TEMATICKÝ MAGAZÍN VYDAVATELSTVÍ ECONOMIA, A.S.

Samostatně neprodejné
04 | 2024

ICT REVUE

Trendy v ERP

Rozvoj pokračuje k flexibilitě a mobilitě, cloudovým řešením, automatizaci a umělé inteligenci.

Kyberbezpečnost

Džin umělé inteligence se už do lahve nevrátí, říká v rozhovoru Chester Wisniewski z firmy Sophos.

Zálohování dat

Máte záložní kopii důležitých dat? A jste si jistí, že se k ní útočníci nedostanou?

Stratox
ENTERPRISES

Bude vaše
konkurence rychlejší?

Éra AI mění požadavky i na enterprise IT.
Klíčovou dovedností budoucnosti bude rychlá
a bezpečná inovace i ve složité infrastruktuře.
Zrychlete s CodeNOW®.

VÍCE SE DOČTETE V ROZHOVORU S PETREM SVOBODOU

Code NOW®

CLOUD NATIVE
COMPUTING FOUNDATION
SILVER MEMBER

ISO 27001

kubernetes CERTIFIED

www.stratox.cz

EK015633-1

OBSAH

MAGAZÍN ICT REVUE – PŘÍLOHA HOSPODÁŘSKÝCH NOVIN A EKONOMU, 10. 4. 2024. Ředitel speciálních projektů Aleš Mohout • Art director Jan Vyhnánek • Editor Martin Knížek (martin.knizek@economia.cz) • Layout Jan Stejskal • Grafika vizuální studio mediálního domu Economia • Adresa redakce Pernerova 673/47, 186 00 Praha 8 • Tisk Triangl, a.s., Praha • Samostatně neprodejné • http://www.hn.cz

Partner magazínu

minerva.

Inzerce

K2

K2 ERP

Podnikový software

pro úspěšné firmy

www.k2.cz

EK015583

ERP: vyšší nároky na bezpečnost i provoz

Dynamický vývoj a změny ve světě, v ekonomice, napříč všemi trhy vedou k hlubokým transformacím. Vyžadují nové přístupy, rychlé reakce a vysokou efektivitu. To vytváří tlak na další rozvoj podnikových informačních systémů.

E

ERP systémy zaznamenaly v posledních letech tlak na zrychlení procesů, širší funkcionalitu, zjednodušení a flexibilitu. Objevily se nové trendy, některé z nich, jako třeba analýza dat a Business Intelligence, využívání programovacích rozhraní API, respektive webových rozhraní a služeb či přístup prostřednictvím mobilních zařízení se už postupně staly standardem. Další směry aktuálně nabývají na významu. Mezi ně patří vysoké nároky na flexibilitu a mobilitu, zavádění cloudových řešení, automatizace a využívání strojového učení a umělé inteligence. A také tlak na kyberbezpečnost, což je téma, s nímž má bolestnou zkušenost stále více firem.

Flexibilita a mobilita kladou nároky na infrastrukturu ERP řešení

Dnešní ERP řešení jsou daleko flexibilnější než například v předcovidovém období. Jsou více zaměřena na kontinuální rozvoj. Reagují pružněji na změny trhu, vývoj technologií i samotného podniku. Mají složité a přesné algoritmy, které procesy zrychlují, poskytují mnohem přesnější reporty a umožňují přesnější plánování. A nejen pod tlakem uživatelů jsou dnes mnohem flexibilnější a mobilnější než v minulosti. „Vše směřuje k flexibilnímu prostředí, v němž si koncový uživatel optimalizuje své obrazovky dle okamžitých potřeb a vyškolený uživatel generuje nové funkce a nové aplikace bez programátorských znalostí. Tyto změny pak bude možné snadno přenášet do vyšších verzí ERP systému, protože budou kódovány v databázi, a nikoli v programech," upřesňuje Vladimír Bartoš, ředitel pro strategii společnosti Minerva Česká republika.

Předávání dat třetích stran přes dávkové importy a exporty či specializovaná rozhraní jsou již téměř minulostí. Nové ERP systémy využívají webové služby a REST API, tedy standardizovaná rozhraní, přes něž aplikace komunikují. Pochopitelně tyto výhody a trendy ale podle Bartoše znamenají výrazně složitější infrastrukturu ERP systémů a také je složitější programování změn funkcí, které nelze vyřešit výše uvedenými metodami. Tím rostou nároky na základy provozního prostředí ERP systémů a na jejich správu.

