat. Databázové komponenty jsou široce dostupné a cena výpočetního výkonu prudce klesá. Na trhu se tak zvětšuje prostor pro individuální integrovaná řešení, jež propojí relativně izolované ostrovy dat do jednoho celku.

Dalším specifikem řady podniků je, že výrobní a provozní technologie (OT) a informační technologie (IT) jsou stále vnímány odděleně. IT pak slouží jen jako servisní a podpůrná sekce pro výrobu. Do hry vstupuje zpravidla až tehdy, když je potřeba řešit nějaký problém. V rámci digitalizace výroby je proto nutné oba světy propojit tak, aby vzájemně těžily jeden z druhého.

DATA O SPOTŘEBĚ ENERGIE A MATERIÁLU VNÍMÁ JAKO DŮLEŽITÁ DATA



Ovšem jen 3 % českých a 7 % slovenských firem tato data využívá na optimalizaci spotřeby.

Bezpečnost je důležitá

Tématem pro digitalizované průmyslové podniky je samozřejmě také kybernetická bezpečnost. Nejde však ani tak o data z výroby. Pokud se útočník dostane například k toku dat z jednotlivých senzorů, budou mu v praxi k ničemu. Bez jejich rozklíčování a zasazení do kontextu z nich nedokáže vyčíst nic relevantního o výrobě ani o podniku jako celku.

Větší riziko spočívá v tom, že průmyslové IoT technologie používané při digitalizaci dělají z každého koncového IoT zařízení potenciální přístupový bod do sítě. Proto je potřeba zajistit, aby se nikdo nedostal přes IoT zařízení a brány IoT sítě pro sběr dat skrze řídící systém až k serverům. To musí být v rámci digitalizace průmyslových podniků perfektně ošetřené.

Investice do digitalizace se rychle vrací

I přes počáteční investice včetně kybernetické bezpečnosti je návratnost projektů digitalizace v průmyslu velmi rychlá. Například energetický monitoring se při stávajících cenách energie dokáže firmě zaplatit do roka. V případě prediktivní údržby v průmyslu je možné díky digitalizaci prodloužit servisní intervaly v průměru o 20 % a díky nižšímu opotřebení lze oddálit i výměnu zařízení. Zákazník díky tomu rozloží náklady do delšího období, což mu návratnost investic do digitalizace bezpečně zajistí. Digitalizace tak může v konečném důsledku rozhodnout i o tom, zda bude podnik konkurenceschopný a dlouhodobě se na trhu udrží, nebo ne. ■

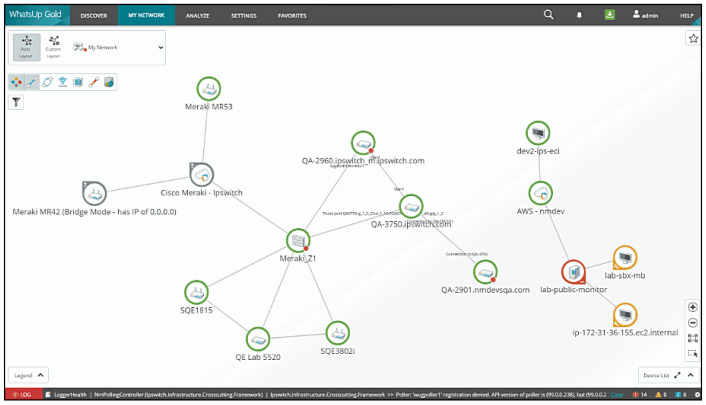
Martin Hummel

Autor článku je architekt IoT řešení ve společnosti Soitron.

Teodor Škereň

Autor článku je Senior Business Development Manager ve společnosti Soitron.

Free verze WhatsUp Gold pro monitorování IT infrastruktury



Firma Progress uvolnila bezplatnou verzi svého řešení pro monitorování IT infrastruktury Progress WhatsUp Gold. Novinka je k dispozici zdarma pro menší firmy a týmy Dev/TestOps, kterým umožní komplexním monitoring napříč lokálními a cloudovými ekosystémy.

Nástroje pro infrastrukturní monitoring jsou stále důležitější s ohledem na dnes typickou rozšířenost hybridního prostředí IT. Poskytují jednotný přístup napříč různými sítěmi a umožňují aby administrátoři měli možnost v rámci svých prostředí vše monitorovat a byli schopni rychle a flexibilně reagovat na změny.

WhatsUp Gold umožňuje i v bezplatné verzi odhalit vše, co je připojeno k síti, vytvořit přehlednou mapu připojených zařízení, spouštět výstrahy a reportovat, stejně jako monitorovat virtuální infrastrukturu až 20 zařízení najednou, respektive 10 zařízení při použití pokročilých doplňkových funkcí, jako je analýza síťového provozu, monitoring výkonnosti aplikací nebo správa logů. V případě potřeby rozšíření umožňuje aplikace bezproblémový přechod na komerční verzi bez ztráty dat nebo nutnosti opětovné konfigurace.

„IT týmy teď dostávají do rukou osvědčené a robustní řešení, které jim jedním pohledem řekne maximum o jejich infrastruktuře a nabídne ucelený přehled o stavu fyzických, virtuálních a cloudových systémů. S bezplatnou verzí zvládnou vizualizovat a řešit problémy dříve, než dokážou ovlivnit další uživatele,“ uvedl Jiří Mazal, obchodní ředitel pro Česko a Slovensko ve společnosti Progress.

Webex pro chytré brýle **Google Glass**

Společnosti Cisco a Google oznámily spojení komunikačního řešení Webex s brýlemi Glass Enterprise Edition 2, jehož cílem je nabídnout řešení pro spolupráci mezi pracovníky v první linii (např. montážními a servisními techniky) a jejich kolegy nebo informačními zdroji v zázemí.

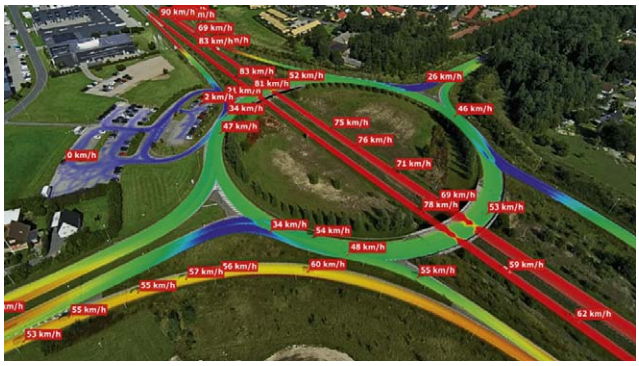
Komunikační řešení Cisco Webex Expert on Demand mění brýle s rozšířenou realitou (AR) na hlasově aktivovanou náhlavní soupravu pro vzdálenou spolupráci. Pracovník v první linii se díky nim může snadno spojit s kolegy, kteří mohou být na stejném místě nebo na více různých místech kdekoli na světě. Tito konzultanti tak mohou pomáhat lidem v terénu, kteří mají díky brýlím obě ruce volné pro manuální činnosti.

Integrace Webex Expert on Demand do Glass Enterprise Edition 2 umožňuje nejen videohovory, ale například i sdílení dokumentů. Komunikace je oboustranná, takže člověk z terénu může svým vzdáleným kolegům posílat třeba videa nebo fotografie. Díky kooperaci více stran je práce rychlejší a efektivnější. Navíc se zvyšuje i bezpečnost, protože pracovník nemusí držet v ruce mobilní telefon, papírové dokumenty, nepotřebuje odbíhat k notebooku a hledat v něm potřebná data apod.

Pracovníci v první linii se mohou do Webexu snadno přihlásit naskenováním QR kódu. Pomocí hlasových příkazů si následně mohou vybrat spolupracovníka z posledních kontaktů, adresáře nebo z prostorů Webex Teams. Mohou tak zahájit hovor nebo odeslat automatickou zprávu s nápovědou vzdálenému odborníkovi. Odborníci v zázemí obdrží požadavek prostřednictvím Webex Teams a mají přitom přístup k anotacím, sdílení obrazovky, sdílení dokumentace a nahrávání.

Webex Expert on Demand umožňuje nejen podporu servisních techniků, montážních nebo stavebních týmů v terénu, ale i pomoc pro auditory a kontrolory, nebo pracovníky ve výrobních halách. Přínosem je také pro lékaře, kteří mohou platformu využívat pro vzdálené prohlížení informací o pacientovi, na dálku konzultovat s dalšími specialisty nebo zaznamenávat operace pro vzdělávací a výzkumné účely.

Aplikace FLOW Traffic od českých vývojářů pro analýzu dopravy



Česká softwarová firma RCE systems představila novou aplikaci FLOW Traffic pro síťové kamery Axis vybavené jednotkou hlubokého učení (DLPU). Jde o aplikaci, která promění výkonnou IP kameru například v počítadlo cyklistů, detektor jízdy na červenou, nástroj k monitoringu obsazenosti parkoviště nebo k adaptivnímu řízení křižovatek.

V tržišti kamerových aplikací Axis Camera Application Plattform (ACAP) se nově objevila dopravně-analytická aplikace FLOW Traffic od českého týmu vývojářů DataFromSky. *„Software značky DataFromSky,*

který se dosud dodával jako serverové či cloudové řešení či v rámci embedded systémů, má už ve světě přes 5000 uživatelů víc než v 50 zemích. Proto jsme rádi, že teď můžeme FLOW představit i jako aplikaci pro nové řady svých kamer Axis s jednotkou DLPU," komentuje Dalibor Smažinka ze společnosti Axis Communications.

Aplikace FLOW Traffic umožňuje uživateli vytvořit si z kompatibilní Axis kamery dopravní senzor podle vlastní potřeby, a to s pomocí intuitivního vizuálního programovacího jazyka. Aplikace FLOW Traffic je zatím k dispozici pro kamery Axis s procesorem ARTPEC-7 a během února 2022 bude i pro modely s ARTPEC-8.

Data extrahovaná z kamery v reálném čase lze potom přehledně vizualizovat na dashboardu s využitím interaktivních widgetů nebo sdílet se systémy třetích stran pomocí otevřeného API. Aplikace je od počátku navržená k provozu v reálném čase, reakce na dění v obraze jsou tak řádově do desítek milisekund. Aplikaci FLOW Traffic lze navíc integrovat s platformami smart city, VMS systémy a podporuje řadu externích periférií (I/O moduly, komunikační moduly atd).

Služba **Kaspersky Takedown Service** pro boj s phishingem

Dnes již bohužel není těžké si představit situaci, kdy kyberzločinci vytvoří podvodnou webovou stránku, která se bude tvářit jako web vaši firmy a jejím cílem je ukrást osobní a přihlašovací údaje vašich zákazníků. Je jistě pochopitelné, že to může vést k poškození firemní pověsti a ke ztrátě příjmů a důvěry zákazníků. Proces odstraňování škodlivých a phishingových domén je ovšem složitý a jeho zvládnutí vyžaduje speciální odborné znalosti, zdroje a čas. Nová služba Kaspersky Takedown Service tento proces zjednodušuje a do značné míry automatizuje v celé šíři od detekce, nahlášení národnímu regulátorovi až po trvalé odstranění hrozby.

Google detekuje každý týden asi 46 000 nových škodlivých stránek, a společnost Kaspersky zablokuje každý den více než 15 000 phishingových a podvodných adres URL. Pokud firma nedokáže zablokovat škodlivý obsah, mohou se její klienti stát obětí podvržených webových stránek a poskytnout útočníkům přístup k jejich osobním a finančním datům. Firmy mohou čelit také závažným únikům dat způsobeným botnety, které jsou ovládány přes příkazové a řídicí servery (C&C) útočníků. To vše může vést k poškození firemní pověsti a ke ztrátě příjmů a důvěry zákazníků. Společnost Kaspersky proto nově nabízí službu Takedown Service, která umožňuje komplexní správu procesu eliminace škodlivých a phishingových domén. Může tak firmám pomoci reagovat na škodlivé zdroje nebo phishingové hrozby zaměřené na ně a jejich zákazníky.

Díky globálnímu dosahu této služby je jedno, kde se škodlivá phishingová doména nachází a Kaspersky Takedown Service ji dokáže zneškodnit. Zajistí přitom všechny potřebné důkazy, včetně kopie webu, snímků obrazovky a výpisu provozu, a to jak ručně, tak pomocí automatizovaných nástrojů. Pak odešle žádost o eliminaci hrozby příslušnému místnímu nebo regionálnímu orgánu, který má zákonná práva nežádoucí zdroj odstavit. Uživatel služby je přitom informován o každém kroku procesu, dokud není podvodná doména úspěšně odstraněna.

Službu lze pořídit samostatně nebo v rámci předplatného služby Digital Footprint Intelligence (DFI). V prvním případě musí uživatel sám předkládat žádosti o odstranění konkrétních nežádoucích domén, které objevil. Ve druhém případě zajišťuje identifikaci škodlivých nebo phishingových zdrojů přímo služba DFI.

Nová verze **Kerio Connect 9.4** nabízí dvoufaktorovou autentizaci

Společnost GFI Software uvedla na trh novou verzi svého řešení Kerio Connect 9.4. Jde o populární řešení elektronické pošty, messagingu a spolupráce, které dnes využívá více než 30 000 zejména malých a středních firem (SMB) po celém světě. Nová verze Kerio Connect 9.4 klade velký důraz zejména na prvky IT bezpečnosti, když nově integruje dvoufaktorovou autentizaci pro zabezpečený přístup a umožňuje přímou integraci s certifikační autoritou Let's Encrypt pro snazší šifrování.

Dvoufaktorová autentizace v nové verzi Kerio Connect 9.4 využívá populární mobilní autentifikátory podporující standard RFC 6238 (jako např. autentifikátory Google a Microsoft) k zajištění tokenu v reálném čase pro potřeby logování uživatelů. Dvoufaktorová autentizace doplňuje zabezpečení Kerio Connect o další vrstvu, jež ochrání organizace zejména v případech, kdy dojde k odhalení uživatelských jmen a hesel prostřednictvím phishingového či malwarového útoku.

Nová verze také usnadňuje šifrování díky lepší integraci s otevřenou certifikační autoritou Let's Encrypt, což umožňuje automatickou obnovu 90denních certifikátů a usnadňuje nastavení TLS protokolu přímo

z grafického uživatelského prostředí. Verze 9.4 rovněž opravila zranitelnosti související s prosincovým bezpečnostním incidentem knihovny Log4j, kterou využívá chatovací funkce Kerio Connect. Aktuálně tak splňuje Kerio Connect maximální úroveň zabezpečení pro organizace a její uživatele.

Konica Minolta rozšiřuje nabídku o řešení **M-Files**

Konica Minolta rozšiřuje svoji nabídku o řešení pro správu elektronických dokumentů od společnosti M-Files. Její řešení využívá prvky umělé inteligence, které umožňují například zrychlit vyhledávání dokumentů nebo zkrátit dobu jejich vytváření. Řešení, které využívají spíše nadnárodní firmy nabídne Konica Minolta i malým a středním podnikům.

„Ačkoli služby v oblasti digitalizace dokumentů v České republice poskytujeme přes deset let, celoevropskou spolupráci s M-Files vnímám jako významný pokrok,“ říká Lukáš Král, produktový manažer ECM Konica Minolta Business Solutions Czech, a dodává: *„Dnes zákazníkům v této oblasti dodáváme naše vlastní řešení, nástroje Microsoft M365, ale i další platformy pro práci s dokumenty nebo automatizaci procesů. Technologie M-Files přitom může fungovat samostatně, nebo může být součástí komplexnějších řešení, ve kterých je více platforem a produktů.“*

Výhodou platformy M-Files je podle Konica Minolta mimo jiné jednoduchá a rychlá instalace bez nutnosti zdlouhavé analýzy nebo migrace dat a nastavení do nového systému. Umělá inteligence si sama zmapuje jednotlivá úložiště a nalezené dokumenty se následně zobrazují v rámci jednoho uživatelského prostředí, kde s nimi mohou zaměstnanci pracovat.

„Při zavádění řešení nechají zákazníci jednoduše všechna svá data na stávajících historických úložištích, jako je SharePoint, OneDrive, Google Drive, síťové disky a další. Vše se automaticky dohledá, propojí a na základě tzv. metadat promítne do jakéhosi virtuálního stromu. Tento princip zároveň eliminuje nebezpečí, že někdo například dokument uloží do nesprávné složky a pak už jej nikdy nedohledá,“ vysvětlil L. Král s tím, že mezi tzv. metadata patří například označení druhu dokumentu, jako je faktura, nákupní objednávka, předávací protokol, kontrolní nebo dodací list, jeho autor, datum vytvoření, částka na dokumentu a podobně.

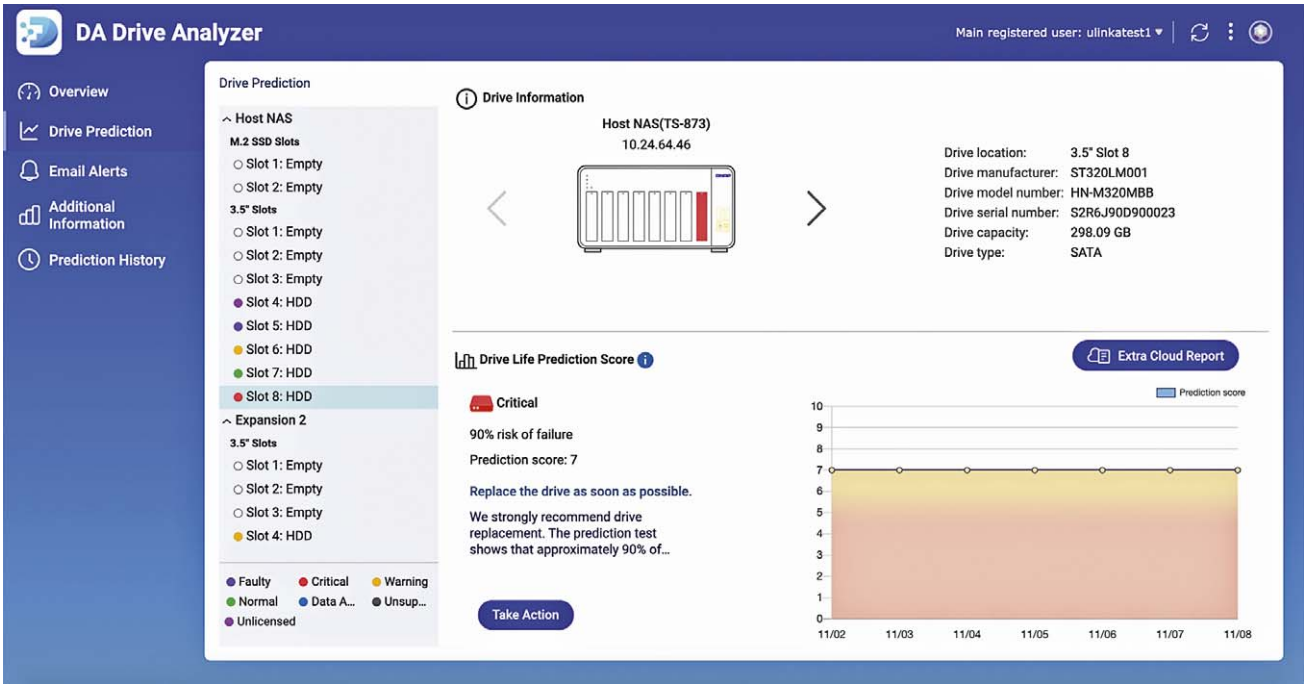
DA Drive Analyzer předpovídá selhání disků v NASu

Společnost QNAP rozšířila nabídku aplikací pro svá NAS zařízení o utilitu DA Drive Analyzer od firmy ULINK Technology, která se zabývá vývojem testovacích nástrojů. DA Drive Analyzer využívá technologii cloudové umělé inteligence, která byla vytrénována na milionech různých disků a díky tomu dokáže předpovídat selhání disků v NASu. Uživatelům tak dává možnost podniknout proaktivní kroky k ochraně před výpadky serverů a ztrátou dat výměnou disků dříve, než skutečně dojde k jejich selhání.

DA Drive Analyzer využívá statistiky z portálu společnosti ULINK a na základě historických údajů o používání milionů disků dokáže predikovat selhání disku, která neodhalí tradiční diagnostické nástroje spoléhající se na prahové hodnoty S.M.A.R.T.

Nástroj DA Drive Analyzer lze stáhnout z App Center. Podporována jsou všechna zařízení QNAP NAS s QTS 5.0 / QuTS hero h5.0 (nebo novější). Podporovány jsou také všechny rozšiřující jednotky QNAP (s výjimkou řady TR).

DA Drive Analyzer zatím nepodporuje disky SAS a NVMe. Některé disky SATA nemusí být podporovány z důvodu nastavení firmwaru nebo výrobce. Před instalací aplikace DA Drive Analyzer tak zkontrolujte seznamy podporovaných modelů na webu QNAPu. ■



Plánování výroby a nákupu

má velké nároky na kvalitu informačního systému a jeho implementace

Vladimír Bartoš

Proces plánování výroby a nákupu je proces s největší přidanou hodnotou, ale také proces, jehož implementace je nejnáročnější, protože je závislý na dobré funkci všech oddělení ve firmě. Stačí jedno nefunkční, a plánování přestává správně pracovat. Navíc nelze použít stejné postupy při plánování projektové a opakované výroby a liší se samozřejmě i plánování dlouhodobé od krátkodobého. Jak tedy má vypadat dlouhodobé plánování ve výrobním podniku?

Dlouhodobé plánování

Dlouhodobé plánování se zabývá ročními výhledy a zkoumá, zda pro plánované tržby budeme mít dostatek zdrojů, jaké vzniknou náklady a zisk. Zatímco dříve se sestavoval dlouhodobý plán na několik let, nyní vzhledem k vysoké dynamice podnikatelského prostředí pracují firmy většinou pouze s ročním plánem.

Vstupem je u opakovaných výrob plán prodeje klíčových výrobků, příp. představitelů skupin výrobků v množství po měsících. Pokud použijeme představitele skupin výrobků, je vhodné definovat i složení těchto skupin včetně předpokládaného poměru prodeje mezi konkrétními výrobky v rámci skupiny, např. představitel JOGURTY má přiřazeny JOGURTY JAHODOVÉ, MALINOVÉ a BÍLÉ, a u každého má definován i procentuální podíl prodeje z celkového plánovaného objemu prodeje jogurtů.

U projektových výrob není předem známo, jaké výrobky budeme pro zákazníky vyvíjet a vyrábět. Máme však většinou definováno výrobkové zaměření. Je proto dobré předdefinovat si v systému typové výrobky se zobecněnými kusovníky a postupy, z nichž pak budeme vyvíjet zákaznické modifikace. Tyto typové výrobky můžeme využít v dlouhodobém plánování stejným způsobem, jako u opakovaných výrob.

Dlouhodobý plán prodeje obvykle sestavuje obchodní oddělení, které má nejlepší představu o tom, co budeme schopni v budoucnu prodat na našich trzích.

Plán prodeje pak podnikový systém rozpadá do ročního plánu výroby a nákupu rozloženého v čase. Plánujeme vždy do neomezených kapacit a kapacitní zátěž porovnáváme

Proč některé firmy nedokážou nastartovat systémové plánování?

Vladimír Bartoš

Před časem jsem prováděl analýzu příležitostí ke zlepšení u jednoho našeho klienta vyrábějícího potraviny a s překvapením jsem zjistil, že nevyužívá systémové plánování, přestože bylo nastaveno a naimplementováno. Na můj dotaz „proč“ jsem dostal odpověď, že MRP plánování je nefunkční, že to zkoušeli a dostávali nesmyslné výsledky. Stačí jim prý doplňování na nastavené meze zásob. Jde o špatný názor, který způsobuje dané firmě škody vlivem neoptimálního nákupu a výroby. Je proti němu potřeba bojovat, a proto začnu krátkou osvětou na téma plánování.

Proces řízení zásob lze rozdělit do několika základních částí:

- Doplňování zásob na nastavené meze,
- MRP plánování do neomezených kapacit,
- APS jemné rozvrhování výroby do omezených zdrojů.

Doplňování zásob je jednoduchý proces, kdy k artiklům dle historické zkušenosti nastavíme mezní zásoby, které pak systém porovnává s aktuálními zásobami, a pokud je skutečnost nižší než mez, dává signál k doplnění. Problémem tohoto přístupu je, že je statický v čase, vychází z historie a nepočítá s budoucností.

Efektivnějším přístupem je dívat se při plánování zásob do budoucna a počítat tak s plánovanými výkyvy prodeje a sezonními prodeji. Toto splňuje MRP plánování. Vyžaduje však samozřejmě více vstupních informací než metoda předchozí. Započítává totiž dynamicky v čase stavy zásob, materiál na cestě, rozpracovanost, kusovníky či receptury výrobků, optimalizační parametry artiklů (průběžné doby dodání a výroby, optimální dávky, kumulace napříč zakázkami, ...) a hlavně zakázky, prognózy prodeje a nastavení sezonních zásob. Sezonní zásoby jsou vlastně bezpečnostní zásoby výrobku nastavené ke konkrétnímu období. Systém se snaží s předstihem, dokud jsou volné kapacity, zajistit vykrytí budoucí sezonní poptávky výrobou. Prognózy prodeje jsou zase předpovědí prodejců, kdy kolik kterých výrobků se pravděpodobně prodá. A právě zde bývá nejvíce problémů s implementací: Kdo bude ty prognózy do systému zadávat? Vždyť trh je nevyzpytatelný! ... Prodejci často odmítají nést odpovědnost za tuto část dat. Zároveň však chtějí, aby výrobky byly skladem vždy, když se jim podaří je prodat. Pokud zásoby skladem nejsou, za viníka je označena výroba. Ta se však brání, že nemohla včas vyrobit, protože nákup nezajistil včas materiál a suroviny.

Pokud vedení firmy na tuto hru přistoupí, jsou nuceni nákupčí a výrobní plánovači prognózovat namísto prodejců. A jistě se shodneme, že jde o řešení nesprávné, protože tito lidé mají k trhu výrazně dále než prodejci.

Když už oddělení prodeje přesvědčíme, aby se prognózování věnovalo, nastává další problém: Proces plánování na prognózy je

s dostupnými zdroji. Tím získáme představu o potřebných kapacitách pro realizaci dlouhodobého plánu i o případných konfliktech a můžeme plán korigovat nebo uvažovat o investicích do zvýšení průchodnosti výrobních zdrojů. Pokud násobíme plán prodeje předpokládanými prodejními cenami, dostaneme plán tržeb po měsících. Pokud násobíme plán výroby kalkulovanými náklady na mzdy, případně různými typy režijních nákladů, dostaneme celkové náklady na mzdy, nároky na zaměstnance i celkové režijní náklady po měsících. A stejně tak násobením plánu nákupu nákupními cenami získáme náklady na nákup v čase s volitelným členěním po klíčových dodavatelích nebo komoditách.

Dlouhodobé plánování se provádí odděleně od existujících zásob a rozpracovanosti a fixuje se kvůli budoucímu porovnávání s vývojem skutečnosti. Rovněž je možné dle něj nastavit rozpočty pro nákup, výrobu a prodej pro průběžnou kontrolu jeho dodržování.

Střednědobé plánování

Cílem střednědobého plánování je včas zajistit materiál pro výrobu. Jen zřídka jsou pro zákazníky přijatelné delší dodací lhůty, než jsou kumulativní průběžné doby nákupu a výroby našich výrobků. Proto nemůžeme čekat na prodejní zakázky, ale musíme začít nakupovat dříve. Neměli bychom nechávat odpovědnost za tyto nákupy na nákupčích, protože nákup je, až na strategické komodity, závislý na plánu prodeje. Je důležité zavést společně s prodejci měsíční cyklus aktualizace prognóz prodeje. Prognózy prodeje se stanovují pro bližší období po týdnech a vzdálenější budoucnost po měsících. Pro každý výrobek nebo skupinu výrobků se společným prodejním trendem je nutné do systému zadat prognózu prodaného množství v čase. V automobilovém průmyslu je běžné, že v rámci společného plánování nemusíte prognózy prodeje stanovovat vy, ale zasílají je přímo vaši zákazníci včetně průběžných aktualizací do vašeho systému pomocí elektronické EDI komunikace ve formě zákaznických rozvrhů (forecastů). U projektových výrob zase spíše čekáme na uzavření konkrétních zakázek. Ale i tady pak bývá tlak na zkracování termínů, proto pokud můžeme využít typový výrobek a začít podle něj plánovat nákup dříve, než konstruktéři a technologové vyvinou a zdokumentují konkrétní zákaznickou modifikaci, bude to určitě výhodou. ▶

složitější než jednoduché doplňování zásob. Prognózovaná množství jsou totiž rozvržená v čase a zakázky, které pak od zákazníků přicházejí, prognózy konzumují. Je to výborná věc, protože to vede ke snižování zásob. Pokud totiž dorazí zakázky v téměř stejném objemu, jako byly naše prognózy, budeme pro ně mít k danému termínu včas přichystané zásoby, vyexpedujeme je a na skladě téměř nic nezbude. Prognózy se ale i samy korigují: Pokud prodáme méně, než jsme prognózovali, prošlá prognóza již přestane být součástí poptávky a zbylé zásoby systém použije pro pokrytí poptávky budoucí. Nebudeme tedy muset tolik vyrábět a zároveň získáme i analýzu úspěšnosti našeho prognózování.

Vygenerované optimalizované výrobní příkazy z MRP plánování jsou pak vstupem do APS plánování, které pracuje ještě přesněji a vyžaduje ještě více vstupních dat.

MRP plánování je základním plánovacím procesem každé firmy. Pokud nedává správné výsledky, je potřeba zkontrolovat výše uvedená vstupní data. Není jich mnoho a za jejich správnost jsou jasně určení zodpovědní uživatelé. Nejčastější chyby spočívají v dávno propadlých nákupních objednávkách a výrobních příkazech, které mají stále otevřené množství. MRP pak samozřejmě očekává, že otevřená množství z těchto dokladů budou přijata na sklad nejpozději teď. Dalším problémem bývá nastavení průběžných dob výroby a nákupu některých artiklů na 0 dnů. Výsledkem je, že systém předpokládá okamžitou realizaci těchto artiklů, což samozřejmě neodpovídá realitě.

Udělal jsem si statistiku mezi našimi stovkami výrobních firem, kolik z nich nepoužívá MRP plánování. Zjistil jsem, že jsou to jednotky a překvapivě se nejedná o strojírenské firmy, ale jde spíše o potravináře. Proč právě oni argumentují složitou údržbou plánovacích dat a nemožností prognózovat, když strojaři mají násobně složitější a četnější technologická data, a ještě hůře předvídatelnou poptávku?

Dospěl jsem k názoru, že hlavním důvodem není to, co obvykle uvádějí, ale situace je mnohem prostší: Plánovač v potravinářské firmě je schopen díky jednoduchosti receptur a menšímu množství výrobních zařízení naplánovat bez systému – v Excelu. Nákupčí je schopen díky obrátkovosti nakoupit potřebné suroviny a materiály i bez MRP plánování. Chybí tedy přirozená motivace vyčistit vstupní data a ladit MRP plánování. To, co je ve strojírenské výrobě nutností, je u jednodušších výrob pouze alternativou.

Naštěstí však už máme mnoho klientů i s opakovanou jednodušší výrobou, kteří využívají nejen MRP plánování, ale přikročili dokonce i k APS rozvrhování. A výsledkem bylo snížení zásob a rozpracovanosti při stejných nebo rostoucích tržbách. Některým zkrátka nestačí, že firma nějak funguje, ale pracují na tom, aby fungovala co nejlépe. ■

Vladimír Bartoš

Autor článku je ředitelem pro strategii ve společnosti Minerva Česká republika.

Podnikový informační systém pak dynamicky v čase porovná tuto nezávislou poptávku se zásobami a plánovanými příjmy z výroby a navrhne hlavní plán výroby včetně jeho optimalizace dle plánovacích parametrů nastavených u výrobků (kumulace výrobních dávek napříč zakázkami za daný časový interval a zohlednění optimálních dávek, případně bezpečnostních a sezonních zásob). Tento hlavní plán současně porovná s kapacitami výrobních zdrojů a zobrazí případné disproporce. Hlavní plánovač pak může plán v množství a čase upravit tak, aby byly výrobní zdroje zatíženy rovnoměrně a poptávka pokud možno uspokojena. Každý zásah plánovače si systém označuje jako fixní, aby nebyl následným přeplánováním zrušen, ale naopak zohledněn v souvislostech. Další plánovací krok rozpadne hlavní plán výroby do výrobních příkazů na podskupiny a polotovary a do nákupních požadavků. Systém opět dynamicky v čase zohlední zásoby, rozpracovanost a materiál na cestě a provede optimalizaci příkazů a nákupních požadavků napříč zakázkami. U projektových výrob se méně využívá optimalizace příkazů a nákupních požadavků napříč zakázkami a více se preferuje adresné plánování s jasnou vazbou na prodejní zakázku. Adresnost na úkor optimalizace se však využívá zejména v horních úrovních kusovníku výrobku, kde jsou polotovary, podskupiny a výrobky jedinečně modifikovány pro zákazníka. Na nižších úrovních u materiálů a dílů se každá firma snaží o unifikace, aby mohla využít optimalizaci dávek a výrobu tak zlevnila a zkrátila. Proto je důležité, aby informační systém umožnil nastavit optimalizační parametry (plánovat adresně / kumulovat dávky za stanovený časový interval napříč zakázkami / zaokrouhlit na stanovené optimální množství / ...) rozdílně k jednotlivým artiklům – materiálům, dílům, polotovarům a výrobkům.

Krátkodobé plánování a rozvrhování

Cílem krátkodobého plánování a rozvrhování je stanovit pořadí operací pro jednotlivá pracoviště tak, abychom dosáhli co nejvyšší efektivity a dodali výrobky včas zákazníkům. Nákup a výroba jsou velmi dynamické procesy, v nichž dochází k výpadkům a skluzům. Proto nelze plánovat týdně, ale potřebujeme přeplánovávat denně, někdy dokonce i uprostřed směny. Důležitými vstupními informacemi jsou výrobní příkazy optimalizované střednědobým plánováním včetně postupů a kusovníků, priority výrobních příkazů dané obvykle termíny prodejních zakázek a zbývající dobou do jejich splnění, dostupnost zásob včetně plánovaných příjmů z nákupních objednávek, kapacity primárních zdrojů (pracovišť, na něž tvoříme frontu práce) a sekundárních zdrojů (nástrojů, operátorů, energií, skladovacích prostor, ...) a parametry ovlivňující efektivitu – matice časů přestavení z výrobku na výrobek. V potravinářství se tyto časy liší např. dle alergenů ve výrobcích nebo kombinace přísad vyžadující delší nebo kratší časy čištění výrobních linek, ve strojírenství jde zase o vstupní materiály, které můžeme na stroji nechat a vyrobit z nich s kratším seřizovacím časem více výrobků, nebo např. při lakování je důležité pořadí výrobků dle barev apod.). V projektových výrobách je důležité mít od počátku výrobek svázaný s polotovary a materiály typovým kusovníkem. Konstruktéři a technologové pak dokumentaci zpřesňují od spodních úrovní kusovníku vždy o krok před uvolněním do výroby. Plánování vždy používá poslední aktualizace kusovníků, takže shora od prodejní zakázky ve vzdálenější budoucnosti plánuje dle typového kusovníku, ale v bližší budoucnosti již přeplánovává dle konkrétní platné dokumentace výrobku.

Jak tedy seřadit výrobní příkazy a jejich operace na pracoviště? Můžeme vsadit na plánovače a jeho zkušenosti. Jako nástroj mu poskytne ERP systém plánovací tabuli s perfektní vizualizací všech výše uvedených informací a souvislostí, předpřipraví mu výrobní příkazy vygenerované střednědobým plánováním na pracoviště a umožní mu tažením myši provádět korekce plánu. Ale co když plánovač onemocní? Co když je potřebných ručních korekcí příliš mnoho? Pak je potřeba implementovat APS pokročilé plánování. Jde o nástroj, který umí využít všechny výše vyjmenované vstupy a nabízí několik předpřipravených pokročilých plánovacích metod, pomocí nichž provede rozvržení operací na pracoviště zcela automaticky. Dokonce nám umožňuje i vytvoření specifických plánovacích metod, pokud máte ve firmě speciální pracoviště, např. procesy pálení dílců z plechů dle pálicích plánů, koprodukty vyráběné současně jedním procesem apod. Naším cílem je pochopit myšlenkové pochody plánovače výroby a převést je do APS plánování. Počítač pak plánuje přesněji a rychleji než člověk, takže můžete plánovat i častěji a plánovač dostává prostor na řešení specifik.

Máte strach, že APS plánování vyžaduje mnoho přesných informací a ty nedokážete zajistit? Ano, úspěšnost závisí na kvalitě informací ve vašem podnikovém informačním systému. Ale zatímco ještě před pěti lety jsme APS implementovali s nejméně ročním posunem po ERP systému, nyní jej implementujeme již pouze s měsíčním posunem, tedy v podstatě společně s ERP systémem.

Jak nám podnik šlape?

A co reporting z plánování? Z dlouhodobé perspektivy porovnáváme dlouhodobý plán se skutečností, u střednědobého a krátkodobého plánování vždy generujeme nový v daném okamžiku nejlepší možný plán. Zajímají nás plánováním generované varovné zprávy, pomocí nichž nás systém upozorňuje na důležité skutečnosti spojené s konkrétními výrobními příkazy nebo nákupními požadavky. Jde o skluzy, žádosti o zkrácení standardních výrobních či nákupních časů, urgence k zahájení aktivit apod. O kvalitě podnikových procesů nás informuje počet takto vygenerovaných varování. Čím je jich méně, tím nám podnik lépe šlape. ■

Vladimír Bartoš

Autor článku je ředitelem pro strategii ve společnosti Minerva Česká republika.

Procesní paralelismus a prediktivní řízení zásobování čerstvými potravinami

Peter Bílik, Martin Kudláč

Chladicí řetězec, jehož součástí je také logistika a distribuce čerstvých potravin, se zařazuje mezi nejsofistikovanější typy logistiky obzvlášť vzhledem k citlivosti a pomíjivosti přepravovaného zboží a specifickým podmínkám jeho přepravy a skladování. O to intenzivněji dopadají na řízení zásobování čerstvými potravinami prudké změny v chování spotřebitelů, jakož i stoupající nároky na služby. I proto přistupují distribuční centra ke kontinuální inovaci a škálování pružnosti procesů zásobování a vychystávání digitálními technologiemi.

Turbulentní období přicházejících a odcházejících pandemických vln mělo zásadní dopad na globální i lokální dodavatelské řetězce. K pandemii se navíc přidávají další faktory, jež mají přímý dopad na zásobování, od vlivů počasí až po prudké změny spotřebitelského chování. Navíc stoupající nedostatek kvalifikované pracovní síly vytváří dodatečný tlak především na distribuční centra, ale i jiné části dodavatelských řetězců.

Sektoru e-commerce a retailu se povedlo zareagovat na výzvy, jež se staly také příležitostmi, částečně i díky omnikanálovému prodeji. Potravinářský segment, a především odvětví distribuce čerstvých potravin (tzv. chladicí zásobovací řetězec), vzhledem na typ přepravovaného zboží a přísné podmínky manipulace, skladování a přepravy, představuje vzhledem na komplexnost procesů jeden z nejsložitějších typů řízení logistiky. Vzhledem k potenciálnímu přerušení potravinářských řetězců musí také distribuční centra postupovat při kontinuální inovaci.

Rozšíření business intelligence

Skladování potravin a jejich distribuce si již za běžných okolností vyžaduje zpřísněná hygienická opatření, jakož i rozložení zboží do různých chladicích zón. Přístup k čerstvým potravinám se ještě zpřísňuje během pandemie, aby se zabránilo kontaminaci zboží a také z důvodů předcházení infekci mezi zaměstnanci. Následné výpadky v docházce zaměstanců by mohly vést k výpadkům v zásobovacích tocích nebo ke zbytečným prostojům, během kterých dochází k vyhnutelnému snižování kvality zboží nebo k jeho exspiraci.

Pandemie přispěla také k další změně, jež se týká zásobovací strategie Just-in-Time (JIT). Neplánované nebo nečekané změny v dodavatelském řetězci nebo ve skladech způsobovaly opoždění nebo výpadky dodávek během pandemie.

Tyhle incidenty se týkaly také nedostatečné viditelnosti probíhajících úkonů a stavu jednotlivých objednávek, jakož i nepřesných dat o zásobách a přesunech zboží, plánování, jež nebylo přizpůsobené na bezodkladné reagování na změny v odběratelských objednávek, na což se také váže nedostatečná pružnost provozních procesů a s ní související udržitelnost provozu i během krizových situací.

Aktuální a správná data jsou klíčová při vytváření lepší business intelligence, kdy podniky mohou dělat obchodní, ale také logistická rozhodnutí podložená relevantními informacemi. Bez ohledu na to, jestli jde o položky, kterým klesá obrátka a z obchodního hlediska se stávají ne příliš zajímavými, nebo o rozložení vysokoobrátkového zboží v bufferovém skladu.

Rozšíření viditelnosti procesů, jako je plánování objednávek, stav vychystávání, nejprodávanější položky (nebo nejméně žádané zboží), obrátkovost, probíhající reklamace a vratky a jejich monitorování v reálném času, přispívají ke zkrácení reakční doby a zvýšení kvality jak taktického, tak i strategického rozhodování při efektivním uspokojování obchodních požadavků maloobchodní a velkoobchodní klientely.

V důsledku pandemie došlo také k zásadním změnám ve spotřebitelském chování. Ty měly nemalý dopad na potravinářský sektor jako zdroj esenciálního zboží. Včasná a přesná data a analýzy umožňují podniku identifikovat nově se formující trendy včas a přizpůsobit jim nejen obchodní, ale také procesní postupy.

Obchodně-distribuční firmy, obzvlášť ty podnikající s čerstvým ovocem a zeleninou, při zavádění prvních koronavirových opatření mohly anticipovat, že korporátní klienti z HoReCa budou představovat velmi malou část odběratelů s náběhem prvních lockdownů, a tudíž se mohly začít soustřeďovat na maloobchodní zakázky a B2C klientelu.

Tomu zodpovídaly také typy nabízeného zboží a složení objednávek (přechod na menší, méněpoložkové objednávky, ale ve větších objemech v porovnání s obsluhováním B2B zákazníků). Mnohé z pandemických návyků se budou normalizovat i pro post-pandemický normál, a stejně tak do plánování vstupuje také sezonní zboží, čemu podniky musí přizpůsobovat také svůj provoz.

Akcelerace vychystávání objednávek správnými daty

Vzhledem na citlivost skladovaného a přepravovaného zboží v potravinářském segmentu musí podniky dbát nejen na správné skladovací podmínky, ale také rozšíření propustnosti skladu, a to nejen během sezonních špiček nebo úzkých hrdel v provozu.

Vychystávaní čerstvého ovoce a zeleniny spolu s dalším potravinovým zbožím a kompletizace

objednávek často prodlužují neaktuální data o dostupnosti zboží, nesprávně označené umístění položek, jakož i nedostupnost zásob.

Tahle kombinace také potenciálně vede k nárůstů chybně vychystaných objednávek, především při prioritním zásobování klientů, kde hraje roli také co nejrychlejší kompletizace a expedování zásilek. Při dodání chybných objednávek tak dochází nejenom k poškození reputace, ale ke generování dodatečných nákladů při reklamaci a vychystání opakované objednávky se správným zbožím.

I proto se řízení zásob řadí mezi klíčové procesy skladové logistiky a zásobování. Přesná data o hladinách zásob předcházejí prodeji zboží, jež momentálně není k dispozici nebo jeho dostupnost je nějakým způsobem limitována. Nedostatečné řízení zásob se navíc může podílet na zpomalování vychystávacích a kompletačních procesů, což může v horším případě vést k hromadnému rušení objednávek a generování ztrát.

K optimalizaci skladových procesů v současnosti významně napomáhají moduly WMS systémů zaměřené na plánování a řízení skladových zásob. Aktuální data o zásobách umožňují WMS systémům automaticky monitorovat úroveň zásob a včasnými notifikacemi zabraňovat poklesu pod kritickou hladinu, a to zejména při strategických položkách a bestsellerech. WMS systémy zároveň regulují také horní hranici zásob, čímž eliminují zbytečné přezásobení, které by mohlo zabírat prostor pro relevantní zboží.

Škálování pružnosti v době rostoucí proměnlivosti

Prediktivní analýzy se však nemusí nasazovat jenom při obchodním plánování. Efektivní uplatnění mají také jako optimalizační strategie při řízení zásob. Prediktivní algoritmy umožňují identifikovat typy zboží, jež se nejčastěji nakupuje nebo také i vychystává dohromady.

Párováním položek na základě opakujících se vzorců spotřebního chování je pak možné vyselektovat typy zboží, jenž se v objednávkách nejčastěji objevují, a skladovat je co nejblíže ke kompletačnímu pracovišti. Zároveň je možné zvýšit strategickou dostupnost zboží s nejvyšší obrátkou jeho uložením v průtokovém skladu a eliminovat tak čas, který by se strávil vychystáváním ve skladu.

Dynamické řízení zásob zároveň umožňuje měnit uložení zboží a párování bestsellerů v reálném čase. Díky tomu sklad a zásobování pružně reaguje nejenom na sezonní nárůst, ale také neplánované výkyvy nebo prudké změny v odběratelských zvycích. Právě zabezpečení pružnosti se stává nevyhnutelným atributem nejen v potravinovém sektoru, ale pro procesy fulfillmentu objednávek všeobecně.

Nárazové vlny poptávek po specifických typech zboží se objevují i mimo již známé a předvídatelné sezonní špičky, včetně prudkých a nečekaných nárůstů a poklesů poptávek po různých typech zboží. Na to, aby stoupající obrátka konkrétních typů zboží nezačala nečekaně zahlcovat vychystávací procesy a nezpomalovat odesílání zkompletovaných objednávek, potřebuje sklad nebo distribuční centrum disponovat procesy, jež jsou pružné a ideálně i škálovatelné.

Elasticita skladové logistiky a fulfillmentu zároveň přispívá k zvýšení udržitelnosti provozních procesů a dodržování dodacích lhůt i v případě rozšiřování prodejních kanálů, expanze do nových teritorií nebo změny segmentace odběratelů. Proto jsou již současné WMS/WES systémy přizpůsobené na provozní model operativního řízení zásob, skladu a objednávek v reálném čase, díky čemuž výrobní i distribuční potravinářské společnosti mohou včasněji a přesněji reagovat na tržní změny.

Transformace na potravinářství 4.0

Řízení chlazeného řetězce, tedy čerstvých potravin a farmacie, patří mezi nejkomplexnější typy logistiky, což s sebou přináší řadu výzev. Přepravování čerstvého zboží vyžaduje speciální skladování a manipulaci se zásobami, pečlivé kontroly, regulované prostředí a adekvátní požadavky na balení. I z toho důvodu je klíčové rychlé a správné zpracování objednávek a efektivní řízení vychystávacích procesů a průtoku skladu.

Vzhledem k dodržování přísných parametrů a udržení kvality čerstvých potravin je nezbytné optimalizovat tok zboží. Zatímco práce s aktuálními datovými analytikami přispívá ke zrychlení a zkvalitnění rozhodovacích procesů, na základě čehož posléze dochází k zrychlení vychystávání, právě povaha skladování a distribuce čerstvých potravin si vyžaduje automatizaci řízení procesů v reálném čase.

Zásobování čerstvými potravinami pozůstává ze série unikátních objednávek, kdy se kombinace jednotlivých SKU a jejich množství neopakuje. Proto se vychystávací proces nedá optimalizovat prostřednictvím standardizace. Objednávky koncových spotřebitelů, podnikatelských subjektů (HoReCa) a supermarketů se navíc chystávají souběžně na kusy nebo váhu, ale i kartony a palety, co dále komplikuje zúžení vychystávacích procesů.

Distribuční centrum čerstvých potravin tak musí být připravené na vychystávání vysoce individualizovaných zadání. Tento typ zpracování velkého množství odlišných požadavků a preferencí, v různých hodnotách a počtech se stává náročné na manuální vychystávání obzvlášť v době, kdy se dodání čerstvého ovoce a zeleniny do 24 hodin od domácích pěstitelů stává ne ani tak konkurenční výhodou, jako spíše standardem. Z pohledu řízení zásob a vychystávání dochází k masové kustomizaci při sestavování a kompletování objednávek, kdy se již konvenční technologie stávají při narůstajícím objemu objednávek nespolehlivými.

Nejčastější technologií, jež se v takovémto případě nasazuje, je WMS systém, v případě pokročilé automatizace nebo semi-automatizace provozu WES systém (Warehouse Execution System). Kromě využití automatizačních technologií, jako zaskladňovací systémy (AS/RS), paletové dopravníky, třídičky a balicky, které WMS/WES systém řídí, jsou klíčovými

inteligentní algoritmy nasazené pro dynamický slotting zásob, kombinované vychystávací strategie a operativní řízení podnikových zdrojů.

Procesní paralelismus a prediktivní řízení

Zatímco WMS systém exceluje při řízení zásob a automatizaci řízení skladu, WES systém nabízí rozsáhlejší možnosti integrace, zejména integraci a řízení přepravných zařízení a manipulační technologie. Rozšířená integrovatelnost a dynamická škálovatelnost WES systému navíc vnášejí do řízení potravinové logistiky větší agilitu a také zvyšují provozní udržitelnost zásobovacích procesů.

Při efektivním řízení zásobování čerstvými potravinami se stává klíčovou technologie digitálních dvojčat (autonomních inteligentních agentů), jež může být součástí WES systémů nebo také pokročilých WMS systémů. Prostřednictvím digitálních dvojčat lze vytvořit virtuální kopii skladu, materiálového toku nebo zásobovacího řetězce, přičemž digitální protějšky zboží, materiál (kupříkladu přepravky) a zásobovacích technologií (AGV, VZV, dopravníkové pásy) disponují vlastní inteligencí a rozhodovací schopností.

Nejenže se podnikové zdroje mohou samy rozhodovat vzhledem k aktuálním okolnostem, přičemž tahle rozhodnutí se posléze realizují ve fyzické realitě skladu nebo distribučního centra, ale také jejich vzájemná interakce umožňuje vytvořit paralelismus v zásobovacím řetězci, obzvlášť při procesu vybavování objednávek (order fulfillment).

Procesní paralelismus znamená, že souběžně probíhají různé procesy související s vychystáváním objednávky v různých částech skladu nebo materiálového toku, které se ale navzájem podmiňují. A stejným principem jsou řízeny i podnikové zdroje.

Kompletizace objednávek před expedicí probíhá tak, aby položky, které jsou momentálně v procesu vychystávání v hlavním nebo bufferovém skladu, mohly být zkompletizované v příslušné objednávce v momentu, kdy jsou všechny vychystávany v správném množství a bez zbytečných prodlev.

Jednotlivé položky jsou přiděleny příslušným skladovým operátorům nebo přepravně-manipulačním technologiím v případě automatizovaného vychystávání, podle časových priorit a klientských preferencí, a podle těchto kritérií, jakož i momentální dostupnosti podnikových zdrojů jsou vytvořené vychystávací seznamy.

Řídící WES systém prostřednictvím technologie digitálních dvojčat vytváří postoupnost jednotlivých aktivit, kterým podle priorit přiděluje podnikové zdroje, které v reálném čase navzájem koordinuje, aby se zamezilo duplicitě operací (dva skladníci vychystávající stejnou položkou pro jednu objednávku) nebo prostojům (vytvoření fronty objednávek čekajících na zkompletizování nebo balení).