> „Směřujeme k flexibilnímu prostředí, v němž si vyškolený uživatel generuje nové funkce bez programátorských znalostí.

text: Marcela Štefcová, foto: Shutterstock

flexibilitu, v cloudu

Aktuálním trendem je cloud

Začátkem loňského roku uváděli přechod na cloud jako hlavní trend v ERP řešeních dva ze šesti odborníků, kterých jsme se ptali, letos již čtyři ze sedmi. Jde o silný trend a stále více podniků na cloudová řešení svých systémů přechází, nemluvě o případech nově pořizovaných nebo generálně updatovaných ERP systémů ve firmách. Jejich flexibilita, škálovatelnost, dostupnost informací v reálném čase, rychlá implementace a ověřené konfigurace, častější updaty nových funkcionalit a nižší počáteční náklady jsou velkými plusy. Navíc znamenají úsporu i ve vlastním personálním zajištění podniků, protože odpovědnost za správnou funkci přebírají profesionálové, tedy dodavatel systému a prostředí. Tuto migraci lze sledovat napříč obory i ve složitějších výrobách a retailu.

Určitým omezením pro podnik, které je třeba řešit hned na počátku, je nutná změna myšlení a přístupu k ERP řešení v cloudu. „Klienti se musí přizpůsobit standardům dodávaného systému a jeho možným konfiguracím a smířit se s faktem, že úpravy na míru jsou komplikované, drahé i personálně nákladné a je vhodné je buď nedělat, nebo řešit systémem dodávek od třetích stran. A přijmout tento fakt, respektive napasovat některé klienty do dodávaných standardů, je a bude velmi těžké," myslí si Petr Schaffartzik, generální ředitel K2 atmitec.

Zabezpečení firmy často řeší až po incidentu

Jednou z dalších výhod cloudu oproti on-premise řešení je přesun odpovědnosti za dostupnost a hlavně bezpečnost na třetí stranu. Právě kyberbezpečnost je nebo by měla být v podnicích zásadním tématem. Přitom podle Schaffartzika podniky často například svou infrastrukturu a její

Inzerce

EK015643

QI NABÍZÍ KOMPLEXNÍ ŘEŠENÍ S DLOUHODOBÝMI PŘÍNOSY

CENTRÁLNÍ MOZEK FIRMY

1 490 implementací

24 let tradice

40 implementačních partnerů

Český informační systém QI podporuje stovky společností při:
- řízení, optimalizaci, digitalizaci i automatizaci firemních procesů,
- zpracování a sdílení podnikových informací,
- úspoře nákladů.

Nasazení QI je konkurenční výhodou pro firmy všech velikostí z nejrůznějších oborů. Mimo jiné dlouhodobě přispívá k bezproblémovému chodu tří známých českých společností, které jeho **přínosy popsaly ve videu**. Jak konkrétně pomáhá, zjistíte na **www.qi.cz/videoreference**

zabezpečení podceňují až do doby, než dojde k významnému incidentu. Firmy také často dostatečně nezálohují nebo zálohy neprobíhají korektně a pak dochází k nevratným ztrátám dat. „První až třetí místo v bezpečnostních opatřeních zaujímá u firem podle mě zálohování dat. Až tak je důležité. Doporučuji je nejen provádět pravidelně, ale také zabezpečit, aby byly zálohy chráněny před neoprávněným přístupem," důrazně doporučuje Tomáš Smutný, generální ředitel QI Group.

Dalším faktorem je bezpečnost koncových zařízení, se kterými uživatel pracuje. „Dnes je zcela běžné přistupovat k ERP systému z mobilních zařízení a přes webové prohlížeče, kde existuje riziko útoku přes některý operační systém, zadní vrátka v zařízení nebo v aplikaci prohlížeče. Na úrovni základní architektury pak je potřeba řešit jednak propojení ERP systému s dalšími prvky, jednak bezpečnost serverů nebo cloudu," upozorňuje Petr Kelar, ředitel společnosti ABIA CZ services.