Zásadní vlastnost při tomto typu automatizace procesů zásobování a logistiky představuje prediktivní řízení operací, jenž se podílí na paralelismu v procesech a včasné a správné synchronizaci operací v jednotlivých částech materiálového toku a vychystávání objednávek.

Prediktivní analytika se většinou využívá při plánování nebo projekci (objednávek, zásob apod.). Současné WES platformy využívající technologie jako digitální dvojčata a IoT využívají predikce v krátkých časových rámcích, zejména při nastavení vychystávacích postupů během jedné pracovní směny a na základě aktuálních množství přijatých objednávek a s momentálně dostupným množstvím podnikových zdrojů.

Právě prediktivní řízení skladových a vychystávacích operací se podílí na funkčním a efektivním provozování masové kustomizace a procesního paralelismu, které stojí za maximalizací objemu vychystaných objednávek, rozšíření průtoku skladu a bezchybným vychystáváním různých typů balení a objednávek (tzv. hybridní vychystávání). Jejich nasazení zkracuje nejenom vychystávací časová okna pro objednávky a čerstvé potraviny, ale zároveň přispívá také ke zkracování chlazeného zásobovacího řetězce.

Nasazení WES systémů pro automatizaci nebo semi-automatizaci procesů komplexního vychystávání objednávek nebo efektivního řízení distribučního centra čerstvých potravin je součástí rozsáhlejší strategie digitální transformace potravinářství a polnohospodářství. Technologie IoT, digitální dvojčata a datová analýza se dostávají i do dalších potravinářských dodavatelsko-odběratelských a zpracovatelských procesů. Dochází tak k digitalizaci tzv. první míle (například u pěstitelů) s predikcemi sklizní, monitoringem a kontrolou kvality potravin. Automatizační tendence dále pokračují při primárním nebo sekundárním zpracování potravin, zejména automatizací výroby (MOM/MES systémy) a efektivním plánováním podnikových zdrojů.

Inteligentní automatizace v distribuci a logistice zahrnuje především analytiku zásobovacího řetězce, řízení chlazeného řetězce, automatizaci skladové logistiky a vychystávání objednávek a řízení přepravy (TMS). V neposlední řadě jde také o digitalizaci poslední míle, zejména omnikanálovou a D2C (direct-to-consumer, přímé dodání zákazníkovi) logistiku, plánování a řízení poptávek, ale také i řízení reverzních toků.

Procesní paralelismus s prediktivním řízením operací prostřednictvím technologie digitálních dvojčat tvoří součást strategie inteligentní automatizace skladu. Tato kombinace přispívá k efektivní horizontální integraci procesů, jež maximalizují efektivnost vychystávacích procesů a řízení zásob čerstvých potravin, čím také akcelerují adaptabilnost logistických operací uvnitř distribučního centra. ■

Peter Bílik

Smart Industry solution designer, ANASOFT

Martin Kudláč

Marketing specialist, ANASOFT

Autoři článku pracují ve společnosti ANASOFT, která se zaměřuje na digitalizaci, optimalizaci a inteligentní automatizaci průmyslu a logistiky, včetně e-commerce, novými technologiemi.

Cesta průmyslu od automatizace k autonomii

Zavádění procesu autonomní výroby vyžaduje holistický přístup

Matthias Roese

Zavedení umělé inteligence do výroby často selhává při přechodu od zkušebního provozu k tomu běžnému. Vyhnout se tomu lze pouze holistickým přístupem, který zohledňuje celé spektrum obchodních, technických a organizačních souvislostí.

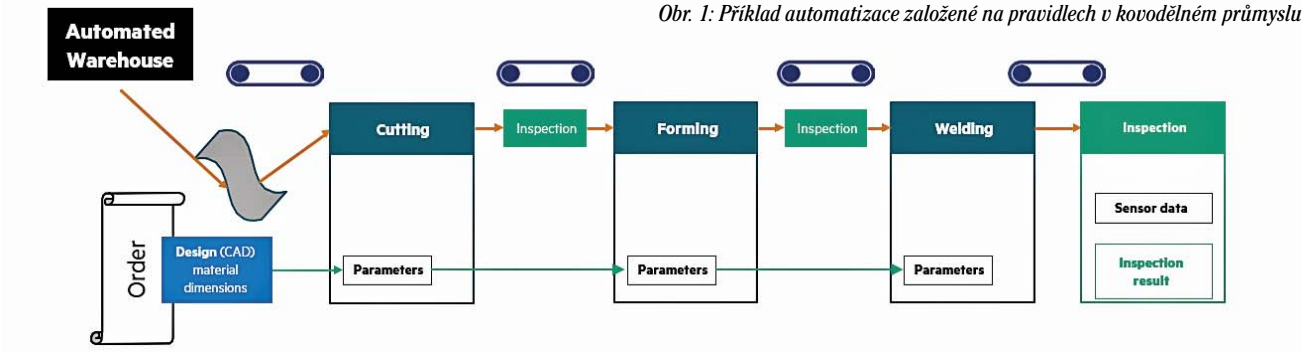
Představme si modelový příklad společnosti zabývající se obráběním kovů. Její výroba je vysoce automatizovaná. Skladový systém umí perfektně vydávat požadované množství plechů, dopravní systémy je podávají přímo do řezacích a vysekávacích strojů, nebo lisů či svařovacích systémů a po každém kroku zpracování probíhá kontrola kvality. Jde o běžný stav společnosti, používající ve výrobě automatizační procesy. Přesto se tato automatizace založená na pravidlech stává stále větším problémem. V posledních několika letech se totiž výroba této kovoobráběcí společnosti zmenšovala a zmenšovala, a to z důvodu změny poptávky, a také kvůli výpadkům dodavatelských řetězců. Proto každý nový díl, který měl být vyroben, vyžadoval nový start výrobní linky, a pro každý procesní krok musely být stanoveny a otestovány nové parametry. To vedlo ke snížení produktivity automatizace a snížení celkové efektivity zařízení (OEE).

Na tyto scénáře ovšem bylo myšleno už když vznikal koncept Průmyslu 4.0. Proto byly definovány hlavní principy autonomních a samoorganizujících se výrobních systémů – které by umožnily dosahovat efektivní hromadné výroby i při výrobě jediné šarže. Hybatelem tohoto způsobu výroby je umělá inteligence (AI) . Ta totiž v případě automatizace založené na pravidlech počítá s možností změn a je schopna autonomně vyvozovat závěry z nasbíraných dat a dat získaných v reálném čase, aby mohla adekvátně, přesně a rychle reagovat na neplánované události.

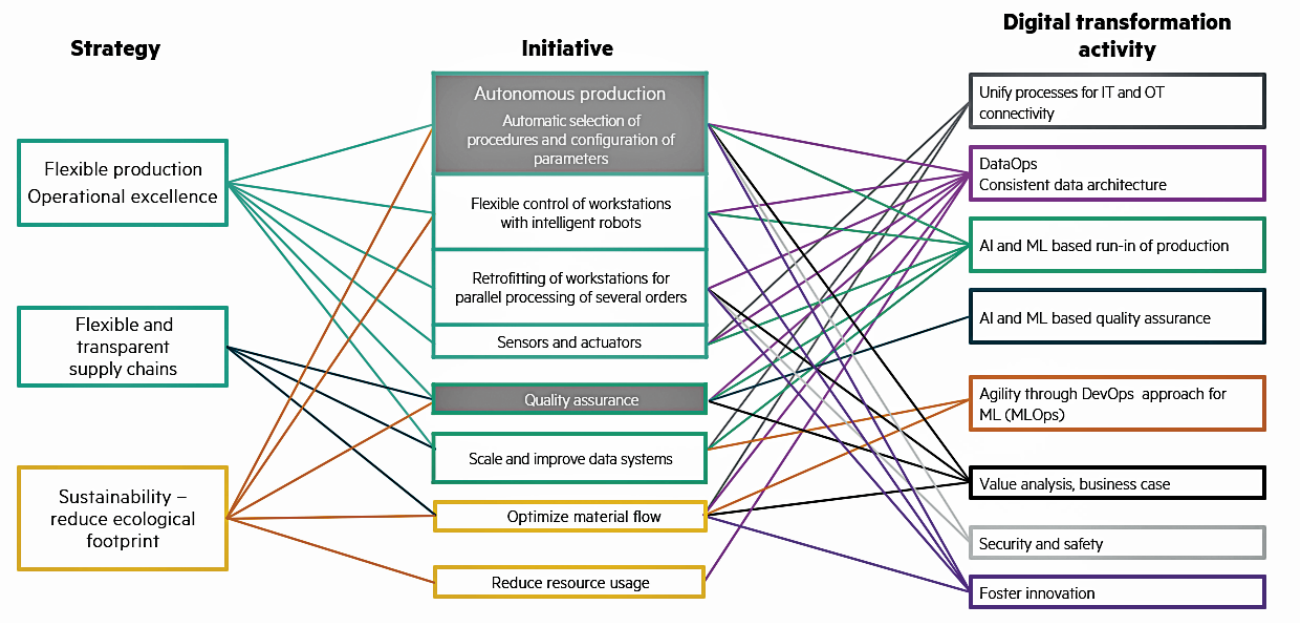
Společnosti podceňují systematické výzvy AI

Po několika letech a velkém množství vypracovaných analýz se zdá, že tento přístup je poněkud deziluzivní. Zatímco proces zavádění umělé inteligence v ostatních odvětvích stále roste, stav umělé inteligence v roce 2021 ve výrobě byl stále daleko pozadu (viz analýza společnosti McKinsey State of AI in 2021). Hlavním důvodem je to, že velké množství projektů plánující využití umělou inteligenci skončí v testovací fázi, tedy Proof of Conceptem (PoC). Příčiny selhání prototypu, který má názorně demonstrovat aplikovatelnost řešení v reálném světě a jeho finanční udržitelnost, jsou hlubší než například nedostatek odborných znalostí nebo rozpočtu – výrobní společnosti v mnoha případech podceňují systematické výzvy při zavádění umělé inteligence do života.

Způsob, jakým jsou PoC nastaveny, jsou toho pouze příznakem. Obvykle totiž probíhají v chráněném prostředí a jsou zaměřeny na aplikaci a trénování modelů AI s daty – často je však opomíjena potřeba integrovat řešení AI do stávající informační a výrobní technologie a jejích procesů. To zahrnuje například správu životního cyklu aplikací a dat, zabezpečení, provozní plánování a kontrolní procesy



Obr. 1: Příklad automatizace založené na pravidlech v kovodělném průmyslu



Obr. 2: Holistický přístup k zavádění AI zahrnuje řadu rozhodnutí (iniciativ) a projektů (aktivit), které jsou odvozeny od hlavních strategií podniku

či provozní bezpečnost. V důsledku toho PoC neposkytuje seriózní důkaz o technické proveditelnosti a ani jej nelze použít k výpočtu solidního byznys modelu.

Holistický přístup k zavádění AI

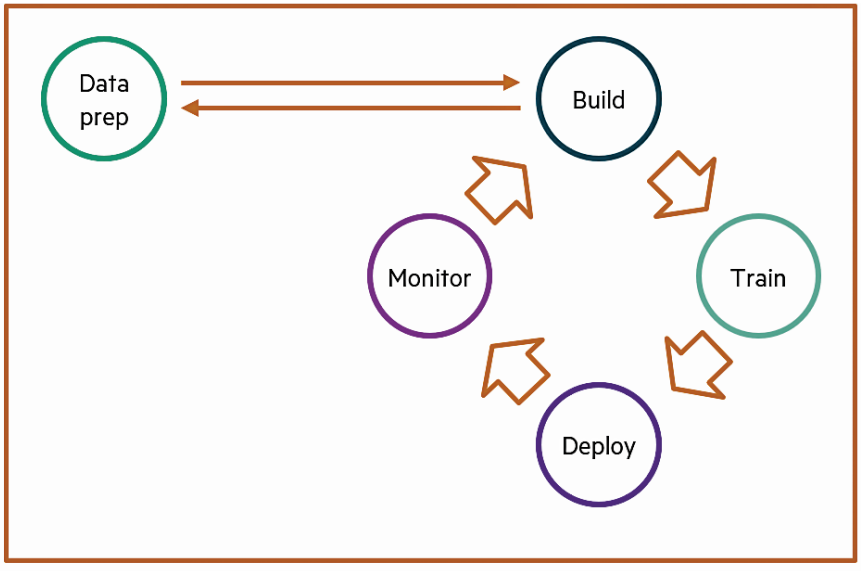
Jakkoli to může znít divně, zavedení umělé inteligence do výroby může být úspěšné pouze s holistickým přístupem. PoC by mělo být pouze na špičce ledovce – výsledkem řady základních rozhodnutí a projektů, kde jsou iniciativy odvozeny od strategií, které jsou implementovány prostřednictvím technických, organizačních a transformačních aktivit.

Holistický přístup k zavádění AI do výroby musí mimo jiné počítat s následující aspekty:

1. Tvorba hodnoty (analýza přínosů a nákladů)

Přidaná hodnota při používání AI je vytvářena prostřednictvím informací, náhledů a (autonomních) akcí a procesů z nich odvozených. Základem jsou dostupná data – data se však nemusí nutně stát užitečnými informacemi pouze při použití umělé inteligence. Stávají se jimi pouze tehdy, jsou-li zpracovávány v konkrétním kontextu a za konkrétním účelem. Analýza tvorby hodnoty na jedné straně hodnotí přínosy informací získaných pomocí AI, na druhé straně určuje kvalitu dat a náročnost na pořízení a zpracování dat a s tím spojené investice do operativní výroby – včetně procesních, technologických a personálních nákladů. Výsledkem je obchodní model.

Obr. 3: Životní cyklus aplikace AI



2. Proces (vývoj a životní cyklus aplikace AI)

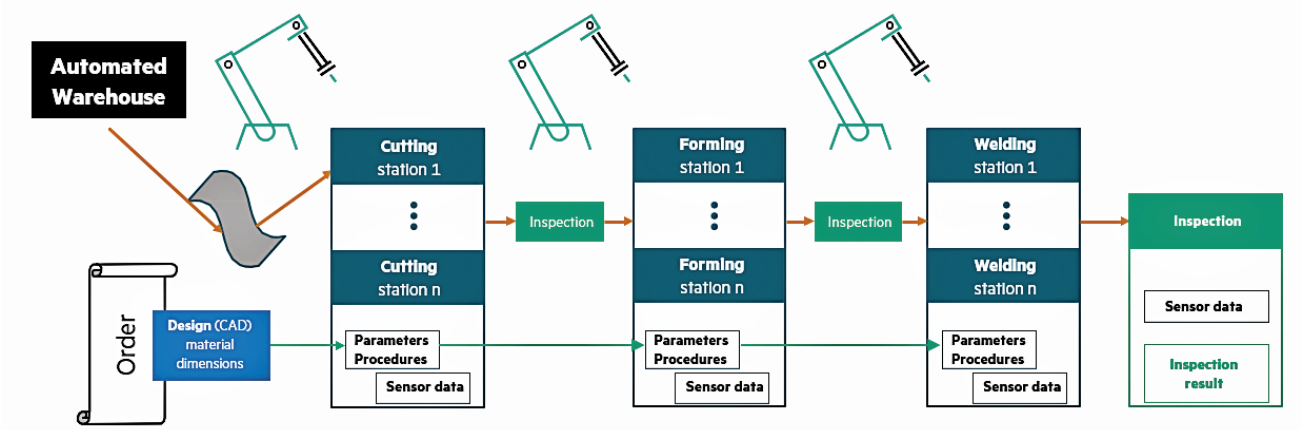
Pokud hodnotová analýza dospěje k pozitivnímu výsledku, začíná vývoj a zavádění AI. To by se mělo řídit filozofií DevOps, ve které spolupracují všechny relevantní týmy z výroby a provozu s odborníky na AI a IT (v kontextu s AI se tomu také říká MLOps a DataOps). Tím je zajištěno, že integrace do IT a výrobních procesů je zohledněna hned od začátku. Návrh řešení nejprve definuje metodu AI a software, který se má použít, a také data pro trénování.

3. Architektura (oddělení dat od aplikací)

Popsané procesy probíhají v IT a výrobních prostředích, která jsou v mnoha společnostech značně fragmentovaná – to znamená, že neexistuje nepřetržitý přístup k nástrojům a datům, procesy se neshodují, chybí standardy a integrované bezpečnostní koncepty. Takové prostředí je smrtící pro jakoukoliv implementaci AI. Proto základem řešení tohoto problému je zavedení datově orientované architektury. Ve svém jádru odděluje data od aplikací, které je generují, jejich směřováním přes centrální datový rozbočovač. Každá aplikace funguje jako producent dat pro datový hub, každý dotaz je spotřebitelem rozsáhlé distribuované databáze. To vše je zakomponováno do zastřešujícího rámce pro správu dat.

4. Kompetence (mezioborová spolupráce)

V mnoha případech jsou PoC nastaveny příliš jednodimenzionálně, protože je provádějí



Obr. 4: Flexibilní, autonomní výrobní proces v kovodělném průmyslu

specialisté na data, kteří rozumí datům a modelům, ale už méně systémové architektuře a IT procesům. Úspěšné zavedení AI však vyžaduje správnou kombinaci dovedností z různých oddělení, aby bylo možné naplánovat, vyvinout, zavést a uvést do provozu samotnou aplikaci a její integraci do IT a výrobních procesů. Typický tým se skládá z následujících rolí, které mohou zastat zaměstnanci, nebo poskytovatele služeb:

- obchodní analytici pro hodnocení přidané hodnoty a nákladů;
- datoví specialisté pro hodnocení procesu, přípravu dat a modelový výcvik;
- specialisté na strojové učení, kteří jsou schopni budovat neuronové sítě;
- datoví inženýři pro plánování a nastavení datového kanálu a zpracování dat;
- softwaroví inženýři, kteří zajišťují integraci v distribuovaném prostředí;
- a nakonec projektový manažer.

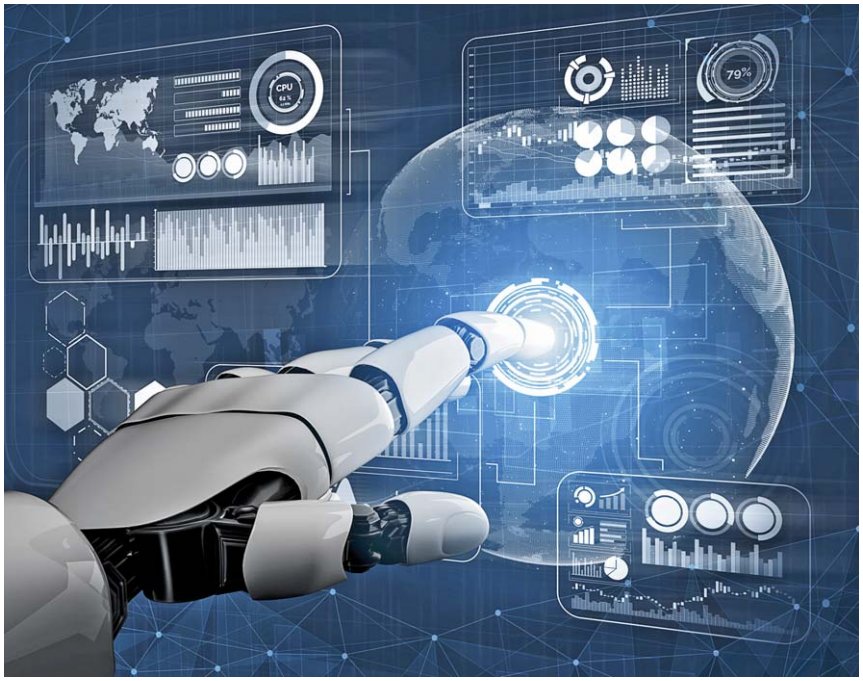
Přechod od automatizace k autonomii

Dobrou zprávou je, že již existují firmy, které pracují na přechodu svých výrobních linek od automatizace k autonomii. Opět si to ukažme na příkladu firmy z úvodu článku věnující se obrábění kovů. Tato společnost začala svou automatizaci založenou na pravidlech doplňovat metodami AI a postupně zapojuje jednotlivá provozní stanoviště do systému flexibilně ovladatelných pracovišť. Ta jsou schopna zpracovávat různé objednávky současně a jejich konfigurace probíhá autonomně a ideálně bez zkušebního provozu.

Z tohoto důvodu společnost zavedla postupy pro vybrané kroky zpracování založené na strojovém učení, tedy doporučení pro akci, například výběrem parametrů. Doporučení zatím nejsou implementována autonomně, protože je nejprve kontroluje pracovník výroby. Stav interních a externích dodavatelských řetězců je potom nově predikován a zohledňován při řízení výroby.

Navazujícím krokem, který společnost teprve čeká, bude autonomní rozhodování. Například výsledky kontroly kvality by měly v případě potřeby spustit dynamickou, nezávislou a mezisystémovou úpravu parametrů. Zejména pokud jde o svařování, má smysl aplikovat strojové učení na předchozí procesní kroky, a dokonce i na celý výrobní proces. Pro optimální využití vstupního materiálu plánuje společnost implementovat inteligentní napojení na systém skladového hospodářství a příchozích objednávek.

Stejně jako u většiny ostatních výrobních podniků, má tato společnost před sebou ještě dlouhou cestu k dosažení vize plně autonomní výroby. Popsaný holistický přístup však zajišťuje, že na této cestě jde správným směrem. ■



Matthias Roese

Autor článku působí na pozici Global Account Director ve společnosti Hewlett Packard Enterprise.

Evropská unie chce omezit možnosti využití umělé inteligence

V roce 2018 se Evropská komise začala věnovat tvorbě nového legislativního rámce, ve kterém usiluje o regulaci systémů umělé inteligence. V současnosti se návrh nařízení známý pod zkráceným názvem Akt o umělé inteligenci nachází na začátku etapy svého konečného schválení. Technologické firmy záměr oceňují, ale nezřídka kritizují stávající podobu návrhu, který obsahuje i některá velmi zásadní omezení, která jsou v rozporu s již zavedenými a ověřenými postupy. V ohrožení je například využití umělé inteligence ve finančním sektoru, ale i jiných odvětvích služeb. Podle navrhované metodiky EU by žádný software umělé inteligence neměl rozhodovat o tom, zda konkrétní člověk má nárok na poskytnutí určité služby. Dotčené firmy proto s napětím sledují, jaká bude finální, schválená verze pravidel.

Po schválení nové legislativy se evropské a mimoevropské firmy, jež působí na jednotném trhu starého kontinentu, budou muset vyrovnat s požadavky a dopady nové regulace. Mezi hlavní povinnosti se zařadí nutnost poskytovat algoritmy a změny v nich nezávislým dozorovým orgánům. Na praktickou aplikaci legislativní úpravy bude dohlížet nově zřízená Evropská rada pro umělou inteligenci.

„Nová legislativa nastaví podmínky pro vývoj a využívaní systémů umělé inteligence, jednu z nejrychleji rostoucích oblastí digitální ekonomiky. Ještě neznáme její konečnou podobu, vše se rozhodne v následujících měsících,“ říká Milena Jabůrková, ředitelka vládních programů IBM Central.

„Je otázkou, jaký to bude mít vliv na dostupnost služeb na evropském trhu a jejich rozvoj. Mám obavu ze schvalovacích procesů, které pokud budou nastaveny neefektivně, mohou se stát výrazně dražšími a pomalejšími, než by bylo únosné“ dodává poslanec Evropského parlamentu Mikuláš Peksa.

Názor českého europoslance lze doplnit komentářem Jana Romportla, ředitele centra umělé inteligence O2 Czech Republic: „Nařízení o umělé inteligenci je zásadním pokusem o globální koordinovanou akci, přinejmenším na půdě EU. Je sice pokusem těžkopádným, nedokonalým, nesoucím značný rukopis EU byrokracie, ale pořád pokusem silným, odvážným, průlomovým a velmi důležitým.“

Dodavatelé, kteří uvádějí řešení vybavená umělou inteligencí na vnitřní trh EU, musí v následujících letech v souvislosti s novou regulací počítat s možnými soudními řízeními. Ta se mohou zaměřit především na rozsah a bezpečnost systémů zaměřených na dohlížení a sledování, ukládání a správu osobních dat.

„Je pochopitelné, že kolem připravované legislativy panuje nemalá nejistota, která bude ovlivňovat vnitřní procesy soukromých společností a jejich investice do umělé inteligence. Potenciálně může dojít k výraznému zpomalení vývoje v oblastech, v nichž systémy s umělou inteligencí pracují s citlivými daty nebo slouží společensky kontroverzním účelům,“ říká Jack Vernon, expert společnosti IDC na software s umělou inteligencí.

Jednotliví dodavatelé společně s uživateli systémů umělé inteligence musejí začít přemýšlet o tom, jak nová legislativa ovlivní jejich aktivity. Čím dřív tuto úvahu zahájí, tím spíše budou schopni předejít pozdějším nepříjemným překvapením.

„Na dopady nařízení Akt o umělé inteligenci se zatím nepřipravujeme a nemáme je finančně podchycené. Zatím nemáme ani odezvu od našich evropských zákazníků. Je to proto, že stále vnímáme vysokou míru nejistoty, co se týče finální podoby a rozsahu regulace,“ doplňuje Petr Baudiš, zakladatel a technologický ředitel společnosti Rossum, a dodává: *„Jsem však přesvědčen, že nedává smysl regulovat plošně umělou inteligenci, ale předcházet nežádoucímu chování v konkrétních citlivých situacích.“*

Rizika umělé inteligence

O umělé inteligenci se ve světě moderních technologií intenzivně hovoří již mnoho let. S jejími aplikacemi, jakkoli může jít o jednodušší formy či dílčí disciplíny, se běžně dostávají do styku i koncoví spotřebitelé. Umělá inteligence se stává všudypřítomnou. Nabízí se otázka, jak chce Evropská komise všechny její stávající i budoucí aplikace prověřit. Odpověď spočívá v metodice, s níž nová legislativa pracuje. Podle stávajícího znění Aktu o umělé inteligenci budou systémy umělé inteligence zařazeny do jedné z následujících kategorií:

- **Nízké či minimální riziko.** Jde o systémy, které nepotřebují zvláštní dozor ze strany regulačních orgánů EU.
- **Systémy s vysokým rizikem.** Ty budou povoleny, pokud budou splňovat parametry regulace. Jejich rizikovost je definována účelem a funkcí. Evropská komise vytvoří celoevropskou databázi pro všechny systémy s vysokým rizikem, což umožní všem národním orgánům, uživatelům i zainteresovaným skupinám ověřit jejich soulad s platnou evropskou legislativou. Mezi oblasti s vysokým rizikem patří například systémy s umělou inteligencí pro zaměstnance, řízení lidských zdrojů a přístup k jejich náboru. Dále půjde o hodnotící systémy, které utváří či kontrolují parametry fyzických osob, a to jak v soukromé, tak ve veřejné sféře. Žádný software umělé inteligence by neměl rozhodovat o tom, zda konkrétní člověk má nárok na poskytnutí určité služby. A konečně sem patří i systémy, které se zabývají sledováním, zadržením či jiným omezováním osobních svobod. Jde převážně o systémy nasazované bezpečnostními složkami.
- **Systémy s neakceptovatelným rizikem.** Do této kategorie spadá software, jenž využívá podprahovou manipulaci, generuje skóre sociálních systémů nebo vykořisťuje určitou skupinu obyvatel a porušuje jejich práva. ■

Jaký bude rok 2022 z hlediska průmyslu?

Přetrvávající nejistota a nedostatek, obavy o bezpečnost dat, lepší konektivita, tlak na udržitelnost...

–InfoConsulting–

Jaký bude rok 2022 pro výrobní průmysl? Sestavili jsme pro vás předpovědi odborníků z IFS, kteří pracují na ERP řešení pro výrobní podniky. Můžete je porovnat s vaším pohledem na budoucnost výrobního průmyslu v lokálních českých či slovenských podmínkách. Nejprve se ohlédněme za uplynulým rokem.

Ohlédnutí zpět

Po turbulencích způsobených pandemií COVID-19 v roce 2020, která otřásla výrobním průmyslem a odhalila mnoho jeho slabých míst, nebyl rok 2021 rokem, v nějž mnozí doufali. I když tolik očekávané a rozsáhlé rozšíření vakcín v Evropě a Severní Americe vedlo ke zmírnění restrikcí a oživení výrobních aktivit, optimismus byl potlačen obavami z přetrvávajících rizik, dalších neočekávaných událostí a jejich možných následků.

V průběhu roku 2021 jsme byli svědky různých narušení, které vedly ke skutečné krizi dodavatelského řetězce. Od nedostatku výrobků, zvyšování nákladů a inflace až po prudký nárůst cen komodit, který byl jejich důsledkem. Výrobci byli nuceni přehodnotit své strategie zásobování a zvýšit zásoby tak, aby k podobným výpadkům nedocházelo znovu. K tomu se přidala rizika spojená s různými variantami COVID-19, kybernetickými útoky, ekologickými problémy, vyššími daňovými sazbami, prudkým růstem cen energií, nedostatkem zaměstnanců a samozřejmě snahou o obnovu a dohnání ztrát, které způsobila pandemie.

Vzhledem k rychlosti, intenzitě a rozsahu pandemie se výrobci museli rychle přizpůsobit a najít nové cesty, jak fungovat, aby přežili. Z toho všeho vyplynulo jedno pozitivum: „Náhlá změna“ se ukázala jako uskutečnitelná a „staré způsoby“ fungování již nebyly udržitelné. Jednou z největších provozních změn byl přechod na práci z domova, který s sebou však nesl zvýšenou zranitelnost informačních systémů. Organizace musely častěji aktualizovat a zvyšovat úroveň kybernetického zabezpečení, aby udržely krok s hrozbami. Přesun obchodních procesů do „virtuálního“ prostředí ale také otevřel příležitosti: v cloudu mohli výrobci propojit více svých aplikací a systémů, propojit data napříč jednotlivými odděleními či divizemi, a tím odstranit provozní sila.

Výhled do budoucna

Předpověď 1: 65 % výrobních společností se přesune na jednu instanci IS

Software a aplikace se vyvíjejí a zdokonalují rychlým tempem – s rychlostí změn roste i hrozba škodlivých útoků. Výrobci přirozeně chtějí nejnovější funkce a vylepšení, aby si udrželi konkurenceschopnost. Vzhledem k velkému množství softwarových platforem zapojených do chodu podniku je to však složité, pracné a nákladné. Výrobci by měli hledat takové partnery, kteří mohou nabídnout řešení pro všechny jejich podnikové procesy na jednom místě, s bezpečnostními aktualizacemi a inovacemi zakomponovanými do klíčového produktu. Mít uživatele v jedné databázi zjednodušuje kontrolu oprávnění a přístupu. Lepší zabezpečení systému je jednou z hlavních výhod provozu řešení v cloudu.

Předpověď 2: 40 % výrobních podniků propojí výrobní stroje s informačními systémy

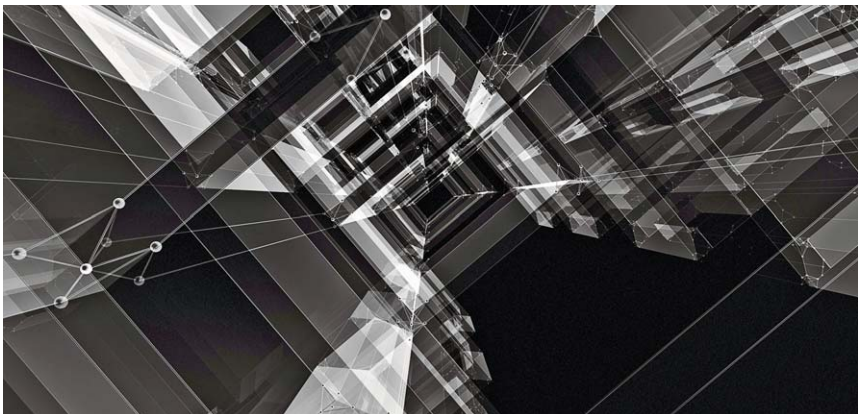
Výrobní podniky vědí, že jejich stroje a systémy generují obrovské množství potenciálně analyzovatelných a užitečných dat. Nicméně vytvoření „jediného zdroje pravdy“ tak, aby mohli k datům jednotně přistupovat, interpretovat je a činit rozhodnutí na základě informací z těchto dat vyplývajících, zůstává velkou výzvou. Klíčová bude spolupráce s takovými dodavateli řešení, kteří pomohou propojit nesourodé systémy. V příštím roce bude stále více podniků propojovat výrobní stroje a další specializované nástroje se svými podnikovými systémy, takže budou moci analyzovat data v rámci svého podnikového řešení. Části podniku to umožní přístup k datům, která dříve neviděli – a navíc v nich budou moci hledat vzájemné závislosti a užitečné informace pro další rozvoj.

Předpověď 3: 50 % výrobních společností se odkloní od metody „just in time“, aby zůstaly agilní

Dodavatelský řetězec byl tvrdě zasažen a výrobci, kteří se spoléhali na klíčové suroviny z jednoho zdroje, byli nuceni změnit své byznys modely, aby se udrželi na trhu. Pokud fungují na principu JIT (Just in Time), musí zvážit vytvoření zásob důležitých komponent, aby byly pokryty nepravidelné dodávky. To je třeba udělat opatrně, protože velikost rezervy se musí řídit prognózou a poptávkou, aby se minimalizoval dopad na cashflow tam, kde jsou marže nízké. Používání bezpečnostních zásob a výpočet bodu objednání za současných podmínek nejsou dostatečně pružné, aby se s tím výrobci vyrovnali, takže budou potřebovat pokročilejší výpočty založené na předpokládané poptávce a prokázané výrobní kapacitě. Podniky se musí podívat na své dodavatelské řetězce tak, aby byly odolnější s využitím všech nástrojů, které mají k dispozici.

Předpověď 4: 80 % výrobců omezí svou závislost na dálkové kontejnerové přepravě

Kdysi rychlá, efektivní, spolehlivá a levná námořní síť (která zajišťovala 90 % světového obchodu, z toho 70 % v kontejnerech) byla v roce 2021 v troskách. To vedlo ke „kontejnerové tragédii“, která vyhnala sazby za přepravu na rekordní úroveň a přiměla některé



vývozce zvýšit ceny nebo jednoduše přepravu úplně zrušit. V roce 2022 budou výrobní podniky hledat větší rozmanitost a flexibilitu v dodavatelských partnerstvích a také v tom, odkud a možná především jakým způsobem získávají materiály, zboží a služby. Například zřizování nových klastrů národní a regionální výroby, známých také jako „proximity sourcing“, což je přístup, kterým je známý oděvní řetězec Zara. V oblasti potravin a nápojů uvidíme, že se výrobci zaměří na budování pevnějších vztahů s více místními dodavateli a ti, kteří se specializují na čerstvé potraviny, kde je doba trvanlivosti obzvláště krátká, budou investovat do maloplošného vertikálního zemědělství. Velkou roli budou hrát také technologie a automatizace. V některých případech pomůže aditivní výroba (AM) získat nezávislost na Číně, a tedy i na dálkové kontejnerové přepravě. Během pandemie již AM začala celosvětově vyplňovat některé mezery v dodavatelském řetězci, jak upozornil časopis Industry Week. Lehkost, s jakou mohou 3D tiskárny přejít z výroby jedné součásti nebo výrobku na výrobu něčeho zcela jiného, totiž výrobcům umožňuje vyřešit alespoň část úzkých míst v dodavatelském řetězci. Inovace v oblasti hardwaru a materiálů však předběhly vývoj softwaru, takže pokud má software oslovit širší škálu výrobců, bude muset dohnat ztrátu. V jednoduchosti tedy budeme svědky posunu směrem ke zkracování dodavatelských řetězců.

Předpověď 5: 60 % výrobních podniků bude považovat snižování uhlíkové stopy za prioritu v rámci svého celkového úsilí o udržitelnost

Rok 2022 bude rokem dekarbonizace a oblast udržitelnosti nabude na významu a naléhavosti. Regulační tlaky, požadavky zákazníků, investoři a další zainteresované strany posunuly udržitelnost na vrchol obchodních priorit a učinily z ní provozní princip budoucího fungování. Vlády a finanční komunita vynakládají značné investice do boje proti změně klimatu – Evropská komise například stanovila cíl „nulových čistých emisí do roku 2050“, čímž na podniky vyvíjí právně závazný tlak, aby snižovaly svou uhlíkovou stopu.

Pro splnění těchto požadavků budou nejdůležitější data. Co to znamená? Výrobní firmy budou potřebovat přístup k přesnějším, podrobnějším a včasnějším údajům, které se budou týkat nejen emisí na úrovni organizace, ale také dílčích emisí spojených s výrobními procesy, přepravou surovin a výrobků a používáním a likvidací výrobků po skončení jejich životnosti.

Schopnost vykazovat podrobná data bude v budoucnu součástí podnikání a technologie bude klíčovým prostředkem pro zachycování, evidenci a sdílení těchto dat v celém hodnotovém řetězci. Někteří výrobci již dnes využívají technologie, jako jsou IoT, Big Data a AI, ale technologie se vyvíjejí obrovskou rychlostí a do budoucna můžeme očekávat další potenciál při řešení otázek udržitelnosti.

Předpověď 6: 70 % výrobních společností znovu získá kontrolu nad svým plánováním na základě údajů z let 2020 a 2021 a zvýší tak svou odolnost

Někteří výrobci se domnívají, že údaje za roky 2020 a 2021 jsou příliš zkreslené na to, aby byly v roce 2022 přínosné. Pokud se v tomto období potýkali s problémy, mohli by je ignorovat a argumentovat tím, že jsou prostě příliš „náhodné“ na to, aby je zohlednili. Naopak, pokud viděli, že objednávky prudce rostou (jako např. v potravinářství a nápojářství), mohou se rozhodnout nebrat v úvahu neobvyklé datové vzorce, aby nevytvářeli příliš optimistické, a tudíž nespolehlivé předpovědi na nadcházejících 18 až 24 měsíců. Oba způsoby jednání by byly chybou. Předchozí narušení dodavatelského řetězce, jako byly například záplavy v Thajsku v roce 2011, byla mnohem více lokalizovaná, trvala relativně krátkou dobu a většinou ovlivnila nabídku, nikoliv poptávku. COVID-19 však byl skutečně globální událostí, která ovlivnila poptávku i nabídku. Výrobci mají stále příležitost poučit se ze zkušeností z posledních dvou let. Pandemie v žádném případě neskončila a další taková událost může být stejně nepředvídatelná a náhlá. Proto by měli výrobní podniky maximálně využít získané poznatky z období let 2020/21:

- Rozlišovat mezi sezónními a vnějšími událostmi, včetně mimořádného dopadu pandemie COVID-19. Ačkoli je očišťování historických dat nezbytné pro zvýšení přesnosti předpovědí, ujistěte se, že si uchováváte data týkající se pandemie, protože se vám v budoucnu mohou hodit, pokud by do vašeho dodavatelského řetězce zasáhla podobná událost.
- Aplikujte scénář „co kdyby“ - analyzujte srovnatelné události a provádějte simulace, které vám pomohou kvantifikovat pravděpodobný dopad potenciální události na příjmy společnosti a její celkovou výkonnost, i na širší dodavatelský řetězec.
- Zaměřte se spíše na dopad na podnikání (napříč regiony, prodejními kanály a profily zákazníků) než na samotnou událost.
- Využívejte strojové učení ke zvýšení přesnosti prognóz, minimalizujte lidské chyby a pro začátek neberte v úvahu nerelevantní data.

Shrnuto a podtrženo...

Výrobní podniky v současnosti stále čelí významným překážkám a narušením. Přesto panuje optimismus, že průmysl zakončil rok 2021 v podstatně silnější pozici ve srovnání se začátkem roku 2020, kdy turbulence začaly. Digitální transformace a konsolidace dat ve výrobě se bude nadále zrychlovat, ale investice do technologií nebudou sloužit jen jako nástroje pro krizovou navigaci. Budou hrát zásadní roli v tom, aby pomohly organizacím zůstat odolné, stát se agilnějšími, rychle reagovat na situaci na trhu a využívat nové příležitosti.

Předpovědi vývoje v oblasti průmyslu pro rok 2022 sestavili Andrew Burton, IFS Industry Director for Manufacturing, a Maggie Slowik, IFS Industry Director for Manufacturing. Překlad a stylistickou úpravu připravila Dana Kovačovičová, manažerka marketingu Info-Consulting Czech s.r.o. ■

Optimalizace logistiky

Martin Plajner

Dodavatelské řetězce se nachází ve stavu, kdy po letech růstu došly do bodu, který viditelně vyžaduje revizi a mnohdy tvrdé zásahy, aby mohly dál efektivně fungovat a plnil tu roli, kterou od nich očekáváme. Optimalizace logistiky a zvyšování efektivity a robustnosti dodavatelského řetězce jako takového je proto v dnešních dnech čím dál tím větší téma. S klienty o něm při našich projektech mluvíme stále častěji a rozdíl oproti předchozím rokům je zřetelný. Pojďme se tedy podívat na to, proč tomu tak je, co tyto procesy znamenají a jaká je cesta právě k optimalitě.

Cíle optimalizace

Pod pojmem optimalizace logistiky, pokud zazní bez dalších souvislostí, je těžké si představit konkrétní procesy. Především proto, že se u každé společnosti jedná o něco trochu jiného. Optimalizuje se tam, kde je největší potenciál, a také s nějakým konkrétním cílem. Protože slabých míst v dodavatelském řetězci je bezpočet, zaměříme se v krátkosti spíše na cíle, které jsou dnes obvykle sledovány.

V první řadě, budu upřímný, se jedná o finance. Rozdíl je především v tom, jestli se mluví o financích na prvním místě, nebo až na druhém. Doplním, že snížením nákladů myslíme spíše jednotkové náklady přepočítané na manipulační jednotky nežli celkové náklady. Motivace k tomuto kroku je asi celkem jasná. Zahrnuje však i takové body, jako pokrytí navýšeného objemu za ideální peníze. Za zmínku stojí ještě to, že aktuálně jsme na českém trhu v zajímavé situaci, kdy někteří zadavatelé přeprav zaznamenávají extrémní růst a někteří naopak zásadní pokles. Fáze růstu má u většiny firem tendenci zanedbávat efektivitu, protože na ni obvykle není čas. Ve chvíli, kdy přechází do stagnace nebo propadu, čas se začne objevovat a s ním i silná potřeba úspor. Někdy je však bohužel pozdě vzít zpět některá rozhodnutí.

Na dalším místě rozhodně stojí dnes hodně skloňovaná odpovědnost k životnímu prostředí. Ať už z vlastní vůle, nebo na základě podmínek odjinud (od zadavatele přepravy, regulací státu, korporátních struktur, ...) se tento požadavek promítá čím dál více do rozhodovacího procesu a změn, které se v dodavatelském řetězci dějí. Tento bod je naštěstí s prvním velmi často provázán, a tak jdou úspory finanční ruku v ruce s emisními. Není tomu tak však samozřejmě vždy, protože pokud se bavíme o změnách technologických nebo ve flotile vozidel, je situace složitější než jen úspora najetých kilometrů.

Třetí zásadní faktor je výstup směrem k zákazníkovi. Zjednodušeně můžeme říkat service level, který je nedílnou součástí každé služby. Ať už je korektně měřen a vyžadován, nebo není, vždy se vyskytuje. Bohužel toto kritérium je obvykle v přímé kontradikci s předchozími dvěma. Dnes už víme, že tlak na same-day a next-day delivery, na které jsme si jako klienti zvykli, vede ve skutečnosti k velikým zdrojům neefektivity a v konečném důsledku tak i plýtvání a zvýšení emisí. Bohužel cesta zpět k D+5 již neexistuje, a tudíž je potřeba s tímto faktorem umět pracovat.

Konkrétní zadání se liší, ve výsledku se v drsných číslech obvykle dají redukovat na ukazatele zmíněné výše. Vznikají tak všechny možné kombinace a dvě nejčastější z nich jsou:

- Zvýšit efektivitu logistiky (tj. snížit náklady, nebo zvýšit objem bez poměrově stejného nebo většího nárůstu nákladů) při zachování service levelu a nezhoršení environmentálních dopadů.
- Snížit dopad na životní prostředí s nízkými dodatečnými náklady bez vlivu na service level.

Tři pilíře distribuční strategie

Spolu s mými kolegy, především Adamem Zdvihalem a Alexandrou Pappovou jsme definovali tři pilíře na cestě k optimalizaci logistiky a zlepšení jejího environmentálního dopadu. Tyto pilíře lze pojmenovat různě: současnost – krátkodobý výhled – dlouhodobý výhled; pochopení dnešního stavu – quick wins – změna logistiky; operativa – taktika – strategie. Ať už tomu budeme říkat jakkoliv, každý z těchto pilířů má svůj význam.

Operativa – k vyhodnocení efektivity potřebujete data

V prvním z nich je klíčové pochopení a správné sledování aktuální realizace distribučních úkonů. Často se setkáváme s tím, že chceme-li se podívat do dat, která jsou uchovávána, a vyhodnotit efektivitu logistiky zpětně, tak data chybí. Obvykle je to z důvodu, že tato data není nezbytné k operativním úkonům uchovávat. Pokud například zasíláme zásilky na pět cílových míst, není již třeba si zpětně

pamatovat, které zásilky byly spolu v autě. Tento stav je na jednu stranu pochopitelný, na druhou stranu znemožňuje hledat příčiny a navrhovat zlepšení. O tom je právě práce v současnosti. Identifikace zdrojů nákladů neefektivity a v neposlední řadě i emisí. Pro to je nutné zaznamenávat, co se děje, a pracovníkům musí být vysvětlen účel tohoto konání. Vždy se totiž ukazuje, že pokud nerozumí našemu cíli, tak ani data, která pomáhají sbírat, nemají nezbytnou kvalitu.

Taktika – není vhodné řešit vše vlastními silami

Ve druhém pilíři, taktice a quick wins je to především o využití těch informací, které jsme získali a kde vidíme potenciál. Na trhu je dnes celá řada řešení, která umějí postihnout jednotlivé problémy, které se v dodavatelském řetězci dějí. Není tak třeba snažit se vše řešit vlastními silami a s některými kroky lze získat vhodnou pomoc, která je založena právě na práci s daty a moderních formách komunikace. Díky tomu tak např. již nemusí mimořádné přepravy vycházet draze. S tím umí pomoci například firma Logsteo, která slouží jako platforma pro komunikaci poptávky dopravy k vybraným dopravcům. Pokud se rozhoduje mezi různými formami přepravy, což je dnes velmi běžné, tak tentokráte např. Wereldo umí navrhnout, zda vzít balíkovku, vlastní přepravu, nebo paletovku. Tyto a další nástroje umožňují rychle zvýšit efektivitu a dojít jak k úsporám finančním, tak ekologickým a v neposlední řadě umožňují snížit nároky na know-how dispečerů. Poslední bod je možná nakonec nejzásadnější, protože dnes pozorujeme velmi problematické momenty spojené s fluktuací a nemocností těchto klíčových pracovníků.

Dlouhodobá strategie

Třetí pilíř je dlouhodobá strategie. Je to sice záležitost nejvzdálenější, ale neméně důležitá. Je známo, že v distribuční síti se nemohou změny stát ze dne na den. Proto je třeba tyto kroky důkladně promyslet a naplánovat. Obvykle zahrnují změnu nebo úpravu skladových lokací, změnu flotily a typu přepravy, nebo přípravu na navýšení objemů a s tím spojené procesní a směnové změny, zavádění automatizace. Tato úloha je extrémně nesnadná, protože do ní vstupuje celá řada neznámých a proměnných faktorů, které ji ovlivňují. V první řadě je zásadní si udělat jasno v tom, jaký je budoucí očekávaný stav. Zde do hry vstupují opět čísla a co nejpřesnější forecast budoucího stavu. Ptáme se na očekávání s výhledem na několik let dopředu, a tudíž svůj díl má i obchodní strategie firmy a analýza produktového portfolia. Další z faktorů jsou dostupné skladovací, personální a procesní kapacity v uzlech distribuční sítě, očekávané změny v dopravní infrastruktuře a na závěr změny ve flotile a cesta k ekologickým formám přepravy (ať už to má být kamion na LNG, vodík, nebo přesun na železnici). Jedná se tedy o komplexní problematiku, která by se správně neměla řešit separátně, ale dohromady, aby společnost jako celek dosáhla optima.

Závěrem

Ať už bude rozhodnuto o využití externí podpory, nebo nikoliv, je třeba nezapomenout, že není možné vynechat kterýkoliv ze zmiňovaných pilířů. Pokud bude chybět byť jen jeden, tak se to dříve nebo později (podle toho, který chybí) ukáže. Nakonec pilíře říkáme právě proto, že jsou potřeba všechny, aby cesta k vytyčenému cíli mohla fungovat. Pevně věřím, že je v silách všech společností, které řeší logistiku zboží, pracovat se všemi třemi oblastmi. Zásadní je vědomá snaha, která toto konání musí provázet, a energie, která se tématu věnuje. Povinnosti všedních dní často vedou k tendenci upřednostňovat dnes před zítra. Je již na uvědomění managementu, že bez strategie a konceptu se jedná pouze o cestu k vlastnímu přepracování. ■

Martin Plajner

Autor článku je expertem na logistiku ve společnosti Logio.

Retail v roce 2022 bude o flexibilitě a automatickém řízení zásob. Technologicky vyzbrojit se musí i ti nejmenší

Roland Džogan

Uplynulý rok se nesl zejména v duchu pandemie covid-19, která zasáhla prakticky všechna odvětví. Jednou z oblastí, které pandemie postihla nejvíce, byl ale bezpochyby mezinárodní obchod. Byli jsme svědky prudkého poklesu globální produkce, celý svět se potýkal s problémy v dodavatelském řetězci, jakým v moderní historii dosud nemusel čelit a v důsledku kterých vznikla na trhu významná nerovnováha mezi poptávkou a nabídkou zboží. Na změny, které pandemie přinesla, byli nuceni bezprostředně reagovat obchodníci a dodavatelé, své chování ale přehodnocovali také zákazníci.

Výsledkem rychlých a nečekaných změn byl zmatek na všech úrovních dodavatelského řetězce. Problémy, s nimiž se dodavatelský řetězec musel v uplynulém roce potýkat, nicméně velmi pravděpodobně potrvají i nadále. Návrat dodavatelského řetězce do stavu před pandemií podle odborníků nelze čekat dříve než v horizontu několika let, pokud vůbec. K vytvoření nové rovnováhy a obnovení zákaznické důvěry proto bude třeba, aby obchodníci přehodnotili svá dosavadní řešení a byli ještě flexibilnější a otevřenější trendům, jimž dalo uplynulé období prostor vzniknout.

Automatizace řízení zásob

Loňský rok ukázal, že neschopnost obchodníků pokrýt poptávku pro ně může být osudná. Ať už se firmy potýkaly s nedostatkem zboží z důvodu zpoždění dodávek ze zámoří, či neschopnosti správně předvídat, jak vysokou poptávku mohou očekávat, nedostupnost poptávaného zboží je ze strany zákazníků vždy vnímána negativně. Není proto divu, že se novým standardem stávají nejen replenishment systémy, ale čím dál častěji také systémy pro redistribuci zboží, které byly dříve vnímány spíše jako příjemný doplněk.