Navíc zajištění ERP systémů s ohledem na kyberbezpečnost není jednouché a vyžaduje kvalifikované odborníky, kterých je nedostatek. „Průměrně trvá 277 dní, než se zjistí narušení bezpečnosti, a jen ve Spojených státech je více než 700 tisíc volných pracovních míst v oblasti kybernetické bezpečnosti," zdůrazňuje Martin Dudek, Solution Architect společnosti SAP. Proto je podle něho důležité, aby firmy upřednostňovaly svou kybernetickou připravenost a reakci na rizika a investovaly do školení a rozvoje svých pracovníků v této oblasti.

> „První až třetí místo v bezpečnostních opatřeních zaujímá u firem zálohování dat. Až tak je důležité.

Četnost kybernetických útoků v posledních letech výrazně vzrostla a byla odhalena řada slabých míst v ERP systémech, které dodavatelé řeší. Ostatně s novou evropskou směrnicí NIS2 a její aplikací do národních legislativ se rozšiřuje počet podniků, jichž se legislativa vztahující se ke kyberbezpečnosti dotýká. Rostou tedy bezpečnostní požadavky a promítají se do nových IT technologií. „Začíná být čím dál více využíván tzv. Zero Trust Security model, který vyžaduje kvalitní řešení bezpečnosti u všech prvků podnikového IT, tedy i u ERP systémů. To vede na jedné straně k urychlení upgradů ERP systémů v podnicích a na druhé straně k vytvoření ERP systémů, které mohou být kontinuálně upgradovány. A protože personální zdroje v IT odděleních podniků jsou v současnosti obvykle nedostačující, směřuje to k poskytování ERP jako služby," shrnuje Vladimír Bartoš.

Dochází tak ke snížení bezpečnostních rizik, jako jsou kyberútoky, ztráta dat či vydírání společností. „V cloudu jsou data zabezpečena na úrovni, kterou si nejen malá či střední,

Inzerce

datamind

Naučíme vaše data **vydělávat**

Průkopníci data science v ČR, se zkušenostmi ze **130+ projektů** a **50+ klientů**. Přinášíme **vysokou návratnost** již od začátku spolupráce. Dodáváme vše datové: integraci, dashboardy i data science modely k cílení a zisku. Jsme průvodci po datech.

Reporting a business inteligence
Mějte přehled o firmě i zákaznících

Datové a marketingové analýzy
Rozhodujte se strategicky

Umělá inteligence a Machine Learning
Využívejte AI ve svůj prospěch

Segmentace zákazníků
Poznejte a oslovte zákazníky

Prediktivní analytika
Předvídejte chování i trh

Datová integrace
Pracujte s daty efektivně a jednotně

... a mnoho dalšího

Microsoft Solutions Partner
Data & AI
Azure

Zavolejte mi, napište mi.

Vymyslíme datovou revoluci na míru i pro Vás.

Jan Matoušek (CEO)
+420 720 705 639
jan.matousek@datamind.cz
www.datamind.cz

EK015642

ale často i velká firma může jen těžko dovolit," je přesvědčen Robert Fárek, ředitel a předseda představenstva společnosti ITeuro.

Velmi rizikovým faktorem u bezpečnosti ERP systémů jsou uživatelé a administrace jejich uživatelských účtů, politika hesel a ověřování přístupu. Jejich podcenění vede často k neoprávněným přístupům a zcizení nebo úniku klíčových dat, které podnikové systémy obsahují. „Mezi aktuální největší hrozby patří ransomwarové útoky, které typicky využívají zranitelnosti na straně uživatelů. Ti, často v dobré víře, obvykle umožní zahájení útoku a zašifrování podnikových dat," varuje Milan Tesař, obchodní ředitel společnosti InfoConsulting Czech.

Úmyslným krádežím dat vlastními pracovníky jde zabránit jen těžko i s nejpřísnějšími pravidly. Těžko lze zamezit například ofocení obrazovky mobilním telefonem. Ale neoprávněné přístupy do systému lze eliminovat vhodnou politikou autentizace a silnými bezpečnostními opatřeními, jako je monitorování aplikací v reálném čase, soulad s místní legislativou a ochrana proti zneužití. A také je podle Tesaře nutná prevence ve formě osvěty. Tedy opakované vzdělávání pracovníků v oblasti kyberbezpečnosti, upozorňování na rizika a vysvětlování jejich dopadů. Důležité je i nastavení a také pravidelné ověřování a zlepšování plánu reakce na incidenty.