Zatímco tradiční replenishment systémy fungují jako počítačový systém, který analyzuje stav zásob a dodací lhůty a na základě výstupních dat automatizovaně objednává zásoby tak, aby odpovídaly předpokládaným potřebám prodeje, do popředí se stále více dostávají systémy, které umí pracovat i se zbožím, jež obchodník již nakoupil. Ani nejpropracovanější replenishment systém totiž nedokáže zabránit vzniku takzvaných mrtvých zásob, tedy kumulaci zboží, které bez užitku leží na skladě.

Mrtvé zásoby se mnoho firem snaží po vlastní ose redistribuovat, dříve nebo později však naráží na to, že redistribuce zboží bez specializovaného řešení nedává ekonomický smysl. Aby se redistribuce vyplatila, je nutné využít forecastovacích a optimalizačních algoritmů navržených přímo pro use-case redistribucí. Ty dokáží spárovat správné výchozí („source stores“) a cílové pobočky („target stores“) a za využití standardních dat, které má k dispozici každá firma pro účely účetnictví, vybrat pouze profitabilní kombinace obchodů a produktů tak, aby se zboží, které bylo mrtvou zásobou, na jiné prodejně transformovalo ve zdravé zásoby, které se přirozeně vyprodají.

Čím automatizovanější a propracovanější systémy budou mít obchodníci k dispozici, tím lépe dokáží na poptávku reagovat a přizpůsobovat se zákazníkům. Vyhráno budou mít ti, kteří se naučí s objednávkami a vlastněným zbožím disponovat tak, aby neměli prázdné regály, ale ani přebytky, které budou řešit nevýhodnými slevovými akcemi. Slevy totiž mají negativní dopad nejen na ziskovost podnikání, ale také na reputaci značky.

Důraz na udržitelnost a cirkulární ekonomika

Potřebu lépe optimalizovat skladové zásoby umocňuje také čím dál větší tlak na udržitelnost. Pandemie covid-19 měla totiž také světlejší stránky – podle dosavadních výzkumů přiměla zákazníky k tomu, aby byli výrazně vnímavější k ekologickým dopadům svého nákupního chování. Mnoho lidí se v průběhu pandemie vrátilo k lokálním nákupům u místních prodejců. Důvodem byla kromě snahy o podporu malých podniků také nespokojenost s velkou zátěží životního prostředí, kterou s sebou přináší nákupy online. Dá se proto očekávat nejen to, že se lidé budou postupně vracet do kamenných obchodů, ale také to, že aktivity podniků v oblasti udržitelnosti budou stále důležitějším faktorem pro úspěch či neúspěch firmy.

Využívání udržitelných materiálů získaných z etických zdrojů, ekologická balení nebo udržitelné skladování je však pouze špičkou ledovce. Prioritou v otázce udržitelnosti by se pro firmy mělo stát především nasazení vhodných technologií pro maximální efektivitu. Ať už se jedná o nakládání s mrtvými zásobami nebo inovace na poli logistiky, chytrá řešení přispívají k udržitelnějšímu podnikání výrazně větší měrou.

Velkým tématem následujícího roku i let dalších bude také cirkulární ekonomika, trend, o kterém je stále více slyšet právě v souvislosti s udržitelností a snížení uhlíkové stopy průmyslu a obchodu. Nalézt řešení, jak co největší množství zboží dokázat vrátit zpět do dodavatelského řetězce, využívat ho opakovaně, recyklovat i znovu prodávat, bude velkou výzvou. Ačkoliv rok 2022 zřejmě nebude rokem průlomovým, má velký potenciál být rokem, kdy se udržitelným řešením v duchu cirkulární ekonomiky položí základy.

Flexibilita v doručování zásilek

Není tajemstvím, že zatímco kamenným obchodům pandemie příliš nepřála, e-commerce zažila v uplynulém roce výrazný vzestup. Online nákupy se staly standardem, na který si zvykli prakticky všichni zákazníci beze zbytku, včetně těch, kteří z něj dříve měli obavy. S jejich rostoucí oblibou však rostou také nároky na větší flexibilitu, a to zejména v otázce doručování. Doručování v režimu same-day, které bylo dříve spíše luxusem či výsadou několika konkrétních segmentů, se bude pomalu stávat nezbytností. Obchodníci, kteří svým zákazníkům dokáží dodat zboží v co nejkratším časovém úseku, co nejpřesněji a poskytnout o doručení maximální možné množství informací, budou mít v roce 2022 velkou konkurenční výhodu.

Same-day delivery kombinuje pohodlí online nakupování s rychlou dostupností produktů, která je typická pro kamenné obchody. Pro firmy působící v e-commerce může navíc fungovat jako skvělý katalyzátor – k nakupování na internetu dokáže přimět i ty skupiny zákazníků, kteří by jindy preferovali návštěvu kamenné prodejny. Aby same-day logistika mohla fungovat, je ale nutné, aby produkty byly lokálně dostupné a obchodníci měli v reálném čase perfektní přehled o svých zásobách, a to jak na skladě, tak v jednotlivých prodejnách. Jedině tak je během procesu objednávky možné zjistit, zda je doručení ve stejný den realizovatelné.

S ohledem na flexibilitu v doručování se čím dál větší popularitě budou těšit také různé alternativní možnosti doručení. Firmy budou nejraději spolupracovat s dopravci, kteří dokáží zajistit doručení zásilek do doručovacích boxů, zajímavou alternativou je také možnost doručení do kufru zaparkovaného auta, která funguje na principu udělení vzdáleného přístupu skrz aplikaci v mobilním telefonu. V současnosti tuto alternativu mohou využívat pouze majitelé několika konkrétních modelů vozů, dá se ale předpokládat, že se v následujících letech stane rozšířenější variantou.

Last-mile řešení

Aby bylo možné zajistit větší flexibilitu v oblasti doručování zásilek, bude pro firmy nezbytné zajistit řešení poslední míle. Technologie, které dnes mají logistické firmy na poslední míli k dispozici, dokáží zákazníkům poskytnout informace o tom, kde se jejich zásilka právě nachází, kdy ji mohou očekávat a všechno mezi tím. Technologie poslední míle může pomoci řešit také neočekávané události v průběhu doručování, jako například náhlé dopravní komplikace. Dokonalá informovanost bude v následujícím roce klíčovým faktorem pro efektivitu logistiky, protože opakovaně doručovaná zásilka z důvodu, že se kurýr mine se zákazníkem, je další zbytečnou environmentální zátěží.

Kvalitní logistika s dobře informovaným zákazníkem je navíc zásadní pro zákaznikovu spokojenost s daným obchodem. Ačkoliv doručení zboží zpravidla zajišťují externí dopravci, ukazuje se, že informovanost o doručení, jeho rychlost, ale i chování kurýra, má na zákaznickou zkušenost s obchodem důležitější dopad než například

ceny produktů. Ve stále rostoucí konkurenci bude proto důležité, aby firmy věnovaly logistice velkou pozornost a logistické partnery si pečlivě vybíraly.

Shrnutí

Jak z výčtu některých z nadcházejících trendů vyplývá, následující rok by se měl nést zejména v duchu vzájemné spolupráce na jednotlivých úrovních dodavatelského řetězce a maloobchodu. Doby, kdy se firmy snažily veškeré kroky pokrýt vlastními silami, jsou nenávratně pryč. Aby bylo možné zákazníkům dodat služby v kvalitě, jakou požadují, je třeba, aby firmy využívaly specializovaná řešení pro řízení skladových zásob, jejich redistribuci a pokud možno i následné doručení směrem k zákazníkům.

Je čím dál jasnější, že retail bude pod narůstajícím tlakem, aby technologicky držel krok s konkurencí v podobě dravé a rychle rostoucí e-commerce. Z chování zákazníků je evidentní, že kamenným obchodům rozhodně neodzvonilo. Aby ale zůstaly konkurenceschopné, musí se technologicky vyzbrojit, což se zdaleka netýká jen těch největších maloobchodních sítí. ■

Roland Džogan

Autor článku je CEO startupu Ydistri, který se soustředí na redistribuci dead-stocku a optimalizaci skladových zásob v retailu.

Nová éra e-commerce

Jak nepromarnit šanci, kterou přinesl skokový růst e-commerce

Matěj Kapošváry

Sen mnohých manažerů e-shopů, kteří před pandemií vytyčovali cíle svým podřízeným, desítky a stovky procent ročně, se stal skutečností. Skokový růst dorazil, sen se vyplnil. Tedy, v roce 2020 dorazila pandemie Covid-19 a s ní masivní úprk zákazníků z kamenných prodejen a provozoven, a to vinou vládních opatření nebo vlivem strachu z nákazy, popř. dalších vlivů. Celý trh e-commerce jen v České republice vyrostl v roce 2020 o 26 %, zatímco předpoklady z roku 2019 byly na úrovni 10 - 15 %. E-shopy u nás poprvé prodaly zboží za více než dvě stě miliard korun a prolomily tak další vysněnou hranici.

Splněný sen

Velcí skákali mnohem výš, než menší, ale problémy s vyřizováním enormního růstu objednávek měli v roce 2020 ale i v roce 2021 téměř všichni. V některých společnostech se dokonce jeden čas zastavovala reklama, protože objednávek bylo tolik, že prostě žádná reklama nebyla potřeba. Připraven nebyl nikdo. Čas na dokonalou zákaznickou zkušenost musel jít na chvíli stranou. Z pohledu zákazníka bylo důležitější převzít nákup od kurýra bezpečně, než se pozastavovat nad ne-přesnou minutou doručení, za kterou by zákazník ještě před pandemií psal zklamané recenze na sociální sítě a požadoval náhrady.

Nová éra? Budoucnost začala před rokem

Pokud se na něčem shodne patrně celý trh, tak je to na tom, že covid akceleroval rozvoj e-commerce a inovací. Zatím, co doznívající pandemie ve verzi Omikron ještě řádí a decimuje dříve jinak velmi kvalifikovaná rozhodnutí plánovačů budoucnosti – obchodních ředitelů, tak vizionáři vidí už současný svět růžověji. Svět, kde už je jen velmi málo odpíračů online technologií napříč věkovými a dalšími kategoriemi, a tím pádem více pravidelných e-commerce zákazníků, než před pandemií. To pochopitelně láká nové e-shopisty a odráží se to v číslech nových e-shopů na našem území o několik málo tisíc ročně až na současných přibližně 50 000 eshopů. To je dáno jednak atraktivitou e-commerce, kterou reprezentují zejména úspěšné e-shopy a pak také tím, že bariéry pro vstup do e-commerce jsou dnes velmi nízké a již delší dobu žijeme v době, kdy začínající online podnikatel nepotřebuje mnohdy téměř ani produkty skladem. Vše, co je potřeba pro vstup do e-commerce, je elementární kapitál na spuštění krabicového e-shopu. U nás v České republice jsme toho dokonalým příkladem s největším počtem e-shopů na hlavu. Nicméně zde platí, že čím snazší je vstup, tím těžší bývá uspět. Budoucnost začala před rokem, není nač čekat, je na čase jednat, protože nic není jako dřív.

Nic není jako dřív, nic není, jak bývávalo

Bariéry úspěchu v e-commerce jsou v dnešním světě extrémně vysoké. Stejně, jako se nastartoval skokově růst, nastartovali se i schopnosti a ochota investovat hlavně na straně těch největších hráčů na trhu. Momentálně je dle nás z pohledu konsolidace trhu nejvíce ohroženou skupinou segment malých a středně velkých e-shopů provozovaných na krabicových řešení, zastaralých technologiích s obtížnou maintenance a slabými vyhlídkami pro další rozvoj, které ovšem i díky pandemii dosahují tržeb mnohdy v řádech desítek či nižších stovek milionů korun ročně a tím pádem je jejich market share pro velké hráče neodolatelným soustem. Jenže čas pro malé a střední e-shopy běží rychleji než před pandemií, a to hlavně z toho důvodu, jak rychle se velcí hráči adaptovali na nové podmínky během pandemie. Zatímco malé a středně velké e-shopy v době růstu měli nejvíc práce s tím, aby vůbec zvládly skokový růst, velké značky, respektive e-shopy dosáhly v oblastech vývoje, logistiky, marketingu, automatizace, sběru dat a dalších e-commerce disciplín pokroku, který jim dává ještě větší zvýhodnění než tomu bylo před pandemií.

Poslední hurá

Návrat zákazníků do kamenných prodejen již z velké části nastal v roce 2021 a bude dále pokračovat, nicméně e-commerce je silnější než kdy dříve. Trh se za poslední čtyři roky prakticky zdvojnásobil, ale relativní růst začal zpomalovat už loni. Naši analytici předpokládají, že v roce 2022 dojde k dalšímu

relativnímu zpomalení a trh bude růst „jen“ o 10 % oproti loňským 14 procentům. To neznamená nic jiného než konec bezprecedentního růstu a snadných úspěchů z posledních let. Domníváme se, že tak vzroste tlak a napětí mezi všemi na společném trhu, kde nejsilnější karty drží velké e-shopy, žolíka mají nepochybně retailové řetězce a Černého Petra drží malé a středně velké e-shopy. Tedy především ty středně velké e-shopy, které mají zajímavý market share a které budou otálet s inovacemi především v oblastech, jako jsou e-commerce řízení, technologie a nastavení služeb a procesů.

Černí koně konsolidace

Jedním z faktorů, který ohrožuje především středně velké e-shopy jsou bezesporu velké nadnárodní platformy typu Amazon či Alibaba, ale ne menší hrozbou do budoucna jsou černí koně - obří nadnárodní řetězce se silnou a známou značkou, vybudovanou důvěrou, enormním množstvím zákazníků a obrovským kapitálem, které ve svém sortimentu nabízí prakticky všechno „od housek po cyklistické dresy“. U těchto hráčů je patrné, že velmi vnímají atraktivní e-commerce čísla v kontextu posledních let (viz tabulka).

B2B v e-commerce

Čím dál častěji se u nás setkáváme také s fenoménem e-commerce v B2B světě a to jak u klasických B2B firem, tak například u již výše zmíněných řetězců, které prostřednictvím svých B2B e-shopů obchodují se svými business partnery nebo franšízanty. B2B e-shopy jsou často, z jistého úhlu pohledu, například v personalizaci dále než e-shopy ve světě B2C. B2B firma potřebuje na svém e-shopu ukazovat svému zákazníkovi všechny varianty produktů s cenami pro konkrétního zákazníka a to včetně přepočtů kurzů, různých dph, individuálních slev a tak dále, což v B2C světě zas až tak běžné není. Není výjimkou, že takové e-shopy obsahují často i vymoženosti ve formě nejrůznějších konfigurátorů řešení např. pro armatury, různé automotive produkty a další. Způsob plateb je v B2B také poměrně dost odlišný a dá se říct složitější kvůli individuálním požadavkům nebo možnostem jednotlivých partnerů. Z tohoto úhlu pohledu by se tedy dá říci, že funkčně jsou v některých ohledech B2B e-shopy dokonce o něco dále ve smyslu složitosti řešení, než běžné e-shopy v klasickém B2C světě. Uvážíme-li tak tyto skutečnosti a dáme je do souvislosti s řetězci a všeobecně známou touhou velkých po větším market share, pak se jeví, že technologický dluh, který se řetězcům obecně přisuzuje v klasickém e-commerce pro ně dost možná nebude tak těžké překonat prostě proto, že už mají zkušenost s vlastním složitým B2B řešením.

Rok	2018	2019	2020	2021
Obrat v miliardách Kč	135	155	195	223
Meziroční růst	17 %	15 %	26 %	14 %

Tabulka: Vývoj obratu e-commerce v Česku

Řetězce už dnes e-shop nevnímají jako konkurenta pro svou síť poboček, ale jako budoucnost, kdy e-shop, aplikace, a pobočka fungují jako jeden symbiotický ekosystém – omnichannel - se stále lepším a lepším zákaznickým zážitkem na straně jedné a tučnými zisky na straně druhé. Řetězce mají všechny předpoklady pro to uspět a ukrást market share malým a středně velkým e-shopům, pokud ty nebudou reagovat na současnou situaci zavčas.

Nepromarnit šanci

To nejhorší, co se může středně velkému e-shopu stát je, že prováhá příležitost, která je nyní na stole. Šanci, kterou mají díky skokovému růstu z předchozích let a která zde bude jen tak dlouho, dokud velké e-shopy a akceschopné retailové řetězce neřeknou dost, váš market share chceme pro sebe my. Nová era e-commerce tedy do značné míry bude charakteristická tím, jak se ti největší budou předhánět v implementaci nových aplikací, funkcionalit, platforem, systémů, služeb, realizací kamenných poboček, špičkovou kreativou svých komunikačních kampaní a tak dále, zatím co je budou dotahovat velcí a akceschopní retailoví hráči. Uprostřed této vřavy v boji o market share budou malé a hlavně středně velké e-shopy jejichž životní prostor se bude logicky zmenšovat, pakliže adekvátně nezareagují a nebudou inovovat.

Byl to náš český básník Jan Neruda, který ve sbírce básní Zpěvy páteční charakterizoval takovou situaci z našeho pohledu zcela přesně: „kdo chvíli stál, již stojí opodál“. A my musíme našemu velikánovi v kontextu situace dát za pravdu.

Nová éra přináší nová řešení

Chtělo by se říct, že recept na řešení je pro všechny velmi jednoduchý. Inovovat, investovat, učinit z e-commerce prioritu a nepodcenit technologie. Zní to jednoduše ale není to úplně tak, a to hlavně z toho důvodu, že na trhu není dostatek kvalitních lidí se zkušenostmi. Ať už odborníků na e-commerce, vývojářů, obchod nebo marketing. Pokud takoví jsou, a jsou ochotni změnit zaměstnavatele, mají svou cenu, která není zrovna malá. Proto v současnosti pozorujeme boom interim rolí např. e-commerce ředitelů a současně růst tzv. co-development projektů, které kombinují to nejlepší od každého. To umožňuje relativně rychle sestavit špičkový tým odborníků a koncentrovat tak co nejvíce know how do plánování, přípravy a samotné realizace. To má pro společnost, která se vydá touto moderní cestou nové éry obrovské výhody v tom, že dosáhne na špičkové know how a technologie zatímco má čas na hledání zapálených talentů, kterými postupně v rámci projektu nahrazuje například vývojáře nebo interim e-commerce odborníky, a získává tak plnou kontrolu nad efektivním vývojem zatímco postupně buduje svůj kvalitní in house tým, který v průběhu transformace získává špičkové know how od těch nejlepších na trhu. ■

Matěj Kapošváry

Autor článku je obchodním a marketingovým ředitelem společnosti Shopsys.

Pokud e-shopy nezohledňují zákaznické chování, připravují se o desítky procent zisků

Gejza Nagy

V Česku aktuálně působí přes 50 tisíc internetových obchodů. Podle dat Asociace pro elektronickou komunikaci (APEK) a nákupního rádce Heureka vzrostly vloni jejich obraty meziročně o 14 procent na 223 miliardy korun. Jen v průběhu posledního listopadového víkendu, kdy obchody lákají na slevové akce v rámci Black Friday, utratili Češi podle českého poskytovatele e-shopové platformy Shoptet 4 miliardy korun. Jejich konverze navíc byly až o 25 procent vyšší oproti předchozím týdnům. Před Vánocemi pak dokonce nakoupili za více než 77 miliard. E-shopy tak mají i na malém tuzemském trhu velký potenciál, mnohdy jej však neumí vytěžit na maximum.

Díky přístupu k internetu jsme se jako lidstvo naučili skvěle vyhledávat informace. „Googlení“ se stalo neodmyslitelnou součástí našich životů a ne nadarmo je magické políčko vyhledávání prvkem, který při příchodu na jakoukoliv stránku hledáme přirozeně jako první. Naše data z více jak 2 000 e-shopů ukazují, že zákazníci používající vyhledávání nakoupí 3–5krát častěji než ti, kteří se na domovskou stránku přišli „jen podívat“. V průměru využívá vyhledávání asi 20 procent zákazníků, v některých odvětvích až polovina nakupujících. Rozhodně ale nejde o zanedbatelné číslo – i v módním odvětví, kde přes vyhledávání nakupuje „jen“ 7 až 15 procent zákazníků, představuje tato skupina přibližně třetinu až polovinu obratu těchto e-shopů.

Příčina nízkých konverzí online zákazníků je tak jednoduchá i složitá současně – pokud zákazník zboží nenajde, nemá si co koupit.

Chyby ve vyhledávání

Nejčastějším důvodem, proč vyhledávač nezobrazí žádné výsledky, je paradoxně lidská chyba. Zákazníci totiž málokdy hledají produkty přesně podle názvu či popisu, pod kterým e-shop daný výrobek eviduje. Zejména nakupující bez znalosti cizích jazyků mají tendenci psát názvy zahraničních značek foneticky, a pokud si s tímto neumí vyhledávací nástroj poradit, logicky připravuje uživatele o možnost nakoupit. To samé platí s ohledem na překlepy, slangové výrazy, cizojazyčné pojmy nebo jednotné a množné číslo.

Naše zkušenost ukazuje, že u e-shopů, které nemají v tomto směru optimalizovaný vyhledávač, končí 10 až 20 procent požadavků bez výsledku. V některých případech to bylo dokonce až 40 procent, což představuje obrovský promarněný potenciál. Pokud se však obchody optimalizaci intenzivně věnují, obvykle toto číslo sníží na 1 až 5 procent. Z principu pravděpodobně nejde dosáhnout „dokonalého“ vyhledávání, které by vždy ukázalo správné výsledky. Může se například stát, že zákazník napíše příliš komplexní frázi, která systém navede mimo nabízené portoflio, nebo e-shop zkrátka zboží vůbec neprodává. Tento problém však lze mitigovat zahrnutím často poptávaného zboží do sortimentu, nebo k takovým poptávkám přiřadit podobné, alternativní produkty.

S podobnými problémy se potýkala například síť lékáren Benu, jejíž původní vyhledávač nedokázal zpracovat fráze o méně než třech znacích. Když tak zákazníci hledali třeba „D3“ vitamin, zboží ve výsledcích nenalezli, ačkoliv je e-shop v sortimentu měl. Nově e-shop zobrazuje výsledky už od zadání jediného znaku, s ohledem na historii nákupů či chování jiných uživatelů. Díky optimalizaci tak dokázal za jediný měsíc testovacího období navýšit konverze z vyhledávání o 9,49 procenta, což v případě byznysu s ročním obratem přes 6 miliard korun jen v Česku není malé číslo. Obdobně na tom je i jeden z největších českých internetových prodejců potravin Košík.cz, který obdobně zvýšil konverze z vyhledávání o 10,5 procenta. Navíc na něm i díky vylepšenému UX využívá funkci vyhledávání až 50 procent zákazníků, zatímco průměr segmentu potravin je kolem 24 procent.

Na délce záleží

Ač se to může zdát neuvěřitelné, přes 80 procent lidstva dnes podle serveru Statista.com vlastní chytrý mobilní telefon. Což znamená až 6,4 miliardy potenciálních zákazníků, kteří mohou nakoupit online. Aby však dokázaly e-shopy využít tohoto enormního zdroje, musejí se naučit pracovat s unikátním chováním, které lidé mají při nakupování online. S rozmachem hlasových asistentů totiž zákazníci používají stále častěji hlasové příkazy i při hledání zboží. Ani zdaleka si však nestačí poradit s převodem mluveného slova na text, vyhledávací nástroj jej také musí umět správně vyhodnotit a například ignorovat slova, která na nalezení produktu nemají vliv.

Pokud například zákazník zadá „černé chytré hodinky s měřením tepu“, měl by vyhledávač umět „pochopit“, co daná slova znamenají. Černou vyhodnotit jako barvu, chytré hodinky jako typ produktu a měření tepu coby jednu z vlastností. A podle toho zobrazit relevantní výsledky. Stejně tak by měl umět vyhodnotit třeba časově omezené akce či relevanci k místu, na němž se zákazník aktuálně nachází. Nebo dokázat zanedbat určitá příliš specifická slova a tím rozšířit potenciální sortiment, pakliže vyhledávání nenabídlo žádné výsledky.

S problematikou dlouhých dotazů se však setkáváme nejen při hlasovém vyhledávání, ale i v segmentu módy. Zatímco v jiných odvětvích zákazníci často používají produktové názvy či kódy (knihy, hry, nábytek, železářství a podobně), v případě oblečení se zadanou frází snaží vyjádřit svou představu. Navíc se stejně jako v kamenných obchodech i ve virtuálních regálech rádi „přehrabují“ a sortiment srovnávají. Podle serveru Statista v průměru zákazníci projdou až 32 stránek se zbožím, než si vyberou kýžený módní produkt – ve všech ostatních segmentech si však téměř 90 procent lidí vybírá pouze z první stránky výsledků.

I produkty míří vysoko

V módním segmentu zkrátka vyhledávač působí jako inspirace pro zákazníka s cílem nabídnout mu co nejvíce možností, z nichž si nakonec vybere jeden ideální produkt. V případě ostatních odvětví však platí, že kvalita předčí kvantitu. Nakupující obvykle mají tendenci kupovat spíše produkty umístěné výše ve výsledcích vyhledávání a na druhou stránku nalezených produktů přejde méně než 10 procent. Z našich zkušeností navíc vyplývá, že nezáleží na tom, jestli zákazníkovi nezobrazíte žádné výsledky, nebo mu ukážete ty, které nejsou relevantní. Pokud nakupující není s navrženým sortimentem spokojený, je přibližně 28procentní šance, že z e-shopu ihned odejde.

Jak tedy navýšit šanci, že zákazník na e-shopu nalezne to, co hledá, a současně redukovat pravděpodobnost jeho odchodu na minimum? Vedle optimalizovaného vyhledávání je jednou ze stěžejních funkcí internetových obchodů doporučování produktů. Takový nástroj by měl mimo jiné umět vzít do úvahy zboží, o které se uživatel zajímal v minulosti, a na jeho základě vyvodit priority zákazníka. Pokud například zjistí, že daná osoba již dříve nakoupila mobilní telefon určité značky, může mu při nákupu doporučit komplementární doplňky či jiné produkty od stejného výrobce, jako jsou ochranná pouzdra, nabíječky, kabely či třeba notebook s operačním systémem ze stejného ekosystému.

Díky strojovému učení však vyspělé nástroje dokážou hledat také souvislosti v rámci nákupního chování zákazníků, kteří s daným produktem interagovali. Pokud například vyhodnotí, že mnoho návštěvníků e-shopu často kupuje více specifických výrobků souběžně, může je nástroj do budoucna rovnou navrhovat společně. Zákazníkům tak ušetří drahocenný čas a navíc zvýší šanci, že si druhý produkt koupí i ti, kteří o něj doposud neprojevili zájem. Další možností je nabízet dražší či kvalitnější alternativy hledaného výrobku či souvisejících produktů v rámci up-sale. Vedle domovské či produktové stránky navíc přijde funkce doporučení produktů vhod třeba ve chvíli, kdy se zákazník dostane omylem na neexistující stránku. Tehdy mu e-shop může nabídnout určité výrobky a zvýšit tak šanci, že nakupující nalezne to, pro co do obchodu přišel.

Rada nad zlato

Poslední kritickou funkcí, kterou by měl každý opravdu efektivní vyhledávač zahrnovat, je takzvaný našeptávač. Ten zákazníkům dokáže zobrazovat návrhy produktů již od prvního zadaného písmene a s každým dalším blíže specifikovat sortiment, který návštěvník obchodu hledá. Pro customer experience má hned několik benefitů. Průběžně zákazníkovi potvrzuje, že hledá správně a že e-shop má požadované zboží v nabídce. Navíc dokáže nakupujícího ušetřit od zadávání celé fráze, či mu dokonce doplnit kontext dotazu – návštěvník totiž často zná pouze část názvu produktu, našeptávač jej tak dokáže efektivně obeznámit se širší nabídkou, která s hledaným heslem souvisí.

Ze zkušenosti rozhodně není našeptávač zanedbatelná funkce ani z pohledu uživatelů, v průměru na navržený produkt klikne 22,77 procenta z nich. Navíc mají produkty nabídnuté skrze našeptávač konverzní poměr 21,15 procenta, tedy dvakrát více než v případě nákupu bez použití této funkce (11,52 procenta). Zákazníci zkrátka při nákupu online chtějí svůj zamýšlený produkt najít co nejrychleji a rádi využijí všech možností, jak tento proces zefektivnit. Pokud tak e-shopy chtějí maximalizovat své zisky, měly by jim vytvořit ideální podmínky a udělat vše pro to, aby nakupující vždy našli přesně to, co hledají. ■

Gejza Nagy

Autor článku je CEO a spoluzakladatel slovenského startupu Luigi's Box.

Automatizace přináší efektivitu v každém odvětví – od vývoje až po kontaktní centra pro zákazníky

Dominika Šindlerová

Automatizace je v dnešní rychle rozvíjející se době jedním z fundamentálních vylepšení pro jakoukoliv firmu. Mohou do ní investovat společnosti v téměř jakémkoliv odvětví a očekávat výrazná zlepšení svého provozu. Nyní se trend automatizace díky technologiím jako je umělá inteligence nebo text-to-speech rychle rozšiřuje také v oblasti kontaktních center – ať už jde o velká call centra nebo menší týmy obchodníků. Zkrátka v jakémkoliv týmu lidí, kde velká část každodenní pracovní agendy spočívá v telefonátech.

Kontaktním centrům může automatizace přinést výrazné výhody, jako je zrychlení stávajících procesů, efektivnější využití času zaměstnanců, lepší koordinace telefonních agentů a dalších zaměstnanců. V neposlední řadě může také zvýšit spokojenost zaměstnanců, která se následně odráží na spokojenosti zákazníků, kterým telefonují. To všechno v konečném výsledku může významně přispět ke snížení nákladů na provoz kontaktního centra a zkvalitnění služeb pro zákazníky.

Zároveň je díky automatizaci snadnější získávat a zpracovávat nejrůznější data. Díky nim lze hlídat reálné vytížení agentů, naslouchat aktuálně probíhajícím hovorům a automaticky zpracovávaným nahrávkám, kontrolovat kvalitu hovorů a zpracovávat data v hovorech získaná. Pracovníci kontaktního centra tak dokáží lépe vytvářet vlastní plán hovorů a plánovat další kroky v komunikaci s konkrétními zákazníky. Co všechno lze tedy v kontaktních centrech automatizovat a jak s implementací automatizace vůbec začít?

Dobrý sluha, špatný pán – telefonní roboty na linky raději nepouštějte

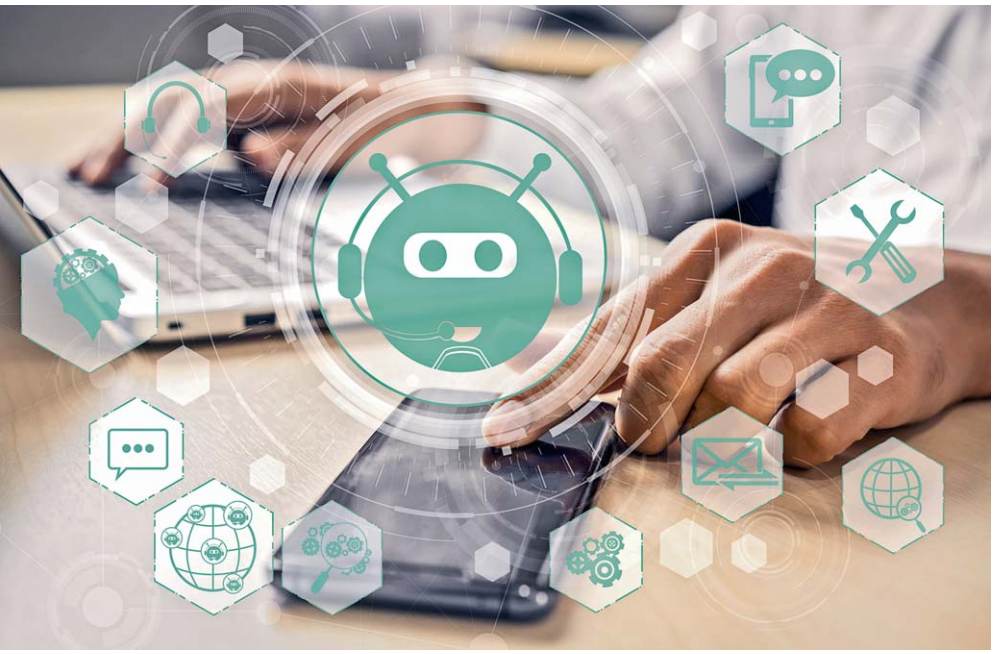
Automatizace procesů v kontaktních centrech může mít vícero podob. Vždy záleží zejména na druhu poskytovaných služeb a hlavně na tom, jakým způsobem si ta které společnost přeje komunikovat se svými zákazníky. Zaměření poskytovaných služeb vždy do značné míry určuje, jaké systémy jsou vhodné na přímou komunikaci se zákazníky, jak se budou stanovovat prognózy nebo jak je potřeba zpracovat získané informace.

Kontaktní centrum musí v první řadě disponovat nějakým komunikačním systémem, typicky hromadně spravovanou e-mailovou schránkou, online chaty nebo má přímo telefonní centrum. Tady už přichází první možnosti určité míry automatizace. Umělá inteligence zvládne obsluhu jednoduchých chatbotů, kteří jsou schopni poradit s některými základními problémy. Například kde najít nějaké informace o zboží a dopravě, v kolik jede tento spoj veřejné dopravy, za kolik je daný produkt atp. Automatizace může také usnadnit správu e-mailů, jejich třídění a návrhy odpovědí už dneska zvládne.

Automatizace telefonátů se na druhou stranu prozatím ukázala jako slepá ulička. Mnoho společností je automatizovat zkoušelo a nadále zkouší, ale často naráží na fakt, že dnešní úroveň technologií zkrátka ještě neumožňuje plně nahradit lidskou bytost. Často je tak nasazení telefonních automatů kontraproduktivní – buď něco akutního vyřešíte za pět minut s člověkem, nebo patnáct minut posloucháte robota a mačkáte čísla, než se k něčemu doberete.

Tento problém se odráží i ve statistikách – podle PwC dává 78 % zákazníků přednost řešení problému s živým člověkem. Podle stejné zprávy každý třetí zákazník už u společnosti znovu nenakoupí, pokud má špatný zážitek se zákaznickou podporou. Firmy tedy musí nové technologie aplikovat s rozmyslem a pouze tam, kde dávají význam – nevyplatí se tlačit novou technologii někam, kde zatím přinese více škody než užitku.

Automatizace a umělá inteligence tak v kontaktních centrech nachází uplatnění nikoliv jako náhrada telefonních agentů, nýbrž jako doplňkový nástroj, který pracovníkům center výrazně ulehčují práci. Ideální oblastí pro automatizaci kontaktních center je zpracování dat, která při telefonátu s klientem získají. Automatizace monotónních administrativních úkonů, jako je přepisování



hovoru do textu, identifikace klíčových údajů a jejich exportování do firemních nástrojů, může agentům ušetřit cenné minuty práce a dovoluje jim soustředit se na to podstatné – poskytování špičkové podpory zákazníkům.

Integrace s dalšími firemními systémy je klíčem k automatizaci kontaktních center

Jak konkrétně taková automatizace může vypadat, diktuje i v tomto případě obchodní zaměření dané společnosti. Můžeme se tak bavit o čemkoliv od přepisů hovorů a jejich lepšího plánování až po automatizovaný export syrových i předzpracovaných dat. Ať už spreadsheetů v tabulkových procesorech nebo do systémů pro správu vztahů se zákazníky (CRM systémy) nebo jiné specializované platformy např. na sales engagement.

Je tak velice důležité, aby komunikační software používaný k přímé komunikaci se zákazníky nabízel firmám co největší rozsah možných integrací se systémy třetích stran. Tímto způsobem se získané informace mohou dostat do všech systémů, se kterými společnost pracuje. Skrze integraci se informace v jednotlivých systémech synchronizují, doplňují se, umožňují je naplno využít. To vše okamžitě bez manuálního zadávání informací do každého systému zvlášť. Uživatel si samozřejmě může zvolit, jaký typ dat by se měl synchronizovat a za jakých podmínek.

Jak začít s implementací automatizace? Musíte vědět, čeho chcete dosáhnout

Automatizace se dá aplikovat v různých směrech, proto je důležité vědět, kde začít. V první řadě je podstatné si jasně nastavit, čeho chceme dosáhnout. A také jaké máme očekávání od zaměstnanců v souvislosti s jejich pracovním výkonem. Jakmile si společnost upřesní, jakého cíle by skrze automatizaci chtěla dosáhnout, může začít hledat řešení, které jí s tím pomůže.

Společnost by si měla nastavit jasné požadavky a parametry, které by daná technologie měla splňovat. Mezi ty může patřit například již zmiňovaná potřeba integrací se stávajícími systémy. Je zbytečné kvůli novému automatizovanému řešení vyměňovat stávající fungující systémy, jen abyste možná později zjistili, že se vám nové řešení nelíbí. Ideální je, aby se do určování těchto parametrů zapojili i sami zaměstnanci z kontaktního centra, kteří budou mít poznatky z každodenního provozu.

Dalším kritériem může být provoz technologie. Má běžet na interních serverech, nebo na cloudu, odkud je přístupný jednoduše odkudkoliv? Velký ohled by firmy měly brát i na bezpečnost používaných nástrojů – úniky dat se s rozšiřující digitalizací služeb dějí čím dál častěji a mohou mít na firmu velice negativní vliv. Proto je dobré zjistit, zda měl poskytovatel v minulosti problémy s bezpečností a jak je řešil.

Velkou úlohu pak samozřejmě hraje i rozpočet, který často rozhoduje, jakým směrem se zákazník vydá. Vzhledem k našim zkušenostem z praxe však můžeme s jistotou říci, že nemalé procento potenciálních zákazníků, kteří zvolili levnější alternativu před kvalitou, se po určité době přesto rozhodne pro nákladnější, ale spolehlivější řešení. Pozitivním trendem posledních let je přesun softwaru na tzv. SaaS model, kdy cloudová řešení bývají postavena na systému pravidelného předplatného. To výrazně eliminuje potřebu jednorázové vysoké investice náročné na cashflow a umožňuje větší flexibilitu.

Najít perfektní řešení může chvíli trvat, ale ve výsledku se vyplatí

Ne vždy se podaří najít hned na první dobrou řešení, které konkrétním požadavkům firmy bude vyhovovat nejlépe. Většina systémů dnes naštěstí zákazníkům nabízí testovací období. Během toho si mohou zákazníci vyzkoušet, jak se jim se systémem pracuje, jak dobře funguje a zda to pro ně bude ta správná volba. Je možné, že některé řešení s sebou přinese další nečekané výdaje, že nemá funkcionalitu, kterou předtím nepotřebovali nebo ji brali za samozřejmost. Nebo není kompatibilní s novým softwarem, který nasazují.

Ve výsledku se však využití určité míry automatizace vyplatí – proč by pracovníci měli ztrácet čas úkony, které počítač zvládne okamžitě? Je lepší poskytnout jim takové nástroje, které jim umožní dělat svou práci lépe a mít tak spokojenější zákazníky, i kdyby to mělo vyžadovat chvilku hledání toho nejlepšího řešení. ■

Dominika Šindlerová

Autorka článku působí na pozici Account Executive ve společnosti CloudTalk

E-shop budoucnosti zná svého zákazníka a umí se mu přizpůsobit

László Szabó

Spotřebitelé si v době pandemie rychle zvykli na online nakupování a vyšší podíl nákupů na internetu nezmizí ani po jejím odeznění. E-shopy však musí nejen udržet stávající zákazníky, ale přivést nové. Správně zvolená strategie digitálního marketingu je účinnou zbraní proti konkurenci. Klíčem pro obchodníky v e-commerce je znát potřeby a chování nakupujících. Věrné zákazníky navíc udrží jen e-shop, který má uživatele na prvním místě.

Nakupující, který je vhodně oslovován, e-shop s ním pracuje a nabízí mu produkt podle toho, jak se na webu pohybuje, bude více přemýšlet, zda jej také koupit. Trendem digitálního marketingu je zcela jistě personalizace, kdy se e-shop snaží poznat každého zákazníka individuálně a přizpůsobuje mu nabídku i komunikaci na míru.

Kdo včas zainventuje do digitálních nástrojů, jak pracovat s jednotlivými zákazníky, bude mít konkurenční výhodu. Moderní řešení, kterým personalizace je, dosáhne větších výsledků pomocí řešení využívající umělou inteligenci a algoritmy. Základem jsou uživatelská data a profilování nakupujícího. K zákazníkovi, který na webu nakupuje opakovaně, budeme přistupovat jinak než k tomu, který je u nás poprvé. A e-shop budoucnosti přesně ví, kdo je kdo, jakou má historii, pro koho je důležitá cena nebo jiný faktor. To můžeme rozeznat na základě signálů – z jakého klíčového slova na web přišel, na co kliknul na dané stránce, co naposledy hledal, co nakoupil. Bez toho, aby internetový obchodník znal předchozí aktivitu zákazníka, není schopen efektivně přizpůsobit nabídku.

Roli hraje chování zákazníka na webu. Jen tak obchodník identifikuje jednotlivé nakupující či skupiny, kteří se vyznačují určitým chováním a přizpůsobí tomu nabídku. Nesmí ale zapomínat na to, že návštěvníci webu jsou především lidé. Důležitým faktorem je také „behaviorální ekonomie", která doplňuje ekonomický aspekt o psychologii. Ne vždy se totiž rozhodujeme racionálně a logicky a to platí i při nákupu. Vliv na ekonomické chování tak mají naše zvyky, nálady či předsudky.

Přestože neexistuje žádné zlaté pravidlo, co přesně má e-shop udělat s jednotlivými skupinami, aby je přiměl k nákupu, lze to rozeznat právě na základě dat. Pokud už například víme, že skupina „bargain hunterů" reaguje na akce a slevy, můžeme na ně přesně zacílit. Jestliže u nich funguje nízká cena a sleva, minule například dobře reagovali na akce typu Black Friday, pak musíme i příště zajistit, aby o nás věděli. Zvolená strategie tak může zahrnovat oslovení personalizovaným e-mailem, remarketingem, PPC kampaněmi či sociálními sítěmi. K nové objednávce může nalákat sleva na míru, která zohlední preference zákazníka. Věrnostní programy zase udělají ze zákazníka věrného propagátora vašeho obchodu.

Správně nastavený e-shop, rychlost načítání, jednoduché navigování nebo pokročilý vyhledávač jsou důležitým faktorem pro pohodlný nákup, který zákazník očekává. Pokud navíc e-shop funguje na zahraničních trzích, musí znát nákupní zvyklosti v dané zemi a zde je svatým grálem lokalizace. Lokální standardy a porozumění potřebám místního trhu je základem úspěchu. Nákup v rodném jazyce je komfortnější pro zákazníky ve středoevropském regionu, s e-shopem v angličtině nepochodíte. U Čechů je v oblibě dobírka, v Maďarsku jsou citliví na chyby v překladu, Rumuni dělají objednávky po telefonu a na Slovensku se dvě třetiny nákupů uskuteční prostřednictvím chytrých telefonů. Uspějí pouze e-shopy, které porozumí potřebám a chování zákazníka. Jen tak si vybudují důvěru a zákazník se bude rád vracet. ■

László Szabó

Autor článku je spoluzakladatel a ředitel rozvoje digitální agentury Growww Digital, která spolupracuje s předními e-shopy na trzích střední a východní Evropy.

Středobodem vývoje retailu jsou technologie

Digitální transformace v maloobchodě již dříve způsobila revoluci ve všech částech procesu – od správy zásob, práce se zbožím, školení, až po marketing, zákaznickou podporu a věrnostní programy. Další metou digitalizace retailu je nabídnout zákazníkům, kteří nakupují zboží ve fyzických obchodech, výhody nakupování v online prostředí a naopak. Zkrátka nabídnout z obou světů to nejlepší pro zákaznický zážitek. Překlenout propast mezi oběma světy pomáhá automatizace.

Maloobchod byl vždy založen na důvěře, která se buduje příkladnou péčí o zákazníky a poskytováním výjimečné zákaznické zkušenosti. Zůstane to tak i nadále, ale způsoby a prostředky obsluhy zákazníků se během následující dekády výrazně změní. *„Středobodem změn jsou technologie. Nakupování budoucnosti bude zajímavější a pohodlnější, a to jak na dálku, tak v obchodech. Více transakcí než dnes bude probíhat přes mobilní zařízení a sociální sítě, přičemž fyzický a virtuální svět se budou díky omnichannel konceptu prolínat. Zákazníci se ve větší míře než dnes dokážou obsloužit sami, přičemž značky budou každého zákazníka perfektně znát, díky čemuž dokážou poskytnout personalizovanou zákaznickou zkušenost,* “ předpovídá Viktória Lukáčová Bracjunová ze společnosti Soitron.

Generální ředitel sítě elektroobchodů NAY Group, do které v Česku patří dceřiná společnost Electro World, Martin Ohradzanský si nadcházející vyvolané dramatické změny dobře uvědomuje. Když zhruba před deseti lety zasedl do ředitelského křesla, měl internetový prodej na celkových výnosech společnosti pouze několikaprocentní podíl. O dekádu později se podílel na celkových tržbách zhruba třetinou. *„V příštích letech se však toho v obchodě změní více než jen poměr oline a offline tržeb. Proto pokrok v digitalizaci a automatizaci je nedílnou součástí naší dlouhodobé strategie,* “ dodává Ohradzanský.

Mezi klíčové technologie pro rozvoj retailu aktuálně patří zejména automatizace procesů s využitím strojového učení a umělé inteligence. Jejich možnosti jsou velmi široké a retail ani průmysl se v jejich aplikaci ještě pořádně nerozjely. Obdobná příležitost se nachází v robotické automatizaci procesů (RPA). Ta umožňuje, aby vybrané činnosti – hlavně ty, při kterých je třeba neustále opakovaně provádět jistou posloupnost kroků na základě jasně definovaných pravidel – dělal namísto člověka softwarový robot.

Automatizace procesů umožňuje zlepšit zákaznické služby a zároveň odlehčit zaměstnance – v prvním kroku zejména ty, kteří pracují v back-office a na call centru. *„Při objednávkách v sezonních špičkách jsme stále častěji naráželi na kapacitní limity. Vykrývat je brigádníky bylo vždy náročné a při růstu prodeje přes internet hrozilo, že některé požadavky nedokážeme naplnit v dostatečně krátkých lhůtách,* “ poukazuje Martin Ohradzanský.

Má-li být společnost dlouhodobě konkurenceschopná a zisková, musí umět obsloužit se stávajícími zdroji více zákazníků – a zvládnout stále větší výkyvy v poptávce. K těm dochází nejen v sezonních špičkách, ale během pandemie i při náhlém zavádění opatření či z důvodu výpadku sortimentu v dodavatelském řetězci.

Proto v Electro Worldu došlo k automatizaci procesů pomocí RPA například při zpracování žádostí o zrušení objednávek. Agenti call centra jich vyřizovali i několik tisíc měsíčně. Při každém stornu se musí učinit několik kroků v různých systémech, například prověřit, zda již bylo zboží vydáno a zda bylo zaplaceno. *„Dnes tyto úkony za zaměstnance provádí automatizovaně robot a ti jsou díky tomu dostupnější pro řešení specifických dotazů či podnětů zákazníků,* “ uvádí Viktória Lukáčová Bracjunová.

Obdobně se v call centru elektrořetězce podařilo zautomatizovat proces vyřizování reklamací v prodloužené záruce, stejně jako vybrané administrativní procesy z oblasti financí a HR. *„Robotizaci plánujeme zavést všude tam, kde nám pomůže odlehčit lidi či zlepšit zákaznické služby, v ideálním případě obojí,* “ vysvětluje Martin Ohradzanský.

Jedním z hlavních cílů automatizace je i zvyšovat loajalitu zákazníků – ať už zkrácením čekání, lepším informováním nebo zavedením nových možností samoobsluhy. *„Kdysi jsme stáli v bankách kvůli každému platebnímu příkazu, dnes všechny transakce provádíme přes internetové bankovnictví. K podobné automatizaci směřuje i retail,* “ uzavírá Martin Ohradzanský. ■

Jak úspěšně vstoupit do světa e-commerce?

Otevření e-shopu je jen špičkou ledovce, firmu to změní od základů

Milan Frýbert

Vstup do světa e-commerce je dlouhodobý trend, ke kterému se nyní přidávají i konzervativní firmy. Ty se nejenže dosud v online prodeji nepohybovaly, ale ani o vstupu do tohoto segmentu neuvažovaly. Řadí se mezi ně například stavební společnosti, které dosud obchodovaly zpravidla přes síť velkoodběratelů, nyní se však rozhodly vstoupit do digitalizace naplno. V praxi to znamená nejen vybudování e-shopu, aby mohly prodávat na přímo, ale zároveň staví i B2B portály pro stávající zákazníky.

Digitalizace těchto firem však neznamená pouze definování a zavedení požadovaného IT řešení, ale často s sebou přináší i změny v procesech firmy. Ty mají dopad například na fungování skladů, expedici zásilek, ale i na způsob práce řadových zaměstnanců. Takové komplexní změny jsou náročné na zavedení a je úkolem dodavatele, respektive IT firmy, aby zákazníka cestou digitalizace provedla.

Pro přechod do onlinu je nejprve třeba změna myšlení ve firmě

Konzervativní firmy, které se rozhodly prodávat online, často mají jen matnou představu o tom, co provoz e-shopu obnáší. Proto je u nich třeba změnit myšlení – neboť internetový prodej je velmi rozdílný od offline prodeje. Nejvíce se to projevuje u samotného zadání, protože neznají běžnou praxi v e-commerce a nedokážou tak ani vysvětlit své požadavky. Očekávají proto pomoc od dodavatele, který tudíž musí mít potřebné know-how.

Prvním krokem pro nastartování spolupráce je sladění očekávání. Problém je často už se stanovením základních cílů, protože neexistují historická data. Klient tak může mít dokonce velmi futuristické myšlenky – například četl o chatbotech s pokročilou umělou inteligencí nebo o prohlížení zboží ve virtuální realitě. Není však třeba mu tyto vize hned od počátku rozmlouvat. Většinou na to dojde až při počítání nákladů, přínosů řešení a jeho návratnosti.

Ideální je klientovi popsat proces fungování e-shopu, co ovlivňuje prodej a jaké se pro to používají nástroje. Sníží se vratky? Budou lepší prodeje? Zkrátí se zákaznická cesta? Zvýší se konverze o 3 %? Jednoduše pokud požadavek přinese byznys, není důvod říkat ne. Naopak doporučujeme držet se osvědčených postupů a nesnažit se zdímat zákazníka za každou cenu. Zatímco velcí hráči si mohou takové experimenty dovolit, pro menší firmu to může být likvidační.

Prvotní dodávka připomíná průzkum bojem

Doporučovanou cestou pro firmy, které budují e-shop jako nový prodejní kanál, je jít formou MVP (minimum viable product, tedy základní životaschopný produkt). A stanovit si klíčové cíle, které musí e-shop splňovat, a tyto cíle doručit nejdříve. Nad dodávkou obvykle bdí projektový manažer, jenž nasazování dalších funkcionalit projednává se zákazníkem a postupně zjišťuje, kdo všechno bude systém využívat. Se všemi uživateli se pak musí bavit a získávat zpětnou vazbu, která je pro další rozšiřování systému klíčová. Díky tomu je možné investovat pouze do funkcí, které budou zákazníci opravdu používat.