> Mezi aktuální největší hrozby patří ransomwarové útoky, které typicky využívají zranitelnosti na straně uživatelů.

Umělá inteligence na pořadu dne

Dalším zřetelným trendem, který je ale některými odborníky zatím vnímán spíše jako příliš „velký humbuk", je využívání umělé inteligence. Strojové učení a umělá inteligence se hojně sklouňují v mnoha oborech a pracuje se s jejich využitím i v aplikacích a systémech pro řízení podniků a jejich byznysů. „Přestože je zde velký potenciál, v praxi jde spíše o specifické využití než široce, nebo dokonce plošně aplikované nástroje. Souvisí to jednak s bezpečností, ale také se zodpovědností. Firmy zůstávají konzervativní a nechtějí svěřit zásadní rozhodování počítačovým algoritmům. Uplatnit se tak AI může zejména tam, kde uživatelům poskytne doporučení a zrychlí jejich práci, za kterou ale budou nadále oni sami zodpovědní," myslí si Petr Kelar.

Zároveň ERP systémy pracují už ze své podstaty s přesnými daty, využívají přesné algoritmy a umělá inteligence své uplatnění nachází podle Petra Schaffartzika zatím spíše v oblastech, které by označil za periferie ERP systému. „ERP lze dnes snadno integrovat s různými nástroji pro vytěžování dokumentů, které umožní jejich ná-

Inzerce

EK015592

sledné automatické zpracování. Umělou inteligenci můžete využít v podobě doplňování popisů k produktům na vašem webu. Nebo alespoň k návrhu takových popisů, které následně upravíte dle svých představ," doplňuje Schaffartzik.

Podle Tomáše Smutného ale začne být využívání AI a strojového učení aktuální. „Automatizovat opakující se úkoly, optimalizovat procesy a poskytovat prediktivní analýzy chce každý," domnívá se Smutný.

Jak rychle si některé klíčové případy najdou místo v každodenní práci uživatelů, podle Milana Tesaře ještě uvidíme. „Copilot dokáže shrnout informace o datech v různých modulech a pomoci s jejich zpracováním díky znalosti dokumentace, strojové učení lze využít při plánování výroby či servisu, anebo při predikcích prakticky čehokoliv na základě dostatečného objemu dat pro trénink modelu. Například predikce cash flow, úspěšnosti obchodních příležitostí, poptávky a podobně," myslí si Milan Tesař.

Podle Roberta Fárka jsou na reálné přínosy AI velké ERP systémy připraveny a existují již první příklady konkrétních realizací. „Využití při zpracování poptávek a nabídek nebo v oblasti údržby strojů a zařízení jsou příklady, kde lze dosáhnout přínosů rychle a efektivně," myslí si Fárek.

Umělá inteligence je využívána nejen pro analýzu a vyhodnocování přesných dat, ale také čím dál více při zpracování nestrukturovaných dat, tedy například založení objednávky či faktury ze skenu, nebo při personalizaci uživatelského prostředí na základě zkušeností, tedy přizpůsobení nabídky podle předchozího chování a potřeb uživatele. Podle Martina Dudka jsou dnes vidět v rámci ERP systémů dva hlavní trendy vývoje umělé inteligence – využívání generativní AI a zefektivňování vývoje a nasazení systému. Dochází například k využívání komunikace v přirozeném jazyce, kdy asistent nebo asistentka odpovídá běžným jazykem na otázky týkající se například klíčových konceptů, systémové navigace a podobně.

„Nesmíme ale zapomínat, že AI je vždy závislé na kvalitě dat, standardizaci systému a podobně. Pokud firmy nemají pořádek v datech, mají složité konfigurace systému ERP, tak využití AI modelů se tím hodně snižuje," upozorňuje Dudek. Lze tedy podle něho říci, že využívání umělé inteligence v systémech ERP v posledním roce výrazně vzrostlo a očekává, že v blízké budoucnosti bude dále růst se zaměřením na zvýšení efektivity, produktivity a rozhodování pomocí pokročilých technologií umělé inteligence.

> Využívání umělé inteligence v systémech ERP v posledním roce výrazně vzrostlo.

Inzerce

text: Marcela Štefcová, foto: archiv firem

Co je největší bezpečnostní hrozbou u ERP systémů?