Je třeba mít na paměti, že vybudování nového systému může ovlivnit způsob fungování firmy. Vybudovat e-shop ke kamennému obchodu, nebo dokonce k celé síti poboček často vyžaduje změny ve skladu či v nákupním oddělení. Mít zboží v centrálním skladu nutně neznamená, že je dostupné i v pobočce (což zákazník nemusí vědět). Jindy může být sklad, třeba i částečně automatizovaný, nastavený na celé palety se zabaleným materiálem, ze kterých ale může být problém oddělit potřebnou část pro menší objednávku. U obchodního oddělení zase mohou nastat potíže s rozličnými zvyklostmi B2B a B2C zákazníků, a to nejen v objemech, ale i v predikovatelnosti a požadavcích na rychlost expedice zboží. Při budování e-shopu jako nového prodejního kanálu je tedy třeba začít od základů.

Řádně zmapujte firemní procesy

Při nasazování nového e-commerce řešení se setkáváme se dvěma rozšířenými mýty. Prvním z nich je, že se celá firma najednou zastaví a management přetlumočí nové procesy

zaměstnancům. Ve skutečnosti se revoluce nekoná, ale vše probíhá za běžného chodu. Dodavatelská IT firma, respektive projektový manažer se průběžně baví se zaměstnanci, procesy zmapuje a zpracuje analýzu. Někdy narazí na vůli a ochotu zaměstnanců změnit zažité návyky, někdy se musí angažovat vedení – prakticky vždy ale lze najít společnou řeč a vysvětlit přínos zavedených změn.

Druhým zažitým mýtem je časová náročnost. Zpracování analýzy může trvat od dvou týdnů po několik měsíců. Zavedení řešení pak bývá relativně jednoduché, může se jednat třeba o čtrnáctidenní testovací období. Nejde však o žádné „školení“, zavedené změny musí být pochopitelné hned a mít viditelný přínos, jinak ztrácí smysl. Na jejich sledování a vyhodnocení pak obvykle stačí měsíc. Na tom se již může podílet zákazník, je však třeba jasně definovat, kde končí role dodavatele.

Jak změřit výsledek, když data chybí?

Firmy, které digitalizují ve stavu „tužka a papír“, nemají k dispozici historická data. To je pro vyhodnocování přínosů nového e-shopu velký hendikep, ale lze ho překonat. Cílem nemusí být jenom samotné zvýšení obratu, ale například zvýšení marže u prodávaných produktů díky vynechání mezičlánků v dodavatelském řetězci. U stavebních materiálů může být rozdíl třeba o 15 %, zatímco u elektroniky nebývá moc z čeho brát – za úspěch lze brát navýšení o 3 %. U módy jsou zase typicky vysoké marže, a to zejména kvůli vratkám. Cílem tak může být zvýšení marží o desítky procent.

Mezi další metriky může patřit doba trvání od expedice po doručení zákazníkovi, nebo lépe od zanesení do systému po doručení zákazníkovi. Rovněž lze spočítat optimalizaci interních procesů, například o kolik procent se zefektivnil (urychlil) daný proces v poměru k vynaloženým nákladům. Ve finále se všechny změny dají přepočítat na peníze – byznysový přínos je pro firmu vždy na prvním místě a na to by měl brát ohled i dodavatel nového e-commerce řešení.

Reporty dodejte všem klíčovým lidem

Firma, která buduje e-shop jako nový prodejní kanál, by měla měřit především jeho kvalitu. To jsou již zmiňované náklady versus obrat, až poté je namístě zaměřit se na jednotlivé základní metriky, které by měl v základu obsahovat a sledovat každý kvalitní e-shop – konverze, počet objednávek, případně množství vratek. Na jejich základě je pak možné vytvářet personalizované reporty a ty dodat klíčovým lidem. Pro každou pozici se jich může definovat celá sada obsahující informace, které daného zaměstnance zajímají.

Příchod nových firem do světa e-commerce je trend, který bude ještě nějaký čas pokračovat. Největší hráči na jednu stranu vyhodnocují big data k lepšímu poznání svých zákazníků a zkouší neustále nové technologie, na druhou stranu vstup do onlinu pro konzervativnější firmy nikdy nebyl jednodušší. Více než kdy dříve tak platí, že o byznys přichází ti, kteří dosud stojí stranou. ■

Milan Frýbert
Autor článku je vedoucím oddělení e-commerce společnosti BOOTIQ, člena skupiny BiQ Group.

Moderní plánování obsluhy přepravních kapacit v logistickém provozu

ti:me SLOT CONTROL

Jaký je ideální stav při realizaci přepravy zboží? Všechny osoby zapojené do realizace přepravy mají veškeré potřebné informace o nakládce, místu určení a času kdy bude řidič obsloužen na příjmu, či expedici, případná zpoždění nebo dřívější příjezdy jsou komunikovány s dostatečným předstihem. Příjem a expedice dokáže naprosto transparentně plánovat rutinní činnosti spojené s manipulací, vychystáváním a příjmem zboží za pomocí online nástrojů, který dává všem zúčastněným přehled v reálném čase.

Vypořádat se s narůstajícími požadavky zákazníků je jedním z hlavních úkolů logistických manažerů. Velkým přínosem jsou nové technologie pomáhající organizovat a automatizovat logistické procesy. S nasazením inovativních software a hardware řešení jsou mimo přínosů spojené výzvy, které je třeba přesně definovat a správně zareagovat.

Je nové řešení vybudované na dostatečně inovativní architektuře? Jak náročná bude údržba systému? Jsou standardizované možnosti napojení na stávající software firemní infrastrukturu a další Hardware prvky? Kolik času nám zabere samotná realizace a spuštění takového řešení? V jakých částech procesního zpracování přináší nové řešení výhody a úspory, jakého jsou typu a v jaké výši? Vzniknou nasazením nového systému výdaje dalším účastníkům zapojeným do procesu rezervace časových oken?

Unikátní aplikace Time Slot Control je připravena pro okamžité nasazení do firemních procesů za účelem automatizovat a digitalizovat činnosti spojené s plánováním a organizací příjmu a expedice. Na principu plánování časových oken jsou do procesu zapojeni jak pracovníci příslušných oddělení, kde manipulace se zbožím, či surovinami probíhá, tak i přepravci organizující pohyb vozidel mezi nakládkou a vykládkou.

Mezi výhody použití aplikace Time Slot Control patří vysoká míra digitalizace a s tím spojená možnost automatizovat rutinní činnosti. Transparentní proces rezervace časového okna pro obsluhu vozu. Vysoká míra informovanosti v reálném čase. Snadná obsluha a plánování pomocí uživatelských rolí a přístupů všech zúčastněných osob jsou jen základním výčtem přínosů využití aplikace. Další přínosy lze najít n nasazení ucelené Yard Management systému. Řešení přináší výhody v podobě předávání informací v reálném čase, transparentního plánování a snížení nákladů na obsluhu přepravních kapacit. ■

Jaké jsou trendy ve vývoji CRM?

Hlavní roli hrají flexibilita, automatizace a dostupnost dat

Michal Smetana

Prakticky žádné obchodní oddělení se v současnosti neobejde bez kvalitního CRM – systému pro řízení vztahů se zákazníky. V první řadě pomáhá plánovat strategické obchodní i marketingové aktivity, sledovat konkurenci nebo zvyšovat profitabilitu. Moderní CRM je zkrátka inteligentní platforma, která umožňuje dělat efektivní byznysová rozhodnutí založená na datech. Dávno však již není doménou velkých korporací, ale poslouží i malým týmům, a to nejen obchodním. Pomáhá tak jednotlivým odděleními napříč firmou maximalizovat efektivitu.

Podmínky na trhu se však neustále mění, čemuž se musí přizpůsobit nejen obchodníci, ale i vývojáři softwaru, kteří jim pomáhají dosáhnout stanovených cílů – v případě CRM poznání zákazníků a budování vztahů. Z pohledu vývoje to znamená především sledovat zpětnou vazbu uživatelů, držet krok s aktuálními trendy a řešit problémy, se kterými se tito uživatelé reálně potýkají. Dobré CRM tak musí plnit řadu požadavků firem, od nástrojů pro získání kvalitních leadů (tedy potenciálních zákazníků) až po zákaznickou podporu. O to složitější je pro vývojáře kvalifikovaně rozhodnout, kterým směrem platformu rozvíjet, které funkcionality dodat skrze vlastní řešení, nebo zda integrovat služby třetích stran.

Kdo jsou dnešní uživatelé CRM?

Uživatelé CRM jsou v dnešní době nejen obchodníci, ale i specialisté z dalších oddělení. Především jde o lidi z obchodních týmů, stále více ale systém začínají používat i marketingoví specialisté, projektoví manažeři, lidé ze zákaznické podpory či z administrativy. Je třeba mít na paměti, že nároky firem se mění a dobré CRM by se jim mělo přizpůsobit. A to na základě výzkumu a dat – všechna byznysová rozhodnutí by zkrátka měla být založená na realitě, nikoli na pocitu.

Například jedním z velkých trendů, ke kterému upírají vývojáři CRM pozornost, je zákaznická podpora. Toto oddělení umožňuje firmě být zákazníkovi po ruce, když potřebuje podat pomocnou ruku, ale zároveň je to nezbytný zdroj zpětné vazby na její produkt. Dobrý poskytovatel CRM by měl brát zákaznickou podporu jako velmi důležitou část vývojového procesu a zkoumat, jaké jsou nejčastější či největší problémy uživatelů. Zároveň sami vývojáři by si měli zákaznickou podporu vyzkoušet v rámci onboardingového procesu, aby problematice lépe porozuměli.

Produktový manažer na rozcestí

Produktový manažer často stojí před těžkým rozhodnutím, kterým směrem platformu rozvíjet. Důležité je pro něj sledovat aktuální trendy a problémy, jež firmy řeší. Nejpalčivější témata, která tu byla před rokem, dávno nemusí být aktuální. Je tedy nutné držet krok jak s konkurencí, tak i s požadavky zákazníků a cílových uživatelů. A naprosto stěžejní je vždy zpětná vazba od reálných uživatelů. CRM by jim mělo práci především usnadňovat, nikoli sloužit vedení firmy jako pomyslný bič na zaměstnance, aby výsledná čísla vypadala hezky v reportingu.

Je přitom namístě zdůraznit, co znamenají ony reálné potřeby zákazníků a uživatelů. Často se stává, že si zákazník vyžádá konkrétní funkcionalitu produktu. To však ještě neznamená, že ji reálně potřebuje, nebo že jde o to nejlepší řešení. Je proto důležité se uživatelů vždy ptát na daný problém, který chtějí touto funkcionalitou vyřešit. Zejména pokud by její vývoj trval měsíce, ale ve finále by vše šlo vyřešit mnohem jednodušším způsobem.

Vztahy firem se zákazníky se mění, proto je třeba udržet si flexibilitu

V rámci analýzy zákaznického chování je důležité vždy sledovat veškeré uživatelské pohyby v rámci produktu, sledovat data, vyvozovat z nich závěry a být schopný na základě těchto dat rychle inovovat. Problém může být například někde v nastavení produktu, kdy uživatel neví, jak pokračovat dál. Pokud bychom tato data nesledovali a nevyhodnocovali, nikdy bychom se o tomto problému nemuseli dozvědět. Výsledkem by byl frustrovaný uživatel, protože by nebyl schopen dosáhnout svého cíle.

A jak se těmto změnám může přizpůsobit velká firma či startup? Pro udržení flexibility je důležité mít dobře nastavené týmy a vývojový proces tak, aby byla firma schopna rychle reagovat na aktuální trendy. V první řadě je třeba mít dedikované týmy, které jsou zodpovědné za určité části produktu – díky tomu mohou být opravdovými experty v dané oblasti a rychle a kvalifikovaně se rozhodovat. Zároveň je nesmírně důležité, aby firma investovala do inovací a vývoje kompletně nových řešení v oblastech, kam směřují aktuální trendy, a ujistila se tak, že dokáže nabídnout nástroje, které řeší problémy moderní doby.

Mezi hlavní trendy patří automatizace a dostupnost dat na jednom místě

Ve světě CRM rezonují poslední dobou dva jasné trendy: automatizace a dostupnost dat na jednom místě. Vše se podřizuje maximální efektivitě, automatizace šetří čas tím, že zbavuje obchodníky repetitivních činností. Umožňuje například rychlejší hledání kvalifikovaných obchodních příležitostí (leadů), případně uzavírání nových kontraktů. Neméně důležitá je i automatizace workflow – systém by měl obchodníkovi umožnit podívat se na způsob jeho práce a sám mu navrhnout zefektivnění pracovního procesu.

Dále je to dostupnost dat na jednom místě – CRM už dávno není jen nástroj pro obchodní oddělení. Lidé napříč firmou potřebují mít kontext. Například které webové stránky uživatel navštívil, jaké marketingové e-maily si přečetl, na co se ptal zákaznické podpory či jaké problémy aktuálně řeší ve svém odvětví. To jsou nedocenitelné informace, které mohou znamenat udržení, nebo ztrátu zákazníka. Konsolidace dat rovněž umožňuje snadné vytváření reportů. Mezi významné technologie pak ještě patří používání integrací s důležitými nástroji k pokrytí kompletního prodejního cyklu, případně integrace se sociálními sítěmi.

Adopce CRM by měla být otázkou nejvýše dnů

Snadné osvojení CRM je jedním ze základních kritérií úspěchu. Zabrat by mělo několik hodin, nebo maximálně dnů, podle velikosti firmy. Rozhodně by však nemělo jít o zdlouhavý proces, naopak by se v něm měl obchodní tým rychle zabydlet. Prim by měla při prvním osahání CRM hrát jednoduchost, tedy dobré UX/UI.

Opět je třeba zdůraznit podporu, která případně provede uživatele základním nastavením, nebo vyřeší jeho problémy. Pro vývojáře navíc neexistuje lepší zpětná vazba, než si o využívání systému popovídat se skutečnými uživateli, kteří jsou v jeho využívání mnohdy až nečekaně kreativní. Jen tak lze zjistit, co je limituje, které funkcionality jsou pro ně zbytečné a které naopak nestačí jejich požadavkům.

Z pohledu vývoje je pak důležitou stránkou ještě bezpečnost a ochrana zákaznických dat, které by měly být vždy na prvním místě. A firmy by k ní měly přistupovat jako k jednomu z hlavních kritérií při výběru nového CRM. Obsahuje totiž veškerá důvěrná byznysová data, je tak nesmírně důležité, aby dobré CRM splňovalo všechny důležité certifikace (například SOC 2, SOC 3, US-EU Privacy Shield nebo ISO/IEC 27001:2013).

Velký potenciál pro CRM platformy leží u menších firem

CRM platformy si za svou existenci prošly poměrně dynamickým vývojem, od prvotního nástroje pro správu leadů se některé z nich rozšířily v masivní platformy, nebo na trhu vznikla naopak řešení pro malé firmy a obchodní týmy. Právě u malého a středního byznysu leží velký potenciál, neboť nemalá část těchto zákazníků ještě neprošla plnou digitalizací. Není vzácností, že taková menší firma využívá nějaké CRM řešení, ale velkou část kontaktů a administrativy drží stále v tabulkách.

Vývojáři, respektive produktoví manažeři tak stojí před velkým úkolem, jak pokrýt celou šíři požadavků svých zákazníků a jakým směrem svou platformu rozvíjet. A to jak z hlediska šíře funkcionalit, tak z hlediska využití pokročilých technologií. To klade na vývojáře, respektive na produktové manažery vysoké nároky na poznání trhu i zákazníků. Jedině na základě dat výzkumu trhu tak lze udělat kvalifikovaná rozhodnutí, jakým směrem se ubírat. ■

Michal Smetana

Autor článku je vedoucím české pobočky startupu Pipedrive.

Moderní řízení skladu – krok za krokem

Radoslav Revenda

V posledních letech se změnilo nejen prostředí, ale také chování zákazníků. Většina prodeje zboží a služeb se přemístila na internet. Dochází k rozvoji e-shopů, digitalizaci nabídky a obchodu, zvýšení poptávky – to vše má dopad také na skladovou logistiku.

Podle posledních statistik je v České republice více jak 50 tisíc e-shopů a trend je stále rostoucí. Také v oblasti velkoobchodu dochází ke sbližování potřeb s maloobchodním prodejem. V konkurenčním prostředí je čím dál více důležitá rychlost a flexibilita, sklad a logistika proto musí pružně reagovat na tyto potřeby.

Typy skladů a jejich potřeby

Abychom mohli správně navrhnout moderní sklad, je potřeba si odpovědět na pár otázek. Jaké bude využití skladu? Jaký budeme mít typ skladovaného sortimentu, objemy skladových položek, rozsah a kvalitu služeb? Tyto a spousta dalších otázek nám dají vodítka pro samotnou realizaci. Například spediční sklad se zásilkami bude mít jiné parametry a potřeby než výrobní sklad, který zajišťuje průběžné zásobování do výrobní linky. Dále je potřeba se podívat do budoucnosti a mít alespoň hrubou predikci, ideálně s horizontem 3–5 let.

Měřitelné parametry pro moderní sklad

Ať už se rozhodujete pro nové, nebo pro úpravu stávajícího řešení skladu, vždy si ověřte jeho aktuální stav a ujasněte, jaké máte očekávání na realizaci změn. To vám pomůže s představou o nákladech a přínosech řešení.

Mezi parametry, na které je vhodné se zaměřit, patří:

- počet skladových položek
- objem jednotlivých skladových položek (obrátka zásob)
- počet a objem příjmů
- průměrný počet položek v příjmu
- počet objednávek
- počet vratek
- definice logistických služeb a jejich kvalita

Abychom v čase dokázali vyhodnotit, jak se naplnily naše představy, pomáhá vytvořit si také ukazatele, díky kterým vidíme, k jakému zlepšení došlo a porovnávat stav před a po změnách (viz tab. 1).

Pohled do budoucna

Pro správné fungování moderního skladu bude potřeba řídit logistické činnosti s využitím nových moderních technologií. Mám na mysli logistický systém WMS (Warehouse Management System), automatizované linky, výtahové systémy či autonomní vozíky. S podporou automatizace totiž dokážete lépe plánovat, vykrývat špičky a být méně závislý na lidských zdrojích.

S rostoucí poptávkou po logistických službách samozřejmě vznikají také nové fulfillment firmy, které dokážou nabídnout kvalitní a spolehlivé služby.

Logistika ve skladě často navazuje na obchodní a nákupní procesy ve firmách a je součástí řízení dodavatelského řetězce (Supply chain management – SCM). Proto je neméně důležité, aby se potřeby obchodních a nákupních týmů zohlednily v návrhu řízení skladu. Zároveň roste poptávka po dynamických simulacích, které dokážou odhadnout, jaké budou limity logistických operací na skladě.

Praktická doporučení při realizaci projektu WMS

Jako dodavatel softwarových řešení, zejména pak adresovaného skladu, doporučujeme při řízení změny postupovat jako u běžného projektu. Tedy jak jsem již zmiňoval, udělejte si analýzu aktuálního stavu, sepište si očekávání, podívejte se do budoucnosti a odhadněte výše zmíněné parametry, vytvořte si zadání a cíle změn. U větších projektů doporučujeme se obrátit na logistické poradenské firmy, rádi vám pomohou se zadáním či realizují audit, případně s vámi vytvoří dynamickou simulaci budoucího skladu. To vám pomůže vybrat vhodného dodavatele technologií.

Můžete se samozřejmě obrátit také na nás, rádi vám poradíme a pomůžeme najít nejefektivnější řešení pro řízení vašeho skladu. ■

Tab. 1: Příklad ukazatelů, díky kterým vidíme, jak sklad funguje a k jakému zlepšení došlo. Můžeme na nich porovnávat stav před a po modernizaci.

Ukazatel	Jednotka
Zvýšení počtu příjmových položek	Pracovník/hodina
Zvýšení počtu expedovaných položek	Pracovník/hodina
Chybovost – plnění SLA chybových položek	Reklamované chybové položky / expedované položky
Zvýšení objemu skladových zásob	Počet skladových pozic / m^2
Snížení inventárního rozdílu	Částka rozdílu (manko + přebytek) / částka celkového objemu skladových zásob
Rychlost naskladnění příjmové položky s navázanou objednávkou až k expedici	Průměrný čas od možného příjmu až po expedici (hodiny)
Podpora legislativy pro nebezpečné látky (ADR)	Zavedení legislativy

Ing. Radoslav Revenda

Autor článku je komerčním ředitelem společnosti E LINKX, a. s.

Už máme e-shop, poptávky rostou, **ale sklad nestíhá?**

Řada nových zákazníků prochází podobným scénářem, zvláště v dnešním digitálním světě. Na místě je proto zvážení moderního logistického řešení, jako je adresovaný sklad, automatizace linky, napojení na dopravce, aplikace pro vlastní přepravu apod. Naše společnost E LINKX je již dlouholetým dodavatelem skladového a logistického řešení pro velké distribuční hráče na trhu.

Nabízíme řešení pro řízení skladu, které zahrnuje evidenci zboží pomocí čtečky čárového kódu, velkou škálu logistických operací, elektronickou komunikaci s přepravci, tisk obchodních dokladů (dodací listy, faktury), produktových štítků a štítků pro přepravce, inventuru celého skladu nebo jeho vybraných částí a řadu dalších funkčností.

Díky vývoji nové vývojové platformy Element jsme schopni nabídnout také doplňková řešení nebo řešení na míru. Jedním z nich je aplikace Sonar, sloužící k řízení vlastní přepravy zboží. Produkt je postaven na principu mikroslužeb (microservices), které lze vzájemně propojit a pokrývají základní logistické funkce. Samotný Element umožňuje poměrně rychlý vývoj aplikací za nižší pořizovací náklady, poskytuje vysokou bezpečnost a dynamiku, self-repair princip, uživatelsky přívětivé webové prostředí a snadnou integraci. ■

Více informací najdete na webu:
www.elinkx.cz

ELINKX

ELINKX

AUTOMATICKÉ ODESÍLÁNÍ ŠTÍTKŮ NA DOPRAVCE

www.elinkx.cz

ERP systém **Esyco Business**

Budoucnost business intelligence

je v propojení kompozitní analytiky a headless BI

-GoodData-

Poskytnout zaměstnancům a zákazníkům přístup ke srozumitelným a konzistentním datům bez ohledu na jejich technické vzdělání – to je hlavní výzva a zároveň trend v oblasti datové analytiky. Pomoci s tím má nový přístup k práci s firemními daty – tzv. composable data and analytics – který s daty a analytikou pracuje jako stavebnice s kostkami. Zároveň zajišťuje potřebnou konzistenci a dostupnost dat.

Tyto závěry vyplývají z průzkumu společnosti GoodData, který realizovala ve spolupráci se společností Puls, jež je součástí skupiny Gartner. Průzkum zjišťoval, jaké potřeby a priority v oblasti datové analytiky má v letošním roce 200 vrcholových manažerů ze středních a velkých firem působících po celém světě.

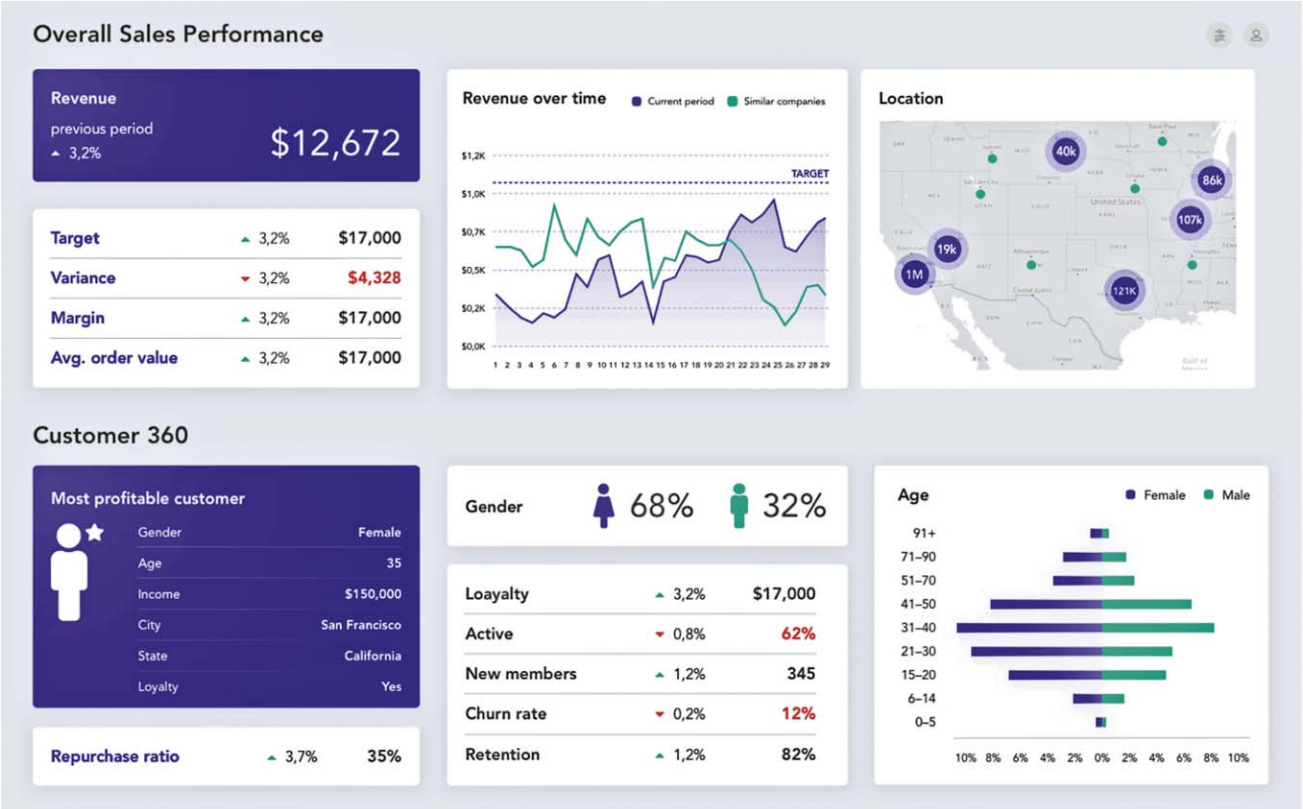
Popisované trendy úzce souvisí s „demokratizací dat“, tedy snahou firem odstraňovat překážky, které brání přístupu k datům a jejich interpretaci v reálném čase. Z průzkumu vyplývá, že ve firmách bude s analytikou pracovat stále více lidí. Budou vznikat multifunkční týmy, které se zaměří na zlepšení analytických dovedností, správu a kvalitu dat.

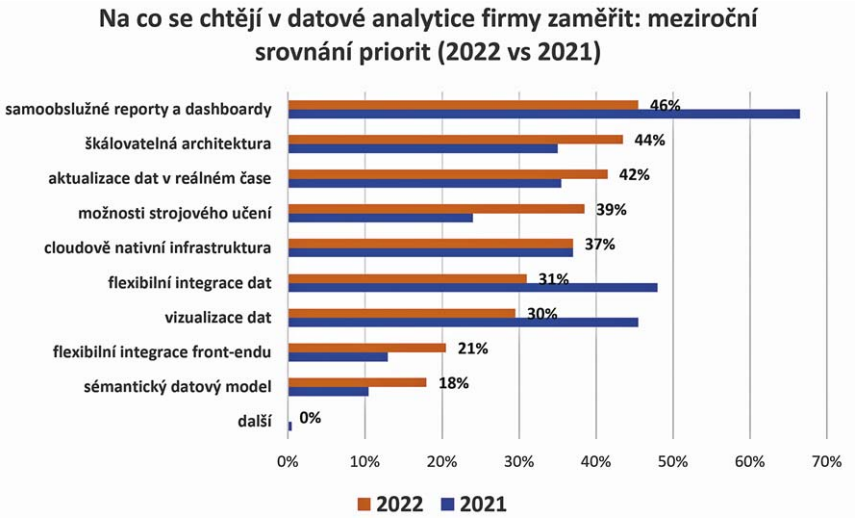
Analytika se postupně přesune do cloudu, a to kvůli uspokojení vyšších nároků na zpracovávaný objem dat a poskytnutí pokročilých funkcí. Podniky také budou hledat rovnováhu mezi flexibilitou a správou svých dat. Díky kompozitní analytice nakonec získají obojí.

„Firmy nejčastěji řeší, jestli potřebné řešení vybudovat interně či si jej zakoupit. Podle našich zkušeností je to spíše otázka vyvažování obou možností než preferování jednoho přístupu před druhým,“ říká Karel Novák, ředitel Professional Services společnosti GoodData (obr. 1).

V budoucnu se také změní distribuce práce mezi IT oddělením a běžnými firemními uživateli. „IT by se mělo zaměřit pouze na správu dat, tedy tvorbu konzistentních pravidel, rozvoj datových aktiv, zajištění rychlé odezvy a zpracování dat v reálném čase. Firemní uživatelé tím získají svobodu inovovat pomocí analytických nástrojů bez použití složitého programování. Z tohoto nového prostředí budou nakonec těžit všichni,“ shrnuje trendy datové analýzy Roman Staněk, generální ředitel společnosti GoodData.

Obr. 1: Ukázka vizualizace samoobslužných reportů a dashboardů.





Obr. 2: Priority firem v oblasti analýzy dat.

Obr. 3: Kdo se ve firmách stará o analýzu dat?

Datová gramotnost či demokratizace dat jsou často skloňovanými pojmy posledních let. Nyní se stávají realitou. Vyplývá to z pořadí priorit dotazovaných společností. Patrná je snaha datovou analytiku zpřístupnit všem zájemcům, tedy i těm netechnicky zaměřeným. Mezi hlavní priority respondentů pro letošní rok patří poskytování samoobslužných reportů a dashboardů (45,5 %), vybudování nebo pořízení škálovatelné datové architektury (43,5 %) a dosažení aktualizace dat v reálném čase (41,5 %) viz obr. 2.

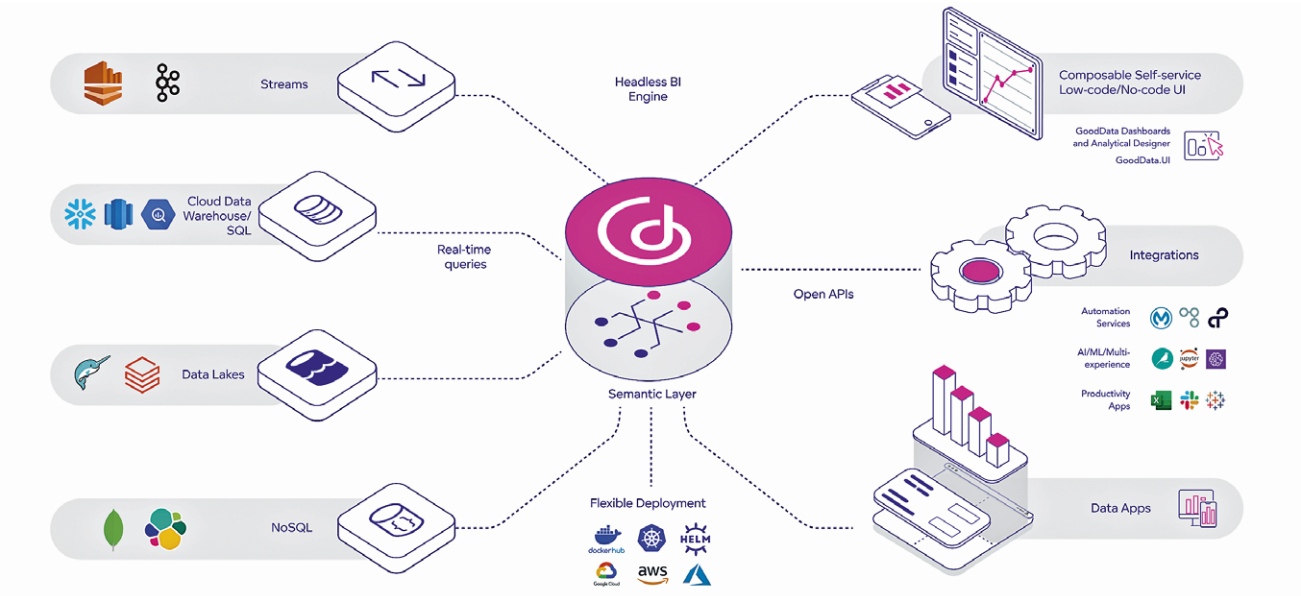
Základním problémem demokratizace dat je zachování jejich konzistence – jak mít jediný správný zdroj pravdy pro celou organizaci. Firmy, které to zvládnou, získají obrovskou konkurenční výhodu. „Díky tomu, že jsme umožnili lidem v mém týmu, kteří nejsou vývojáři či inženýři, manipulovat s daty, přidávat je, vytvářet další dashboardy, můžeme nyní výrazně rychleji reagovat na potřeby zákazníků," říká Bernadette Noone, viceprezidentka společnosti Technomic, která poskytuje služby v oblasti potravinářství (obr. 3).

Zpřístupnění dat často brání nesoulad v komunikaci mezi technologicky orientovanými IT odborníky a zbytkem společnosti. Potřební odborníci jsou totiž obvykle členy IT oddělení (38 %) nebo oddělení analýzy dat (37 %). Toto tradiční rozdělení, kdy technologové pracují bez zpětné vazby od „netechnických" kolegů, vytváří řadu bariér a může vést k přetížení zdrojů. Získané výstupy mohou být navíc pro uživatele nesrozumitelné. Spolupráce na vytváření, definování a označování metrik je pro přijetí analytiky zásadní.

Se sblížením světa analytiků a běžných uživatelů pomáhá nový přístup: kompozitní datová analytika (tj. datová analytika se stavebnicovou strukturou, kterou lze skládat podobně jako kostky), jež je propojena s otevřenou formou business intelligence, tzv. headless BI. Headless BI zajistí, že všichni koncoví uživatelé budou pracovat s jednotnými daty, a přitom poskytne každému přesně to, co potřebuje, díky jedinému zdroji metrik a sdílenému sémantickému modelu. Všechny analytické výstupy tak pracují se stejnými výpočty a datovými sadami.

„Kompozitní analytika a tzv. headless BI se liší od tradičních řešení business intelligence (BI), protože spravuje základní infrastrukturu způsobem, který umožňuje oddělit výpočet od vizualizace," vysvětluje Karel Novák. Oddělením těchto dvou mechanismů mohou týmy IT a analytiků udržovat firemní data zabezpečená a konzistentní. Obchodně orientované týmy přitom mohou samostatně integrovat vybrané nástroje a získávat potřebné informace uživatelsky přívětivým způsobem (viz. obr. 4). ■

Obr. 4: Kompozitní analytika a tzv. headless BI umožňují oddělit výpočet od vizualizace. Všichni uživatelé pracují s jednotnými daty, a přitom mohou samostatně integrovat vybrané nástroje a získávat potřebné informace uživatelsky přívětivým způsobem.



Dodavatelé IT řešení pro logistiku (únor 2022) zkrácená verze				
Jméno společnosti	ABIS Czech, a.s.	AIMTEC a. s.	Algotech, a.s.	Allium, s.r.o.
Web	www.abis.cz	www.aimtecglobal.com	www.algotech.cz	www.allium.cz
Rok založení společnosti v ČR	2004	1996	1997	1994
Počet zaměstnanců v ČR	20	170	98	40
Oblasti působení na trhu				
Řešení pro warehouse management	Ano	Ano	Ano	Ano
Řešení pro audit hmotných toků – traceabilita	Ne	Ano	Ano	Ano
Řízení dopravy, monitoring vozů, plánování tras	Ne	Ano	Ne	Ano
Systémová integrace logistických řešení	Ano	Ano	Ano	Ano
Outsourcing logistických řešení	Ne	Ano	Ano	Ano
Nabídka v oblasti identifikace zboží a řízení skladů				
Snímače čárového kódu	Ano	Ano	Ano	Ano
Snímače RFID	Ano	Ano	Ano	Ano
Mobilní terminály	Ano	Ano	Ano	Ano
Vozíkové terminály	Ano	Ano	Ano	Ano
Průmyslové snímače	Ano	Ano	Ano	Ano
Tiskárny etiket	Ano	Ano	Ano	Ano
Softwarová řešení WMS	Ano	Ano	Ano	Ano
Bezdrátové sítě	Ano	Ano	Ano	Ano
Hlasové aplikace	Ano	Ano	Ano	Ano
Monitoring vozů a plánování tras				
Plánování vozového parku – fleet management	Ne	Ne	Ne	Ano
Plánování a optimalizace tras	Ne	Ano	Ne	Ano
Analýza přepravních nákladů	Ne	Ne	Ano	Ano
Řízení kombinované přepravy	Ne	Ne	Ano	Ano

Jméno společnosti	Compas automatizace, spol. s r.o.	Control spol. s r.o.	CyberSoft, s.r.o.	DATA-NORMS s.r.o.
Web	www.compas.cz	www.control.cz	www.cybersoft.cz	www.data-norms.cz
Rok založení společnosti v ČR	1990	1994	2000	1997
Počet zaměstnanců v ČR	100	32	30	
Oblasti působení na trhu				
Řešení pro warehouse management	Ano	Ano	Ano	Ano
Řešení pro audit hmotných toků – traceabilita	Ano	Ano	Ne	Ano
Řízení dopravy, monitoring vozů, plánování tras	Ne	Částečně	Ne	Ano
Systémová integrace logistických řešení	Ne	Ano	Ne	Ano
Outsourcing logistických řešení	Ne	Ne	Ne	Ano
Nabídka v oblasti identifikace zboží a řízení skladů				
Snímače čárového kódu	Ano	Ano	Ano	Ano
Snímače RFID	Ano	Ano	Ne	Ano
Mobilní terminály	Ano	Ano	Ano	Ano
Vozíkové terminály	Ano	Ano	Ne	Ano
Průmyslové snímače	Ano	Ano	Ne	Ano
Tiskárny etiket	Ano	Ano	Ano	Ano
Softwarová řešení WMS	Ano	Ano	Ano	Ano
Bezdrátové sítě	Ano	Ano	Ano	Ano
Hlasové aplikace	Částečně	Ne	Ne	Ano
Monitoring vozů a plánování tras				
Plánování vozového parku - fleet management	Ne	Ne	Ne	Ano
Plánování a optimalizace tras	Ano	Částečně	Ne	Ano
Analýza přepravních nákladů	Ne	Ano	Ne	Částečně
Řízení kombinované přepravy	Ne	Ne	Ne	Ne

Jméno společnosti	EPRIN spol. s r.o.	First Line Software s.r.o.	Gatema IT a.s.	GEMCO, s.r.o.
Web	www.eprin.cz	First Line Software	https://www.gatemait.cz/	www.gemco.cz
Rok založení společnosti v ČR	1992	2015	1992	1995
Počet zaměstnanců v ČR	41	50	200	
Oblasti působení na trhu				
Řešení pro warehouse management	Ano	Ano	Ano	Ano
Řešení pro audit hmotných toků – traceabilita	Ano	Ano	Ano	Ano
Řízení dopravy, monitoring vozů, plánování tras	Ne	Ano	Ne	Ne
Systémová integrace logistických řešení	Ano	Ano	Ano	Ne
Outsourcing logistických řešení	Ne	Ano	Ne	Ne
Nabídka v oblasti identifikace zboží a řízení skladů				
Snímače čárového kódu	Ano	Ano	Ano	Ano
Snímače RFID	Ano	Ano	Ano	Ano
Mobilní terminály	Ano	Ano	Ano	Ano
Vozíkové terminály	Ano	Ano	Ne	Ne
Průmyslové snímače	Ano	Ano	Ano	Ne
Tiskárny etiket	Ano	Ano	Ne	Ano
Softwarová řešení WMS	Ano	Ano	Ano	Ano
Bezdrátové sítě	Ano	Ano	Ne	Ano
Hlasové aplikace	Částečně	Ne	Ne	Ne
Monitoring vozů a plánování tras				
Plánování vozového parku – fleet management	Ne	Ano	Ne	Ne
Plánování a optimalizace tras	Ne	Ano	Ne	Ne
Analýza přepravních nákladů	Ne	Ano	Ne	Ne
Řízení kombinované přepravy	Ne	Ano	Ne	Ne

Údaje uvedené v přehledu poskytli samotní dodavatelé na základě výzvy redakce a jsou pouze orientační. Redakce neručí za jejich správnost a úplnost. Bližší informace najdete na jimi uvedených webech a na ***www.SystemOnLine.cz****, kde jsou všechny přehledy průběžně aktualizovány.*

				Plnou verzi s podrobnějšími informacemi najdete na www.SystemOnLine.cz
ANASOFT	**artipa.software**	**Balíkobot**	**BARCO, s.r.o.**	**CID International, a.s.**
www.anasoft.cz	www.artipa.com	www.balikobot.cz	www.barco.cz	www.cid.cz
1994	2008	2017	1993	1996
		30	13	35
Ano	Částečně	Ne	Ano	Ano
Ano	Ano	Ne	Ano	Částečně
Ano	Ne	Ne	Ne	Ano
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ne	Ne	Ano
Ano	Ne	Ne	Ano	Ano
Ano	Ne	Ne	Ano	Ano
Ano	Ano	Ne	Ano	Ano
Ano	Ne	Ne	Ano	Ano
Ano	Ne	Ne	Ano	Částečně
Ano	Částečně	Ne	Ano	Ano
Ano	Ano	Ne	Ano	Ano
Ano	Ano	Ne	Ano	Ano
Ano	Ne	Ne	Ne	Ne
Ano	Ne	Ne	Ne	Ano
Ano	Ne	Ne	Ne	Ano
Ano	Ne	Ne	Ne	Ano
Ano	Ne	Ne	Ne	Ano

DEPOTO	**DIGITECH ČR, spol. s r.o.**	**DROPTOP COMPUTING s.r.o.**	**DYNAMIC FUTURE s.r.o.**	**EDITEL CZ s.r.o.**
www.depoto.cz	www.digitech.cz	www.droptop.cz	www.dynfut.cz	www.editel.cz
	1999	1993	2001	1994
		8	8	34
Ano	Ne	Ano	Částečně	Ne
Ne	Ne	Ano	Ano	Ne
Ne	Ano	Částečně	Ne	Ne
Ano	Ano	Ano	Ano	Ano
Ne	Ano	Částečně	Částečně	Ano
Ano	Ano	Ano	Ne	Ne
Ano	Ne	Ano	Ne	Ne
Ano	Ano	Ano	Ne	Ne
Ano	Ne	Ano	Ne	Ne
Ne	Ne	Ano	Ano	Ne
Ano	Ne	Ano	Ne	Ne
Ano	Ano	Ano	Ano	Ano
Ano	Ne	Ano	Ne	Ne
Ne	Ne	Částečně	Ne	Ne
Ne	Ano	Ne	Ne	Ne
Ne	Ano	Částečně	Ano	Ne
Ne	Ano	Částečně	Ne	Ne
Ne	Ano	Částečně	Ne	Ne

GRiT, s.r.o.	**ICZ a.s.**	**ITeuro, a.s.**	**KARAT Software a.s.**	**KODYS spol. s r.o.**
www.grit.cz	logistika.i.cz	www.iteuro.cz	www.karatsoftware.cz	www.kodys.cz
1992	1997	2000	1990	1991
80	480	40	96	55
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Částečně	Ano	Ano
Ano	Ne	Částečně	Částečně	Ano
Ano	Ano	Částečně	Ano	Ano
Ano	Částečně	Ne	Ne	Ne
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ne	Ne	Ano
Ano	Ne	Ne	Částečně	Ne
Ano	Ne	Ne	Částečně	Ano
Ano	Ne	Ne	Částečně	Ne
Ano	Ne	Ne	Částečně	Ne

Dodavatelé IT řešení pro logistiku (únor 2022) zkrácená verze					
Jméno společnosti	KTK SOFTWARE s.r.o.	KVADOS, a.s.	M.O.S., spol. s r.o.	MAPFACTOR, s.r.o.	Minerva Česká republika, a.s.
Web	www.ktksoftware.cz	www.kvados.cz	www.autotacho.eu	www.mapfactor.com/	www.minerva-is.eu
Rok založení společnosti v ČR	1992	1992	1991	2001	1992
Počet zaměstnanců v ČR	15	180	3	10	100
Oblasti působení na trhu					
Řešení pro warehouse management	Ano	Ano	Ne	Ne	Ano
Řešení pro audit hmotných toků – traceabilita	Ne	Ano	Ne	Ne	Ne
Řízení dopravy, monitoring vozů, plánování tras	Ne	Ano	Ne	Ano	Ano
Systémová integrace logistických řešení	Ano	Ano	Ne	Ano	Ano
Outsourcing logistických řešení	Ano	Ano	Ne	Ne	Ano
Nabídka v oblasti identifikace zboží a řízení skladů					
Snímače čárového kódu	Ano	Ano	Ne	Ne	Ano
Snímače RFID	Ne	Ano	Ne	Ne	Ano
Mobilní terminály	Ano	Ano	Ne	Ne	Ano
Vozíkové terminály	Ne	Ano	Ne	Ne	Ano
Průmyslové snímače	Ano	Ano	Ne	Ne	Ano
Tiskárny etiket	Ano	Ano	Ne	Ne	Ano
Softwarová řešení WMS	Ano	Ano	Ano	Ne	Ano
Bezdrátové sítě	Ano	Ano	Ne	Ne	Ano
Hlasové aplikace	Ne	Ano	Ne	Ne	Ano
Monitoring vozů a plánování tras					
Plánování vozového parku – fleet management	Ne	Ano	Ne	Ano	Ano
Plánování a optimalizace tras	Ne	Ano	Ne	Ano	Ano
Analýza přepravních nákladů	Ne	Ano	Ne	Ano	Ano
Řízení kombinované přepravy	Ne	Ano	Ne	Ano	Ne

Jméno společnosti	NAVISYS s.r.o.	OLTIS Group a.s.	POINT.X spol. s r.o.	PRYTANIS a.s.	QI GROUP a. s.
Web	www.navisys.cz	https://www.oltis.cz/	www.pointx.cz	www.prytanis.cz	www.qi.cz
Rok založení společnosti v ČR	1997	2004	1991	2020	2000
Počet zaměstnanců v ČR	34	248	25	25	43
Oblasti působení na trhu					
Řešení pro warehouse management	Ano	Ano	Ano	Ano	Ano
Řešení pro audit hmotných toků – traceabilita	Ano	Částečně	Ano	Ano	Ano
Řízení dopravy, monitoring vozů, plánování tras	Ano	Ano	Ano	Ano	Částečně
Systémová integrace logistických řešení	Ano	Ano	Ano	Ano	Ne
Outsourcing logistických řešení	Ano	Ano	Ne	Částečně	Ano
Nabídka v oblasti identifikace zboží a řízení skladů					
Snímače čárového kódu	Ano	Ano	Ano	Ano	Ano
Snímače RFID	Ano	Ano	Ano	Ano	Částečně
Mobilní terminály	Ano	Ano	Ano	Ano	Ano
Vozíkové terminály	Ano	Ano	Ano	Ano	Ano
Průmyslové snímače	Ano	Částečně	Ano	Ano	Ano
Tiskárny etiket	Ano	Ne	Ano	Ano	Ano
Softwarová řešení WMS	Ano	Ano	Ano	Ano	Ano
Bezdrátové sítě	Ano	Ano	Ano	Ano	Částečně
Hlasové aplikace	Ano	Ne	Ano	Částečně	Ne
Monitoring vozů a plánování tras					
Plánování vozového parku – fleet management	Ano	Ano	Ne	Ano	Ano
Plánování a optimalizace tras	Ano	Ano	Ano	Ano	Ano
Analýza přepravních nákladů	Ano	Ano	Ne	Ano	Ano
Řízení kombinované přepravy	Ano	Ano	Ne	Ano	Ano

Jméno společnosti	Sewio Networks	Solitea Byznys	SolverTech, s.r.o.	Vision Praha s.r.o.	ZETES Czech Republic
Web	www.sewio.net	www.byznys.eu	www.solvertech.cz	http://www.vision.cz/	www.zetes.com
Rok založení společnosti v ČR	2014	1991	2009	1999	1990
Počet zaměstnanců v ČR	33	90	13	50	22
Oblasti působení na trhu					
Řešení pro warehouse management	Ano	Ano	Ne	Ano	Ano
Řešení pro audit hmotných toků – traceabilita	Ano	Ano	Ne	Částečně	Ano
Řízení dopravy, monitoring vozů, plánování tras	Ne	Ano	Ano	Ano	Ano
Systémová integrace logistických řešení	Částečně	Ano	Ano	Ano	Ano
Outsourcing logistických řešení	Ne	Ne	Ne	Ne	Ne
Nabídka v oblasti identifikace zboží a řízení skladů					
Snímače čárového kódu	Ne	Ano	Ne	Ano	Ano
Snímače RFID	Ne	Ano	Ne	Ano	Ano
Mobilní terminály	Ne	Ano	Ne	Ano	Ano
Vozíkové terminály	Ne	Ano	Ne	Ano	Ano
Průmyslové snímače	Ne	Ano	Ne	Ano	Ano
Tiskárny etiket	Ne	Ano	Ne	Ano	Ano
Softwarová řešení WMS	Ne	Ano	Ne	Ano	Ano
Bezdrátové sítě	Ne	Ano	Ne	Ano	Ano
Hlasové aplikace	Ne	Ano	Ne	Částečně	Ano
Monitoring vozů a plánování tras					
Plánování vozového parku – fleet management	Ne	Ano	Ne	Ano	Ano
Plánování a optimalizace tras	Ano	Ano	Ano	Ano	Ano
Analýza přepravních nákladů	Ne	Ano	Ano	Ano	Ne
Řízení kombinované přepravy	Ne	Ano	Ne	Ano	Ne

Údaje uvedené v přehledu poskytli samotní dodavatelé na základě výzvy redakce a jsou pouze orientační. Redakce nenese za jejich správnost a úplnost. Bližší informace najdete na jimi uvedených webech a na ***www.SystemOnLine.cz****, kde jsou všechny přehledy průběžně aktualizovány.*

Útoky typu credential stuffing stále častěji nahrazují útoky hrubou silou, jsou rychlejší a nebezpečnější

Petr Mojžíš

Útoky na přihlašovací údaje (hesla) byly v minulosti běžně prováděny buď pomocí sociálního inženýrství, nebo tzv. hrubou silou. První metoda funguje i nadále velmi dobře, ale vyžaduje dobré cílení, čas a pečlivou přípravu. Druhá metoda je ale postupně nahrazována mnohdy rychlejší a účinnější variantou s pomocí „credential stuffingu".

Útok na hesla hrubou silou (brute force) spočívá ve využití automatizace pokusů o přihlášení do nějakého systému – heslo je zkrátka překonáno díky jeho nalezení postupným zkoušením zásadního množství kombinací. U číselných hesel (například PIN do telefonu) tedy stačí zkoušet postupně všechny kombinace, u znakových či složitějších hesel se pak zpravidla využívalo také zkoušení kombinací nebo různé druhy slovníků. Nevýhodou brute force ale byla časová náročnost a také to, že proti postupnému zkoušení tisíců a tisíců kombinací se systémy dokážou poměrně účinně bránit – při dalším a dalším chybném pokusu zpomalí možnost zkoušet další kombinaci, případně kompletně zablokují systém, z něhož pokusy přicházejí.

Credential stuffing využívá toho, že jsou k dispozici databáze uniklých přihlašovacích údajů – kompletní kombinace uživatelských jmen, e-mailů a hesel. Útočníci pak využijí takovéto databáze a s pomocí automatizace zkoušejí uniklé kombinace. Zvyšuje se tím šance na úspěch, a navíc je běžné, že touto cestou zkoušejí získat přístup k řadě webů či aplikací.

Pokud se jim podaří přístup získat, následují krádeže identity, phishing, podvody založené na vydávání se za různé subjekty a další druhy zneužití dat. V mnoha případech je možné získané přístupy využít i třeba pro nákupy na internetu, ale třeba i pro průmyslovou špionáž. Tento druh útoků bývá úspěšný hlavně proto, že uživatelé běžně používají opakovaně stejné heslo. Stačí, aby uniklo jednou, a útočníci se pak dostanou do všech dalších účtů, které uživatel má.

Rozsáhlé databáze přihlašovacích údajů jsou běžně dostupné na černém trhu a mohou být výsledkem cílených hackovacích kampaní na objednávku. Už v roce 2020 například Akamai upozorňovali, že dochází k růstu credential stuffing útoků proti médiím a novinářům.

Jak se proti credential stuffingu bránit?

Tou nejlepší obranou by bylo přejít na **používání multifaktorových a bezheslových autentizačních procesů** – u těch je přihlášení do systémů podmíněno ověřením přes jiný faktor než pouze přes heslo: minimálně přes zaslání dodatečného jednorázového kódu na e-mail nebo pomocí SMS, ale ideálně přes nějaký druh bezpečnostního klíče, pomocí biometrie či mobilního autentizátoru.

Navíc v samotných systémech je vhodné monitorovat podezřelé chování uživatelů a náhlé změny (anomálie) vzorců obvyklých činností v kombinaci se zabezpečením webových aplikací pomocí tzv. pokročilých web-aplikačních firewallů (WAF), které poměrně s vysokou přesností dokážou odhalit např. právě útoky typu credential stuffing.

Samotní uživatelé navíc mohou úniky jimi používaných hesel hlídat ještě například za pomoci služby HaveIBeenPwned.com. V případě zjištěného úniku nějakého hesla je nutné toto heslo okamžitě jednou provždy přestat používat.

Ve firemním prostředí je dále na místě školit zaměstnance a vysvětlovat, jak s hesly nakládat a jak vytvářet hesla bezpečná, a zároveň tyto uživatele pravidelně testovat v odolnosti potenciálního předání přístupových údajů, například za pomoci řízených phishingových kampaní.

Pro zodpovědné společnosti navíc platí, že by měly hlídat případné úniky hesel na dark webech, pomocí systematických služeb typu Cyber Threat Intelligence (doporučuje se vyhledávat jednak uniklá hesla k firemním účtům, ale i uniklá hesla k soukromým účtům například top-managementu či jiných privilegovaných zaměstnanců).

Zneužívání firemních hesel lze bránit také pomocí technologií, které detekují a blokují použití stejných (firemních) hesel v soukromých systémech (například aby zaměstnanec nemohl použít některé z firemních hesel při přístupu na soukromý Facebook či soukromý e-mail).

Pokud není možné přejít na bezheslové přihlašování, tak by uživatelé měli v maximální míře využívat tzv. dvoufaktorovou (2FA) nebo multifaktorovou (MFA) autentizaci. Ta se týká jak osobních účtů, tak těch firemních. U všech privilegovaných účtů (např. účty administrátorů, účty aplikací apod.) by navíc měly být využívána výrazně přísnější pravidla, např. pravidelná změna hesel, využívání heslových trezorů a ideálně kompletní systémy PAM (Privileged Account Management). ■

Petr Mojžíš

Autor článku je konzultantem kybernetické bezpečnosti ve společnosti ANECT.

Digital Services Act

Petra Věžníková

V prosinci roku 2020 představila Evropské komise balíček dvou nařízení, která mají nastavit nová pravidla pro fungování digitálního prostředí v Evropské Unii. Prvním z nich je návrh nařízení o jednotném trhu digitálních služeb, známý jako Akt o digitálních službách (Digital Services Act, „DSA"), přinášející řadu podstatných změn, které dopadnou i na české provozovatele těchto služeb.

Návrh byl předložen, je projednáván a veřejnosti prezentován spolu s návrhem dalšího nařízení, kterým je Akt o digitálních trzích (Digital Markets Act, „DMA"), který vám blíže představíme v příštím čísle. Oba tyto návrhy – jakožto součást digitální strategie Evropské Unie - mají aktualizovat zejména unijní směrnici o elektronickém obchodu (2000/31/ES), která byla přijata před dvaceti lety a už poněkud nestačí moderním trendům. Návrhy směřují k posílení jednotného digitálního trhu, k čemuž má sloužit i zvolená forma.

Hlavními cíli DSA je vytvořit bezpečnější digitální prostředí pro uživatele (tedy pro příjemce digitálních služeb) a usnadnit rozšiřování menších platforem, malých a středních podniků a startupů – nastavit „rovné podmínky hry" (level playing field), a tím v konečném důsledku podpořit inovace, růst a konkurenceschopnost na jednotném digitálním trhu i na vnitřním trhu Evropské Unie celkově.

Načasování legislativního procesu

Návrhy obou nařízení, tedy jak DSA, tak DMA, byly Komisí schváleny 16. prosince 2020. V průběhu roku 2021 byl návrh několikrát projednáván v rámci prvního čtení na půdě Rady EU. Předpokládáme, že v příštím roce dojde k jeho projednání i na úrovni Evropského parlamentu. Optimistický odhad pro schválení je rok 2023/2024.

Na koho se DSA vztahuje?

Nařízení upravuje harmonizovaná pravidla **pro poskytování zprostředkovatelských služeb** na vnitřním trhu, zejména upravuje rámec pro podmíněné zproštění odpovědnosti poskytovatelů zprostředkovatelských služeb ale taky nové povinnosti. Hlavními adresáty jsou tedy poskytovatelé zprostředkovatelských služeb. Některé povinnosti jsou pak stanoveny jen pro specifické kategorie poskytovatelů zprostředkovatelských služeb, jak si ukážeme dále:

- **Zprostředkovatelská služba** je souhrnné označení pro službu prostého přenosu, službu ukládání do mezipaměti nebo hostingovou službu.
- **Služba prostého přenosu** spočívá v přenosu informací poskytovaných příjemcem služby v komunikační síti nebo ve zprostředkování přístupu ke komunikační síti – adresáty nařízení tak budou například poskytovatelé síťové infrastruktury, poskytovatelé připojení nebo registrátoři domén.
- **Služba ukládání do mezipaměti** (caching) spočívá v přenosu informací (poskytovaných příjemcem služby) v komunikační síti a zahrnuje automatické dočasné přechodné ukládání informací.
- **Hostingová služba** spočívá v ukládání informací poskytovaných příjemcem služby na jeho žádost; spadají sem veškeré služby, které ukládají uživatelská data (např. webhosting a cloudové služby či online platformy).
- **Online platformy** nařízení definuje zvlášť, a to jako poskytovatele hostingové služby, který na žádost příjemce služby ukládá a veřejně šíří informace (to neplatí pro situace, kdy je tato činnost nepodstatnou a pouze pomocnou funkcí jiné služby a z objektivních a technických důvodů ji nelze používat bez této jiné služby a integrace této funkce do jiné služby není prostředkem k obcházení této právní úpravy). Online platformami jsou například internetová tržiště (Aukro), obchody s mobilními aplikacemi (Google Play, AppStore), platformy pro sdílenou ekonomiku (Bolt, Airbnb, Uber), sociální sítě, atd.

Zvlášť návrh nařízení definuje i tzv. **velmi velké online platformy**. Těmi jsou online platformy, které poskytují své služby alespoň 10% obyvatelstva EU (resp. alespoň 45 milionům příjemců služby v EU měsíčně).

Příjemcem služby je pak fyzická nebo právnická osoba, která využívá příslušnou zprostředkovatelskou službu. Nařízení se použije na zprostředkovatelské služby poskytované příjemcům služby, kteří mají místo usazení nebo bydliště v Evropské Unii, a to

bez ohledu na místo usazení poskytovatelů těchto služeb. Podobně jako např. u GDPR i zde vidíme extrateritoriální účinek evropské právní úpravy.

Co upravuje Digital Services Act?

Odpovědnost poskytovatelů zprostředkovatelských služeb za obsah informací

V prvé řadě návrh upravuje výjimky z odpovědnosti, respektive rámec pro podmíněné zproštění se odpovědnosti poskytovatelů zprostředkovatelských služeb. Oproti stávající úpravě se pravidla téměř nemění (alespoň prozatím: zejména větší státy se snaží na poskytovatele přenést větší míru odpovědnosti). Nařízení pro jednotlivé kategorie poskytovatelů stanoví výjimky, při jejichž naplnění může dojít ke zproštění odpovědnosti za přenášené či ukládané informace.

V případě prostého přenosu není poskytovatel odpovědný, pokud

- není původcem přenosu,
- nevolí příjemce přenášených informací, a
- nevolí a nemění obsah přenášených informací.

V případě cachingu není poskytovatel odpovědný, pokud:

- nemění informace,
- vyhoví podmínkám přístupu k informacím,
- dodržuje pravidla o aktualizaci informací,
- nepřekročí povolené používání technologie s cílem získat údaje o užívání informace, a
- urychleně smaže nebo zamezí přístup, jakmile zjistí, že informace byly odstraněny/blokovány ve zdrojovém uložišti, nebo pokud tak nařídí soud nebo správní orgán.

V případě hostingu není poskytovatel odpovědný, pokud:

- neví o protiprávní činnosti nebo nezákonném obsahu, nebo
- jakmile zjistí protiprávní činnost nebo nezákonný obsah, urychleně jej odstraní nebo znemožní přístup.

Vymezení **nezákonného obsahu** je poměrně široké. Mohou jím být *„jakékoli informace, které samy o sobě nebo ve vztahu k určité činnosti včetně prodeje zboží nebo poskytování služeb nejsou v souladu s právem Unie nebo právem některého členského státu, a to bez ohledu na přesný předmět či povahu tohoto práva“*. Tedy například nezákonné nenávistné projevy, teroristický obsah, nezákonný diskriminační obsah, sdílení obrázků s dětskou pornografií, nezákonné sdílení soukromých fotografií bez souhlasu, kybernetické pronásledování, prodej nevyhovujících nebo padělaných výrobků, neoprávněné použití materiálů chráněných autorským právem, činnosti zahrnující porušování právních předpisů na ochranu spotřebitele atp.

Oproti některým dřívějším návrhům není v nařízení zakotvena povinnost nezákonný obsah aktivně vyhledávat. Toto vzešlo z předlegislativních konzultací jako jeden z hlavních požadavků poskytovatelů. To ale nebrání poskytovatelů provádět vlastní dobrovolná vyšetřování a nezákonný obsah vyhledávat. Dále je upravena povinnost součinnosti s vnitrostátními justičními nebo správními orgány (ta bude rovněž spočívat v znepřístupnění obsahu nebo poskytnutí informací).

Povinnosti poskytovatelů zprostředkovatelských služeb

Návrh dále stanovuje celou **řadu povinností**, které dopadají jak na všechny poskytovatele zprostředkovatelských služeb, tak na jednotlivé specifické kategorie (pro velmi velké online platformy je povinností stanoveno nejvíce).

Povinnosti, které dopadnou **na všechny** poskytovatele zprostředkovatelských služeb:

- zřídit jednotné kontaktní místo pro komunikaci s veřejnými orgány (pokud nemá poskytovatel provozovnu v EU povinnost jmenovat zástupce),
- podávat zprávy o transparentnosti: minimálně jednou za rok publikovat zprávu o veškerém moderování obsahu, které prováděl v příslušném období (obsahuje např. informace o počtu příkazů obdržených od orgánů členských států; počtu oznámení uživatelů ohledně nezákonného obsahu; moderování obsahu z vlastního podnětu poskytovatele),
- uvést ve svých podmínkách informace o veškerých omezeních, která používají k moderování obsahu (včetně rozhodování založeného na algoritmech),
- spolupráce s vnitrostátními orgány po vydání příkazu - povinnost plnit příkazy vnitrostátních orgánů ohledně nezákonného obsahu.

Poskytovatelé **hostingových služeb** mají navíc povinnost zavést mechanismy pro oznamování a pro přijímání opatření ohledně nezákonného obsahu informovat příjemce o konkrétních provedených opatřeních (včetně odůvodnění).

Další řada povinností se týká **online platforem***, například:

- zavést interní mechanismus pro vyřizování stížností a sjednávání nápravy a mimosoudní urovnávání sporů,
- v rámci oznamovacích mechanismů nastavit procesy pro přednostní vyřizování podnětů od tzv. důvěryhodných oznamovatelů,
- zavést opatření pro pozastavení služeb příjemcům včetně stanovení ochranných prvků proti možnému zneužití,
- ověřovat totožnost obchodníků, kteří v rámci platformy uzavírají smlouvy se spotřebiteli (*Know Your Business Customer*),
- zajistit transparentnost internetové reklamy včetně označení reklamy a jejího objednatele,
- oznamovat trestné činy a zabraňovat jejich páchání.

(* nevztahuje se na platformy, které jsou mikropodniky nebo malými podniky)

Na **velmi velké platformy** pak dále dopadají povinnosti v oblasti řízení rizik a další povinnosti:

- povinnost alespoň jednou ročně provést posouzení rizik (specificky pak v otázce šíření nezákonného obsahu, negativních dopadů na výkon základních práv a ochrany soukromí, a úmyslných manipulací s jejich službou),
- zmírňovat výše uvedená rizika,
- provést alespoň jednou ročně audit nezávislým auditorem a přijmout opatření na základě auditu,
- v případě používání doporučovacích systémů, uvést ve svých podmínkách hlavní parametry nastavení a možnosti ovlivnění parametrů doporučení,

Povinnost poskytovatelů podle DSA	ZS	HS	OP	+ OP
zprávy o transparentnosti	•	•	•	•
přijetí podmínek zohledňujících základní práva	•	•	•	•
spolupráce s vnitrostátními orgány	•	•	•	•
kontaktní místa (+ zákonný zástupce)	•	•	•	•
oznámení, opatření a poskytování informací uživatelům		•	•	•
mechanismus pro vyřizování stížností a mimosoudní řešení sporů			•	•
důvěryhodní oznamovatelé			•	•
opatření proti nekorektním oznámením			•	•
ověřování totožnosti dodavatelů-třetích stran (KYBC)			•	•
transparentnost internetové reklamy			•	•
oznamování trestných činů			•	•
povinnosti v oblasti řízení rizik + kontrolor shody				•
audit vnějších rizik a odpovědnost vůči veřejnosti				•
doporučující systémy - transparentnost a možnosti volby přístupu k informacím				•
sdílení údajů s úřady a výzkumnými pracovníky				•

Legenda: ZS = zprostředkovatelské služby, HS = hostingové služby, OP = online platformy, +OP = velmi velké online platformy)

- v případě zobrazování reklamy zveřejňovat archiv informací ohledně zobrazených reklam,
- poskytnout koordinátorovi digitálních služeb a pověřeným osobám (výzkumní pracovníci),
- určit osobu odpovědnou za sledování souladu s DSA,
- zapojit se na výzvu Komise do tvorby kodexů a krizových protokolů (viz. tabulka).

Provádění a vymáhání nařízení

Dohled nad dodržováním DSA na národní úrovni mají mít tzv. koordinátoři digitálních služeb (jejich roli budou zastávat orgány určené příslušným členským státem). Dále nařízení zavádí Evropský sbor pro digitální služby, který má být nezávislou poradní skupinou tvořenou představiteli národních koordinátorů digitálních služeb. Další pravomoci (zejména pak v oblasti dohledu nad velmi velkými online platformami) pak mají příslušet Komisi. Národní koordinátoři i Komise budou moci mimo jiné provádět kontroly na místě a za nedodržení nařízení ukládat sankce až do výše 6% ročního příjmu nebo obratu poskytovatele zprostředkovatelských služeb (resp. do výše 1 % v případě poskytnutí nesprávných, neúplných nebo zavádějících informací nebo neumožnění kontroly na místě).

Na závěr: Co přinese DSA pro jednotlivé stakeholdery?

Ačkoliv jde prozatím pouze o návrh nařízení a jeho finální podoba se může v průběhu legislativního procesu ještě měnit, již z předloženého textu můžeme vidět, že nová evropská regulace digitálních služeb přinese řadu nových povinností zejména pro větší poskytovatele digitálních služeb a potřebu se na tyto změny připravit a zakomponovat nové prvky do svých procesů. Zároveň si však Komise od nových pravidel slibuje zvýšení právní jistoty a umožnění snazší expanze a podnikání i pro menší poskytovatele digitálních služeb; a širší nabídku, nižší ceny, transparentnější informace a nižší riziko vystavení nezákonnému obsahu pro uživatele digitálních služeb, ať už z řad podniků nebo pro spotřebitele. ■

Mgr. Ing. Petra Věžníková

Autorka článku je advokátka ve společnosti Squire Patton Boggs, kde se zaměřuje na právo digitálních technologií (ochrana osobních údajů, kyberbezpečnost, regulace elektronických komunikací a soutěžní právo).

Získávání souhlasu se sběrem a zpracováním cookies od 1. ledna 2022

Jiří Matzner

Na základě novely zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „zákon o elektronických komunikacích“), došlo od 1.ledna 2022 k zásadní změně týkající se sběru a zpracování tzv. cookies. Od nového roku je totiž ke zpracování cookies vyžadován výslovný souhlas uživatele webové stránky.

Vzhledem k tomu, že cookies mimo jiné naplňují definici osobních údajů ve smyslu nařízení EP a Rady (EU) č. 2016/679, ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“), bude muset předmětný souhlas splňovat širokou paletu podmínek a náležitostí.

Změna z režimu „opt-out“ na režim „opt-in“

Cookies jsou malé datové soubory ukládané na zařízení uživatele při návštěvě webové stránky, jenž mimo jiné zvyšují uživatelský komfort, a to především při dalších návštěvách webové stránky, kterou uživatel již dříve navštívil. Pro provozovatele webových stránek ovšem zpravidla není hlavním přínosem sběru cookies zlepšování uživatelského komfortu, ale především sledování chování uživatelů na webu, sledování počtu návštěvníků webu či tvorba cílené reklamy. Sběr cookies je tak z pohledu provozovatelů webu klíčový především z obchodního a marketingového hlediska.

Na základě novely zákona o elektronických komunikacích došlo počátkem letošního roku ke zcela zásadnímu obratu v podmínkách sběru a zpracování cookies. Změna spočívá v tom, že sběr cookies je nově založen na tzv. „opt-in“ principu, a nikoliv již na principu „opt-out“, který se uplatňoval před účinností novely zákona o elektronických komunikacích. Znamená to, že uživatelé webových stránek dnes musí se sběrem a zpracováním cookies poskytnout svůj předchozí výslovný souhlas. Výjimku představují pouze tzv. nezbytná cookies, bez nichž by webové stránky prakticky nemohly fungovat. Zpracování všech ostatních typů cookies (např. statistických, marketingových nebo preferenčních) ovšem dnes už podléhá výslovnému předchozímu souhlasu uživatele.

Náležitosti souhlasu se zpracováním cookies z pohledu GDPR

Provozovatelé webů tak od nového roku musí mít na svých webových stránkách umístěn souhlas se zpracováním cookies (tzv. cookies lištu), na jehož základě budou vybírat od uživatelů souhlas se sběrem a zpracováním cookies a informovat je o existenci cookies a jejich praktické využitelnosti. Nad rámec uvedeného musí souhlas se zpracováním cookies rovněž splňovat veškeré náležitosti kladené nařízením GDPR na souhlas se zpracováním osobních údajů, jelikož zpracováním cookies bude zpravidla docházet i ke zpracování osobních údajů uživatelů (jakožto subjektu údajů). Především bude třeba dodržet požadavky GDPR kladené na svobodu, určitost, vědomost a informovanost uživatele při udílení souhlasu. V neposlední řadě bude třeba dbát na to, aby udělení souhlasu se sběrem cookies bylo zpětně prokazatelné, s ohledem na případnou kontrolu ze strany dozorového orgánu – toto by mělo být vzato v úvahu zejména při volbě technického řešení.

Jak hodnotit přínos novely zákona o elektronických komunikacích?

Je samozřejmě otázkou, do jaké míry lze změnu zákona o elektronických komunikacích považovat za přínosnou. Z pohledu provozovatelů webových stránek totiž došlo nejen k navýšení nákladů na úpravu webových stránek, za účelem doplnění cookies lišty, ale současně se dá očekávat i výrazné snížení objemu sběru např. marketingových, statistických nebo preferenčních cookies. Uživatelé totiž s největší pravděpodobností nebudou mít motivaci „proklikávat se“ cookies lištami a udělovat provozovatelům souhlasy zpracovávat jednotlivé typy cookies. Toto bezesporu může mít negativní dopady na byznys provozovatelů webu s ohledem na případný „remarketing“, cílenou reklamu nebo sledování návštěvnosti a celkové funkčnosti webových stránek. Provozovatelé webových stránek tedy s novelou přirozeně nemohou být spokojeni.

Zůstává tedy otázkou, zda novela zákona bude přínosem alespoň pro uživatele. Z pohledu ochrany osobních údajů bezesporu ano, jelikož většina uživatelů si nebyla vědoma široké škály možného využití cookies a nyní bude mít mnohem efektivnější a transparentnější možnost volby při udělování souhlasu se zpracováním cookies. Na druhou stranu však zaznívá i řada názorů na straně samotných uživatelů, že jsou pro ně cookies lišty „obtěžující“ a výrazně snižují uživatelský komfort při užívání webu, jelikož prakticky při každé nové návštěvě určité webové stránky je nutné udělovat souhlas se sběrem cookies. Nehledě na to, že i před účinností novely zákona o elektronických komunikacích byla ochrana soukromí v rukou uživatelů, kteří si prostřednictvím nastavení internetového prohlížeče mohli cookies na svém zařízení omezit, nebo zakázat podle potřeby.

Závěr

S ohledem na shora uvedené argumenty se přínos změny režimu sběru cookies dá považovat přinejmenším za diskutabilní, jelikož ani samotní uživatelé, na jejichž ochranu byla změna zákona do právního řádu včleněna, nejsou v názorech na uvedenou změnu jednotní a řada z nich ji z čistě praktických důvodů neváhá kritizovat. Je však stále předčasné činit v tomto směru ukvapené závěry o přínosu novely, která nabyla účinnosti relativně nedávno a je možné, že teprve čas ukáže její reálné dopady. ■

JUDr. Jiří Matzner, Ph.D., LLM.

Zakladatel advokátní kanceláře MATZNER Legal

ITAM musí být proaktivní a hledět do budoucnosti,

říká David Foxen, zakladatel poradenské agentury SAM Beast

David Foxen má dlouholeté zkušenosti v oblasti IT Asset Managementu (ITAM). Svým klientům ušetřil miliony liber díky implementaci a rozvoji fungujících ITAM procesů. Je zakladatelem poradenské agentury SAM Beast. Svou vášeň pro ITAM sdílí prostřednictvím živých kanálů na LinkedIn a YouTube. Požádali jsme ho o rozhovor, ve kterém jsme hovořili o tom, proč by se ITAM měl dívat více do budoucnosti.

Jak zmiňujete na LinkedIn, ITAM doslova milujete. O důležitosti ITAM sice nikdo nepolemizuje, ale málokdo se pro něj opravdu nadchne. Co se vám na ITAM tak líbí?
ITAM je pro mě nejlepší věc na světě. Nikdy jsem ve své kariéře nedělal nic jiného, ale miluji to, protože opravdu věřím v hodnotu, kterou může přinést organizacím a všem zúčastněným. Vezměte si například bezpečnost informací. Tam ITAM nesmírně pomáhá tím, že identifikuje starší hardware a software, kterému končí životnost. Můžeme pomoci při nákupu a sestavování rozpočtu. Je tolik oblastí, se kterými můžeme pomoci. Pak tu máme moderní trendy, jako je FinOps. ITAM můžeme využít ve vztahu k FinOps, abychom ušetřili peníze. Můžete udělat gap analýzu a okamžitě začnete šetřit peníze. ITAM rozhodně není nuda! Je skvělý!

Jaká je největší hodnota, kterou ITAM organizacím přináší?
Tradičně to byla finanční optimalizace a dodržování právních předpisů, ale s nedávnými událostmi přináší ITAM mnohem větší kontinuitu a stabilitu. Vzpomeňte si, jak to vypadalo, když udeřila pandemie COVID: Všichni popadli veškerý dostupný hardware a začali pracovat z domova. A teď si každý říká, kde to všechno je? V tomto prostředí přináší ITAM kontrolu a přehled po celou dobu životního cyklu. To je klíčové. ITAM nyní podporuje byznys a hraje mnohem proaktivnější roli než kdy dříve.

Pravděpodobně největší revoluce v oblasti ITAM v poslední době přišla s dominancí SaaS. Jednou z jeho výhod je usnadnění nákupu softwaru pro koncové uživatele. Na druhou stranu se to může IT oddělení rychle vymknout kontrole. Jaké jsou největší problémy při správě SaaS?
Kdysi jste mohli mít obrovské množství různých aplikací a téměř žádné licence. SaaS vám pomůže udržet váš IT majetek v souladu s právními předpisy. Stále sice musíte hlídat sdílení účtů, ale dodržování licenčních podmínek je díky SaaS jednodušší. Z hlediska dodržování předpisů také pomáhá, že dodavatelé mají svůj portál. Pokud nemáte ITAM nástroj, můžete se alespoň podívat na portál. Již nemáte žádnou výmluvu, proč neoptimalizovat výdaje na SaaS.

Na druhou stranu je správa cloudového prostředí složitá. Z tohoto důvodu vznikl FinOps. I v případě cloudu je třeba dbát na konfiguraci, abyste měli jistotu, že skutečně šetříte náklady a správně jej optimalizujete. Společnosti, které začaly využívat cloudová řešení, se nyní při výběru softwaru primárně soustředí na poskytovatele takovýchto služeb. Způsoby pořizování softwaru se tak rychle mění. ITAM musí těmto změnám porozumět a umět se přizpůsobit.

Další věcí, na kterou je třeba myslet, je stínové IT. Pokud začnete detailněji analyzovat všechny firemní výdaje, najednou si uvědomíte, že je toho spousta, o čem nemáte žádný přehled. Jedním ze způsobů, jak získat větší kontrolu, je zavést proces, kdy všichni uživatelé, kteří žádají nový software, komunikují přímo s pracovníky zodpovědnými za ITAM. Nechovejte se jako softwarová policie, ale vysvětlete jim, proč to děláte a jak to pomáhá celé firmě.

Součástí vaší práce je firemní poradenství v oblasti softwaru pro ITAM. Kdy má organizace začít uvažovat o investici do nástroje pro ITAM? Jaká je hranice, kdy už si firma nevystačí s tabulkovou evidencí v Excelu?
Excel je stále světově nejpoužívanější nástroj pro ITAM. I když máte fantastický ITAM software, stále budete pro některé účely používat Excel. Existují určité spouštěče, které odstartují přechod z tabulkové evidence. Jedním z nejčastějších je externí nebo interní audit. Viděl jsem například i společnosti, které používaly tabulky s 10 000 řádky. Ve skutečnosti však neexistuje žádná konkrétní hranice. Záleží spíše na tom, jak vážně lidé ve firmě berou ITAM. Obvykle si v určitém okamžiku začnou sami uvědomovat, že zavedení vhodného ITAM nástroje je investice s dobrou návratností. Protože stejně jako v jiných oborech, lidé nejvíce rozumí řeči peněz a návratnost investic je nejlepším argumentem pro zavedení ITAM nástroje.

Jak lze spočítat návratnost investice do ITAM?
Nejprve je třeba počítat přímé úspory, které získáte díky konsolidaci podrobné evidence softwaru a hardwaru nebo konsolidaci SaaS řešení. Dále ušetříte značné množství času, který lidé tráví nad nepřehlednými tabulkami. A za třetí, usnadníte práci všech zainteresovaných stran. Všichni zaměstnanci jsou zákazníky ITAM. Pokud máte notebook, jste zákazníkem ITAM. Proto je důležité mít vždy na paměti své koncové uživatele a další zúčastněné strany.

ITAM je poměrně rozsáhlá disciplína. Pro firmy, které s ní teprve začínají, to může být velmi náročné. Kde bych měl při zavádění ITAM ve firmě začít? Jak lze rychle prokázat jeho přínos?

Obvykle provádím GAP analýzu ve správě majetku a hodnotím celkovou úroveň firemních postupů. Detailně se pak podívám se na kontrolní mechanismy a procesy. Pokud hledáte rychlý způsob, jak prokázat přínos ITAM, stačí se podívat na využívání Microsoft365. Vyžádejte si report z HR, vyjeďte si report využití Microsoft365 a porovnejte. Díky této jednoduché analýze zjistíte, že za licence zbytečně utrácíte. Tímto způsobem rychle prokážete hodnotu ITAM.

Další důležitou věcí hned na začátku je zapojení všech zúčastněných stran. Prezentujte, co plánujete v rámci ITAM dělat. Jaké konkrétní výhody může ITAM přinést do jejich každodenní práce a jejich oddělení jako celku. Investujte do vztahů a získejte si důvěru. To je k nezaplacení.

Rovněž konzultujte plánové změny přímo s koncovými uživateli. Vždy jim ukažte reálný přínos: S použitím nových postupů ušetříme tuto částku v nákladech.

• • •

Bezpečnost IT je dnes jedním z nejdiskutovanějších témat. Jak může ITAM přispět k bezpečnosti IT?

Spousta organizací utrácí nemalé prostředky na zabezpečení dat, zatímco ITAM sedí v rohu s obyčejným Excelem. IT bezpečnost je však pro ITAM jeden z nejdůležitějších partnerů a existuje zde řada synergií. Co se týká softwaru, ITAM schvaluje používání softwaru a poskytuje lidem z IT bezpečnosti informace o tom, co se ve firmě skutečně používá. Můžeme také snadno dohledat starý software představující bezpečnostní hrozbu.

Také lze Bezpečnost IT zapojit do kontroly a prověřování nových softwarových nástrojů, které organizace plánuje implementovat. Pokud někdo požaduje nový software, který neznáte, požádáte je nejprve o kontrolu.

Co se týká hardwaru, můžete jim reportovat hardware, kterému končí životnost a podpora. Spolupráce je důležitá i pro celý související postup vyřazení: Likvidace zařízení způsobem, který zajistí, že jsou všechna data nenávratně smazaná před tím, než hardware opustí firmu. Na druhou stranu bezpečnost IT může zase pomoci nám: například identifikací rizik v podobě stínového IT.

• • •

Je evidentní, že vás ITAM nesmírně baví. Jak vidíte jeho budoucnost?

ITAM se tradičně dívá spíše zpět. Rád bych, aby se ITAM díval více dopředu. Místo toho, aby zpětně vyhodnocoval chyby a obviňoval lidi za špatné výsledky auditu, měl by být proaktivní a lépe rozumět, co se ve firmě chystá. Přecházíme na cloud? Jak s tím můžeme pomoci? Jak můžeme snížit náklady? Vidím, že server je využíván jen pár minut denně. Když to víme, můžeme zajistit, aby spotřebovával jen odpovídající množství cloudové kapacity, a ušetřit peníze. Vidíme, že se chystá zdražení? Uzamkněme cenu aplikace. Můžeme být proaktivní při obnovování. Atd.

Nemůžeme změnit minulost a napravit ji, ale můžeme napravit budoucnost. Aby se vám to povedlo, potřebujete mluvit se všemi zúčastněnými a zjistit, jak můžete pomoci. Opravdu musíme změnit mentalitu směrem k budoucnosti. ■

Rozhovor připravil Jan Škrabánek, konzultant společnosti ALVAO.

• • •

(Ne)výhody vysoké dostupnosti

IT infrastruktury

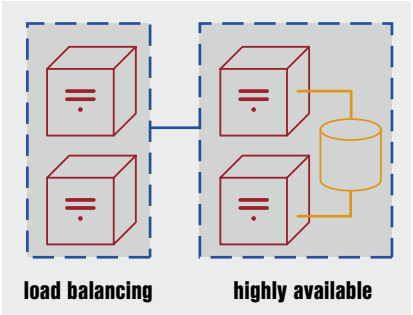
Ondřej Flídr

Vysoká dostupnost či high availability (HA) je už řadu let synonymem spolehlivosti a odolnosti IT infrastruktury. Kdo svůj online projekt neprovozuje „v há-áčku“ jako by nebyl. Co se pod tímto pojmem ale opravdu skrývá? Jak se vysokodostupnostní infrastruktura vůbec staví? Komu se vyplatí do ní investovat, a komu ne?

Zjednodušeně řešeno, vysoká dostupnosti je způsob, jak zajistit, aby váš online projekt „ustál“ běžné provozní problémy, jako je např. selhání části vašeho hardwaru. Díky tomu nemusíte vy ani váš IT tým řešit ve 3 ráno krizovou situaci a váš zákazník, a někdy ani CEO firmy nepozná, že na pozadí odešel třeba jeden z vašich disků.

Proč (ne)chtít vysokou dostupnost

Pro byznys jsou nejlepší zákazníci, kteří jsou spokojení, pak se vracejí. V dnešní době vysokou dostupnost se samozřejmostí už předpokládají. Jakmile svůj projekt začnete provozovat v HA režimu, dopad případných technických problémů na zákazníka je minimální. To má pozitivní dopad na vaše finanční ohodnocení a nervy.



Neméně důležitá je i technická stránka věci, konkrétně minimalizace času potřebného na údržbu a zjednodušení škálování. Aplikace běžící na HA infrastruktuře umožní vašemu vývoji dělat násobně rychlejší a bezpečnější upgrady. A to z důvodu možnosti využít tzv. rolling upgrady. Novou verzi aplikace nasadíte pouze na jeden server na produkci. V případě problému vše jednoduše obnovíte na verzi původní. Produkce z pohledu zákazníka vám zatím bezpečně jede z ostatních serverů s původní verzí aplikace.

HA infrastruktura je i mnohem lépe připravena na rychlé škálování, a bude tak držet krok s růstem vašeho projektu. Umožňuje škálování nejen vertikální (přidávání výkonu, např. RAM), ale i horizontální (přidávání dalších strojů), které je u rapidně rostoucích projektů nevyhnutelné. Pokud vám naopak všechno běží na jednom serveru, můžete škálovat jedině vertikálně, a to navíc velmi omezeně. Na nečekaný výkyv v návštěvnosti např. při výprodejích tak nemáte šanci rychle zareagovat a celé infrastruktuře hrozí, že nápor neustojí.

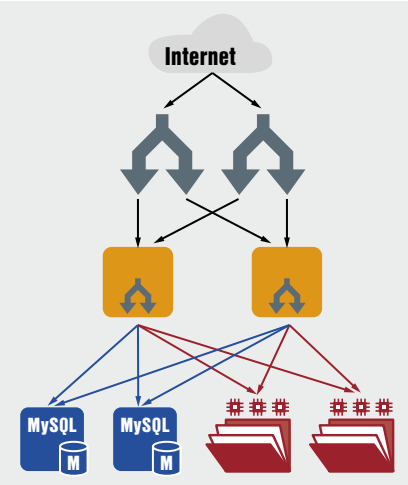
Minusem je bezpochyby cena. Kvalitní HA infrastrukturu z definice nelze udělat levně. Ve srovnání s non-HA se pohybujete ve 2–3 násobku ceny. Důvodem je podstata vysoké dostupnosti – máte okamžitě k dispozici výkon, který se hodí až v momentě, kdy vám selže některá komponenta.

V potaz je také potřeba vzít, že správa HA infrastruktury je mnohem složitější než péče o jeden server. Pokud chcete mít infrastrukturu připravenou téměř na vše, potřebujete load balancing a řadu dalších věcí. Proto se doporučuje nechat návrh i péči o HA infrastrukturu seniorním adminům ve vašem týmu, nebo zvolit poskytovatele, který má s vysokou dostupností mnohaleté zkušenosti.

Vysoká dostupnost tedy není pro všechny. Vždy je nutné spočítat cenu rizika – jak moc si nemůžete dovolit výpadek. Například na začátku podnikání, kdy máte desítky zákazníků, se vám taková investice pravděpodobně nevyplatí. A pro účely vývojového a testovacího prostředí je HA režim také většinou zbytečný. **Pokud vás hodinový výpadek produkce ale stojí desítky tisíc a ničí vaši rozjetou značku, vysoká dostupnost je pro vás jako dělaná.**

Na co si dát pozor

Většina debat o vysokodostupnostní infrastruktuře se točí primárně okolo samotného nastavení aplikačních a databázových serverů, load balancingu a redundantního storage. Aby vaše infrastruktura byla opravdu high availability, potřebujete také záložní připojení k síti. Přestože můžete mít skvělé zázemí a ostřílené adminy, kteří vám připraví všechny load balancery, aplikační a databázové servery, pokud do vaší serverovny vede jen jedno připojení k internetu, nejedná se zcela o HA infrastrukturu. Stačí totiž jeden neopatrný bagrista 100 km od vás, který kabel překopne. Totéž platí pro routery – spoléhat se jen na jeden je rizikové. Nejvyšší dostupnosti také nedosáhnete bez redundance elektrického napájení, která vaše servery dokáže udržet v provozu i v případě výpadku.



Asi už tušíte, že dosáhnout plně vysoké dostupnosti ve vlastní serverovně je velmi obtížné, a navíc extrémně drahé. Z tohoto důvodu většina firem takto komplexní infrastrukturu svěří zkušenému poskytovateli hostingových řešení, který má potřebné know-how i redundanci všech komponent. Například ve vshosting máme 4 nezávislé optické linky do internetu, zdvojené routery i energetickou soustavu a vysokodostupnostní infrastrukturu zajišťujeme i pro ty nejsložitější české projekty. ■

Ondřej Flídr

Autor článku je Senior Infrastructure Admin ve společnosti vshosting.

50 % firem nemá oddělený vývoj od produkce a riskují milionové ztráty

Firmy dávají klidně statisíce do marketingu, aby předehnaly konkurenci. Byly první. Ve vyhledávačích, v obratu… Platí agenturám, aby byly více vidět. Mají billboardy na nejfrekventovanějších a nejluxusnějších místech v centru Prahy, milionovou reklamu v televizi a plné sklady sezonního zboží. Teď si představte, že tohle všechno uděláte, zařídíte, vymyslíte. Máte pocit mírného natěšení z rostoucích objednávek. Pak si zadáte do prohlížeče URL adresu vašeho obchodu. A tam „Chyba 500: Služba není k dispozici."

Mnoho firem se soustředí na vysokou dostupnost infrastruktury, možnosti rychlého škálování a zabezpečení proti kyberútokům. Na jedno z nejdůležitějších opatření proti výpadkům ale často zapomínají.

Dle našich statistik je přes 95 % „spadnutí" webu způsobeno neodborným zásahem programátora. Protože více než 50 % firem v českém online prostředí nemá oddělené vývojové prostředí od toho produkčního. Každá chyba na produkci se přitom okamžitě projeví i z pohledu zákazníka.

Co to vlastně znamená? Proč je vývoj v produkčním prostředí tak nebezpečný? A jak celou infrastrukturu nejlépe nastavit tak, abyste eliminovali riziko? Sepsali jsme to nejdůležitější.

Vývojové vs. produkční prostředí

Vývojové prostředí má sloužit jen a pouze k vývoji a testování nového softwaru či nových funkcí. V tomto prostředí mohou vývojáři experimentovat bez obav, že by ohrozili produkci.

Produkční prostředí je naopak to, kde aplikace běží „naostro" – například e-shop, kde zákazníci vyhledávají a zkoumají produkty, dávají je do košíku a platí za objednávky. Produkce je jednoduše to, co je vidět pro běžného uživatele. Ale zároveň i všechny systémy v pozadí, které jsou pro funkci aplikace zásadní (databáze, skladové systémy atd.).

Hlavně: produkční prostředí je to, které vydělává. Proto by se kolem něj mělo chodit obloukem a ještě navíc po špičkách. Každý problém se tu totiž rapidně změní v ušlý zisk.

Rizika společné infrastruktury

Z vývoje spojeného s produkcí vstávají zkušeným administrátorům vlasy na hlavě. Pokud totiž svůj dev tým necháte dělat změny přímo na produkci, může se snadno stát, že ven pustí nedostatečně otestovaný software, který rozbije celou aplikaci. Výsledek? „Spadne" produkce.

Když budete mít dostatečnou smůlu, vaše aplikace nepojede několik hodin nebo způsobí řadu komplikací, jako třeba poškození databáze. Přeloženo do řeči peněz to může znamenat klidně i statisícové škody.

Obzvlášť bolestivé jsou tyto případy v době vysokého provozu na vašem webu. U e-shopů jde typicky o vánoční sezonu. Mnohé firmy přijdou za hodinový výpadek o desítky tisíc. V případě výrobních firem dochází k ještě větším škodám. Selhání interních systémů, na kterých je celý chod firmy závislý, znamená nefunkční skladovací systémy, CRM, účetnictví, prostě všechno.

Za 16 let fungování vshostingu jsme podobných situací viděli mnoho. Proto našim klientům doporučujeme, aby nový software tvořili a testovali jedině ve vývojovém prostředí, a teprve poté nasadili do produkce. Jedině tak se můžete vyhnout situaci, že si shodíte produkci v pátek večer těsně před Vánoci, protože programátoři na poslední chvíli spustili novou verzi aplikace, která nebyla pořádně otestovaná.

V rámci odděleného vývojového prostředí můžete bez rizika spouštět nové verze aplikace a každou dobře otestovat. Umožní vám také aktualizovat nové verze jednotlivých serverových komponent (databáze, PHP, apod.) a otestovat jejich kompatibilitu a funkčnost. Teprve až si budete jisti, že vše správně funguje, převedete vše do produkčního prostředí. Celkově si tak ušetříte mnoho komplikací i eliminujete riziko obrovských ztrát.

Jak oddělit vývoj a produkci: praktické tipy

Vývoj a produkci je třeba oddělit už na úrovni hostingového řešení. Vývojové prostředí by navíc mělo být zcela identické s tím produkčním. Nemůže se stát, že by na produkčních serverech běžela například jiná verze PHP než ta, která je na serveru pro vývoj.

Vývojové prostředí si často vytvářejí a spravují vývojáři sami. To vede k tomu, že vývojová infrastruktura se od té produkční dramaticky liší a navzdory otestování se nová verze aplikace na „ostré" infrastruktuře chová úplně jinak. Proto by vývojové prostředí mělo být zajišťováno stejným poskytovatelem hostingu, který spravuje i produkci.

Ve vshostingu vám rádi nezávazně poradíme s výběrem nejvhodnějšího řešení. Pomůžeme vám navrhnout vhodnou konfiguraci pro vaše vývojové a testovací prostředí tak, aby plně odráželo produkci a zároveň abyste zbytečně neplatili za výkon, který nepotřebujete. ■

vshosting

Vyzkoušeli jsme za vás profesionální 4K monitor AOC s chytrým připojením USB-C

-lg-

Společnost AOC nabízí širokou škálu monitorů pro různé způsoby využití od malých přenosných monitorů, z nichž jsme vám jeden představili minule, až po velké profesionální monitory určené pro náročnější uživatele. Právě pro ně nabízí AOC monitor U32P2CA, který jsem měl možnost krátce testovat.

Než se dostanu k jeho primárním vlastnostem, tedy kvalitě zobrazení, musím jako podstatnou přednost testovaného monitoru zmínit konektivitu USB-C pro možnost připojení jediným kabelem k notebookům, tabletům a mobilním zařízením, kdy je současně přenášen video-signál nebo data na připojené externí disky. Monitor je totiž vybaven 4portovým rozbočovačem USB 3.2, a splní tak částečně i funkci dokovací stanice. S připojenými periferiemi (klávesnice a myš) prostřednictvím USB rozbočovače lze ovládat notebook připojený přes USB-C. Navíc jsou připojená zařízení současně napájena (až 65 W).

Proč tyto možnosti zdůrazňuji hned na prvním místě? Flexibilita připojení monitoru je dnes totiž důležitější než kdy dříve. Mnoho profesionálních uživatelů je nyní zvyklých používat své notebooky k práci téměř odkudkoli. Jakmile je to ale možné, potřebují se rychle a snadno připojit k velkému monitoru. A právě to monitor U32P2CA nabízí – rychlé připojení a velkou pracovní plochu se špičkovou kvalitou obrazu. A monitor U32P2CA je opravdu velký. Jeho 32" VA panel s nativním rozlišením 4K (3840×2160) nabízí spoustu místa. Dokonce tolik, že jsem si na práci na tak velkém monitoru musel pár dnů zvykat. Velmi brzy jsem ale zjistil, jak velký displej s vysokým rozlišením přispívá ke zvýšení produktivity. Můžete totiž otevřít více oken a provádět více úkolů současně bez přepínání mezi aplikacemi na pozadí. Aby bylo možné co nejlépe využít velikost a rozlišení, monitor podporuje režim Picture-by-Picture (obraz vedle obrazu).

Když už je zmínka o obrazu, pojďme si říct něco o jeho kvalitě. Jedním slovem je výborná. Monitor U32P2CA má vysoký kontrastní poměr 3000:1 a jas 350 nitů, díky čemuž je použitelný i v jasně osvětlených místnostech. Nabízí nadprůměrně široké pokrytí gamutu (119% sRGB, 97,3% AdobeRGB, 90,7% DCI-P3) a je dodáván ve zkalibrovaném továrním nastavení. Na přiloženém protokolu si tak můžete zkontrolovat průměrnou barevnou odchylku a výsledky testu uniformity podsvícení. Ve své cenové kategorii nabízí U32P2CA opravdu hodně. Kvalita zobrazení uspokojí i náročné uživatele a limitující je pouze 8bitová barevná hloubka. Minimální odezva 4 ms a obnovovací frekvence 60 Hz jsou pro tento typ monitoru standardem. Nejde navíc o zásadní parametry, protože na hry se mnohem lépe hodí jiné monitory, ať už z nabídky AOC, nebo jiných značek.

Předností monitoru je i design s velmi úzkými rámečky po stranách, což kromě atraktivního vzhledu usnadňuje vytvoření konfigurace tvořené několika monitory.

Kromě konektivity a kvalitního displeje je pro monitor důležitý i flexibilní stojan, který umožňuje přizpůsobení polohy displeje do optimální výšky a sklonu, což stojan monitoru U32P2CA dokonale splňuje (nastavení výšky o 150 mm, otočení o ±180°, velkorysý rozsah naklonění a režim pivot). Snadno tak najdete nejpohodlnější a nejzdravější polohu. V rámci ochrany zdraví můžeme ještě zmínit funkce Flicker Free a Low Blue Light, které redukují únavu očí a přispívají tak k pohodlnější a produktivnější práci. Technologie AOC Flicker Free eliminuje blikání monitoru, což přispívá k menšímu zatížení zraku a menší únavě uživatele. Režim AOC Low Blue Light zase redukuje modrou složku vyzařovaného světla, což přispívá k většímu pohodlí uživatele při dlouhodobé práci nebo při použití monitoru v prostředí se slabým osvětlením nebo i ve tmě.

V době testování stál monitor AOC U32P2CA přibližně 11 500 Kč včetně daně, což z něj dělá velmi atraktivní volbu vzhledem k jeho velikosti, funkcím, parametrům a kvalitě. ■

IT Systems

Leden – Únor
Január – Február

PŘÍLOHA IT SECURITY 2022

Tradiční bezpečnostní přístupy
vám v cloudu příliš nepomůžou

Rizika ransomwaru
u tradičních metod ochrany dat

Zranitelný lidský faktor
umožňuje obejít i dvoufázové ověření

Nastal konec hesel,
jak je známe a není to špatně

Biometrická řešení
mohou řešit víc problémů najednou

Chcete zlepšit ve firmě bezpečnost?
Narazíte na neochotu zaměstnanců

PŘEHLED DODAVATELŮ ŘEŠENÍ INFORMAČNÍ BEZPEČNOSTI

Chcete zlepšit ve firmě bezpečnost?

Narazíte na neochotu zaměstnanců

-anect-

Jsou si vaši zaměstnanci vědomi bezpečnostních rizik? Staráte se pravidelně o jejich vzdělávání? Podnikáte řadu aktivních kroků, které mají pomoci zajistit počítače, mobilní zařízení i firemní sítě před útoky a hrozbami? Důležité je si uvědomit, že vzdělávání uživatelů je nedílnou součástí této ochrany. Na rozdíl od technických řešení není práce se zaměstnanci tak přímočará, a i přes veškerou snahu budou snahám o vzdělání odolávat ba mnohdy aktivně bojovat.

12 % zaměstnanců se v rámci aktuálního průzkumu společnosti Blue Fort Security vyjádřilo, že je nic nepřesvědčí, aby kybernetickou bezpečnost brali více vážně. Každý desátý člověk ve firmě vám tak bude připravovat při školení nepříjemná překvapení a neuděláte s tím vůbec nic. Se zbylou většinou to ale v praxi nebývá o nic lepší. Jak uvádí Petr Mojžíš, konzultant kybernetické bezpečnosti ve společnosti ANECT: *„proto je pro vzdělávání nutné hledat neustále nové cesty a motivace lidí. Ideální přitom je nevědomé vzdělávání či vzdělávání, které uplatní i v soukromém životě.* “ Tím se zvyšuje šance, že se člověk v kritický okamžik zachová přesně, jak má.

Zaměstnanci, ale i externí dodavatelé běžně a často sdílí hesla, stahují soubory z internetu, které nemají žádný vztah k jejich práci, stejně tak jako používají firemní zařízení pro osobní potřeby. Tyto nedostatky se o to výrazněji projevily v době pandemie a práce z domova, kde se k firemním počítačům i mobilním zařízením běžně dostávají další členové rodiny. Nechybí ani používání firemních zařízení v domácnostech bez povolení.

Vysoké riziko, zhruba u pětiny uživatelů, představuje i ztráta zařízení, kde se opět negativně podepsala právě práce z domova či na dálku. Oproti předchozím letům totiž daleko více pracujeme s notebooky a dalšími zařízeními z domova či mimo kanceláře. Problémem ve firmách je pak i nedostatek technologií a prostředků pro sledování zařízení lidí opouštějících firmu, jejich ochrana i postupy, jak řešit případné ztráty či napadení.

S pokračující pandemií, zvyšující se komplexností systémů a stoupající odbornosti útočníků je navíc velmi málo pravděpodobné, že by se snad situace mohla zlepšit. Nepřispívají tomu ani zjištění z nedávného výzkumu v USA, kdy se u pětiny firem příchodem pandemie zhoršil stav bezpečnosti.

Mnoho specialistů zastává postoj, že na uživatele nelze spoléhat vůbec, a vše je třeba řešit technickými opatřeními, která znemožní uživateli udělat chybu. Tak vznikají požadavky

na dlouhá složitá hesla, která je třeba často měnit, automatické odhlášení od počítače, kdykoli uživatel jen na minutu odejde, i mnohem složitější technické vychytávky. Firmy na druhou stranu potřebují, aby zaměstnanci měli především dostatečný prostor na práci. *„I sebe chytřejší bezpečnostní opatření je tak snadno smeteno ze stolu, pokud ve firmě neexistuje dostatečně silné uvědomění, co reálně hrozí. Vzdělávání je tak obecnou cestou k dosažení bezpečného prostředí nutnou, ať jsou zaváděna jakákoli opatření. Namísto zákazů je přitom třeba lidsky vysvětlovat i temnou stranu mince* “, dodává Petr Mojžíš.