Milan Tesař
obchodní ředitel,
InfoConsulting

Otázka kyberbezpečnosti je v souvislosti s ERP zásadní, protože tyto podnikové systémy obsahují klíčové podnikové informace a zpracovávají citlivé transakce. Mezi aktuální největší hrozby patří ransomwarové útoky, které typicky využívají zranitelnosti na straně uživatelů. Ti, často v dobré víře, obvykle umožní zahájení útoku a zašifrování podnikových dat. Prevencí je na jedné straně osvěta a vzdělávání uživatelů, na straně druhé připravenost IT na podobný druh incidentů. Zálohování dat do oddělené lokality, klidně i offline, a nastavení, pravidelné ověřování a zlepšování plánu reakce na incidenty (disaster recovery plan).

Vladimír Bartoš
ředitel pro strategii,
Minerva

ERP systémy jsou velmi komplexní a mívají dlouhý životní cyklus. Proto je firmy provozují ve starších verzích, které ale současné požadavky na bezpečnost nesplňují. Dřívější řešení bezpečnosti založené na interní síti chráněné na hranicích proti externímu prostředí je kvůli rozšíření vzdáleně pracujících uživatelů neúčinné. Čím dál více se využívá zero trust security model, který vyžaduje kvalitní řešení bezpečnosti u všech prvků podnikového IT, tedy i u ERP systémů. To vede jednak k urychlení upgradů ERP systémů v podnicích, jednak k vytvoření ERP systémů, které mohou být kontinuálně upgradovány. A protože personální zdroje v IT odděleních podniků jsou často nedostačující, směřuje to k poskytování ERP jako služby (SaaS).

Tomáš Smutný
generální ředitel,
QI Group

Z mého pohledu nejde v prvé řadě o ERP, ale primárně musíte zabezpečit podnikovou síť. ERP je jen jeden ze softwarů, který může být postižen. Mezi největší hrozby patří kybernetické útoky, s ransomwarem se setkala již téměř každá firma. Proto zálohujte, zálohujte a zálohujte. Dále je to slabá autentizace, která umožní útočníkům získat přístup k účtům a datům i v ERP. A také jsou to zastaralé aktualizace a záplaty, které ERP vystavují bezpečnostním hrozbám. Pokud tedy údržbu zanedbáváte, zbytečně riskujete.

Petr Schaffartzik
generální ředitel,
K2 atmitec

Kyberbezpečnost ERP systémů v první řadě souvisí s infrastrukturou, na které je systém provozován, a jejím zabezpečením. Podniky tuto problematiku podceňují až do doby, kdy dojde k významnému incidentu. V oblasti infrastruktury platí, že nejlepší zabezpečení nabízí komerčně provozované cloudy. Bezpečnost vlastních ERP systémů je nutné řešit už na úrovni vývoje formou například penetračních testů. Tím nejrizikovějším prvkem z pohledu kyberbezpečnosti jsou také u ERP systémů lidé. Administrace uživatelských účtů, zvolená politika hesel nebo například dvoufaktorové ověření při přihlašování do systému jsou nutnými předpoklady.

Robert Fárek
ředitel a předseda
představenstva,
ITeuro

Osobně si myslím, že účinným lékem je cloud. Systém i data jsou v cloudu zabezpečena na takové úrovni, kterou si prostřednictvím vlastních sil a investic může střední, ale i větší firma jen těžko dovolit. Bezpečnost je jedním z hlavních pilířů cloudových služeb. Chápu, že cloud je v české kotlině stále ještě přijímán s rezervami a spoustou námitek. Je třeba se o tom otevřeně bavit. V oblasti kyberbezpečnosti jsem přesvědčen, že je to rozhodně správná cesta a zároveň silný argument pro rozhodnutí přesunout ERP systém do cloudu.

Martin Dudek
Solution Architect,
SAP

Mezi největší kybernetické bezpečnostní hrozby pro systémy ERP patří neoprávněný přístup, narušení dat a útoky malwaru. Pro zmírnění těchto rizik je důležité zavést silná bezpečnostní opatření, jako je monitorování aplikací v reálném čase a ochrana proti zneužití. Důležité je také vyhodnocovat, sledovat a dokumentovat zranitelnosti v souladu se standardy správy zranitelností podniku. Jedním z problémů při zabezpečení systémů ERP je nedostatek kvalifikovaných odborníků a složitost systémů. Je důležité, aby společnosti upřednostňovaly svou kybernetickou připravenost a reakci na rizika a investovaly do školení a rozvoje svých pracovníků v oblasti kybernetické bezpečnosti.