Většina firem vstupuje do problematiky vzdělávání zaměstnanců v bezpečnosti s nějakým základním desaterem. Počet návyků, které by se měli lidé osvojit, je však mnohem více. *„A tak často proti dobře míněné snaze firmy stojí neochota zaměstnanců dodržovat bezpečnostní opatření a bezpečné chování. Faktor, se kterým při plánování musíte počítat, a budovat bezpečnost organizace ve více vrstvách tak, aby při narušení jedné vrstvy zafungovala vrstva další,* “ uzavírá Petr Mojžíš. ■

Kybernetické útoky jsou jednodušší než si myslíte

Filip Štěpánek

S rostoucí mírou digitalizace přibývá článků a diskuzí na téma kybernetické bezpečnosti. Pokud bychom se bavili s pracovníky zodpovědnými za bezpečnost podniku, tak bychom jejich zkušenosti mohli zařadit do dvou skupin – na ty, kteří s napadením mají již zkušenosti a snaží se na bezpečnostní hrozby reagovat, a na ty, kteří o napadení buď neví, nebo si jej nepřipouštějí.

Za vším stojí lidský faktor

Zkušenosti ukazují, že za většinou úspěšných útoků stojí lidský faktor, který poskytl informace anebo přístup útočníkovi. Pro představu se jedná třeba o otevření nebezpečné přílohy elektronické pošty, podlehnutí útoku na vrstvě sociálního inženýrství, případně může jít o bezpečnostní incident způsobený nedbalostí neboli porušením bezpečnostní politiky bez zlého úmyslu – příkladem jsou špatně chráněné či spravované přístupové údaje. Mezi bezpečnostní incidenty spojené s lidským faktorem patří i ty způsobené zaměstnanci. Ti se ze svých osobních důvodů mohou cítit nedoceněni nebo mají další pohnutky, proč způsobit škodu svému zaměstnavateli potažmo kolegům. I když poslední jmenovaný příklad bývá nejnebezpečnějším, stále zůstává nejčastější příčinou úspěšného útoku nepozornost nebo pohodlnost vlastních zaměstnanců.

Bezpečnostní politiku řada lidí vnímá jako tzv. „nutné zlo“, případně se s ní vůbec nemusí ztotožňovat. Bohužel toto vnímání obvykle platí nejen pro běžné zaměstnance/uživatele IT systémů, ale dokonce i pro jejich administrátory. Není proto překvapením, když se uživatelé snaží bezpečnostní opatření obcházet. Výsledkem je celkové snížení bezpečnosti systémů, ke kterým přistupují. Útočníci pak mohou využít situace a pomocí technik sociálního inženýrství cílit na zaměstnance a získat přístup do vnitřní sítě, který by za jiných okolností nebyl dostupný. Nejběžnějším způsobem bývá rozesílání škodlivých zpráv elektronickou poštou, vytipování a cílení obětí na sociálních sítích a rovněž vydávání se za zaměstnance technické podpory. Jinými slovy, útočník se snaží vystupovat jako důvěryhodný účastník komunikace, potažmo se často pokouší vyvolat nátlak a zmanipulovat oběť tak, aby provedla operaci či rozhodnutí, které by za normálních okolností neučinila. Konkrétně se může jednat o poskytnutí přístupových údajů, vyzrazení důvěrné anebo osobní informace o svém okolí, spuštění škodlivého kódu či neuvědomělé poskytnutí přístupu.

Jak se (ne)stát obětí

Nejčastěji uváděným příkladem útoku bývá tzv. „ransomware“ – v tomto případě se jedná o aplikaci škodlivého kódu, který je spuštěn jako škodlivá příloha elektronické pošty rozesílané útočníkem. Ransomware následně zašifruje obsah datového úložiště, čímž znemožní přístup k datům/používání počítače, dokud oběť nezaplatí výkupné útočníkovi. Popsaný problém se může týkat jak jednotlivých uživatelů, tak napadení celé podnikové sítě.

Vytipování oběti lze provést náhodně – útočník bez specifických parametrů rozešle škodlivé zprávy a pouze bude čekat, kdo z nepozornosti spustí přílohu. Anglicky se průběh popisuje jako „phishing“ – lidově lze termín vyložit jako „rybka která se chytí“. Tento útok může snadno cílit na domácí uživatele. Variantou je tzv. „spear-phishing“, kdy se útočník snaží využít osobní informace z okolí oběti s cílem působit důvěryhodně. Takováto činnost se provádí, jestliže se osoba dostane do zájmové oblasti útočníka, anebo pokud útočník cílí na vyšší zisk ze své činnosti. Nezřídka jsou takové útoky cílené na podnikové sítě.

V případě úspěšného útoku může dojít ze strany oběti k zatajení dané skutečnosti – u firemních zaměstnanců mohou být důvodem obavy z reakcí zaměstnavatele nebo domnělý pocit, že zaměstnanec danou situaci vyřeší sám. Skutečností však zůstává, že pokud došlo nebo mělo dojít k útoku, je potřeba situaci řešit konzultací s odborníky a ujistit se, že po útoku nehrozí či nepřetrvává žádné další nebezpečí – jak uživatelům, tak cíleným systémům.

Další skupinou uživatelů, kterou je třeba zmínit, jsou ti, kteří se stali cílem útoku a v podstatě o něm neví. Příkladem je oběť vytěžená útočníkem o důvěrné informace anebo uživatel, od kterého útočník přístup k důvěrným informacím získal (elektronická pošta, sociální sítě). Pokud by útočník cílil na firemní systémy a sítě, získává přirozeně dlouhodobou výhodu ve formě přístupu k citlivým informacím bez jakékoliv detekce.

Rada na závěr

Výše popsané problémy je možné řešit efektivně bez vynaložení značných finančních či technických prostředků. Klíčem jsou pravidelná školení, a především spolupráce a komunikace s uživateli. Obezřetní uživatelé, kteří nevnímají bezpečnostní mechanismy jako „komplikaci“, mají větší šanci předejít bezpečnostním incidentům.

Zároveň by se nemělo zapomínat, že i když je lidský faktor klíčem k zajištění kybernetické bezpečnosti, existují i další možnosti, které mohou posloužit útočníkovi k realizaci jeho cílů. Jedná se o SW/HW vybavení IT systémů a sítě, jejichž konfigurace a dohled je doménou odborníků. Pokud tyto nejsou efektivně navrženy a spravovány, může dojít k bezpečnostnímu incidentu technicky zdatným útočníkem bez účasti lidského faktoru. ■

Filip Štěpánek

Autor článku působí jako Security Architect ve společnosti Accenture.

Tradiční bezpečnostní přístupy vám v cloudu příliš nepomůžou

Stanislav Klubal

Cloudová řešení se oproti tradičnímu on-premise přístupu v mnohém liší. To, že tato řešení jsou vystavena za vnějším perimetrem vlastní in-house sítě provozované v rámci veřejného internetu, s sebou přináší řadu výhod, ale i nezanedbatelná bezpečnostní rizika.

Dnešní veřejné cloudové platformy nabízejí snadnou ovladatelnost a jednoduchou práci s cloudovými zdroji. Celkově umožňují podstatnou optimalizaci a úsporu nákladů na provoz, bez nutnosti pořizovat a spravovat vlastní hardware. Nižších nákladů je dosaženo sdílením zdrojů mezi mnoha zákazníky, kteří jsou softwarově izolováni. Takové řešení však nahrává agresorům, kteří mohou vést útoky vůči celé řadě cílů současně, případně zneužít nalezené zranitelnosti u více zákazníků, replikovat útoky na různých platformách a tak dále.

I když poskytovatelé cloudových služeb dělají pro bezpečnost svých řešení maximum, nemalý díl odpovědnosti připadá na koncového zákazníka. Problém je, že klienti bohužel ne vždy disponují dostatečným know-how a ne vždy využívají bezpečnostní konfigurační potenciál v plném rozsahu. Častěji se spokojí s výchozím nastavením, což se ukazuje jako nedostatečné a v některých případech přímo rizikové.

Většině rizik spojených s únikem dat v cloudu lze předcházet

Úniky dat se řadí mezi nejčastější hrozby v cloudovém prostředí. Podle DivvyCloud přišly firmy v roce 2019 jen v důsledku chybné konfigurace o více než 3,18 triliónů dolarů. Úniky dat jsou pro cloudová prostředí větší hrozbou než v případě in-house řešení, a to i z důvodu velkých přenosů dat mezi zaměstnanci a cloudovými systémy.

Většině rizik spojených s únikem dat v cloudu však lze předcházet. Každá firma by měla mít definovány obchodní hodnoty svých dat a dopady v případě jejich ztráty. Měla by mít propracovaný incident-response plán zohledňující podmínky dané poskytovatelem cloudu a zákony na ochranu osobních údajů. Jedním z nejúčinnějších a zároveň nejméně nákladných způsobů ochrany citlivých údajů je vhodná eliminace přístupu k nim a zároveň i jejich důsledné zálohování.

V případě napadení úložiště ransomwarem může reálně dojít ke ztrátě všech dat v důsledku jejich zašifrování a k požadování zaplacení nemalé částky za jejich opětovné dešifrování. Problémům s vydíráním společnosti útočníky lze předejít vytvořením distribuovaného backup systému. Data jsou v tomto případě zálohována ve více systémech a lokalitách tak, aby se zabránilo jejich ztrátě v rámci individuálního SAN (Storage Area Network) systému.

Zranitelná API představují přímé riziko

Bezpečnostní incident může vzniknout v důsledku celé řady pochybení. K naprosto běžným stále patří nedostatečná ochrana hesel a slabá politika nevynucující silná hesla. Opakují se chyby ve správě identit a přístupů nebo absence automatické a pravidelné rotace kryptografických klíčů a hesel.

Zanedbávají se hrozby spojené s tím, že se nevynucuje multifaktorová autentizace, podceňuje se nebezpečí sledování přenášených dat… I to sebedrobnější opomenutí nahrává útočníkům, kteří se mohou snadno vydávat za legitimní uživatele a ohrožovat celý firemní systém.

Řešením je striktní politika přístupu pro cloudové uživatele a identity – limitování přístupů je pro bezpečnost cloudového systému zásadní. Zaměstnanec by měl disponovat jen těmi přístupy, které potřebuje ke své práci. S tím mohou pomoci pravidelné audity zaměřené na úroveň přístupů zaměstnanců v rámci cloudového systému s cílem identifikovat ty nepotřebné a neopodstatněné a odstranit je.

Mnohdy jediným vstupním vektorem do jinak chráněné neveřejné části cloudového prostředí bývají Application Programming Interfaces (APIs) a User Interfaces (UIs). Vzhledem k tomu, že se starají o interakci s cloudovými systémy, patří pravděpodobně k jeho nejexponovanějším částem.

V čem je největší problém? Zranitelná API mohou představovat přímé bezpečnostní riziko s naprosto zřejmými dopady na důvěryhodnost firmy, její integritu a dostupnost. V minulosti jsme byli svědky celé řady reálných kauz spojených s chybami v zabezpečení API, například při ukládání hesel v čitelné podobě, přístupné tisícům zaměstnancům poskytovatele cloudových služeb (viz případy Facebooku, Googlu, Twitteru nebo GitHubu).

Útočníci se v cloudu zaměřují na privilegované účty

Jednou z relativně nových forem kybernetických útoků cílících na cloud je cryptojacking. Vzhledem k tomu, že neovlivňuje samotnou funkčnost služeb v cloudu, ale má vliv na zdroje, je obvykle hůře detekovatelný. Útočníci zneužijí cloudové prostředky k těžbě kryptoměn, což vede k vyšším nákladům na provoz, vyššímu vytížení zdrojů, a tím i ke zpomalení.

To může být mylně přisuzováno například nedávným updatům, pomalejší rychlosti internetové konektivity a dalším podobným procesům. Proto je třeba neustále monitorovat neobvyklé chování systému, jeho zpomalení nebo podezřelé zvyšování provozních nákladů.

Zcizení účtu, ať už zaměstnaneckého, či dokonce administrátorského, může útočníkům otevřít dveře k citlivým firemním informacím. Zákeřnost takového postupu tkví v tom, že v inkriminovanou dobu nemusí být vždy možné detekovat jakoukoli škodlivou aktivitu.

V cloudovém prostředí se útočníci zaměřují na vysoce privilegované, a tím pádem rizikové účty, jako jsou servisní cloudové

nebo subscription účty. Podle Cloud Security Alliance patří tento typ útoku mezi tři největší bezpečnostní rizika v cloudovém prostředí.

Rizikových faktorů je v případě útoku na účet celá řada a většina z nich není nijak překvapivá. Možnosti prolomení hesla nahrává především slabá politika hesel. Proto je tak důležité pravidelné školení zaměstnanců v oblasti bezpečnosti, především ohledně socialingu a phishingových útoků. Jde o náročný dlouhotrvající proces, který však svým významem pro bezpečnost firmy předčí řadu nákladných technologických opatření.

Bezpečnost systému mohou narušit i externí aplikace

Jak už jsme zdůraznili, vnější perimetr cloudového prostředí je přístupný – narozdíl od on-premise řešení – nejen zaměstnancům nebo zákazníkům, ale také případným útočníkům. Proto i chyby autorizace přístupu ke službám, aplikacím či datům a konfigurační chyby mohou pro útočníka znamenat volnou vstupenku do firemního cloudového prostředí. Z toho důvodu je třeba provádět pravidelné audity konfigurace nastavení cloudových služeb a penetrační testy vnějšího perimetru cloudové infrastruktury.

Jedním ze způsobů, jímž se agresoři mohou dostat do systému, je sběr a sdílení cloudových dat s útočníkem, a to bez vědomí vlastníka a za pomoci spywaru. Spyware pronikne dovnitř jako skrytá komponenta aplikačního vybavení instalovaného v cloudu nebo skrze jiné sofistikované metody. Na začátku tohoto procesu může figurovat klamavá reklama, webová stránka, e-mail nebo IM (instant messaging). Řešení v tomto případě spočívá především v monitorování přihlášení z neobvyklých lokalit, v neobvyklých časech a pravidelné vyhodnocování rizik instalovaných aplikací a autorizovaných zařízení.

Jakkoli může být bezpečnost cílového systému na vysoké úrovni, nasazení externí aplikace snadno přispěje k její výrazné degradaci. Služby třetích stran, mezi něž patří i aplikace, mohou představovat závažné bezpečnostní riziko, a proto by měl jejich nasazení předcházet pečlivý výběr a schvalovací proces. Stejně tak je bezpečnostním rizikem vystavení služby (například SQL serveru) bez patřičného zabezpečení a hardeningu.

Nebezpečí se týká především veřejně vystavených zranitelných či nedostatečně konfigurovaných služeb, jako jsou databáze, úložiště, služby pro vzdálenou správu apod. Hrozbě nahrává nedostatečná kontrola přístupů (IP white-list) i absence provádění pravidelných záplat. Vedle penetračních testů a pravidelné aplikace updatů a patchů lze problém řešit především pečlivým výběrem aplikací třetích stran a omezením přístupu pouze pro povolené IP rozsahy.

Více než čtyři z deseti útoků jsou vedeny zevnitř firem

Přesun z on-premise řešení, včetně zachování všech interních bezpečnostních IT kontrol, není vždy možné uskutečnit v poměru 1:1. Cloudové prostředí má svá specifika, nástroje a služby. Firemní prostředky vystavené v cloudovém prostředí mimo firemní síť, provozované na infrastruktuře, kterou navíc společnost ani nevlastní, s sebou přinášejí zcela nové výzvy.

Bezpečný návrh cloudové infrastruktury a strategie je absolutním základem pro úspěšný a bezpečný přesun do cloudového prostředí, včetně samotného nasazení softwaru a následného provozu v něm. Pro společnost je rozhodující nasazení správných bezpečnostních nástrojů, které zajišťují dostatečnou vizibilitu a umožňují monitoring cloud-based zdrojů a jejich ochranu před útoky a útočníky z veřejné sítě, včetně těch interních.

Hovoříme-li o útočnících, kteří naleznou slabinu v našem vnějším perimetru a snaží se dostat dovnitř s cílem ukrást data, často mylně předpokládáme, že útok musí být veden „zvenčí“. Realita je však jiná. Podle průzkumu společnosti McAfee stojí za 43 % všech úniků dat útoky zevnitř společnosti a většinou jsou prováděné samotnými zaměstnanci. Abychom to však neviděli úplně černě, nemusí jít vždy o úmysl; únik dat může jít i na vrub obyčejné lidské chyby.

Přesto je pro společnosti klíčové správné nastavení off-boarding procesu, protože nemalé množství společností je „hacknuto“ právě nespokojenými bývalými zaměstnanci v důsledku jejich „odplaty“. Tzv. „insideři“ obvykle nemusí složitě obcházet firewally, virtuální privátní sítě a další bezpečnostní ochranné prvky, ale mohou v rámci důvěryhodné úrovně zneužít svých přístupů k získání citlivých dat, a mít tak přímý přístup do sítí a počítačových systémů.

Kybernetický zločin je výdělečný byznys

Cloudová infrastruktura je vystavena ve veřejném internetu, na sdílené platformě pro více zákazníků. Smyslem takového řešení je především optimalizovat náklady. Vzhledem k tomu, že tato infrastruktura není vždy dokonale zabezpečena, stává se pro svůj citlivý a cenný obsah vyhledávaným cílem profesionálních skupin útočníků, kteří mají v úmyslu na datech profitovat.

Útočníci mají propracovaný systém, díky němuž mohou nalezené zranitelnosti opakovat vůči celé řadě dalších uživatelů. Výjimkou nejsou kybernetické útoky sponzorované cizími státy nebo konkurencí. Cílem může být exfiltrace citlivých dat, jejich zašifrování, krádež obchodních tajemství, jejich následné zveřejnění, prodej nebo vydírání oběti. Ani střední či malé firmy proto dnes nesmí podceňovat ochranu proti DoS/DDoS útokům, nemluvě o pravidelně prováděných bezpečnostních auditech a penetračních testech.

Je-li společnost zcela závislá na cloudovém prostředí a provozuje-li v cloudu business-critical data nebo důležité interní či zákaznické aplikace, může ji útok cílící na odepření služby zcela ochromit. Při tomto typu útoku agresoři zahltí cílové systémy velkým množstvím webového provozu, který není možné kapacitně obsloužit, což vede k nedostupnosti služeb, a to nejen pro klienty, ale i pro samotné zaměstnance či obchodní partnery.

Bezpečnost máme stále ve svých rukách

Cílem tohoto textu nebylo podat kompletní výčet hrozeb v cloudovém prostředí a jejich řešení, jde spíše o nástin rizik typických právě pro cloud. To, zda budou zákazníci spoléhat na bezpečnost výchozí konfigurace cloudových služeb nebo dají přednost hardeningu konfigurace, je čistě jejich rozhodnutí.

Jedno je však jisté. Váhy odpovědnosti za určité oblasti se oproti klasickému on-premise řešení při nasazení v public cloudu výrazně liší. Pozitivním zjištěním je, že celá řada oblastí a jejich bezpečnost zůstává v našich rukách. Abychom je mohli chránit efektivně, musíme především vědět, proti čemu vlastně stojíme a bojujeme. ■

Stanislav Klubal

Autor článku je Senior Cyber Security Specialist ve společnosti AEC a.s.

Moderní kyberbezpečnostní software **ochrání data i před záškodníkem uvnitř firmy**

Richard Brulík

Se všudypřítomnou digitalizací a rozšířenou prací na dálku (ať už ve formě hybridního nebo full-remote pracovního režimu) je kyberbezpečnost ve firmách důležitější, než kdy předtím. Únik citlivých firemních dat, jako jsou interní finanční údaje, osobní údaje zaměstnanců anebo zákazníků, duševní vlastnictví nebo budoucí produktové plány, může pro firmy znamenat někdy až fatální následky.

Zneužití údajů konkurencí pro získání konkurenční výhody, přetažení zákazníků a zaměstnanců, pokuta od státu za nedostatečnou ochranu osobních údajů nebo nesprávné účetnictví mohou, a v minulosti už se to také mnohokrát stalo, firmu úplně položit. Nejhůř přitom úniky dat dopadají paradoxně na ty nejmenší firmy a podnikatele, kteří na rozdíl od velkých korporací nemají dostatečné zázemí a prostředky na to, aby ho ustály.

Insideři jsou hlavní příčinou úniků dat, často neúmyslně

Významný potenciál pro únik dat představují interní lidé z firmy – zaměstnanci, dodavatelé – tzv. insideři. S rozvojem digitalizace se jimi způsobený počet úniků zvyšuje. Pandemie a masový přesun zaměstnanců na práci z domova tento trend ještě významně urychlila. Podle zprávy 2021 Data Exposure Report od Code42 a Ponemon Institute pravděpodobnost úniku souborů způsobeného zaměstnancem vzrostla během pandemie o 85 %. Podle další zprávy, Insider Data Breach Survey 2021 od Egress, v roce 2020 94 % organizací zažilo únik dat způsobený zaměstnancem.

Při narušení bezpečnosti zaměstnancem nejde ve většině případů o zlý úmysl, ale o nedbalost. Podle zprávy 2022 Cost of Insider Threats Global Report od Ponemon Insitute jde o 56 % případů úniků způsobených insiderem. Zpravidla se jedná o nedodržení interních pravidel při nakládání s daty, obcházení firemních nástrojů při přenosu dat skrze služby třetích stran, neodstranění firemních dat po odchodu z firmy, ztrátu zařízení s údaji nebo kvůli podlehnutí phishingu.

Nicméně větší vrásky na čele firmám dělají insideři se zlým úmyslem, kteří záměrně chtějí data z firmy vynést a způsobit jí tím škodu. Důvody mohou být četné – msta nespokojeného zaměstnance, naštvání po výpovědi, finanční incentiva zvenčí. Poslední dobou se rozmáhají podvodníci, kteří získají a zneužijí přístupy nějakého insidera. Podle Ponemon Institute stojí insideři se zlým úmyslem za 26 % případů úniků dat, podvodníci figurují v 18 % případů – jejich počet se však za poslední rok zdvojnásobil.

Na rozdíl od neúmyslného úniku, kdy data v řadě případů nemusí způsobit žádný větší problém, u zlého úmyslu je způsobení škody přímým záměrem. To reflektují průměrné náklady vynaložené na vypořádání se s následky úniku (vyšetřování, opravy bezpečnostních chyb, pokuty…). Zatímco u nedbalého zaměstnance vyjde jeden únik průměrně na zhruba 10,5 milionu korun, u zlého úmyslu už to je 14 milionů. Podvodníci s ukradenými přístupy jsou však s přehledem nejnákladnější – firmy v průměru stojí 17,5 milionu na únik.

Zabránit únikům lze, je však potřeba k problému přistupovat komplexně

Ochranu firemních dat je nutné řešit na několika úrovních – procesní, lidské a technologické. Každá firma, bez ohledu na její velikost, by měla mít nastavené jasné postupy, jak s firemními daty nakládat, jakým způsobem si je předávat, jak postupovat v případě úniku. Klíčová je také informovanost zaměstnanců o tom, proč data chránit, co firmě a zaměstnancům hrozí při úniku. Pravidelná školení o nakládání s daty by proto měla být základem.

Z technologického pohledu existuje určité nutné minimum, které by každá firma měla implementovat a jenž zároveň nepředstavuje žádné výrazné investice. Jedná se o poměrně jednoduché zásady jako je dvoufázové ověřování přístupu k firemním systémům (e-mail, sdílené úložiště atp.), používání silných hesel, využívání šifrovaných fyzických úložišť, nevyužívání neschválených služeb třetích stran, neotevírání podezřelých e-mailů a zkrátka pozorný a opatrný přístup k firemním datům. To všechno stojí minimální náklady a může významně pomoci efektivní ochraně.

Moderní bezpečnostní software dokáže rizika identifikovat dny až týdny dopředu

Pro skutečně solidní zajištění dat se dnes firmy jen stěží obejdou bez bezpečnostního softwaru. Zde dlouho vládl přístup prevence úniku dat (DLP). Ten spočívá v nastavení pasivních tvrdých překážek, např. povolování přístupů nebo omezování možností sdílení. DLP si bohužel získalo trochu negativní pověst – mnoho systémů bylo nákladných, složitých na implementaci, náročných na hardware a příliš mnoho omezovalo práci zaměstnanců, kteří potřebovali větší flexibilitu.

Dnes už to není realitou. V posledních letech se kyberbezpečnost výrazně mění, a to právě v reakci na velký nárůst vnitřních hrozeb. Bezpečnostní software nové generace kombinuje pasivní přístup tradičního DLP s novými aktivními funkcionalitami, které v Safetica označujeme jako ITP – prevenci před vnitřními hrozbami. Ty aktivně hlídají činnost uživatele a neustále vyhodnocují riziko pro data, se kterými pracuje. Například zaznamená vybočování ze vzorců chování, podezřelé přesuny souborů, přistupování k neobvyklým informacím nebo podezřelé časy a místa přístupu k souborům.

Moderní ITP si můžeme představit jako na vrtulník, který z výšky sleduje, jak podezřelé kradené auto z jiného státu krouží kolem zlatnictví a mapuje okolí. ITP v tu chvíli pošle k autu hlídku, která potenciální nebezpečí zastaví. Pokud by však i přesto došlo k realizaci pokusu o vyloupení zlatnictví, narazí zloději na připravené pevné zátarasy DLP, které loupež překazí nebo výrazně zkomplikují. ITP dokáže podezřelé chování identifikovat hodiny až týdny předtím, než dojde k samotnému úniku dat. Poskytuje tak daleko více času k eliminaci rizika. DLP funkcionality jsou pak tou poslední tvrdou bariérou, která může únik zastavit.

Z dat Ponemon Institute přitom vyplývá, že čím dříve se únik podaří zastavit, tím méně firmu stojí. V průměru přitom firmám po začátku úniku trvá 85 dní ho zastavit nebo zabránit následkům. Toto číslo oproti předchozímu roku vzrostlo, což jde ruku v ruce s častějšími incidenty.

Bezpečnost versus pohodlí

Preventivní omezení nakládání se soubory přirozeně mohou být otravná, protože mohou snižovat rychlost práce kladením překážek i v případech, kdy to není nutné. A lidé jsou jenom lidé, takže přirozeně hledají nejsnazší a nejrychlejší cestu, jak práci dokončit. Proto je možné, že než aby se zaměstnanec snažil půl hodiny přesvědčovat firemní sdílené úložiště, že opravdu chce sdílet soubory s někým mimo firmu (například s dodavatelem nebo klientem), rozhodne se prostě systém obejít a poslat jim to přes Ulož.to nebo Messenger. Pohodlné? Rozhodně. Rizikové? Velice.

Kromě opatření, školení a bezpečnostního softwaru nesmějí firmy zapomenout ani na lidský faktor. Proč lidé obcházejí bezpečnostní opatření? Co můžeme změnit, aby to napomohlo zodpovědnějšímu chování? To jsou otázky, které si bohužel mnoho firem při nastavování ochrany dat neklade. Aby zaměstnanci dodržovali opatření, je potřeba jim nejprve dát vhodné nástroje k práci. Zároveň je vše nutné přizpůsobit činnosti firmy. Něco jiného se hodí pro agenturu, která každodenně posílá stovky souborů desítkám klientů, něco jiného pro výrobce produktů, který potřebuje hlídat své výrobní tajemství a není důvod posílat z firmy něco jiného než faktury a objednávky.

S postupem technologií také klesá náročnost a nákladnost bezpečnostního softwaru. Kyberbezpečnostní firmy začínají spouštět nové SaaS produkty. Ty běží na cloudu, představují minimální zátěž pro koncové zařízení a neotravují uživatele ani administrátory s aktualizacemi. Navíc jsou hrazeny na bázi pravidelného předplatného a ne jako jednorázová investice. Výrazně se tak rozšiřuje jejich využitelnost a zároveň se zvyšuje jejich finanční dostupnost i k těm nejmenším podnikům. Nicméně ani on-premise řešení pro větší firmy, které chtějí mít software na svých interních serverech, nezůstávají pozadu a trendem je co nejvíce minimalizovat jejich dopady na efektivitu práce.

K ochraně dat je nutné přistupovat s ohledem na zaměstnance

Počty případů úniků dat budou s postupující digitalizací ve světě postaveném na sběru dat pravděpodobně růst i nadále. Firmy však mají možnost velké části z nich zabránit, konkrétně 56 %. Jestliže jsou firemní opatření příliš komplikovaná a zaměstnanci nacházejí efektivnější řešení problémů mimo firmou schválené nástroje, nelze se divit, že data utíkají. Firmy musí vycházet vstříc potřebám zaměstnanců ve volbě používaných nástrojů a nastavovaných opatření.

Pokud budou firmy dodržovat minimální technologické standardy, zaměstnanci jsou proškolení a umí efektivně používat vhodné pracovní nástroje, a to všechno je zastřešeno moderním bezpečnostním softwarem, který aktivně vyhledává potenciální hrozby i u insiderů se zlým úmyslem, pak se jim podaří výrazně eliminovat riziko úniku a spojených nákladů. ■

Richard Brulík

Autor článku je CEO společnosti Safetica.

Biometrická řešení mohou řešit víc problémů najednou

Martin Vápeník

S nástupem pandemie se biometrie rychle stala technologií, ve které organizace spatřily způsob, jak vyřešit víc problémů najednou. Pryč jsou doby, kdy byly obdobné systémy vnímány spíše jako technologické bonbónky. Nástup covid-19 změnil tyto technologie na životně důležité a kdo je využíval, dokázal pokračovat například v získávání nových klientů. Díky biometrii mohly banky, které musely v časech lockdownů zavřít pobočky, pokračovat v získávání klientů a poskytování úvěrů na dálku přes obrazovku smartphonů, a to při dodržení všech regulatorních požadavků. Ostatní většinou pouze sledovali odliv zákazníků ke konkurenci.

Jinde začala biometrie plnit úkol bezdotykového vrátného. Systémy tvářové biometrie se rychle uzpůsobily nové realitě a dovedly rozeznávat tváře zaměstnanců či klientů i přes respirátory. Letiště a další místa, kde se musí shromažďovat větší počet lidí, pochopila, že s biometrií dokáží fungovat lépe, rychleji a bez toho, aby vznikla místa, kde je příliš mnoho lidí najednou. A také bez zbytečných doteků, přes které se může nekontrolovaně šířit nákaza.

Zralá technologie a covid jako akcelerátor

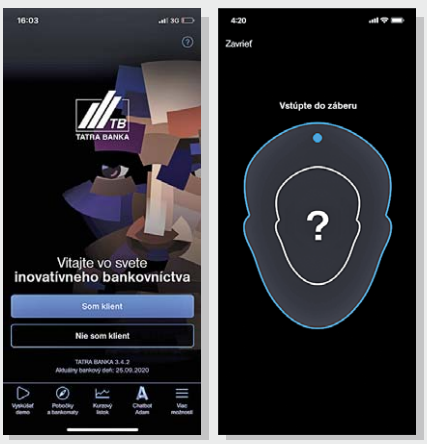
Rychlý nástup biometrie do nových odvětví v roce 2020 byl souhrou více okolností. Přesnost a rychlost technologie rostla už několik let raketovým tempem. Podle přepočtů amerického vládního institutu NIST, který dělá standardizovaná srovnání biometrických algoritmů, vzrostla přesnost tvářové biometrie jen mezi lety 2014 až 2018 dvacetinásobně. K dalšímu růstu ještě pomohla dostupnost stále silnějších grafických karet. Grafické procesory se velice dobře hodí – kromě hraní počítačových her nebo těžby kryptoměn – také na zpracování obrazu a trénování umělé inteligence, přesněji složitých neuronových sítí. Ty jsou dnes základem všech algoritmů tvářové biometrie.

Velkou výhodou také bylo, že běžný uživatel byl již zvyklý na využívání biometrických prvků. Lidé od spuštění FaceID na iPhonech objevili pohodlí odemykání smartfonů vlastní tváří nebo otiskem prstu. Využití v jiných prostředích, včetně tak citlivé oblasti jako osobní finance, proto bylo i pro běžného uživatele samozřejmostí. Pokrokové firmy jako třeba Home Credit, který na dálku poskytuje úvěry například ve Vietnamu nebo na Filipínách, vsadily na biometrii jako prostředek efektivního získávání klientů na dálku už dlouho před pandemií. Ostatní, kteří měli obavy, jestli je technologie dostatečně zralá a bezpečná, to zjistili teprve nedávno pod tíhou bezprecedentní situace.

Další algoritmy na pomoc

Kromě samotné přesnosti tvářových algoritmů – ty otiskové už dlouho dosahují téměř stoprocentní přesnosti – přibývaly i další technologie nezbytné k ověřování identity na dálku. Tou jednodušší částí je automatizovaná kontrola dat z identifikačních dokladů v registru obyvatel. Dnešní aplikace dokáží přesně přečíst jakýkoli doklad a jeho data porovnat s databází ministerstva vnitra. Zatímco v Česku zákony tento přístup neumožňují, na Slovensku to možné je. Porovnání v kombinaci s tvářovou biometrií vyloučí jakoukoliv snahu o zneužití kradeného nebo zfalšovaného dokladu. Druhou, technicky komplikovanější součástí, je ověření živosti koncového zákazníka. Základní přístup – videohovor s call centrem banky – má hned několik nevýhod. Je omezen kapacitou centra, ale hlavně narušuje

Biometrii využívá ve své mobilní aplikaci i slovenská Tatra banka.



plynulost celého procesu. Při dálkovém otevírání účtů s povinným videohovorem nedokončí proces 70 až 90 procent zákazníků.

Automatizovné algoritmy, které například generují náhodně se pohybující tečku na obrazovce a sledují pohyb očí, redukují toto procento zhruba na polovinu. Díky pokroku v AI je ale možné už dnes posoudit živost i z jediného selfíčka – tyto procesy už dokončí prakticky každý, jejich úspěšnost je více než 99 procent. Pro provozovatele takového systému je to skvělá zpráva, protože dokáže velice rychle, zhruba do jedné minuty, proměnit každého zájemce na zákazníka. A to při splnění všech regulatorních nařízení a bez zvýšené míry rizika.

Další sektory chtějí klienty na dálku

Bankovnictví ale není jediným odvětvím, které pochopilo význam biometrie pro získávání klientů. Mobilní operátoři rovněž umí ověřit identitu na dálku a poslat novému klientovi SIM kartu kurýrem bez potřeby budování poboček. Loni tak začal budovat svou klientskou bázi virtuální operátor Radost na Slovensku nebo Vodafone v Ománu. A i kurýr je v tomto modelu jen dočasným řešením – nástupem eSIM smartphonů bude možné poslat elektronickou SIM kartu přímo do telefonu a poskytovat tak služby okamžitě pár minut po registraci.

Firmy sdílené ekonomiky si takto na dálku zvládají ověřovat identitu svých klientů i poskytovatelů služeb. Taxislužba Careem v Dubaji například díky ověření přes mobil dokáže zkontrolovat, jestli vůz řídí licencovaný řidič, a ne některý z jeho přátel. Rychlý pohled na tablet vybavený biometrickou identifikací umí říct kontrole, jestli v autobuse s dělníky sedí pouze lidé, kteří tam opravdu patří. Smart budovy zase využívají rozpoznávání tváře nejen na otevírání turniketů, ale také na automatické přivolávání výtahů na správné podlaží nebo zpřístupnění pouze těch kanceláří, do kterých má zaměstnanec oprávnění vstoupit. To vše bez potřeby zavádění čipových karet a řešení situací, kdy je lidé ztratí či zapomenou doma. Návštěvníky je možné registrovat a přidělit jim vstupní oprávnění jednoduše ofocením tváře a klikem v databázi. Mnoho firem přichází za poskytovately biometrických řešení s vlastními nápady na využití technologie pro zlevnění a zjednodušení vlastního provozu – a málokdy odchází s prázdnou.

Začaly to vlády

Donedávna přitom byly biometrické technologie zejména doménou vlád, i tam ale nové technologie rozšiřují možnosti uplatnění. Indonésie například provozuje druhý největší biometrický systém na světě, který dokáže identifikovat lidi i přes mobilní zařízení na sběr otisků prstů. Výrazně zkrátil čas při identifikaci tisíců obětí tsunami před pár lety. V západoafrické Guinei pomohla biometrie při organizování voleb. Zaručila nejen to, že každý člověk měl pouze jeden hlas (podvody s vícenásobnou registrací bývají časté), ale dala také volební právo lidem bez dokladů. Pokročilé algoritmy na určování věku zabezpečily, že z databáze byly vyřazeny děti do 18 let, které se využívají na volební podvody. Po dobrých zkušenostech z voleb začala využívat vlastní biometrický systém také guinejská policie, která tak přešla z papírové identifikace otisků prstů na počítačovou a otevře tak rychlou identifikaci nejen pro hrstku odborníků v hlavním městě Conakry, ale pro všechny policisty v zemi.

Boom v biometrii jako prostor pro nová řešení

Stále dynamičtěji rostoucí poptávka po biometrických řešeních v různých oblastech a odvětvích dala v Praze vzniknout inkubátoru Biometric Ventures, jehož cílem je identifikovat inovativní nápady pro využití biometrické technologie. Dodá odbornost a spolehlivé algoritmy, což může vyústit v další globální řešení, která se mohou rozvíjet zcela nezávisle. Přihlásit se může kdokoli s dobrým nápadem, zkušený tým mu pomůže s vyhodnocením a realizací.

Na světě jsou již první dvě řešení. Jedním z nich je automatické ověření skutečného věku podle tváře pomocí selfie nebo krátkého videa, využitelné například při koupi alkoholu nebo vstupu na weby s omezením věku, což chrání děti a mladistvé před nevhodným obsahem.

Druhým je řešení pro oblast péče o seniory. Algoritmy pomohou nejen s otevíráním dveří, ale rozeznají také polohu lidí a jejich těl. Pokud někdo leží delší dobu než je obvyklé nebo náhle spadne, systém dokáže okamžitě upozornit personál a tím zajistit pomoc. V současnosti je ve vývoji systém prevence pádů formou automatického vyhodnocení předcházejícího chování, jako je vstávání z postele nebo chůze bez chodítka, čímž by bylo možné na hrozící pád upozornit ještě předtím, než k němu dojde. ■

V západoafrické Guinei pomohla biometrie při organizování voleb.

Martin Vápeník

Autor článku je CEO společnosti Biometric Ventures.

Nastal konec hesel, jak je známe

Přihlašovacím heslům pomalu zvoní umíráček, ale není to špatně

Petr Zajíček

Představte si, že je říjen 2050 a školní třída v rámci Měsíce kybernetické bezpečnosti navštívila místní muzeum. Jeden z žáků zírá na podivný shluk písmen, symbolů a čísel a ptá se učitele: „Co je to?“ „To je heslo,“ odpoví učitel. „Tvoji rodiče hesla užívali k přístupu ke svým zařízením a aplikacím. Ale už neexistují.“ Zanikla hesla? Jak k tomu došlo? Odpověď je jednoduchá: biometrie a digitální certifikáty.

Nepředbíhejme ale příliš. Vraťme se raději do roku 2022. Už dnes ale čelíme problémům s hesly. Příliš mnoho hesel je na obtíž – nemluvě o vymýšlení a pamatování silných hesel splňujících specifické požadavky. Podle studie „Biometric Usage Study“ společnosti Dell Technologies považuje 62 % pracovníků v USA vymýšlení, pamatování a pravidelnou obměnu hesel za obtěžující. Jiná celosvětová studie Dell Technologies „Brain on Tech“ zjistila, že když bylo uživatelům předloženo dlouhé a obtížné heslo pro přístup k počítači a měli ho zadat pod časovým tlakem, jejich stres během pěti sekund zesílil o 31 % a nadále rostl, a to i po úspěšném přihlášení.

Tyto výsledky potvrzují, že pro většinu z nás není dobrá praxe užívání hesel prioritou, ale naopak nepříjemnou nutností. Mnoho z nás dělá přesně to, co nám bylo řečeno, abychom nedělali – opakovaně používá stejné heslo, volí slabá hesla nebo si je poznamenává na lepicí štítek na okraji monitoru. Pro zvýšení bezpečnosti zaměstnavatelé obvykle od zaměstnanců vyžadují, aby dodržovali minimální požadavky na sílu hesel a pravidelně je obměňovali. To však zaměstnancům nebrání v chování, kterým kvůli svému pohodlí bezpečnost naopak ohrožují.

Takové chování se však netýká pouze pracujících dospělých. Nedávný průzkum NIST zkoumal znalosti problematiky hesel a způsoby jejich užívání mezi americkými studenty základních a středních škol. Ukázal, že žáci základních škol se učí a chápou správné postupy týkající se hesel, avšak v praxi se jimi mnohdy neřídí. Ve věku dospívání mnozí začnou hesla sdílet s ostatními, aby si vybudovali přátelství a důvěru. Pokud tedy většina lidí chápe důležitost správné hygieny hesel, ale nikdo se necítí povinen ji praktikovat, kam to povede?

Biometrie nastupuje

Myšlenka použití biometrie k identifikaci jedince je stará stovky let. Existují důkazy, že otisky prstů byly používány jako stopa konkrétní osoby již v roce 500 před naším letopočtem. A biometrické technologie existují již několik desítek let. V zařízeních koncových uživatelů se tato technologie nicméně začala objevovat teprve počátkem 21. století. Dnes už je většina lidí obeznámena s používáním biometrie k odemykání svých zařízení a aplikací. Když jsme před několika lety poprvé viděli, jak lidé odemykají své chytré telefony pouhým pohledem, považovali jsme to za žhavou novinku. Nyní se to stalo samozřejmostí.

S rostoucí oblibou biometrie jako pohodlného a bezpečného způsobu automatického rozpoznávání uživatelů bude tradiční heslo pro spotřebitele i podniky mnohem méně atraktivní variantou. Biometrické technologie se navíc neustále vyvíjí díky zdokonalování snímačů a využití rozpoznávacích algoritmů založených na umělé inteligenci. Výsledkem je lepší uživatelská zkušenost a zároveň zlepšení modelu zabezpečení.

Pokročilé funkce zabezpečení zařízení, jako jsou čtečky otisků prstů nebo rozpoznávání obličeje, jsou nyní běžně dostupné i na firemních noteboocích střední třídy. Užívají se jako součást vícefaktorového ověřování, které uživatelům nabízí bezpečnější způsoby přístupu k jejich zařízením, aplikacím a datům než snadno prolomitelná hesla. Již zmiňovaný výzkum Biometrics Usage Study zjistil, že v amerických firmách, kde jsou k dispozici počítače s biometrickým zabezpečením,

přibližně 80 % zaměstnanců uvádí, že tuto funkci používají, a 64 % zaměstnanců, kteří ji k dispozici v současnosti nemají, uvedlo, že by ji užívali, pokud by tu možnost měli. Není to jen z pohodlnosti – pracovníci také věří, že by tyto funkce mohly pomoci udržet firemní data v bezpečí. A u správců IT to zase zvyšuje důvěru, že zařízení a uživatelé v jejich síti jsou autentičtí.

Možná se ptáte, proč je biometrie bezpečnější než hesla. Hesla jsou řetězce znaků, které webová stránka nebo služba ověří a umožní uživateli přístup. Silná hesla jsou navržena tak, aby bylo obtížné je uhodnout nebo replikovat, ale i ta nejsložitější hesla mohou být odcizena nebo prozrazena. Ke kontrole identity uživatelů se stále častěji vyžaduje vícefaktorové ověření. Biometrie při něm hraje klíčovou roli jako nejobtížněji replikovatelný faktor ze tří možných: něco, co znáte (vaše heslo/PIN), něco, co máte (vaše zařízení nebo bezpečnostní token) a něco, co jste vy (otisk prstu nebo tvář). Spojení autentizace s biometrickou shodou uživatele představuje pro kyberzločince nejobtížnější prolomitelnou metodu. Po provedení místní autentizace je uvolněn zabezpečený digitální certifikát pro webovou stránku nebo službu k autorizaci uživatele.

Vzhledem k obecné ochotě zaměstnanců využívat biometrické bezpečnostní funkce na počítačích se nabízí reálná příležitost k dalšímu zavádění biometrických prvků, zejména s nástupem generace Z do pracovního procesu. Tato generace vyrostla s digitálními technologiemi a je zvyklá užívat čtečky otisků prstů nebo rozpoznávání obličeje na svých chytrých telefonech. Pravděpodobně by jí nikterak nevadilo užívat tytéž technologie na počítačích a dalších zařízeních. Nastal čas, aby firmy přehodnotily, jak zajišťují zabezpečení na zařízeních svých zaměstnanců, a při dalším cyklu obměny počítačů zvážily zavedení biometrie.

Do té doby

Ještě nějakou dobu potrvá, než se hesla nadobro stanou minulostí. Ale s postupným zdokonalováním a rozšiřováním biometrických technologií je jen otázkou času, kdy budeme moci blaženě zapomenout na komplikované kombinace znaků, aniž bychom tím ohrozili bezpečnost. Do té doby existují jednoduché způsoby, jak každý z nás může jít na kyberbezpečnost chytře a svá data chránit, aniž se musel přespříliš stresovat hesly:

- Používejte správce hesel k vytvoření silných kombinací a jejich uchovávání na bezpečném místě.
- Využívejte vícefaktorové ověřování a digitální certifikáty k ověřování identity a bezpečné komunikaci.

Každý říjen v rámci Měsíce kybernetické bezpečnosti se zamýšlíme nad uplynulým rokem v oblasti kybernetické bezpečnosti, oslavujeme úspěchy, učíme se ze zkušeností a hledíme do budoucnosti. Technologie stále více pronikají do našich každodenních životů. To vytváří živnou půdu pro podvratné živly. Než nastane budoucnosti bez hesel, je na každém z nás, abychom šli na kyberbezpečnost chytře. ■

Petr Zajíček

Autor článku je Client Solution Field Product Manager ve společnosti Dell Technologies.

Tři tipy pro prevenci narušení v rámci řízeného přenosu souborů (MFT)

Mark Towler

Nedávno jsem mluvil s jedním klientem a diskutovali jsme o důležitosti zabezpečení dat v jejich řešení pro řízení přenos souborů (Managed File Transfer, MFT). Řekl něco, co mi utkvělo v paměti: „My víme, že jsme paranoidní. Ale jsme dostatečně paranoidní?“ Nad tím je třeba se pozastavit, protože to nejen odhaluje obavy uživatelů MFT ohledně bezpečnosti, ale také to, odkud vycházejí. Všichni se shodneme, že bezpečnost stojí na prvním místě. Můžeme si však být jisti, že je dostatečně bezpečná? Odpověď je vlastně docela jednoduchá: jakou úroveň bezpečnosti skutečně potřebujeme?

Každá organizace má vlastní, jedinečné požadavky na bezpečnost. V ideálním případě to bude to nejlepší možné zabezpečení. V reálném světě to tak ale nefunguje. A to kvůli faktorům, které je potřeba brát taky v potaz – jako jsou náklady, pohodlí uživatelů či obecná neznalost možných zranitelností. Klíčem pro každou organizaci je proto zjistit, jakou úroveň bezpečnosti potřebuje, jakou si může reálně dovolit a jakou budou uživatelé ještě tolerovat. Proto neexistuje jedno univerzální řešení otázky bezpečnosti MFT.

Je potřeba mít ale možnost volby. Všechny MFT systémy využívají při přenosu souboru šifrování, ale ne všechny budou tyto soubory šifrovat i v klidovém stavu (alespoň ne bez příplatku). Některé umožňují nastavit, zda šifrovat či nikoli – což paradoxně neznamená menší úroveň bezpečnost. Pokud například využíváte pro ukládání dat MS Azure Blob, jsou tato data šifrována automaticky ze strany Microsoftu. To se ale nemusí líbit zase někomu jinému nemluvě o tom, že nemusí důvěřovat ani tomuto šifrování.

Dalšímu zase může vadit snížený výkon způsobený opětovným šifrováním a dešifrováním těchto dat při každém přístupu k nim (což je významný problém, pokud se jedná o stovky přenosů denně). Totéž platí pro řadu dalších bezpečnostních funkcí, jako je obnovení

hesla na základě bezpečnostních otázek nebo vícefaktorové ověřování (MFA). Mohou třeba fungovat pro vás, ale také nemusí. Pokud ale řešení MFT nenabízí možnost volby, pak nebude vyhovovat ani specifickým bezpečnostním požadavkům, které na něj budete klást.

Je důležité se zaměřit hlavně na funkce, které vám za vaše peníze nabídnout maximum z bezpečnosti. Tyto tři funkce jsou z mého pohledu ty nejdůležitější, které byste měli implementovat, abyste předešli bezpečnostním incidentům.

1. Důkaz o neoprávněném vniknutí

Pokud se na vás vztahují předpisy jako HIPAA, GDPR, CCP, SOX, PCI-DSS nebo jiné, není to vlastně volba, ale povinnost. Musíte být kdykoli schopni prokázat, že daný přenos dat byl po celou dobu bezpečný a že k němu měly přístup pouze oprávněné osoby. To znamená, že musíte mít data šifrovaná během přenosu (přenos mezi lidmi nebo systémy) i v klidu (když jsou uložena). Musíte být také schopni vytvořit report, který toto zobrazí

spolu s podrobnostmi o každém, kdo k těmto datům přistupoval. Tento druh reportu by měl systém MFT vytvářet na vyžádání automaticky, a to nejen pro případné auditory, ale také proto, abyste mohli potvrdit, že nedošlo k žádnému narušení dat. I když nejste povinni dodržovat předpisy, je to užitečná funkce, která zajistí, že budete mít přehled o tom, co se stalo. A to je to první, co se po vás bude chtít, jakmile dojde k úniku dat, nebo když se do vaší sítě dostanou nezvaní hosté.

2. Vícefaktorové ověřování (MFA)

Tato metoda je z hlediska uživatelského pohodlí nejtěžší, ale zároveň přináší největší užitek. Vícefaktorové ověřování přidává do procesu přihlašování další vrstvu ochrany a potvrzuje, že přihlašující se osoba je skutečně ta, za kterou se vydává. Vyžaduje něco, co zná (přihlašovací jméno a heslo), s něčím, co má (telefon, generátor tokenů atd.). Efektivně tak činí ukradené heslo nepoužitelným. Zloději hesel totiž potřebují také přístup k telefonu nebo autentizátoru uživatele. Neberte mě za slovo, a nechte se přesvědčit zkušeností Microsoftu, který se této tématice věnoval. Jejich 300 milionů systémů Azure, je neustále pod drobnohledem útočníků a jediná věc, která dosud zabránila v 99,9 % případů k jejich průniku, bylo zavedení MFA. Pokud neuděláte vůbec nic jiného, abyste zvýšili své zabezpečení, implementujte aspoň MFA. Pro zabránění průnikům udělá víc než dalších deset bezpečnostních metod dohromady.

3. Pravidelná rotace šifrovacích klíčů

Šifrovací klíče jsou doslova zlatým klíčem ke všem datům v MFT. Pokud se k nim dostane neoprávněná osoba, získá přístup ke všemu a to většinou bez vašeho vědomí. Rozumná bezpečnostní politika vyžaduje jejich pravidelnou výměnu, což je doporučený osvědčený postup podle PCI-DSS. Pravidelné obměně klíčů může zabránit povětšinou lidská chyba nebo obyčejná lenost. Měli byste se ujistit, že vaše řešení MFT nejen že umožňuje bezpečně a snadno rotovat šifrovací klíče přímo z rozhraní, ale také poskytuje nějaký způsob monitorování stavu změn šifrovacích klíčů. Je důležité, abyste byli schopni zjistit kdy a zda vůbec byly klíče změněny. V ideálním případě by MFT mělo nabízet funkci, která bude klíče rotovat automaticky, abyste nebyli zranitelní.

Další možnosti pro bezpečnost

Tyto tři tipy jsou samozřejmě jen začátkem. Existují desítky dalších vlastností, funkcí a osvědčených postupů, které můžete implementovat, abyste zabránili průnikům a posílili svou bezpečnost. Každý z nich se pojí také s různými úvahami a kompromisy. Vyplatí se vám pro úsporu nákladů a pohodlí hostovat MFT v cloudu? Budou uživatelé tolerovat vynucené přijetí zásad před přihlášením? Požadují zákazníci rychlejší přístup, než vám dovolí vaše bezpečnostní postupy? Na tyto otázky nedokáže odpovědět nikdo jiný než vy.

Výše uvedené tipy jsou ale skvělým začátkem. Každopádně byste měli pravidelně vyhodnocovat své bezpečnostní postupy i to, jak je uživatelé dodržují. Jen tak naleznete rovnováhu v otázce bezpečnosti MFT. Bezpečnost je hlavně na vás, sami víte nejlépe, zda jste již dostatečně paranoidní. ■

Mark Towler
Autor článku působí na pozici Senior PMM ve společnosti Progress.

Cesta k lepšímu zabezpečení

je v pronájmu řešení a využívání externích služeb

Četnost kybernetických útoků na firmy stoupá. Jenom za loňský rok čelilo některému z IT bezpečnostních incidentů rekordních 79 % evropských firem. Jak vyplývá z rozsáhlého šetření bezpečnostní společnosti Kaspersky, společnosti přesto nevynakládají dostatečné prostředky na prevenci před takovými útoky. Řešením by pro ně mohl být pronájem hotových řešení a využívání externích služeb.

Kybernetické útoky na firmy všech velikostí se stávají stále nebezpečnější hrozbou a dělají vrásky na čele manažerům po celé Evropě. K dispozici jsou přitom sofistikovaná řešení, která jim mohou pomoci ochránit firemní majetek nebo alespoň snížit finanční dopady v případě, že by byl útok úspěšný. Paralelně s vývojem kybernetických hrozeb se totiž vyvíjejí i bezpečnostní řešení a služby.

„Vzhledem k tomu, že více než tři ze čtyř (79 %) firem se již někdy staly obětí kybernetické kriminality, musí zapracovat na posílení obrany a používat nejmodernější technologie pro ochranu svého majetku a prevenci narušení bezpečnosti," upozorňuje Miroslav Kořen, generální ředitel společnosti Kaspersky pro region východní Evropy.

Miroslav Kořen, generální ředitel společnosti Kaspersky pro region východní Evropy

Nedávný průzkum společnosti Kaspersky však ukazuje, že 23 % manažerů v Evropě připouští nedostatečné investice jejich firmy do prevence před kybernetickými bezpečnostními incidenty. Nadpoloviční většina (63 %) z 1 500 dotazovaných manažerů přitom připustila, že se obává kybernetických útoků. Více než polovina oslovených manažerů (53 %) také neskrývá obavy, že zaměstnanci nedodržují bezpečnostní zásady a postupy.

„Náš průzkum jasně ukazuje, jaké problémy musí firmy bez ohledu na svoji velikost řešit, ať už se jedná o chyby zaměstnanců, e-mailové útoky nebo rostoucí složitost IT infrastruktury. Pomoc nabízejí sofistikovaná bezpečnostní řešení, která zvládají více než jen ochranu koncových bodů, lepší zpravodajství o hrozbách (TI) a budování bezpečnostního povědomí zaměstnanců. Ideální je vybrat si služby jednoho partnera v oblasti kybernetické bezpečnosti, který nabízí jak technologii, tak odborné znalosti, abyste získali komplexní ochranu a měli přehled o všem, co se ve vaší síti děje. Firmy tak dokážou lépe reagovat na současné i budoucí kybernetické hrozby," říká Miroslav Kořen.

Pronájmem hotových řešení firma ušetří

Co tedy mohou firmy udělat pro lepší zajištění svojí bezpečnosti? „Zásadním krokem může být integrace SOC (Security Integration Center) a SIEM (Security Information and Event Management). Pro malé a střední firmy je nejjednodušším způsobem, jak čelit současným výzvám v oblasti zabezpečení IT, získat důvěryhodnou externí odbornou pomoc. Nemusí tak pracně hledat a platit vlastní kyberbezpečnostní odborníky, místo toho jim pomohou specializované služby. Například nástroj Kaspersky Managed Detection and Response dokáže identifikovat a zastavit útoky již v jejich rané fázi, než útočníci dosáhnou zamýšlených cílů," konstatuje Miroslav Kořen.

Investice do externího zabezpečení IT se vyplatí a pomáhají předcházet závažným incidentům. Průzkum společnosti Kaspersky zjistil, že firmy, které si kybernetickou bezpečnost zajišťují externě, čelily o téměř 10 % menšímu počtu kybernetických incidentů než firmy spoléhající pouze na interní zdroje. V roce 2021 se proto firmy začaly více zajímat o externí pomoc.

Další průzkum společnosti Kaspersky pak zjistil, že firmy všech velikostí se stále častěji obracejí na poskytovatele spravovaných služeb (MSP), aby si zajistily lepší ochranu v náročném prostředí. Rychlé zavádění nových technologií, nové pracovní postupy a růst složitosti infrastruktury přiměly firmy k tomu, aby řešení bezpečnosti svěřily vysoce kvalifikovaným odborníkům mimo svoji organizaci.

Externí služba pracuje pořád a uvolní vám ruce

Firmám zásadně pomohou specializované sady nástrojů pro účinnou ochranu koncových bodů, detekci hrozeb a reakci na ně. Díky nim včas odhalí a odstraní i nejnovější typy hrozeb nebo skryté útoky. Základní ochranu koncových bodů vybavenou funkcemi EDR a MDR poskytuje například řešení Kaspersky Optimum Framework. Bezpečnostní tým firmy by měl mít zajištěný přístup k nejnovějším informacím o hrozbách, například formou pravidelných odborných školení, která budou průběžně zvyšovat jeho odbornou kvalifikaci. Bezpečnostními školeními, a to nejlépe několikrát ročně, by měli procházet i všichni zaměstnanci, aby měli povědomí o bezpečném chování na internetu a dokázali včas odhalit pokusy o cílené útoky, které využívají metod phishingu nebo sociálního inženýrství.

Důležitá je integrace odborných znalostí a technologií. Pokud získáte obojí od jednoho důvěryhodného partnera, který poskytuje integrované a alespoň částečně automatizované služby, budete mít přehled o veškerém dění ve firemní síti, ušetříte čas a zvýšíte efektivitu. Váš bezpečnostní tým se pak bude moci věnovat důležitějším záležitostem. ■

Nezměnitelnost záloh jako poslední vrstva kybernetické ochrany

Aleš Hok

Zálohování je vnímáno jako poslední vrstva kybernetické ochrany. K obnově ze záloh dochází zpravidla až tehdy, když selže všechno ostatní. Když se podíváme deset let zpět, co jsme tehdy řešili? Řešili jsme, jak zákazníkům pomoct s ochranou systémů a dat pomocí zálohovacích řešení. Tím největším strašákem tehdy bylo selhání a chyby hardwaru. Ale dnes jsme jinde. Hardwarových selhání už se nebojíme. Dokážeme je efektivně řešit dokonce několika způsoby. Dnes se bojíme darebáků v podobě kybernetických útočníků.

Útoky na zálohy

Útočníky můžeme rozdělit do dvou skupin. První skupinou jsou útočníci, jejichž cílem je z nějakého důvodu, danou organizaci co nejvíce poškodit. Ve druhé skupině jsou pak útočníci, kteří chtějí na svých obětech vydělat. Ať už je to prodejem odcizených dat, vydíráním, nebo kombinací obojího. Tak jako tak, naší přirozenou snahou je postavit útočníkům do cesty co nejvíce překážek.

Ať už je cíl útočníka jakýkoli, zálohy mu zpravidla stojí v cestě. Je proto logické, že posledním krokem v dokonání zkázy v podobě zašifrování, nebo smazání dat, je útočníkova snaha zbavit se záloh. Pokud má útočník přístup do sítě po delší dobu a získá přístupové údaje do úložiště záloh nebo dokonce do samotného zálohovacího řešení, pak se mu to podaří.

Ochrana před sebou samým

Abychom zálohy ochránili, je nutné vědět, jak na to. A používat taková zálohovací řešení, která nedovolí útočníkům smazat, poškodit a zašifrovat zálohy, nebo s nimi jakkoli jinak manipulovat. Představme si, že útočník ví úplně o všem, co správce provádí a dokáže zachytit všechny přístupové údaje, které správce používá. Pak je to sice nelehký úkol, ale rozhodně není nemožný. Podívejme se jak na to:

Proaktivní, aktivní, reaktivní...

I když tento text popisuje jen vybrané bezpečnostní prvky zálohovacího řešení, neměli bychom zapomínat na to, že ucelená kybernetická ochrana se skládá z proaktivní, aktivní a reaktivní ochrany. Jednou z takovýchto ucelených zálohovacích platforem je Acronis Cyber Protect. Ta vedle zálohování a Disaster Recovery umožňuje navíc aktivovat emailovou ochranu, posuzování zranitelností, patch managment, antivir a další prvky bezpečnosti, a minimalizovat tak hrozby útoků na zálohy.

2FA autentizace

V zálohovacím řešení zapněte dvoufaktorovou autentizaci. Pokud nejde o útok podporovaný lidmi zevnitř organizace, je málo pravděpodobné, že by se útočníkovi podařilo ovládnout jak přístup do zálohovacího řešení, tak zároveň třeba i mobilní zařízení správce.

Žádné centrální uchovávání klíčů

Přestaňte využívat centrální databázi šifer zálohovacího řešení a začněte využívat šifrování archívů bez centrálního uchovávání klíčů. Ačkoliv zálohovací řešení samotné může být poměrně robustní, databáze s šiframi může být jeho slabým místem. Pokud se totiž podaří z databáze vyčíst pověření do úložiště záloh, pak je možné zálohy smazat. Pokud lze z databáze odcizit šifry záloh, pak je možné přečíst jejich obsah.

Nezměnitelnost záloh

Začněte využívat možnost nezměnitelnosti záloh tzv. immutable backups. Jednoduše řečeno, v zálohovacím řešení určíte, že zálohy ukládané do daného úložiště nemohou být po definovanou dobu jakkoli změněny. A to ani tehdy, má-li útočník plný přístup do samotného zálohovacího řešení. Princip tohoto časového zámku totiž nejde obejít ani úpravou retenční politiky plánu zálohování.

Aktivní ochrana zálohování

Začněte využívat vestavěnou aktivní ochranu zálohování. Pokud to zálohovací řešení umožňuje, aktivujte systém self-defense. Ten zabrání jakémukoli procesu spuštěnému na stroji se zálohovacím agentem v přepisu, smazání, poškození, zašifrování záloh. Chráněný stroj se tak vlastně stává zároveň ochráncem záloh před sebou samým a před na něm spuštěnými procesy, včetně malwaru a ransomwaru.
K tomu navíc dokáže zastavit kryptování, přepisování MBR, neoprávněnou těžbu kryptoměn a vypínání ochran, které jsou iniciovány z tohoto zařízení.

Nezměnitelnost záloh není nadstandard

Většina těchto kroků často představuje poslední vrstvu ochrany před úspěšným útokem a dnes by měly být standardem zálohovacích řešení. Pokud je dodavatel zálohovacího řešení nabízí za tučný příplatek, měli bychom zpozornět. Nabízí se paralela s nákupem vozidla a jeho výbavy. U automobilu je možné připlatit si za lepší výbavu jako je autonomní parkování, adaptivní tempomat a další vylepšení. Ale ABS, ESP, bezpečnostní pásy a brzdy jsou za všech okolností součástí základní výbavy. Stejně by to mělo platit i pro zálohovací řešení. Bezpečnostní prvky musí být jeho samozřejmou součástí. A pokud jde o zálohovací řešení, která takové možnosti nenabízejí vůbec, od těch je dobré držet se co nejdále. ■

Aleš Hok

Autor je obchodní ředitel společnosti ZEBRA SYSTEMS zastupující společnost Acronis v ČR a SR.

Zranitelnost Log4j

V čem je jiná a co to znamená pro podnikovou IT bezpečnost

Michal Hebeda

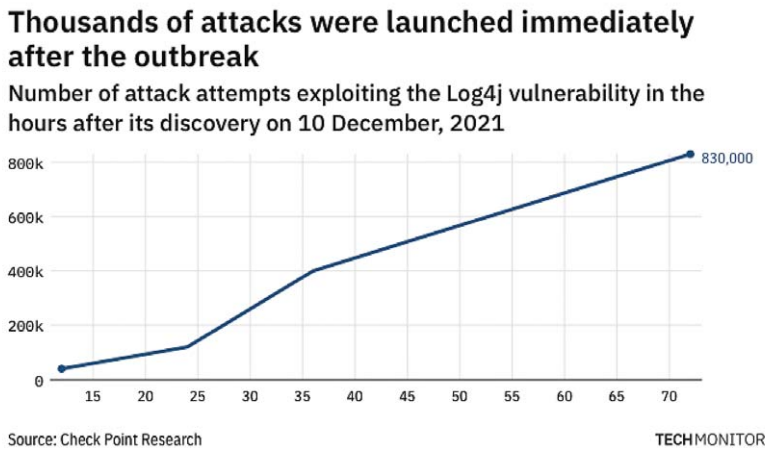
V dnešní době ani neuplyne týden, abychom se nedozvěděli o nějaké nové zranitelnosti. Avšak zranitelnost objevená 8. prosince loňského roku se tak trochu vymyká – nejde o zranitelnost v konkrétní aplikaci nebo operačním systému, ale postiženou je knihovna Log4j z dílny nadace Apache. Tato knihovna, založená na programovacím jazyce Java, byla a je velmi často používána vývojáři různých aplikací a zařízení. Pomáhá jim řešit problematiku logování událostí a vyhledávání v nich, což je potřeba takřka v každé aplikaci, zejména v těch serverových.

Kdo všechno může být postižen a jaké mohou být následky? Na první část otázky není jednoduché odpovědět, neboť na rozdíl od klasické zranitelné aplikace nemusí mít administrátor povědomí o tom, že v některém z používaných software byla tato knihovna použita, případně v jaké verzi. To jej staví do značně nevýhodné role, protože musí spolu s dodavateli prověřit všechny používané aplikace a spoléhat na to, že výrobci rychle zareagují a doporučí buď nějakou rychlou opravu, nebo urychleně dodají opravný patch pro svou aplikaci či zařízení. Čistě technicky vzato mohou být postiženy opravdu různorodé aplikace ať již od těch nejmenších vývojářů nebo až po velké světové výrobce. A nemusí se jednat pouze o softwarové aplikace, ale též o hardwarová zařízení, jako jsou například síťová úložiště a další.

Téměř milion útoků za tři dny

Autor zmiňované knihovny nadace Apache uvedl, že postiženy jsou všechny verze od 2.0 až po 2.14.1. Útočníkovi zranitelnost umožňuje vhodně zaslaným dotazem vyvolat chybu a následné stažení a spuštění vlastního kódu, což může vést k získání kontroly nad daným počítačem, zcizení dat nebo přihlašovacích údajů. Jak je vidět, následky mohou být nedozírné a škody opravdu velké. S vydáváním záplat to také nebylo jednoduché, neboť díky zaměření útočníků na tuto knihovnu ji ihned podrobili zkoumání a našli nové jiné zranitelnosti. Již ne tak významné, ale i tak nebezpečné. Podařilo se až napotřetí a za bezpečnou je považována verze 2.17.

Útočníci na sebe nenechali dlouho čekat a začali masivně útočit již od prvních hodin od objevení zranitelnosti. Zprvu se jednalo o méně sofistikované útoky, například cryptomining – těžba kryptoměn. Což pro oběť paradoxně mohlo být štěstí v neštěstí – zjistili, že jsou napadeni a nepřišli o žádná data. Sofistikovanější a složitější útoky následovaly vzápětí, značná část z nich spočívala v přípravě prostředí pro budoucí útoky. Společnost Checkpoint uvádí, že 72 hodin po zveřejnění zranitelnosti bylo zaznamenáno přes 800 tisíc různých útoků, zneužívajících zranitelnosti Log4j.



Proč je zranitelnost Log4j jiná?

Nyní se dostáváme k tomu, proč je tato zranitelnost tak jiná než předešlé a proč klade na správce systémů zvýšené nároky. U klasických zranitelností například v aplikacích postačí správci systému ověřit, zda používaná verze aplikace patří mezi zranitelné a pokud ano, tak zajistit upgrade na verzi bezpečnou (za předpokladu, že ji výrobce již vydal), případně izolování takové aplikace od vnějšího či vnitřního prostředí. V našem případě se ale nejedná přímo o aplikaci, ale knihovnu, kterou vývojář mohl či nemusel použít. Obvykle není veřejně dostupná informace o verzích použitých knihoven.

Před správci systémů tak leží daleko obtížnější úkol – musí kontaktovat všechny dodavatele aplikací a zařízení a zjišťovat, zda daná knihovna v nich byla či nebyla použita. V kladném případě vyžadovat příslušnou opravu nebo doporučení, jak systémy zabezpečit, aby zranitelnost nemohla být zneužita. Na místě je také kontrola, zda již k útoku v dané síti nedošlo (lze využít například vyhledávání řetězců `*${jndi:ldap://}*`, `*${jndi:rmi://}*`, `*${jndi:ldaps://}*` v lozích serveru).

Nutno také podotknout, že Národní úřad pro kybernetickou bezpečnost (NÚKIB) vydal reaktivní opatření, které správcům kritické infrastruktury nařizuje a ostatním doporučuje provést patřičné kroky. Je vidět, že jde opravdu o závažné ohrožení bezpečnosti a není dobré jej brát na lehkou váhu.

V takovéto situaci jistě každý správce IT systému ocení, pokud jeho dodavatel reaguje pružně a rychle. Proto společnost GFI Software velmi rychle vydala doporučení, jak přenastavit a tím zabezpečit poštovní server Kerio Control a ještě před Vánoci byl vydán opravný patch. Současně s tím byl upraven produkt GFI LanGuard tak, aby detekoval zranitelnou verzi knihovny Log4j v nainstalovaných aplikacích. ■

Michal Hebeda

Autor je Sales Engineer ve společnosti ZEBRA SYSTEMS, distributora GFI Software.

Běžný firewall nestačí

Nový pohled na zabezpečení sítě

Kybernetických útoků přibývá. Česká republika dlouhodobě nepatří mezi premianty, co se síťové bezpečnosti týče, spíše naopak. Proč tomu tak je? A jaké je řešení této situace? Právě na toto téma jsme se v našem Kernun CSIRT týmu zaměřili a jsme přesvědčeni, že známe cestu. Říká Vojtěch Bumba, ze společnosti Trusted Network Solutions, která je tvůrcem bezpečnostních řešení Kernun.

Internet je nebezpečné místo

Jak ví každý, kdo se někdy byť jen zběžně zabýval kyberbezpečností, Internet je plný útočníků. Běžní uživatelé to často necítí, Internet je pro ně prohlížení webu, případně instant messaging aplikace v telefonu, ale nás, co jsme měli odvahu nahlédnout pod pokličku, občas budí ze spaní myšlenka na zapomenuté otevřené porty na perimetru vnitřní sítě. Všichni si ještě velmi živě pamatujeme na hrozivý kybernetický útok na Benešovskou nemocnici z roku 2019. Očekávání, že tato událost povede ke zlepšení ochrany podobných krizových zařízení se ukázala jako mylná v okamžiku, kdy byla úspěšně napadena Fakultní nemocnice Brno, a to o pouhý jeden rok později.

Nastává doba neviditelná

Nedá se předpokládat, že by zvyšující se počet bezpečnostních incidentů v České republice byl chybou správců sítí. Každá organizace, včetně obou zmiňovaných, má firewall, který se stará o ochranu vnitřní sítě. Problémem je, že principy ochrany, na kterých současná bezpečnostní řešení pracují, přestávají fungovat. Nové standardy protokolů pro šifrovanou komunikaci, jako například TLS 1.3, DNS over HTTPS nebo DNS over TLS, sice skrývají uživatelskou komunikaci před útočníky, ale bezpečnostním expertům komplikují práci úplně stejně. Kontrola obsahu provozu na perimetru sítě je čím dál složitější, a my jsme přesvědčeni o tom, že do budoucna přestane být možná úplně.

Jak rozpoznat útočníka?

Jak tedy kontrolovat síťový provoz? Stále navyšovat výkon hardwaru, aby byl schopen rozlamovat čím dál složitější šifrovací protokoly, je nejen ekonomicky náročné, ale hlavně to brzy nebude mít žádný efekt. Komplexnost bezpečnostních protokolů se zvyšuje mnohonásobně rychleji než výkon firewallů.

Pro řešení tohoto problému je nutné začít o bezpečnosti přemýšlet úplně novým způsobem. Pokud je aktuálně největším zádrhelem šifrování, proč se nepodívat na informace, které máme a které se nešifrují? Takovými informacemi jsou například IP adresy komunikujících stran. Pokud bychom byli schopni rozhodnout o každé IP adrese, zda se za ní skrývá útočník nebo ne, nebylo by vůbec potřeba dívat se do obsahu komunikace. Jak ale zjistit, kdo je za IP adresou a jak je nebezpečný?

Řešením je adaptivnost

Adaptivnost je vlastnost bezpečnostního řešení Kernun Adaptive Firewall, která přesně tohle umí. Na základě reputace komunikujících IP adres je schopna okamžitě rozhodnout, zda se má komunikace zablokovat, nebo povolit. Pro získání této informace používá databázi aktivních hrozeb, kterou vytváří a spravuje Kernun CSIRT. Databáze aktivních hrozeb je unikátním výsledkem spolupráce Kernun CSIRT týmu s národními bezpečnostními autoritami, správci páteřní sítě českého Internetu a dalšími CSIRT týmy státní správy i komerčních firem.

Pro tvorbu této databáze jsou využívány tisíce sond rozmístěných po střední Evropě, které monitorují nebezpečné aktivity v Internetu a reportují je. Na základě těchto informací potom inteligentní algoritmus vyhodnocuje například četnost výskytu jednotlivých IP adres, nebezpečnost jejich chování a neustále tak adaptivně upravuje jejich reputaci. Takto získané reputace jsou potom vstupem pro Kernun Adaptive Firewall, který má díky tomu aktuální informace o všech útočnících, kteří se v českém Internetu pohybují a je schopen je identifikovat a zablokovat.

Na kontextu záleží

Že znalost širšího kontextu chování IP adresy v Internetu je klíčová pro určení její nebezpečnosti si můžeme demonstrovat následujícím příkladem. Představte si několik krátkých SSH spojení z jedné adresy na druhou, která proběhla v rámci krátkého časového úseku. Je to útok nebo není? Může jít o útočné pokusy uhodnout heslo, anebo o legitimní zkopírování několika menších souborů. Standardní IPS systém to může buď odmítnout nebo povolit. V každém z těchto případů jde o riziko vzniku false-positive nebo false-negative, případně systém vytvoří pouze varování a rozhodnutí nechá na člověku.

Oproti tomu má Kernun Adaptive Firewall díky databázi aktivních hrozeb navíc informaci, že se tato adresa pokusila provést obdobná SSH spojení také na tisíce jiných adres. V takovém případě ji považuje

za útočnou a spojení nepovolí už při prvním pokusu, protože adresa má špatnou reputaci. Naopak absence jakéhokoliv podezřelého chování zdrojové adresy ve sledované páteřní síti českého Internetu ukazuje, že adresa bude s vysokou pravděpodobností neškodná. Situace se může ale rychle změnit. Pokud se začnou z této adresy objevovat spojení pochybná, její reputace se rapidně sníží a další spojení s ní už nebudou povolena.

Plug and Protect

Zapojení firewallu, jeho konfigurace, zvolení a nastavení správných bezpečnostních politik je často komplikovaná činnost, které se správci sítí obávají. S myšlenkou na vysokou uživatelskou přívětivost a zároveň silné zabezpečení chráněného subjektu jsme Kernun Adaptive Firewall připravili tak, aby byl už ve výchozí konfiguraci nastaven v duchu best practices a ochrana byla okamžitá a silná.

Administrátor se tak nemusí obávat dlouhého konfigurování bezpečnostních služeb. Zařízení funguje ve smyslu plug and protect. Po zapojení jsou automaticky zapnuty všechny důležité prvky ochrany, jako je výše zmiňovaná adaptivnost, tradiční IPS modul zajišťující pokročilou kontrolu paketů, webový filtr Kernun Clear Web, který se stará o filtraci webového provozu, a v neposlední řadě stavový firewall se základními ochrannými mechanismy, jako je zajištění směrování, blokování podvržených paketů a podobně.

Adaptivnost funguje

O tom, že nový přístup k řešení síťové bezpečnosti je validní a funkční, se již mohli přesvědčit uživatelé a organizace, se kterými jsme adaptivní firewall společně testovali. Ve všech případech se efekt dostavil okamžitě. V síťovém provozu byly detekovány nebezpečné prvky, které klasickými firewally bez obtíží prošly.

Stejných výsledků testování bylo dosaženo i v případech, kdy bylo nasazení nového aktivního síťového prvku do stávající infrastruktury klienta z různých důvodů neschůdné. V těchto případech jsme nabídli a provedli kontrolu provozu tzv. pasivně. Testování probíhalo formou analýzy logovacích souborů provozu, který prošel jejich stávajícím bezpečnostním řešením, a který byl porovnán s naší databází aktivních hrozeb. Ve všech případech došlo k nalezení několika stovek, v některých případech i tisíců, IP adres, o kterých již Kernun Adaptive Firewall věděl, že jsou nebezpečné.

V českém kyberprostoru bezpečněji

Je třeba si uvědomit, že pro úspěšný průnik do sítě stačí útočníkům jediná nebezpečná IP adresa, která projde. Příklady toho, že útočníci mají navrch vidíme v médiích stále častěji. Pokud ale budou na těchto místech přítomna data o aktivních hrozbách, půjde se včas a efektivně chránit.

Jak jsme zjistili při testování, nasazení adaptivního firewallu v ostrém provozu je oproti běžným bezpečnostním řešením mimořádně účinné, a to právě díky unikátní znalosti aktivních hrozeb. Jestliže v českém Internetu probíhá nějaký cílený kybernetický útok, Kernun Adaptive Firewall se o něm záhy dozví a útok automaticky zablokuje. Chrání tak konkrétní cíle přímo v místě svého nasazení. ■

Zranitelný lidský faktor umožňuje hackerům obejít i dvoufázové ověření

Je dobře známo, že pro bezpečný přístup k on-line službám už dlouhou dobu nestačí používat jen uživatelská jména a hesla. Proto se používá další level zabezpečení – vícefázové ověřování – které se stalo v mnoha případech nutností. K přihlašování pomocí hesla přidává ještě další nezávislou metodu. Jak se však ukázalo, ani toto nemusí být dostačující, zejména v případě cílených útoků. Problém není v samotné technologii, ale největší slabinou, jak se ukazuje, je i tady sám uživatel. Proti automatizovaným útokům chrání dvoufaktorová autentizace téměř stoprocentně.

Studie ukazují, že k více než 80 % všech bezpečnostních narušení dochází v souvislosti s hackingem. Především z důvodu kompromitovaných a slabých přihlašovacích údajů. Čísla, která přitom zveřejnila společnost Microsoft naznačují, že uživatelé, kteří povolili vícefázovou, nebo také dvoufaktorovou autentizaci, nakonec zablokovali asi 99,9 % automatizovaných útoků. *„To je skvělé číslo, ale jako u každého dobrého řešení kybernetické bezpečnosti útočníci mohou přijít na způsoby, jak ho obejít. A jak dokládá nedávný případ kryptoměnové burzy Coinbase, to se také stalo,“* prozrazuje Martin Lohnert, odborník na kybernetickou bezpečnost ze společnosti Soitron.

Jak lze zabezpečení obejít?

Dvoufaktorovou autentifikaci lze obejít na základě jejího principu fungování. Tedy prostřednictvím vypátrání, lépe řečeno odcizení např. jednorázových kódů zaslaných v SMS na mobilní telefon uživatele. Tato metoda spočívá v tom, že hackeři nejprve na základě vyzrazeného seznamu e-mailů zašlou uživatelům e-mailové sdělení, které se tváří např. jako zpráva od banky. Pokud v něm uživatel klikne na odkaz, dojde k otevření webové stránky, která vypadá legitimně – jako kdyby byla banky. Uživatelé, kteří si dávají pozor a mají jisté IT znalosti, odhalí, že něco může být špatně. Většinou se podvržená stránka ukrývá na internetové adrese, která nepatří bance a obsahuje například překlep.

Až sem nejde o žádnou nově používanou techniku. Nové je to, co následuje potom. Jako URL adresa se použije něco ve tvaru www.mojebanka.cz.resethesla.cz. Na první pohled jde o doménu banky, takže vše vypadá v pořádku, ale zkušený uživatel ví, že doména druhého řádu není www.mojebanka.cz, ale resethesla.cz. A v tom je velký rozdíl, protože tato doména patří útočníkům. Ještě více alarmující je, že pokud na tento web přejde uživatel z mobilního telefonu, tak se mu v případě, že adresa banky je delší, nemusí zobrazit celá. Tudíž vidí jen to, na co je zvyklý. V tomto případě nejde o žádnou technickou chybu, ale o využití zranitelnosti UX – tedy toho, že víme, že browser v mobilu zobrazí jen určitý počet znaků URL adresy a ten zbytek je skrytý. Podvodná stránka může v případě tohoto „triku“ také použít SSL zabezpečení (URL začíná https://), aby díky v browseru zobrazenému zámku evokovala v uživatelích pocit bezpečnosti. Málokdo, si totiž otevírá a ověřuje detaily certifikátu, kterým je SSL šifrované.

Martin Lohnert, odborník na kybernetickou bezpečnost

Vše začíná phishingem

Pokud na podvrženou adresu uživatel skočí, pak hackeři využijí phishingový útok. K tomu stačí, aby jejich web 1:1 vypadal jako ten patřící bance. Na přihlašovací stránce uživatel zadá jméno a heslo. Tím hacker získá první klíč pro vstup. Okamžitě, tedy v reálném čase po obdržení, tyto údaje ručně zadá do opravdového webového rozhraní banky. Ta jeho majiteli na jeho mobilní telefon pošle autentifikační SMS kód, a pokud ho uživatel zadá opět do podvržené stránky, má hacker, co potřebuje.

Během chvilky se ocitne v internetovém bankovnictví uživatele, na nic nečeká a zadá příkaz k platbě. Ten je zapotřebí opět potvrdit. Proto opět uživateli na mobil přijde SMS kód, ale protože stále na podvržené stránce čeká na vstup do banky, tak se mu v tomto mezidobí zobrazí například hlášení, že ho přihlašují, ať chvilku počká. Následně se zobrazí informace o tom, že první přihlášení se nepovedlo a ať zadá druhý SMS kód, který mu byl právě odeslán. „A to je ten kód, který slouží k potvrzení provedení skutečné platby. Jestliže si tohoto upozornění v SMS uživatel nevšimne, a zadá ho do phishingové stránky, hacker ho přepíše do internetového bankovnictví a peníze se mu povede z účtu odčerpat,“ prozrazuje Martin Lohnert.

Přepisování kódů pod palbou

Jak je vidět, i s minimálními úsilími lze prorazit dvoufázové autentifikační zabezpečení. *„Proto je mnohem bezpečnější používat novější typy dvoufázového ověřování, a to prostřednictvím specializovaných aplikací. V nich je právě eliminováno riziko přepisování kódů a vše se děje v rámci rozhraní banky automaticky,“* uvádí Martin Lohnert. Starší podoby, tedy právě ruční přepisování jsou přitom dále využívány nejen různými službami – mimo jiné v aplikaci Google Authenticator, Microsoft Authenticator a právě některými bankami.

Ačkoliv musí být splněno několik podmínek a na sebe navazujících kroků, aby výše uvedené útoky fungovaly, prokazují zranitelnost ve dvoufázových identifikačních metodách založených na SMS a také to, že tyto útoky nevyžadují vysoké technické schopnosti. ■

6 důvodů, **proč do firmy pozvat hackera**

-tz-

Penetrační testování má zásadní vliv na bezpečnost systémů a infrastrukturu každého podniku. Etický hacker pomůže zabránit škodám, které můžou dosáhnout i desítek milionů korun. Cena za „pentest“ přitom představuje sotva půldruhého procenta ročních investic do IT technologií a kyberbezpečnosti.

Trend digitalizace firemních operací a procesů má sklon podceňovat nová technologická rizika, kterým jsme vystavení. Při vývoji aplikací hraje velkou roli čas, za který jsou programátoři schopní práci dokončit. I proto vznikají softwarové zranitelnosti, kterých útočníci využívají.

„Ve větším výrobním podniku může vzniknout ekonomická ztráta přes padesát milionů korun za jediný den,“ varuje David Pícha ze společnosti Integra Czech Republic. „Setkal jsem se s podniky, které investovaly do kybernetické bezpečnosti velké prostředky, ale bohužel zcela nesprávně. Z pohledu vedení to vypadá, že mají zabezpečení na vysoké úrovni, ale v kybernetickém prostoru to tak nefunguje. Do bezpečnosti se musí investovat rozvážně a strategicky, aby se vyloučila slabá místa,“ dodává.

Pro příklad: firma s obratem okolo 2,5 miliardy korun investuje zhruba deset milionů do nákupu IT technologií a služeb a dalších 3,5 milionů do kyberbezpečnosti. Do penetračních testů často vůbec neinvestuje, ačkoli náklady na ně by vyšly zhruba na dvě stě tisíc, tedy 1,48 % z celkových investic do informačních technologií a služeb. Penetrační testování stojí od padesáti do víc než tří set tisíc korun – v závislosti na velikosti IT infrastruktury firmy, a tedy potřebného času lidské práce.

Penetrační testování, nazývané také etické hackování, je forma hodnocení IT bezpečnosti, která testuje počítačový systém, síť nebo softwarovou aplikaci, aby zjistila bezpečnostní chyby, které by útočník mohl zneužít.

Mezi šest hlavních důvodů, proč by každá firma měla provést penetrační test patří:

1. Ukáže sílu aktuálního zabezpečení

Pentest ukazuje vektory kybernetických útoků, které by mohly ovlivnit aktiva IT podniku, data, lidi nebo fyzické zabezpečení – odhaluje tak, jak odolné je vaše IT zabezpečení proti hackerským útokům.

2. Předcházení kybernetickému útoku

Firma by měla vědět, jak důležitý je plynulý provoz IT infrastruktury – kolik by ji stál hodinový, denní nebo týdenní výpadek. Pokud nezná odpovědi na tyto otázky, měla by najmout odborníka, který analyzuje současný stav kybernetické bezpečnosti. Výsledek analýzy poskytne nejen seznam prioritních cílů, kterých je třeba dosáhnout k zabezpečení podnikání, ale i případné finanční ztráty způsobené výpadkem.

3. Testování nových technologií

Nové produkty nebo technologie jsou jedním z hlavních cílů penetračních testů. Implementace do podniků provádějí většinou partnerské firmy, které se zaměřují na včasné a úspěšné provedení implementace. Druhý případ je například při koupi společnosti a migraci jejich IT, zde se otevírá spousta neznámých, které je potřeba otestovat.

4. Zkouška bezpečnostního týmu

Po provedení penetračních testů odhalíte, jak rychle a zda vůbec váš bezpečnostní tým takovou činnost zaznamená a jak se zachová. Může to být obzvlášť užitečné k vypracování plánu reakce na mimořádné situace, jako jsou hackerské útoky.

5. Reputace

Pokud jste správci jakýchkoliv citlivých dat externích firem nebo zákazníků, tak vám penetrační testy pomůžou předejít úniku informací a následnému poškození pověsti firmy. Ztráta důvěry často vede k poklesu příjmů i zisku.

6. Regulace a compliance

Společnosti jako jsou například úvěrové instituce a poskytovatelé platebních služeb jsou povinni penetrační testování provádět. Porušení takové povinnosti může znamenat pokutu, trestní odpovědnost, nebo i ztrátu oprávnění podnikat. ■

Rizika ransomwaru u tradičních metod ochrany dat a koncept obnovy Cyber Recovery

Aleš Koreček

Není snadné psát o ransomwaru bez určité míry pesimismu. Téměř denně se dozvídáme o dopadech kybernetických útoků na životy lidí i chod podniků. Škody se zdaleka netýkají jen hospodaření firem, ale způsobují rozsáhlé problémy v celé naší společnosti tím, že narušují veřejné služby, a dokonce i zásobování potravinami a lékařskou péči. A pokud pro nás z událostí posledních let vyplynulo nějaké poučení, pak to, že musíme být připraveni na cokoli.

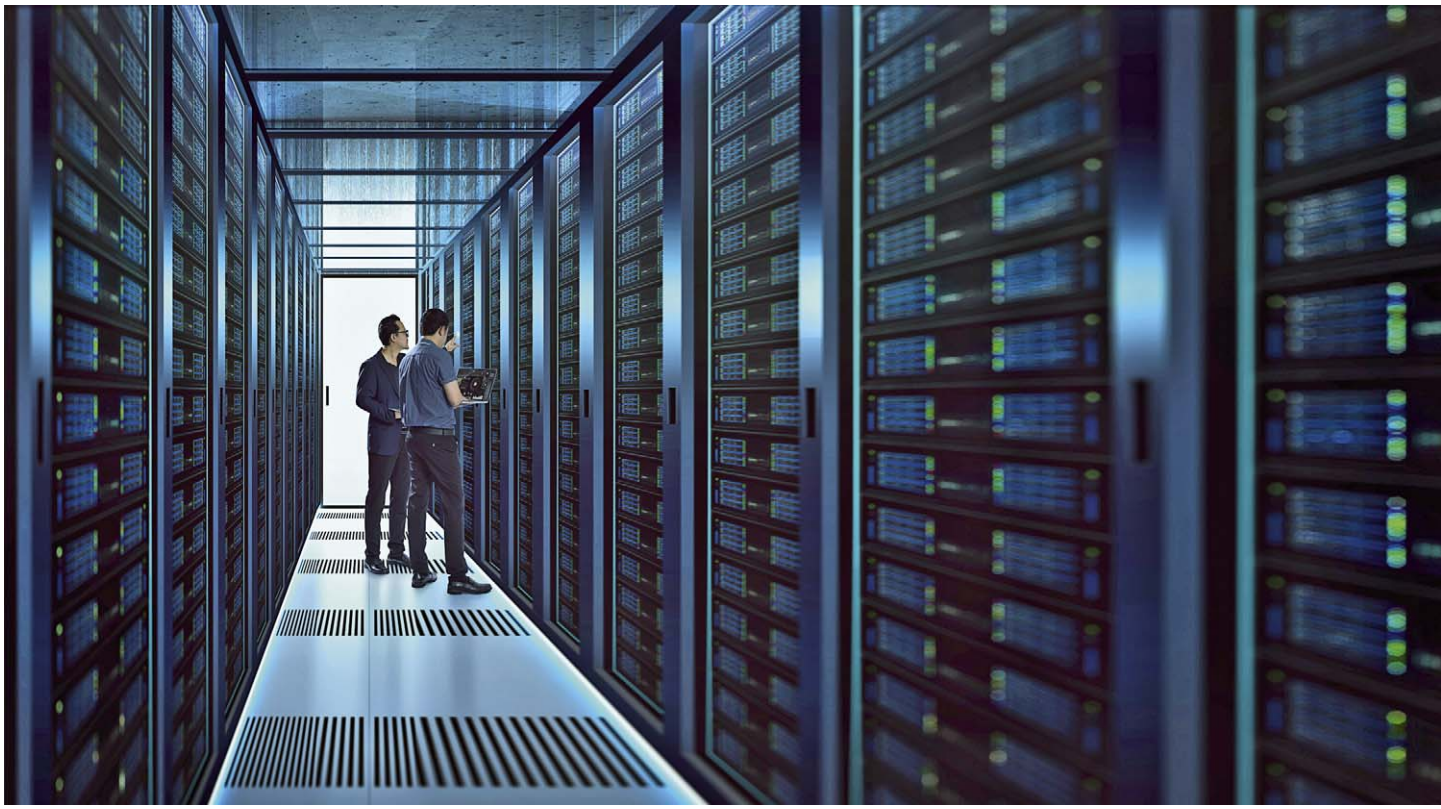
O statistiky a projekce, které vykreslují pochmurný obraz ekonomických ztrát a poškození reputace v důsledku kybernetických útoků, není nouze. Přesto jim ti, kdo mají za úkol chránit své organizace před ransomwarem a dalšími sofistikovanými kybernetickými hrozbami, mnohdy nevěnují patřičnou pozornost. Studie Dell Technologies s názvem Globální index ochrany dat (HDPI) 2021, která vychází z celosvětového průzkumu mezi vedoucími pracovníky v IT, zkoumala, jak podniky a organizace čelí rostoucím výzvám v oblasti ochrany dat a kybernetické odolnosti. Odhalila přitom zajímavou skutečnost, a to, že podniky dosahují pokroků v digitální transformaci navzdory nízké úrovni důvěry, pokud jde o jejich připravenost chránit data a schopnost zotavit se z ransomwarových útoků.

Je krutou ironií (a stále nákladnějším paradoxem), že ačkoli jsou data všeobecně považována za nezbytnou složku inovací, jsou zároveň nejzranitelnějším prvkem celého IT. Šíření kybernetických hrozeb, rozmach multicloudu, rozložení tradičních a nativně cloudových pracovních zátěží mezi edge, lokální datová centra a cloudová prostředí a nástup nových technologií, jako je AI/ML, společně vnáší do podnikového IT značnou složitost. Nárůst práce na dálku tyto problémy ještě více prohloubil.

Z výzkumu GDPI vyplývají tři zajímavé údaje:

- 82 % dotázaných se domnívá, že řešení ochrany dat jejich organizací nebudou zcela splňovat budoucí nároky
- 74 % zaznamenalo zvýšené riziko kybernetických hrozeb v souvislosti s nárůstem počtu zaměstnanců pracujících z domova
- 67 % si není zcela jisto, zda všechna kritická podniková data lze v případě destruktivního kybernetického útoku obnovit

Je zřejmé, že náročnost ochrany dat i množství potenciálních směrů útoku dramaticky narůstá, přičemž se stírají hranice mezi tradiční ochranou dat a kybernetickou odolností.



Zajištění kybernetické odolnosti – na základě komplexní strategie pro identifikaci, ochranu, detekci, reakci a obnovu například po napadení ransomwarem nebo jiném typu útoku – vyžaduje několik vrstev ochrany, které zajistí, že kritická data budou před potenciálními útoky chráněna a izolována od rizikového prostředí. V takovém chráněném rámci lze data po útoku ransomwarem s jistotou obnovit a urychlit tak obnovu běžného provozu podniku.

Ke složitosti moderní ochrany dat přispívá také ochrana nativně cloudových aplikací, kontejnerů Kubernetes a pracovních zátěží SaaS. A samozřejmě potřeba spolehlivé, konzistentní a účinné ochrany dat v různých veřejných cloudových prostředích zajištění bezpečnosti dále komplikuje.

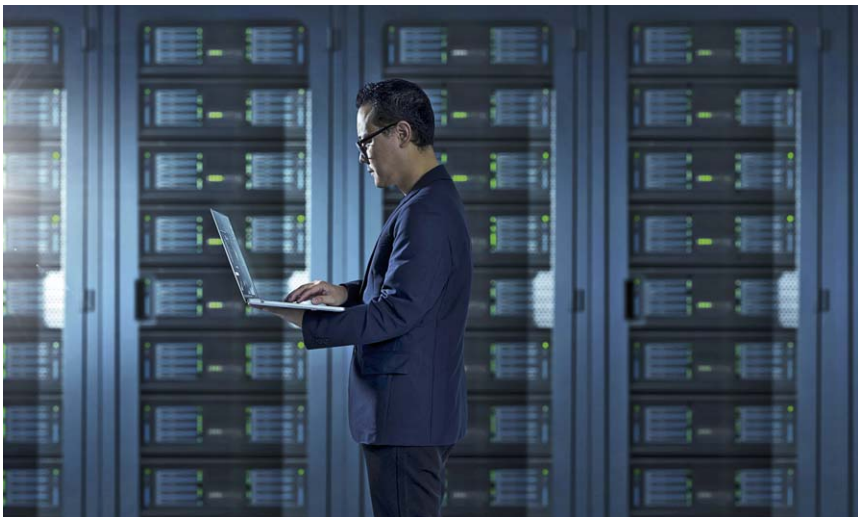
Většina plánovačů IT projektů si navíc není jistá, zda jejich stávající řešení ochrany dat vyhoví všem budoucím nárokům. Nastupující technologie jako AI/ML a IoT v kombinaci s předpokládaným prudkým nárůstem objemu dat v edge prostředích postaví podniky a organizace všech velikostí před další nelehké otázky spojené s ochranou dat. Příznivé je, že AI/ML lze využít i v rámci moderních bezpečnostních strategií k propojení bezpečnostních produktů, řešení a služeb do uceleného moderního konceptu ochrany a zabezpečení dat.

Pro mnoho subjektů se složitost ochrany nově vznikajících technologií pouze znásobí, musí-li se uchýlit ke spolupráci s více dodavateli bezpečnostních řešení, aby si zajistily potřebnou kybernetickou odolnost a ochranu dat v hybridních, multicloudových a edge prostředích. Tato komplikovanost s sebou mnohdy nese značné náklady. Subjekty, které využívají více různých dodavatelů ochrany dat, zaznamenávají o 66 % větší ztráty dat oproti těm, které spolupracují pouze s jedním dodavatelem.

Celkově studie HDPI 2021 vyznívá varovně, ale ukazuje i cestu, jak předejít problémům, které mohou podkopat sebedůvěru a zpomalit vaši transformaci. Progresivní organizace, které chápou, co je v dnešním světě založeném na datech v sázce, zavádí strategie kybernetické odolnosti k boji proti nebezpečí ransomwaru a dalších kybernetických útoků. Úspěšná realizace takové strategie propojuje pracovníky, procesy a technologie do uceleného rámce, který chrání celý podnik, organizaci nebo subjekt.

Jak do strategie ochrany dat zapadá koncept obnovy Cyber Recovery?

Investice do nově vznikajících technologií v rámci digitální transformace jsou bezpochyby chvályhodné, avšak přináší s sebou moderní



hrozby, kterým lze čelit pouze pomocí moderních řešení. Podniky si musí uvědomit, že tatáž data, která jsou klíčovým prvkem jejich podnikání a na nichž staví své transformační snahy, jsou zároveň cílem počítačových zločinců. Aby ochrana dat byla v souladu s tempem zavádění nových technologií, potřebují moderní bezpečnostní řešení. Tradiční ochrana dat je stále potřebná, ale jak ukazuje studie GDPI, sama o sobě nedostačuje a nebyla koncipována pro zabezpečení komplikovaných moderních prostředí a ochranu proti novým hrozbám, jako je ransomware a další typy útoků.

Koncept obnovy Cyber Recovery se odlišuje od tradičního zálohování a zotavení po havárii (Disaster Recovery, DR) v několika ohledech. Poskytuje další vrstvy fyzického a logického zabezpečení na úrovni řešení, systému i dat/souborů, aby byla při uchovávání kritických dat zajištěna integrita, důvěrnost a dostupnost pro případnou obnovu.

Cyber Recovery se zaměřuje na ochranu a izolaci kritických dat od kybernetických hrozeb a potenciálních směrů útoku v zabezpečeném, nezměnitelném datovém trezoru, z něhož je možná obnova v případě potřeby. Na rozdíl od tradičních řešení obnovy po havárii (DR) řeší Cyber Recovery navíc ochranu kritických dat před kybernetickými hrozbami, ale funguje společně s DR, které chrání před jinými výpadky.

Zotavení z destruktivního kybernetického útoku řeší jiný typ události a může se výrazně lišit od zotavení po výpadku napájení, požáru, záplavě nebo jiné pohromě. Kybernetické útoky se obvykle neomezují na konkrétní místo, takže jejich dopad lze často pociťovat globálně, a to i při použití tradičních řešení DR. Efektivnější než provozovat geograficky odloučená datová centra proto bývá infrastrukturu vedle fyzické separace oddělit i logicky, aby se omezilo šíření malwaru a zmenšil prostor pro možný útok.

Postupy obnovy mohou být náročnější a zdlouhavější kvůli související forenzní práci s týmy kybernetické bezpečnosti. Proto má zavedení rychlého a spolehlivého řešení obnovy zásadní význam z hlediska schopnosti podniku rychle se z výpadku zotavit a obnovit provoz. Ransomware a další formy kyberterorismu možná způsobují vážné škody mnoha subjektům, ale přijetí porážky jako předem daného výsledku není řešením. Inovace v oblasti moderní ochrany dat a kybernetické obnovy zavdávají do budoucna důvod k optimismu.

Důvěra ve schopnost zotavit se z destruktivní události je klíčovým faktorem při budování kybernetické odolnosti. Data jsou alespoň na určité úrovni kritickou složkou každé organizace a jejího samotného fungování. Proto je naprosto zásadní aktivně zavádět technologie, které budou podporované ověřenými a dokumentovými programy obnovy, které tvoří poslední linii obrany podniku. K zajištění rychlé a celoplošné obnovy na podnikové úrovni je nezbytné vypracovat program kybernetické obnovy organizace, který sladí postupy obnovy s důležitostí jednotlivých podnikových procesů nebo aplikací pro běžný provoz. To umožňuje opětovné zprovoznění klíčových funkcí podniku v co nejkratším čase – o což jde samozřejmě v první řadě! ■

Aleš Koreček

Autor článku působí na pozici Data Protection Solution Presales Manager CEE ve společnosti Dell Technologies.