42 | PRAGUE

LOV IT TALENTŮ

CO DĚLÁ ŠKODA AUTO NEBO ČSOB JINAK?

Téměř 40 % českých IT firem plánuje letos nábor nových vývojářů; trh je ale ve stavu akutního nedostatku kvalitních IT pracovníků. Jak tuto situaci vyřešili ti největší hráči v oboru jako Škoda Auto, ČSOB, Microsoft nebo SAP? Spojili se formou partnerství se špičkovým IT inkubátorem 42 Prague a zajistili si tak pravidelný přísun kvalitních IT talentů přímo od zdroje. A navíc získali konkurenční výhodu díky podpoře inovací a rovnosti v IT.

JAK SE RODÍ VÝJIMEČNÉ TALENTY

42 Prague je bezplatný institut programování a nezisková organizace. Využívá praktické, projektově orientované učení a zohledňuje aktuální i budoucí potřeby trhu. Díky tomu vychovává absolventy, kteří jsou nejen technicky zdatní, ale zároveň se profilují jako opravdoví průkopníci ve svém oboru. Jsou přirozeně proaktivní a mají chuť přinášet vlastní inovativní řešení. Vynikají v praktickém řešení problémů a jsou zvyklí pracovat a doručovat výsledky samostatně s vlastní motivací, aniž by potřebovali neustálý dozor.

VÝRAZNĚ NIŽŠÍ NÁKLADY NA NÁBOR VÝVOJÁŘŮ

Hlavním motivátorem firem pro partnerství s 42 Prague je přímý kontakt s talenty institutu. "Studenti se s našimi partnery seznamují již během studia formou prezentací, panelových diskusí nebo díky mentoringovému programu, po dokončení vzdělávacího programu mají pak firmy možnost nabídnout absolventům navazující stáže nebo rovnou pracovní pozice. To vše bez tradičních nákladů na nábor například přes headhunting. Jelikož se studenti seznamují se zástupci firem v průběhu studia, jejich následná adaptace u partnerů je výrazně snazší a riziko odchodu ve zkušební době nižší. Absolventi 42 Prague jsou zárukou kvality a loajality," říká CEO 42 Prague Peter Podprocký.

Partnerství s 42 Prague otevírá dveře k nejlepším IT talentům a umožňuje přímý pohled do srdce IT komunity včetně networkingových eventů. Partnerství také podporuje celoživotní bezplatné vzdělání a transformaci českého pracovního trhu. Propojte se s lídry trhu jako Škoda Auto, ČSOB, Microsoft nebo SAP a zajistěte si své místo v budoucnosti IT.

SPOJTE SVOU ZNAČKU S BUDOUCNOSTÍ IT

Spolupráce s 42 Prague ale není jen o finančních benefitech. Je to také příležitost posílit povědomí o značce ve vzdělávacím a technologickém prostředí. Spojením s 42 Prague dávají firmy najevo svůj závazek k inovacím a podpoře budoucí generace IT profesionálů, nebo třeba také k větší genderové vyváženosti ve světě IT. To je obzvláště cenné v dnešním konkurenčním prostředí, kde uvědomělá značka podporující SDGs přitahuje nejen top talenty, ale i lukrativní zákazníky.

Zjistěte více o partnerství s 42 Prague

text: redakce, foto: Minerva

Neopakujte chyby za miliony korun

Výrobní podniky v Česku investují do informačních technologií desítky milionů korun a ročně jsou pak nuceny vynakládat další miliony na různé upgrady, náhrady nefunkčních částí nebo nápravy předchozích chyb ve své IT strategii. Některým často opakovaným chybám by se přitom podle Vladimíra Bartoše, ředitele pro strategii společnosti Minerva, mohly jednoduše vyhnout.