Přehled dodavatelů řešení informační bezpečnosti (únor 2022) zkrácená verze					
Jméno společnosti	ABIS ITS, s.r.o.	Accenture CE B.V.	Actinet IS s.r.o.	AEC a.s.	ANASOFT, s.r.o.
Web	www.abis-its.cz	www.accenture.com	www.actinet.cz	www.aec.cz	www.anasoft.com
Rok založení společnosti v ČR	2016	1991	1999	1991	1994
Počet zaměstnanců v ČR	6	2000	25	80	5
Oblasti působení na trhu					
Služby - bezpečnostní analýza, konzultace, audity....	Ano	Ano	Ano	Ano	Ano
Návrh a implementace bezpečnostních řešení	Ano	Ano	Ano	Ano	Ano
Outsourcing bezpečnostních řešení	Ano	Ano	Ano	Ano	Ano
Nabídka v oblasti služeb informační bezpečnosti					
Analýza rizik	Ano	Ano	Ano	Ano	Částečně
Implementace bezpečnostní politiky	Ano	Ano	Ano	Ano	Ano
Penetrační testy	Částečně	Ano	Ano	Ano	Částečně
Bezpečnostní audity	Částečně	Ano	Ano	Ano	Ano
Služby certifikace systémů bezpečnosti	Ne	Ne	Částečně	Ano	Částečně
Školení informační bezpečnosti	Ne	Ano	Ano	Ano	Ano
Source-code Review	-	ANO	NE	ANO	ANO
Security Awareness	-	ANO	ANO	ANO	ANO
Nabídka v oblasti technologií informační bezpečnosti					
Antimalware (antivir, antispyware...)	Ano	Ano	Ano	Ano	Ano
Detekce a prevence průniku IDS/IPS	Ano	Ano	Ano	Ano	Ano
Řešení autorizace a autentizace	Ano	Ano	Ano	Ano	Ano
Ochrana dat, prevence ztráty dat (anti-theft protection)	Ano	Ano	Ano	Ano	Ano
Systémy šifrování elektronického komunikace a dat	Ano	Ano	Ano	Ano	Ano
Řešení pro zálohování a obnovení dat	Ano	Ano	Ne	Ne	Ano
Systémy pro zajištění souladu s předpisy	Ne	Ano	Ne	Ano	Ano

Jméno společnosti	DNS a.s.	Flowmon Networks a.s.	GORDIC spol. s r.o.	ICZ a.s.	Lasting shield
Web	www.dns.cz	www.flowmon.com	https://www.gordic.cz/	www.iczgroup.com	lastingshield.cz
Rok založení společnosti v ČR	1997	2007	1993	1997	2020
Počet zaměstnanců v ČR	102	110	250	320	1
Oblasti působení na trhu					
Služby - bezpečnostní analýza, konzultace, audity....	Ano	Ne	Ano	Ano	Částečně
Návrh a implementace bezpečnostních řešení	Ano	Částečně	Ano	Ano	Ano
Outsourcing bezpečnostních řešení	Ne	Ne	Ne	Ano	Ano
Nabídka v oblasti služeb informační bezpečnosti					
Analýza rizik	Částečně	Ne	Ano	Ano	Částečně
Implementace bezpečnostní politiky	Ano	Částečně	Ano	Ano	Ano
Penetrační testy	Částečně	Ne	Ano	Ano	Ano
Bezpečnostní audity	Částečně	Ne	Ano	Ano	Ano
Služby certifikace systémů bezpečnosti	Částečně	Ne	Ne	Ano	Ano
Školení informační bezpečnosti	Ano	Ne	Ano	Ano	Ano
Source-code Review	NE	-	NE	NE	-
Security Awareness	ANO	-	NE	ANO	ANO
Nabídka v oblasti technologií informační bezpečnosti					
Antimalware (antivir, antispyware...)	Ano	Ne	Ne	Ano	Ne
Detekce a prevence průniku IDS/IPS	Ano	Částečně	Ne	Ano	Ne
Řešení autorizace a autentizace	Ano	Ne	Ne	Ano	Ne
Ochrana dat, prevence ztráty dat (anti-theft protection)	Ano	Ne	Ne	Ano	Ne
Systémy šifrování elektronického komunikace a dat	Ano	Ne	Ne	Ano	Ne
Řešení pro zálohování a obnovení dat	Ano	Ne	Ne	Ano	Ne
Systémy pro zajištění souladu s předpisy	Ano	Ne	Ano	Ano	Ne

Jméno společnosti	RSM CZ a.s.	Samohyb s.r.o.	SEFIRA spol. s r.o.	SOITRON s.r.o.	Sunsec s.r.o.
Web	www.rsm.cz	www.goodaccess.com	www.sefira.cz	www.soitron.com	www.sunsec.cz
Rok založení společnosti v ČR	1993	2014	1995	2005	2003
Počet zaměstnanců v ČR	260	25	38	67	10
Oblasti působení na trhu					
Služby - bezpečnostní analýza, konzultace, audity....	Ano	Ne	Ano	Ano	Ano
Návrh a implementace bezpečnostních řešení	Ano	Ne	Ano	Ano	Ano
Outsourcing bezpečnostních řešení	Ano	Ano	Ne	Ano	Ano
Nabídka v oblasti služeb informační bezpečnosti					
Analýza rizik	Ano	Ne	Ne	Ano	Ano
Implementace bezpečnostní politiky	Ano	Ano	Ne	Ano	Ano
Penetrační testy	Ano	Ne	Ne	Ne	Částečně
Bezpečnostní audity	Částečně	Ne	Ne	Ano	Ano
Služby certifikace systémů bezpečnosti	Ne	Ne	Ne	Ne	Ne
Školení informační bezpečnosti	Částečně	Ne	Ne	Ano	Ne
Source-code Review	-	-	NE	NE	-
Security Awareness	-	-	NE	-	-
Nabídka v oblasti technologií informační bezpečnosti					
Antimalware (antivir, antispyware...)	Ano	Ne	Ne	Ano	Ano
Detekce a prevence průniku IDS/IPS	Ano	Ano	Ne	Ano	Částečně
Řešení autorizace a autentizace	Ano	Ano	Ano	Ano	Ano
Ochrana dat, prevence ztráty dat (anti-theft protection)	Ano	Ano	Ne	Ano	Ano
Systémy šifrování elektronického komunikace a dat	Ano	Ano	Ano	Ano	Ano
Řešení pro zálohování a obnovení dat	Ano	Ne	Ne	Ano	Ano
Systémy pro zajištění souladu s předpisy	Ne	Ano	Ne	Ano	Částečně

Údaje uvedené v přehledu poskytli samotní dodavatelé na základě výzvy redakce a jsou pouze orientační. Redakce nenese za jejich správnost a úplnost. Bližší informace najdete na jimi uvedených webech a na ***www.SystemOnLine.cz****, kde jsou všechny přehledy průběžně aktualizovány.*

Plnou verzi s podrobnějšími informacemi najdete na www.SystemOnLine.cz

Annex NET s.r.o.	AXENTA a.s.	COMGUARD a.s.	Corpus Solutions a.s.	Data Protection DC, s.r.o.	DCIT, a.s.
www.annexnet.cz	www.axenta.cz	www.comguard.cz	www.corpus.cz	DPDC	https://www.dcit.cz
1997	2009	2006	1992	2014	1993
14	25	24	50	20	80
Ano	Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano	Ano
Částečně	Ano	Ano	Ano	Ano	Částečně
Ano	Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ne	Ano
Ano	Ano	Ano	Ano	Ano	Ano
Ne	Ano	Ano	Ano	Ne	Ne
Ne	Ano	Ano	Ano	Ano	Ano
-	-	-	ANO	NE	ANO
ANO	-	-	ANO	ANO	ANO
Ano	Ne	Ano	Ano	Ano	Ne
Ano	Ano	Ano	Ano	Ano	Ne
Ano	Ano	Ano	Ano	Ano	Ne
Ano	Ano	Ano	Ano	Ano	Ne
Ano	Ano	Ano	Částečně	Ano	Ne
Ano	Ano	Ano	Částečně	Ano	Ne
Ano	Ano	Ne	Ano	Ano	Ne

Master Internet s.r.o.	MONET+, a.s.	MWT Solutions S.A.	Netia s.r.o.	Network Security Monitoring Cluster	Q - COM, spol. s r.o.
www.master.cz	www.monetplus.cz	mwtsolutions.eu/cs/	www.netia.cz	www.nsmcluster.com	www.q-com.cz
1998	1996	2017	2010	2010	1998
80	250		10		12
Ano	Částečně	Ano	Ano	Ano	Ano
Ano	Ano	Ano	Ano	Ano	Ano
Ano	Částečně	Částečně	Ano	Ano	Ano
Ano	Ano	Ne	Ano	Ano	Ano
Částečně	Ano	Ne	Ano	Ano	Ano
Ano	Částečně	Ne	Ne	Ano	Ano
Ano	Částečně	Ne	Ano	Ano	Ano
Ne	Ne	Ne	Ano	Ne	Ano
Částečně	Ne	Ne	Ano	Ano	Ano
ANO	-	-	-	-	NE
ANO	-	-	-	ANO	NE
Ano	Ne	Ano	Ne	Ano	Ne
Ano	Ne	Ne	Ne	Ano	Ne
Ano	Ano	Ano	Ne	Ano	Ne
Ano	Ne	Ano	Ne	Ano	Ne
Ano	Částečně	Ne	Ne	Ano	Ne
Ano	Ne	Částečně	Ne	Ano	Ne
Ano	Částečně	Ano	Ne	Ano	Ne

System4u a.s.	Trusted Network Solutions, a. s.	Unicorn a.s.	VUMS DataCom, spol. s r.o.	Zebra systems, s.r.o.
www.system4u.cz	www.tns.cz	https://unicorn.com/	www.datacom.cz	www.zebra.cz
2004	2000	1990	1993	1993
30	25	1994	16	15
Ano	Ano	Ano	Ano	Částečně
Ano	Ano	Ano	Ano	Částečně
Ano	Ano	Ano	Ne	Částečně
Ano	Ano	Ano	Ano	Částečně
Ano	Ano	Ano	Ano	Ne
Ne	Ano	Ano	Ano	Ne
Ne	Ano	Ano	Ano	Ne
Ano	Částečně	Ano	Ne	Ne
Ano	Ano	Ano	Ano	Ne
-	NE	ANO	NE	-
-	ANO	ANO	ANO	-
Ne	Ano	Ne	Ne	Ano
Ne	Ano	Ne	Ne	Ano
Ano	Ano	Ne	Ano	Částečně
Ano	Částečně	Ne	Ne	Ano
Ano	Částečně	Ne	Ne	Částečně
Ano	Ne	Ne	Ne	Ano
Ano	Částečně	Ne	Ne	Částečně

Chcete zlepšit vaši kyberbezpečnost?

Nejdřív si udělejte pořádek v účtech

Marcel Poul

Počet kybernetických útoků vůči organizacím se rok od roku zvyšuje. Mění se přitom způsob a cíl útoků, ale základní princip stále platí – aby mohl kybernetický útok napáchat škodu, musí využít nějaké zranitelnosti vašeho IT systému. Jednou z typických zranitelností je přitom neřízená správa přístupů do IT systémů. Víte kam přesně mají přístup vaši zaměstnanci, jaké další typy účtů ve vaší organizaci používáte a kdo je jejich vlastník? Pokud ne, jak chcete útoku efektivně předcházet?

Pandemie ještě více umocnila možnost práce se vzdáleným přístupem (VPN, RDP, ssh, apod...) zaměstnanců a vzdálenou plochu využívá čím dál více externistů. Otázkou však je, jak často se taková udělení certifikují, kdo je vůbec povolil a s jakou platností. Občas se stane, že i IT začne podléhat setrvačnosti zaběhnutých procesů.

Představme si, že jsme opravdu pod útokem. Útočník kompromitoval účet našeho administrátora. Kam všude se teď může dostat? Dokážeme ho odstřihnout, aniž bychom zastavili běh firmy a způsobili provozní ztráty? V takových chvílích může jít o minuty, které ve výsledku ušetří i miliony. S pořádkem v přístupech do systému může pomoci Identity Management software (IdM).

IdM pomůže „narovnat“ účty

Identity manager má několik základních principů, které udrží vaše přístupy v perfektní kondici. Postará se o centrální správu a přehled o všech účtech v organizaci. Stanovuje jednoznačnou odpovědnost za přidělení přístupu. Díky IdM je možný i rychlý audit všech spravovaných účtů. Samozřejmostí je i automatizace některých procesů, jako jsou třeba tvorba či odmazávání přístupu na základě jasně definovaných pravidel.

Na jaké účty se často zapomíná?

Pokud řešíme správu přístupů, pak každého napadnou účty zaměstnanců. Ano, mít přehled o účtech zaměstnance je základ pro kvalitní identity management. Avšak kromě běžných účtů máme i takové, na které se často zapomíná, a přesto jsou zajímavé. Mnohdy pro útočníky ještě daleko zajímavější než účet řadového zaměstnance:

- Účty externistů – Nejen zaměstnanci vykonávají práci v rámci firemních IT systémů. Velmi početnou skupinou uživatelů jsou externisté, mezi které počítáme například externí dodavatele, kteří bývají zřídka kdy centrálně evidováni. Dále to jsou stážisté, ti bývají často evidování v personálním systému. Často to jsou kontraktoři, kteří evidování v systémech nebývají, stejně jako účty partnerských společností. Nejen, že externisté bývají zřídkakdy evidování na jednom místě, zapomíná se hlavně na jejich včasné ukončování a revizi jejich přístupů. Vzdálené přístupy, které často používají, jsou vydávány na dlouhou dobu, někdy neomezeně. Jednou z nejhorších praktik správy účtů externistů je vydávání sdílených přístupových účtů – například jeden účet pro celou partnerskou firmu. Při případných problémech pak není vůbec zřejmé, kdo a kdy případný zásah provedl.
- Vzdálené přístupy – Speciální typ účtů, který využívají jak interní zaměstnanci, tak externisté, jsou vzdálené přístupy. Evidence vzdálených přístupů a jejich pečlivá správa by měla být jedním ze základů identity managementu. Stanice, ze kterých se do interní sítě vzdáleně přistupuje jsou totiž málokdy spravovány danou firmou, je tedy potřeba se k nim chovat nanejvýš nedůvěřivě a při případné kompromitaci být schopni je rychle zablokovat.
- Privilegované účty – Sem můžeme počítat účty s vyššími privilegii, než mají běžní uživatelé. Často jde o účty, pod jejichž právy běží například IT služby v organizaci nebo účty pro administraci nějakého systému. Správu speciálních účtů může v základu zabezpečit identity management – udrží přehled o tom, kdo a kdy ho založil a jaké má například skupiny v doméně AD a kdo je vlastník (fyzická osoba) daného účtu. Pokud daný vlastník odejde, IdM vyzve oprávněné osoby k nastavený nových vlastníků tak, aby v organizaci nezůstávaly speciální účty mimo evidenci. Real time řízení přístupu k privilegovaným účtům, jako je možnost dočasně pod účtem pracovat, pak řeší specializovaný software PAM (privileged access management).
- Dočasné a testovací účty – Velký problém jsou účty, které někdo vytvořil jen k určitému krátkodobému použití nebo rychlému testování, aniž by je následně smazal. Toto „smetí” nejen znepřehledňuje správu účtů, ale často není znám ani jejich majitel a účel. Při kompromitaci pak vůbec není jednoduché určit rozsah napáchaných škod.

V organizacích se vyskytují různé typy učtu a s ohledem na kyberbezpečnost je nutné se jimi zabývat. Neřízení přístupů nejenže znepříjemňuje práci IT pracovníkům, ale může představovat poměrně nemalou bezpečnostní hrozbu. ■

Mgr. Marcel Poul

Autor článku je expert na správu účtů v IT a ředitel realizace projektů společnosti BCV solutions.

Nová všestranná kamera s optickým zoomem

Společnosti Axis uvedla na náš trh novou kameru AXIS Q1715. Jde o je tzv. block kameru, která je svým designem uzpůsobená ke všestrannému použití s různými úchyty, kryty a pouzdry. Nabízí HD-TV rozlišení 1080p při 60 snímcích za sekundu a díky 21násobnému optickému zoomu je využitelná i při dohledu na větší vzdálenosti.

Díky procesorové jednotce hlubokého učení (DLPU) je možné přímo v kameře používat aplikace založené na umělé inteligenci. K rozpoznávání a analýze záznamu nebo živého obrazu pak lze využít aplikace třetích stran od většiny dodavatelů na trhu. Přímo v kameře jsou zdarma dvě předinstalované aplikace. AXIS Live Privacy Shield pro dynamické maskování scény v reálném čase a ochranu soukromí lidí při monitorování videa v interiéru i exteriéru. Aplikace AXIS Object Analytics pak umožňuje klasifikaci objektů (rozlišování lidí a vozidel, včetně jejich typů, například osobních vozů, autobusů, nákladních aut, motocyklů či kol). Obě uvedené aplikace navíc můžou být zdrojem analytických metadat pro další využití.

K všestrannosti nové kamery přispívá široké spektrum montážních doplňků, včetně krytů a pouzder, díky nimž se kamera přizpůsobí každému prostředí. Její součástí je také sériový port k ovládání polohovací jednotky nebo motorů na otáčení a naklápění. Díky rozhraní I2C je pak možné ovládat infračervený přísvit a s pomocí HDMI a HD-SDI výstupů lze zobrazovat živé video přímo na monitoru.

AXIS Q1715 disponuje i technologií širokého dynamického rozsahu a dokáže i při špatném osvětlení poskytovat kvalitní barevný obraz. Kameru lze napájet stejnosměrným proudem nebo prostřednictvím PoE vstupu, takže i v případě výpadku proudu má kamera k dispozici redundantní napájení. Hlídané vstupy navíc v případě přerušení spojení odešlou upozornění.

QNAP se pouští i do oblasti videokonferencí

Společnost QNAP, která patří mezi přední značky v oblasti síťových úložišť (NAS), se nově pouští i do oblasti videokonferencí. Představila totiž zařízení KoiBox-100W, které vychází z konceptu privátního cloudu, využívá videokonferenční operační systém KoiMeeter, nabízí 2,5" pozici pro disk SATA pro ukládání videí a zvuku ze schůzek a klade důraz na soukromí a zabezpečení. Poskytuje tak bezpečnou komunikační platformu pro spolupráci napříč týmy. KoiBox-100W je zajímavou alternativou konferenčních systémů založených na protokolu SIP.

KoiBox-100W je přenosné a snadno použitelné zařízení – stačí jej připojit k zobrazovacímu zařízení HDMI a síti. Umožňuje tak mohou zahájit videokonference nebo bezdrátové prezentace bez nutnosti složitého nastavení. Stačí zavolat jiný systém KoiBox-100W, nebo systém

KoiMeeter na zařízení QNAP NAS, nebo mobilní aplikaci KoiMeeter, nebo kompatibilní systém SIP (například Avaya nebo Polycom) a spustit videokonferenci ve vysokém rozlišení, případně se připojit k jiným cloudovým konferenčním místnostem.

Při videokonferencích realizovaných pomocí zařízení KoiBox-100W je zajištěna vyšší bezpečnost a soukromí ve srovnání se schůzkami pomocí veřejných cloudů, ale QNAP se nabrání ani integraci s nimi. Kromě videokonferencí v privátním cloudu zařízení KoiBox-100W tak umožňuje i připojení k hovorům Zoom, Skype, Microsoft Teams, Cisco Webex a Google Meet. Umožňuje tak zefektivnit tak komunikaci mezi různými platformami.

Kromě videokonferencí umožňuje KoiBox-100W bezproblémovou bezdrátovou projekci až ve 4K na monitor, velký displej nebo jiné zobrazovací zařízení, které je k němu připojené (např. projektor). Nastavení prezentace je přitom mimořádně jednoduché. Stačí otevřít webový prohlížeč a zadat IP adresu vzdáleného displeje a promítat na něj obrazovku vybrané aplikace nebo celé obrazovky počítače. V jedné společné prezentaci lze přitom zobrazit až čtyři rozdělené obrazovky z různých zařízení.

Pro sdílení obrazovky mobilního telefonu stačí naskenovat QR kód zařízení KoiBox-100W a promítat obrazovku mobilního telefonu nebo displej fotoaparátu na monitor, který je k němu připojený.

Mezi další funkce zařízení KoiBox-100W patří automatické přijímání hovorů, adresář a funkce Insight View, která umožňuje účastníkům schůzky vzdáleně sledovat prezentaci na jejich počítačích.

Nový kompaktní mesh systém a extender

Společnost D-Link oznámila uvedení nových zařízení série EAGLE PRO AI, konkrétně nových mesh systémů M15-2, M15-3 a extenderu E15, na český a slovenský trh. Nové produkty pro vytvoření Wi-Fi 6 sítě se průběžně optimalizují a nastavují pomocí umělé intelligence. Poskytují tak bezproblémovou konektivitu pro domácí použití i do menších kanceláří.

Nové produkty nabízejí kombinovanou dvoupásmovou bezdrátovou rychlost až 1 500 Mb/s s nejnovějšími technologiemi Wi-Fi 6, jako jsou 1024 QAM, MU-MIMO a OFDMA. Jsou navrženy s vestavěným optimalizátorem Wi-Fi s umělou inteligencí (AI Wi-Fi Optimiser), který se neustále připojuje k nejvhodnějšímu kanálu Wi-Fi, a optimalizátorem provozu s umělou inteligencí (AI Traffic Optimiser), který upřednostňuje nejkritičtější využití internetu, což zajistí stabilní připojení a lepší uživatelský zážitek v online prostředí.

Vestavěný AI Assistant navíc neustále automaticky diagnostikuje síť, monitoruje využívání dat a nabízí doporučení. Tyto informace jsou poté přístupné prostřednictvím aplikace EAGLE PRO AI nebo webového rozhraní.

Nové mesh systémy EAGLE PRO AI M15-2 a M15-3 (v balení s 2 nebo 3 jednotkami) jsou navrženy pro pokrytí plochy až 370 m2 Wi-Fi signálem, respektive 500 m^2 (v případě 3 jednotek), s možností rozšíření až na čtyři jednotky.

Nový síťový mesh extender EAGLE PRO AI E15 pak umožňuje rozšířit Wi-Fi tam, kde je nejvíc potřeba a v kombinaci se stávajícím inteligentním routerem nebo s mesh systémy plně využívá všechny funkce AI a vytváří inteligentní síť mesh Wi-Fi, která se neustále optimalizuje a zlepšuje. Integrovaný gigabitový port zároveň umožňuje prostřednictvím extenderu připojit zařízení kabelem k Wi-Fi.

Epson představil novou generaci projektorů s vysokou svítivostí

Epson uvedl svou nejnovější generaci laserových LCD projektorů, které nabízejí vysokou svítivost, ale přesto jsou relativně velmi kompaktní. Nová řada PU2200U zahrnuje dva nejmenší a nejlehčí modely se svítivostí 20 000 lumenů na světě, které jsou o 70 % menší a o 50 % lehčí než jejich předchůdce (EBL20000U). Nová řada projektorů byla navržena pro použití ve velkých posluchárnách, na živých akcích, koncertech a v konferenčních místnostech. Kromě výrazně snížené velikosti a hmotnosti nabízí nižší spotřebu energie, snazší instalaci, nastavení a zjednodušenou údržbu.

Řada PU2200 obsahuje modely se svítivostí 13 000 lm, 16 000 lm a 20 000 lm s rozlišením WUXGA, a podporou HDR. Nová generace je zpětně kompatibilní s existujícími objektivy Epson a projektory se tak snadno integrují do současných instalací.

Nová řada umožňuje také skládání obrazů bez použití počítače. To znamená, že je možné zkombinovat obraz ze dvou podporovaných projektorů a tím zdvojnásobit jas. Mezi další vlastnosti patří funkce NFC pro snazší instalaci, která umožňuje komunikaci mezi projektory a chytrými zařízeními Android kompatibilními s NFC, i když je projektor vypnutý.

Nová řada je také odolnější proti prachu, protože hermeticky uzavřená optická soustava a jednotka laserového zdroje světla zabraňují kontaminaci prachem, což zajišťuje delší životnost. Optická soustava a modul zdroje světla mají certifikaci IP5x a používá vysoce účinný systém kapalinového chlazení.

Pokud máte přepínač na stole, měl by být hezký

Společnost D-Link udělala radost všem, kteří chtějí, aby technika, která nás obklopuje byla nejen výkonná, ale také hezká. Uvedla na náš trh neřízený 6-portový switch DMS-106XT, který je velmi elegantní a právem získal ocenění za design Red Dot Award a Good Design Award. Stolní switch se nachází v odolném matně šedém krytu z hliníkové slitiny a jeho konstrukce bez ventilátorů zajišťuje vyšší spolehlivost a mimořádně tichý provoz.

Novinka rozšiřuje rodinu Multi-Gigabit zařízení D-Link, které jsou určené pro malé podniky a náročné uživatele, kteří hledají vysoce výkonné, ale zároveň i cenově výhodné řešení síťové konektivity.

Přepínač DMS-106XT nabízí pět 2,5gigabitových portů a 10gigabitový uplink. Multi-Gigabit porty jsou zpětně kompatibilní se stávajícími zařízeními a kabely. To umožňuje prakticky okamžité nasazení DMS-106XT v místech, kde se požaduje větší šířka pásma.

Pro náročné instalace ve firmách i domácích sítích disponuje režimem Turbo, který okamžitě sníží latenci u časově citlivých aplikací a umožní port-based QoS pro upřednostnění prioritních dat v síti, jako jsou hry nebo streamování 4K/8K videa.

Nové chromebooky pro hybridní způsob práce

Společnost Acer představila tři nové chromebooky určené pro uživatele, kteří potřebují bezpečné, snadno ovladatelné a cenově dostupné zařízení pro zábavu, komunikaci i produktivní práci. Mezi novinkami je konvertibilní model Acer Chromebook Spin 513 s 13,5" displejem s poměrem stran 3:2 a dva cenově dostupnější modely Acer Chromebook 314 a 315, které nabízejí velmi atraktivní poměr ceny a užitné hodnoty. Oproti předchozí generaci budou i modely 314 a 315 vybaveny IPS displeji (u vyšší verzí), což by mělo zásadně zlepšit nabízený uživatelský zážitek.

Chromebooky využívají operační systém Chrome OS, který zajišťuje rychlý start, snadné používání, minimální nároky na správu a údržbu systému, robustní zabezpečení a delší výdrž baterie díky velmi malým nárokům na výkon hardwaru. Chromebooky podporují webové aplikace a aplikace na Google Play, takže jejich uživatelé mají přístup k široké nabídce oblíbených aplikací pro produktivní práci, vzdělávání, kreativitu i další činnosti.

Nejzajímavější z nově uvedených modelů je Acer Chromebook Spin 513 (CP513-2H), který je díky štíhlému designu a odolnému hliníkovému tělu ideálním chromebookem, který si můžete vzít s sebou do školy i do práce. Je poháněn novým procesorem MediaTek Kompanio 1380 s osmi jádry pro práci na více úlohách současně. Pro spíše pracovní využití je určen 13,5" displej s poměrem stran 3:2, který uživatelům poskytuje na obrazovce o 18 % více vertikálního prostoru, takže na ní uvidí více obsahu a nebudou muset obraz tak často posouvat. Displej má rozlišení 2 256 × 1 504 px a velmi úzké bočními rámečky (pouze 7,7 mm).

Acer Chromebook Spin 513 je díky své konvertibilní konstrukci skvělou volbou pro ty, kteří si své zařízení berou s sebou na cesty. Může přecházet mezi čtyřmi různými režimy používání, jako je režim stanu pro využití prostor s nedostatkem místa, například ve vlaku nebo letadle, či režim tablet pro použití na cestách. Vyznačuje se přitom odolností armádní úrovně MIL-STD 810H. Vestavěná Wi-Fi 6 pomáhá udržovat spolehlivé připojení k sítím a hotspotům. Chromebook je navíc do míst se slabým osvětlením vybaven podsvícenou klávesnicí a portem USB-C pro připojení k periferiím, přenos dat a nabíjení mobilních zařízení. Ve výbavě nechybí ani dvojice reproduktorů směřující vzhůru, které poskytují vysoce kvalitní zvuk bez zkreslení, ať už při sledování streamované zábavy, nebo při videohovorech, kdy najde uplatnění i dvojice mikrofonů.

Novinky od TCL

V záplavě novinek, které byly uvedeny na veletrhu CES 2022, se objevilo i několik nových přenosných zařízení značky TCL. Jde o novou generaci brýlí TCL NXTWEAR AIR, vůbec první notebook TCL s operačním systémem Windows a tablet řady NXTPAPER s netradičním displejem.

Tablet TCL NXTPAPER 10s se odlišuje od běžné produkce především svým displejem, který se neleskne a vizuálně se podobá papíru. Využívá totiž 10 ochranných vrstev, které zachovávají přirozené barvy obrazu, a novinka je tak velmi šetrná k očím uživatele. Redukce modrého světla je prioritou a tato funkce je zabudována přímo do softwaru i hardwaru zařízení. Displej redukuje modré světlo procházející obrazovkou o více než 50 %. Pohled na obrazovku tabletu je tak mnohem pohodlnější.

TCL NXTPAPER 10s má přibalené pero T Pen pro psaní poznámek na displej, který dokáže rozeznat více úrovní přítlaku. Baterie s kapacitou 8000 mAh zajistí celodenní výdrž. Volitelná je klávesnice Folio Keyboard a podložka Writing Board.

Další novinkou z dílny TCL jsou chytré brýle NXTWEAR AIR, které podle výrobce dokážou po připojení ke kompatibilnímu smartphonu nebo notebooku vytvořit dojem sledování 140palcové obrazovky ze vzdálenosti čtyř metrů. Mohou tak sloužit pro sledování filmů na cestách, pro hraní her, ale i nikým nerušenou kancelářskou práci. Oproti předchozí generaci jsou nové brýle ještě lehčí (váží jen 75 gramů) a pohodlnější. Díky dvěma displejům typu Micro OLED s rozlišením 1080p poskytují brýle obraz se sytými barvami a skutečnou černou barvou. Nová generace brýlí se bude dodávat se dvěma vyměnitelnými tvary předních skel, aby vyhověla různým stylům uživatelů.

Společnost TCL také nově rozšiřuje svou nabídku o notebooky. První vlaštovkou je notebook TCL BOOK 14 Go s operačním systémem Windows 11. Má úhlopříčku displeje 14,1 palců, profil tenký jen 13,95 mm a hmotnost 1,3 kg. Notebook nabízí mobilní připojení 4G LTE a vynikající výdrž baterie díky použité platformě Qualcomm Snapdragon 7c. Potěší i možnost plynulého přepínání mezi připojením Wi-Fi a 4G. ■

Acer představil čtyři nové chromebooky

se 14ti a 15palcovým displejem

Společnost Acer představila koncem loňského roku čtyři nové chromebooky, které vycházejí vstříc potřebám různých typů uživatelů od domácích a firemních uživatelů až po studenty. Nové chromebooky jsou vybaveny nejnovějšími procesory Intel nebo MediaTek (model 514) a technologií Wi-Fi 6. Dva z nich, modely 515 a 514 jsme měli možnost testovat přímo u nás v redakci, a proto můžeme potvrdit, že jde o skvělé chromebooky s prvotřídním designem a odolnou konstrukci.

Všechny nové chromebooky Acer podporují aplikace z Google Play a webové aplikace poskytované z cloudu, které jsou stále populárnější a rozšířenější. Nativní integrace chromebooků s cloudem od Google je velkou předností pro současný moderní, hybridní styl práce v různých prostředích a na různých zařízeních. Přechod mezi různými zařízeními je u chromebooků prakticky bezešvý a pro uživatele není důležité zařízení, na kterém pracuje, ale jeho data, která má dostupná odkudkoli a kdekoli.

Modely v provedení Enterprise navíc odemykají integrované možnosti systému Chrome OS pro jednoduché nasazení a správu chromebooků ve firmách. Mimořádně snadné nastavení a ovládání je ovšem typickou vlastností všech chromebooků, které mají integrované zabezpečení, velmi rychle se nasazují a snižují celkové náklady na vlastnictví. Velmi příjemnou vlastností chromebooků jsou také průběžné aktualizace systému i aplikací, které uživatele prakticky nijak neomezují a neobtěžují.

Acer k uvedeným výhodám chromebooků přidal u svých novinek navíc rychlejší datové úložiště, které bylo dříve typickou slabinou většiny notebooků. Díky Aceru už není a jeho nové modely nabízejí skvělý poměr ceny, výkonu a uživatelské přívětivosti.

Acer Chromebook Spin 514

První novinkou, kterou bych vám chtěl představit je konvertibilní 14" model Acer Chromebook Spin 514 (CP514-2H), který je nabízen i ve variantě Enterprise. Jde o model s kompaktním designem a 14" Full HD IPS displejem, který má úzké okraje na všech čtyřech stranách, což umožňuje dosáhnout 84% poměru obrazovky k tělu.

Chromebook Spin 514 pohání procesory Intel Core 11. generace (podle modelu až Core i7) a nabízí vysoký výkon, ale přitom pracuje tiše díky konstrukci bez ventilátorů. Při videokonferencích využívá Full HD webovou kameru s modrým skleněným filtrem a technologií redukce šumu, která poskytuje jasnější obraz a redukuje světelné odlesky. Dva reproduktory zařízení směřující nahoru lemují klávesnici a v kombinaci se dvěma mikrofony zajišťují při videokonferencích čistý zvuk.

Nové Chromebooky Spin 514 a Chromebook Spin Enterprise 514 jsou velmi odolné a mají zesílenou konstrukci s hliníkovými horními a spodními kryty a mají díky tomu certifikaci MIL-STD 810H. Mezi další klíčové atributy nových chromebooků patří touchpad ze skla Corning Gorilla Glass, podsvícená klávesnice a Wi-Fi 6.

Acer Chromebook 515 – výkon a konference s velkým 15,6" displejem

Další novinkou je model Acer Chromebook 515 (CB515-1W/T), který je také nabízen i ve variantě Acer Chromebook Enterprise 515. Jde o ideální zařízení pro podniky využívající cloudové technologie. Nové chromebooky řady 515 mají 15,6" Full HD IPS displej s volitelným multidotykovým ovládáním a jsou poháněny procesory Intel Core 11. generace a výkonnou grafikou Intel Iris Xe. Jsou vybaveny PCIe NVMe úložištěm s kapacitou až 512 GB a až 16 GB paměti RAM, což například

umožňuje probuzení chromebooku z režimu spánku za méně než sekundu.

Notebooky Chromebook 515 a Chromebook Enterprise 515 mají stylový hliníkový horní kryt a zesílenou konstrukci, a proto se mohou pochlubit odolností na úrovni armádní normy MIL-STD 810H. Hladký touchpad ze skla Corning Gorilla Glass zajišťuje plynulé a přesné ovládání, posouvání a rolování, zatímco podsvícenou klávesnici vylepšuje přítomnost numerického bloku.

Nové 15,6" chromebooky jsou vybaveny dvěma všestrannými porty USB 3.2 Gen 2 Type-C (jeden na každé straně) pro přenos dat, napájení a sdílení obrazu a zvuku na externích displejích. Připojují se bezdrátově pomocí Wi-Fi 6 a jsou vybaveny i rozhraním HDMI a čtečkou karet microSD.

Acer Chromebook 514

Nový Acer Chromebook 514 (CB514-2H/T) má ultrapřenosný design a je poháněn osmijádrovým procesorem MediaTek Kompanio 828, který s přehledem zvládá velmi úsporný operační systém ChromeOS a poskytuje celodenní, až 15hodinovou výdrž baterie a lze jej rychle nabít až na 50 % kapacity této baterie za pouhých 30 minut. Jde o elegantní zařízení, které váží pouhých 1,3 kg a je tenké 16,85 mm, takže je dostatečně kompaktní pro časté přenášení. Stylový hliníkový horní kryt poskytuje ochranu proti promáčknutí, zatímco touchpad ze skla Corning Gorilla Glass zajišťuje plynulé ovládání. Čtrnáctipalcový matný displej Chromebooku (volitelně multidotykový) má úzké rámečky a ve výbavě nechybí ani podsvícená klávesnice.

Acer Chromebook Spin 314

Poslední novinkou v nabídce Aceru je cenově dostupný Chromebook Spin 314 (CP314-1H/N), který je vybaven nejnovějšími procesory Intel, 14" dotykovým Full HD IPS displejem s úzkými rámečky a nabízí cca 10hodinovou výdrž na baterii, což z něj dělá dobrou volbu například pro studenty. Mnoho z nich jistě potěší, že model Spin 314 je vybaven ekologickým touchpadem OceanGlass vyrobeným výhradně z plastového odpadu, který byl recyklován do textury připomínající sklo. Acer Chromebook Spin 314 je také vybaven širokou škálou možností připojení – portem USB 3.2 typu C, dvěma porty USB 3.2 typu A, portem HDMI, čtečkou karet MicroSD a technologií Wi-Fi 6. ■

Skupina ICZ má nového generálního ředitele

Dan Rosendorf se stal novým generálním ředitelem Skupiny ICZ a zároveň byl zvolen i předsedou představenstva skupiny. O změně na těchto pozicích rozhodl jako jediný akcionář ICZ Holding. Změna byla plánovaná dlouhodobě a je účinná od 1. února 2022. Dan Rosendorf ve Skupině ICZ působí od roku 2012 a v posledních letech zastával pozici ředitele sekce Bezpečnosti.

Dosavadní generální ředitel a předseda představenstva Bohuslav Cempírek ve Skupině ICZ zůstává i nadále. Nově bude zastávat pozici Chief Operations Officer a bude se věnovat aktivní obchodní činností u stávajících i nových zákazníků. Jako generální ředitel a předseda představenstva úspěšně působil 15 let.

Michal Andraško je novým obchodním ředitelem Asseco Solutions

Řady top managementu společnosti Asseco Solutions posílil Michal Andraško, zkušený obchodník a manažer, který se stal novým obchodním ředitelem českého lídra na trhu ERP systémů. Michal Andraško je absolventem několika univerzit, kde vystudoval marketing, ekonomii a management. Celý svůj profesní život, který započal již při studiu střední školy, se věnoval prodeji v oblasti informačních a komunikačních technologií. Postupně získával cenné zkušenosti a zastával vyšší a vyšší, posléze manažerské pozice. Poslední zkušenost byla ve Twisto payments na pozici Head of Sales.

Nordic Telecom mění výkonného ředitele

Na pozici výkonného ředitele v telekomunikační společnosti Nordic Telecom nastoupí od 1. února letošního roku Libor Dočkálek (48). Ten působí ve vysokých manažerských pozicích firmy již od jejího založení před šesti lety. Poslední dva roky zastával Dočkálek funkci ředitele pro strategii a produkty. Nahrazuje dlouholetého CEO Jana Čorneje, během jehož působení se stal Nordic Telecom jedním z pěti největších poskytovatelů internetového připojení v Česku.

Novým generálním ředitelem CDC Data byl jmenován Pavel Smoleň

Společnost CDC Data, poskytovatel komplexních ICT služeb, oznamuje významné personální změny. Novým generálním ředitelem společnosti se od 6. ledna 2022 stal Pavel Smoleň. Na této pozici vystřídal zakladatele a spolumajitele CDC Data Luboše Strapinu, který se ke stejnému datu přesunul do představenstva společnosti.

Další personální změny v CDC Data: novým obchodním ředitelem se stane Martin Bedroš. Dosavadní obchodní ředitel Jiří Prokeš bude zastávat pozici provozního ředitele společnosti.

Kateřina Trčalová nově řídí marketing systémů HELIOS

Management firmy Asseco Solutions posílila Kateřina Trčalová, která se stala novou šéfkou marketingového oddělení. Kateřina působí v Asseco Solutions již od roku 2006 (s přestávkou na rodičovskou dovolenou) a pracovala zde postupně na několika pozicích v oblasti marketingu. Díky svým úspěchům na předchozích pozicích byla na počátku letošního roku pověřena řízením marketingu systémů HELIOS.

Ireneusz Kubies bude řídit rozvoj partnerské sítě Inforu v regionu CEE

Společnost Infor oznámila, že na pozici Alliance Director pro region CEE byl nově jmenován Ireneusz Kubies. Ve své pozici bude řídit a rozvíjet partnerství s aliančními partnery společnosti Infor v regionu s důrazem na rozvoj cloudových nabídek Infor postavených na platformě Amazon Web Services (AWS).

Ireneusz Kubies pochází z Polska, ale studoval a nyní žije v Praze. Hovoří česky, slovensky, polsky, anglicky a rusky. Součástí týmu Infor CEE se sídlem v Praze je už od roku 2014, kdy nastoupil jako regionální Channel and Direct Sales Manager. Dnes je zodpovědný za rozvoj regionálních aliančních strategií a řízení vztahů s partnery z řad systémových integrátorů, technologickými či konzultačními partnery.

Před svým nástupem do společnosti Infor strávil 4 roky v Hewlett-Packard jako Account Executive pro střední a východní Evropu a předtím v ICZ jako Product Management Manager. Vystudoval Fakultu strojní na Českém vysokém učení technickém (ČVUT) v Praze, obor automatizované systémy řízení.

ČMIS posiluje technologický tým

Technologická společnost ČMIS posiluje své technické oddělení. Na pozici CTO nově nastoupil Jindřich Mičán, který přišel z firmy DataSpring. Své dlouholeté vývojářské i manažerské zkušenosti chce zúročit i ve ČMIS, zaměří se především na zkvalitnění stávajících služeb pro nové i stávající klienty, mezi něž patří například e-commerce lídři Rohlík.cz, Shoptet nebo Pilulka.cz. Rovněž

se bude věnovat optimalizaci interních procesů a posilování stávajícího technického týmu.

Asseco Solutions má nového ředitele vývoje

Řady top managementu Asseco Solutions nedávno rozšířil nový ředitel divize vývoje, Ing. Petr Vítek. Jeho úkolem je stále zlepšovat kvalitu produktů i služeb českého lídra na trhu ERP. Petr Vítek vystudoval obor hydraulika na Fakultě strojní ČVUT, ovšem už od dětství se intenzivně zajímal o informační technologie. Od 90. let pak pracoval na mnoha IT projektech, především pro české banky, kde vedl vývojové týmy. Před nástupem do Asseco Solutions působil v ČSOB.

Softwarový dům **eMan vede Michal Košek**

Pražskou vývojářskou společnost eMan, zalistovanou na pražské burze Start počínaje novým rokem vede Michal Košek, jeden ze zakládajících členů firmy. Po více než jedenácti letech přechází z postu provozního ředitele a v roli CEO vystřídá Jiřího Horynu, který bude nadále zastávat roli předsedy představenstva.

V brněnském vývojovém centru SAP Labs vzniká nové oddělení

V brněnském vývojovém centru SAP Labs se otevírá nové oddělení Business Process Intelligence, které plánuje vytvořit silný tým místních vývojářů. Oddělení povede Jana Honková, manažerka startupu Signavio, který před rokem převzala společnost SAP. Brněnské oddělení se bude věnovat tzv. process miningu, tedy analýze a vylepšování firemních procesů na základě nasbíraných dat. Moravská metropole je první lokací ze střední a východní Evropy, kde oddělení zaměřené na analýzu firemních procesů vzniká. Do budoucna uvažuje SAP rozšířit oddělení Business Process Intelligence i do dalších lokalit v regionu střední a východní Evropy. Mezi kandidáty figuruje Bratislava či Budapešť.

Tricentis otevírá v Praze **výzkumné a vývojové centrum**

Společnost Tricentis, která je globálním lídrem v oblasti testování moderních cloudových a podnikových aplikací, otevírá v Praze výzkumné a vývojové centrum, které nabídne práci více než 200 lidem včetně netechnických pracovních pozic. Prioritou ale bude získání schopných vývojářů. Jedním z cílů pražského centra Tricentis totiž bude podpořit uvedení dalšího řešení pro automatizaci testování na trh.

Do Česka míří 28 miliard na podporu digitalizace

V rámci pocovidové obnovy unijní ekonomiky bylo České republice z evropského Nástroje pro oživení a odolnost alokováno bezmála 180 miliard korun, kdy 15 procent – necelých 28 miliard – připadne digitalizaci. O dotace na digitalizační procesy se mohou podělit soukromé firmy, státní podniky, orgány státní a veřejné správy i startupy.

Digitalizace je jedním ze dvou hlavních pilířů Národního plánu obnovy; nástroje podpory, jehož finální podobu zástupci České republiky složitě vyjednávali u Evropské komise. Jednotlivé pilíře Národního plánu obnovy mají vlastního gestora, tedy orgán státní správy, který je odpovědný za distribuci finančních prostředků NPO koncovým příjemcům. V případě digitalizace jsou to většinově Ministerstvo průmyslu a obchodu a Ministerstvo vnitra, na které se pak jednotliví žadatelé obrací.

„O dotaci na digitalizaci může žádat každý subjekt splňující podmínky vypsané právě pro jejich skupinu. Alokovaných 28 miliard korun bude rozděleno mezi šest takzvaných komponent, kde například veřejné správě je přiděleno přes 7 miliard, start-upům a novým technologiím pak přes 5,5 miliardy,“ dodává Jaromír Hanzal, předseda Asociace pro aplikovaný výzkum v IT (AAVIT).

Tab. 1: Finanční prostředky alokované na digitální transformaci. Zdroj: AAVIT

Komponenta	Alokace v mil. korun
Digitální služby občanům a firmám	2 857
Digitální systémy veřejné správy	7 054
Digitální vysokokapacitní sítě	5 787
Digitální ekonomika a společnost, inovativní start-upy a nové technologie	5 710
Digitální transformace podniků	5 000
Zrychlení a digitalizace stavebního řízení	1 446

Kromě toho, že digitalizace značně napomáhá produktivitě trhu a technologickému rozvoji, může značně snížit emise takzvaných skleníkových plynů. Digitalizace tak umožní splnit kritéria Zelené dohody pro Evropu, v níž se Česká republika zavázala ke snížení produkce oxidu uhličitého o 55 procent do roku 2030. Vzhledem ke struktuře českého hospodářství, které stále z velké části tvoří průmysl, by digitální inovace měly zjednodušit jednotlivé interní procesy, a tím i snížit jejich emise.

„Značný rozdíl může nastat třeba v emisích z dopravy. Například rozvoj technologií v oblasti rozšířené a virtuální reality zjednoduší firmám vyrábějícím jakékoli stroje potřebné pravidelné revize a s tím spojené výjezdy – jejich produkty totiž mohou v tomto prostředí revidovat ‚na dálku'. Dalším příkladem mohou být i aplikace jako Bank ID, díky které občané ušetří řadu zbytečných cest na úřady,“ vysvětluje Michal Košek, CEO společnosti eMan.

Systém bankovní identity je jedním z předních projektů vize digitálního Česka. Výhody vnímají nejen uživatelé, ale i samotní dodavatelé služeb ve veřejném a soukromém sektoru.

„Je nepochybné, že rozšiřování digitalizace je zásadní pro další rozvoj konkurenceschopnosti naší ekonomiky. Skutečnost, že o digitalizované služby mají rostoucí zájem domácnosti i firmy, nám potvrdil i rychlý nárůst obliby využívání bankovní identity k online prokazování totožnosti nejen vůči bankám, ale i vůči státu a také firmám. Když jsme si loni dělali průzkum spokojenost s využíváním bankovní identity, ukázalo se, že výhrady mají lidé vůči stále nízkému počtu digitalizovaných služeb. Rozšíření nabídky digitalizovaných služeb je oblast, na kterou se musí stát i firmy intenzivně zaměřit,“ zdůraznil Petr Zíma, manažer bankovní identity v České spořitelně. ■

IT Systems – specializovaný měsíčník o podnikové informatice

Ročník 24, číslo 1–2/2022
Cena výtisku 110 Kč/5 € (včetně DPH)
Roční předplatné: 990 Kč/39,50 € (včetně DPH)

Vydavatel
CCB, spol. s r. o., Okružní 19, 638 00 Brno
IČO: 18825435, DIČ: CZ18825435

Šéfredaktor
Ing. Lukáš Grásgruber (grasgruber@ccb.cz)
Tel.: 545 222 773

Redakce
Ing. Karel Heinige (heinige@ccb.cz)
Zdeněk Gric (gric@ccb.cz)

Elektronická média
Michal Romaňák (romanak@ccb.cz)
Václav Buk (buk@ccb.cz)

Redakční rada
Ing. Miloš Grásgruber, Ph.D.
doc. Ing. Branislav Lacko, CSc.
Ing. Jiří Löffelmann, Ph.D.
Ing. Petr Sodomka, Ph.D.
Ing. Aleš Studený

Inzerci přijímá
Ing. Jan Přikryl (prikryl@ccb.cz)
Karel Matoušek (matousek@ccb.cz)
Tel.: 545 222 779

Předplatné a distribuce
Tamara Olivová (predplatne@ccb.cz)
Tel.: 539 007 977

Distribuce na Slovensku
Mediaprint-Kapa Pressegrosso, a.s.
Stará Vajnorská 9, P.O. BOX 183,
830 00 Bratislava
Infolinka: 0800 188 826
E-mail: objednavky@ipredplatne.sk
www.ipredplatne.sk

Grafické zpracování
Vedoucí: Ing. Roman Zavřel
Zlom a sazba: grafické studio CCB

Tisk CCB, spol. s r.o, vedoucí Martin Procházka

Registrace MK ČR E 8163, ISSN 1802-002X
Nevyžádané příspěvky se nevracejí, za obsahovou správnost článků ručí autor.
Odborné příspěvky jsou recenzovány.

SEZNAM INZERENTŮ

Vydání **IT Systems 3/2022** bude věnováno IT řešením v sektorech:
- **Banky a finance, pojišťovnictví**
- **Veřejný a státní sektor**
- **Zdravotnictví, Služby**

Zaměříme se mimo jiné na témata:
- CX trendy, omnichannel, digital onboarding, RPA
- CRM – automatizace kontaktních center, chatboti
- BankID v praxi, digitalizace pojišťovnictví
- Oborová BI řešení, pokročilé technologie pro analýzu dat
- Využití technologií AI v praxi
- HRM/HCM, docházkové systémy
- Digitalizace státní správy a veřejného sektoru
- IT řešení pro zdravotnictví – eHealth
- Moderní řešení pro práci s dokumenty, digitalizace, automatizace workflow
- ITSM – výběr řešení pro řízení IT služeb a správu IT infrastruktury, SDx
- Kybernetická bezpečnost, zabezpečení a řízení hybridní pracovní síly

Do IT Systems 3/2022 připravujeme **přehled CRM řešení** na trhu.

Součástí vydání bude **příloha ERP systémy I/2022**, ve které se zaměříme na témata:
- **ERP trendy** – flexibilita, mobilita, důraz na UX a možnosti integrace, automatizace procesů, technologické trendy...
- **ERP v cloudu** – výhody, nebo omezení?
- **Jaké budou ERP systémy v době postcovidové?**
- **Klíčové otázky při výběru ERP systému** – jaké vlastnosti ERP systému nejvíce ovlivňují jeho dlouhodobý přínos pro podnik?
- **Příprava a realizace ERP projektů, kritická místa ERP projektů, nejčastější problémy a chyby při implementaci ERP systémů, modernizace a rozvoj ERP**
- **Skryté možnosti** – jak naplno využít možnosti ERP systému
- **Digitalizace zlozvyků** – jak současně digitalizovat a optimalizovat procesy
- **Branžová ERP řešení** – jak na výběr a implementaci ERP systému s vysokou mírou customizace, ERP systémy z hlediska potřeb různých odvětví
- **Modernizace a rozvoj ERP systému** – release management

Součástí přílohy bude také **přehled ERP systémů** na trhu.

Viditelnější.
Silnější.
Bezpečnější.

Mysleli jste si, že nejste připraveni na EDR?
Nyní už jste.

go.kaspersky.com/optimum

kaspersky

BRING ON THE FUTURE

Optimalizujte logistické procesy s EDI

✓ Ušetřete náklady

✓ Zvyšte kvalitu služeb

Bez ohledu na oblast, ve které poskytovatel logistických služeb působí, hlavní zásadou zůstává: „Čas jsou peníze."

Aby bylo možné dodat správné zboží ve správném čase na správné místo, musejí si obchodní partneři rychle a efektivně vyměnit a zpracovat velké množství informací.

Harmonizace této výměny dat pomocí EDI (elektronické výměny dat) přináší podstatné zjednodušení výměny informací.

Výhody procesů podpořených EDI

- Vysoký stupeň automatizace procesů
- Eliminace ručního zadávání dat a souvisejících chyb (dodací listy, stavy skladových zásob)
- Kratší doba odezvy na objednávky klientů
- Možnost dlouhodobého plánování

EDI zprávy týkající se skladového hospodářství

Dodací list: DESADV
Potvrzení příjmu zboží: RECADV
Zpráva o stavu skladových zásob: INVRPT

EDI zprávy týkající se procesu dodávek

Expediční příkaz: INSDES
Dodací list: DESADV
Faktura za logistické služby: INVOIC

EDI zprávy týkající se objednávkového procesu

Objednávka zboží: ORDERS
Dodací list: DESADV
Faktura za zboží: INVOIC

www.editel.cz

editel

obchod@editel.cz
+420 261 009 011