Jaké nejčastější chyby české firmy při investicích do IT systémů dělají?
Nejsložitější oblastí na implementaci je oblast plánování výroby a nákupu. Zasahuje do prodeje, nákupu, výroby, technické přípravy, skladů a stačí jedna nefunkčnost a plánování přestává dávat použitelné výsledky. Jádrem plánování je podnikový informační systém ERP, který všechny tyto oblasti musí pokrývat. Přesto se překvapivě často setkávám s názorem: „Nefunguje nám plánování – přikoupíme k našim systémům ještě APS, pokročilé plánování.“ Jde tedy o další investici v hodnotě jednotek milionů korun s velmi komplexním rozhraním na stávající ERP systém – ten totiž musí do APS předávat zakázky, nákupní objednávky, zásoby, rozpracovanost, naplánované výrobní příkazy s postupy a kusovníky, zdroje s jejich kapacitními kalendáři a zpět musí přebírat optimalizovanou frontu operací pro jednotlivé stroje. Šance tohoto postupu na úspěch je nulová. Pokud v ERP nefunguje MRP plánování na střednědobé úrovni, nemůže fungovat ani APS podrobné plánování.

Co dalšího ve firmách často nefunguje?
Téměř každý týden procházím výrobní prostory některé firmy a několikrát jsem si všiml, že se tam vyskytují potemnělé obrazovky, které zřejmě měly něco ukazovat. Vysvětlením překvapivě často bylo: „Implementovali jsme MES, ale informace z něj téměř nikdo nevyužívá.“ Podnětem pro jeho zakoupení byl vágní požadavek managementu na digitalizaci výroby nebo snaha získat pár výrobních ukazatelů. Důvodem špatného využívání výrobního informačního systému bývá jeho slabá integrace s ERP. Pokud totiž ERP nepředává do MES naplánované výrobní příkazy s vyskladňovacími seznamy a postupy, alternativy, odkazy na výkresy či 3D modely, zásoby, materiál na cestě, docházku nebo předává jen část z těchto údajů, nemůže MES správně koordinovat práci operátorů. Pokud pak ERP nevyžaduje od systému MES zaevidované výdeje materiálů do výrobních příkazů, přípravné a výrobní časy, hlášení a opravy neshod, příjmy z příkazů a další informace, aby mohl o výrobě správně účtovat a navázat plánováním, chybí zásadní motivace a tlak na aktivní využívání MES systému a ten pak umírá.

Bývá problém také v ERP systému?
V posledních dvou letech nás oslovily už čtyři výrobní podniky, v nichž jsme dříve skončili ve výběrovém řízení na ERP systém druzí, že vypisují nový výběr a chtějí nás v něm. Jeden z nich dokonce chce implementovat nový ERP již počtvrté za posledních deset let! Důvody opakovaných implementací bývají tři: systém nemá potřebnou funkcionalitu, nemá dobrou podporu nebo jeho dodavatel není schopen poskytnout svému klientovi dostatečnou podporu při digitalizaci nebo při reengineeringu podnikových procesů.

Jaký ERP systém je pro výrobní podnik lepší: lokální, nebo globální?
Informační systém se zahraničními implementacemi kdesi v Evropě není automaticky globálním systémem. Stačí i malý systém s dobrým marketingem a cenou a můžeme jej instalovat přes šikovné partnery kdekoli. Globální systém poznáme podle větších instalací v pobočkových firmách, kde dokáže plánovat ve složitějším organizačním prostředí. Pak máme záruku, že bude mít širší funkcionalitu i v dalších procesech a že bude dlouhodobě ekonomicky a funkčně stabilní. Ale určitě neplatí, že každý globální ERP má vše, co bude firma potřebovat. Lze je rozdělit na All in One a Best of Breed. První se snaží řešit vše, najdeme je nejen ve všech výrobních odvětvích, ale i ve službách či obchodě. Jejich implementace je drahá a dlouhá. Best of Breed ERP systémy se zaměřují na konkrétní výrobní odvětví a tam poskytují hlubokou funkcionalitu. Lze je rychle naimplementovat a převzít z nich odvětvové standardy.

Jak tedy optimálně stavět ERP?
Můžete si nejprve vybrat levnější ERP systém. Až zjistíte, že to není ono, můžete přikupovat další specializované systémy, pracně je integrovat a každá změna v některém z nich vyvolá dominový efekt. Ve výsledku to bude drahé, zdlouhavé a nikdy to nebude fungovat jako perfektně integrovaný celek. Nebo můžete svůj nedostatečný ERP systém vyměnit za Best of Breed, který má na potřebné úrovni integraci se světovým APS, přímo obsahuje MES, umí se napojovat na stroje a podobně. Proč to dělat složitě, když to jde jednoduše?

Text vznikl ve spolupráci se společností Minerva

Vladimír Bartoš, ředitel pro strategii společnosti Minerva

> “ Globální systém poznáme podle větších instalací v pobočkových firmách, kde dokáže plánovat ve složitějším organizačním prostředí.

GIRITON

Domluvme si schůzku a ukázku systému:

+420 728 543 275 | **info@giriton.com**

Docházkový a HR systém GIRITON

Chtějte od svého docházkového systému **maximum**.

www.giriton.com

Moderní docházkový systém

Evidence docházky, služebek, homeofficů, přesčasů, hlídání zůstatků dovolených, stravenek, noční, práce o víkendu, ve svátek, osoby na pracovišti, příplatky na míru...

Žádosti

Podávání a schvalování žádostí (o dovolenou i další aktivity) z píchaček, mobilní appky i z webu, včetně dodržení nastavených limitů...

Plány směn

Plánování směn, registrace na směny a ohlídání limitů osob přihlášených na směny. Dodržení legislativy (povinné odpočinky atp.), žádosti o změny směny...

Plánované úlohy, notifikace

Hlídání přítomnosti na pracovišti, notifikace o 300 hod u DPP, konci zkušební doby, konci prac. smlouvy, automatické notifikace o neočekávaných událostech.

Čas na projektech

Vykazování práce na projektech a zakázkách, výpočet nákladovosti projektů, úprava hodinové odměny dle projektu...

Tiskové sestavy a exporty

Desítky tiskových sestav, které lze ukládat i do excelu, exporty do mzdových systémů, exporty na míru a REST API.

NOVINKA

HR systém

Nový modul HR systém nabízí digitalizaci personalistiky. Evidenci prac. smluv, školení, majetku, knihu úrazů a další. Založte si vlastní agendy, využijte generování dokumentů a digitální podepisování eIDAS, upozornění na termíny a spoustu dalších funkcí, které vašemu HR ušetří čas.

Whistleblowing

Nově nabízíme také tzv. **whistleblowing funkci**. Umožňujeme bezpečně zasílat anonymní podněty jak z píchacích hodin, tak z mobilní aplikace i z webu. Plníme požadavky na zákon o ochraně oznamovatelů a usnadníme vám vytvořit spokojenější pracovní prostředí.

+420 728 543 275 | **info@giriton.com** | **www.giriton.com**

EK015652

Džin umělé inteligence se už do lahve nevrátí

text: Radek Kubeš, foto: Sophos

Umělá inteligence bude hrát významnou roli na straně kyberzločinců i obránců, tvrdí **Chester Wisniewski**, globální technický ředitel kyberbezpečnostní společnosti Sophos.

Budeme-li chtít z umělé inteligence vytěžit maximum, musíme zdokonalit způsob jejího využití jako rozšíření schopností lidí, říká Chester Wisniewski. Zločinci nemají datové vědce a pravděpodobně budou i nadále jednoduše zneužívat veřejně dostupné nástroje. „Jakákoli regulace AI bude účinná jen pro ty, kteří chtějí hrát podle pravidel," dodává ke snahám EU o její regulaci Wisniewski, který má více než 25 let zkušeností v oblasti bezpečnosti IT. Tempo objevování nových hrozeb se podle něj zpomalilo, s inovacemi dnes kyberzločinci přicházejí častěji spíše v sociální rovině než v technické oblasti.

Kybernetické bezpečnosti se věnujete již více než 25 let, je něco, co by vás mohlo opravdu překvapit?
Usilovně se snažím sledovat nejnovější trendy a výzkumy, abych se velkým překvapením pokud možno vyhnul. Přesto se občas zničehonic objeví něco skutečně inovativního. Je to ale vlastně dobře, protože s každým novým způsobem zneužití mezery v zabezpečení můžeme kreativně vymýšlet, jak rizika zmírnit a zajistit ještě lepší ochranu.

Jak dlouho obvykle trvá výzkum nové hrozby, aby bylo možné vydat doporučení k jejímu zmírnění?
Na tuto otázku je obtížné odpovědět, protože definice hrozby je velmi široká. Ve většině případů existují dva typy řešení – nejprve to okamžité, reaktivní, které má „zastavit krvácení". Ale pak potřebujeme dlouhodobější řešení, které bude k ochraně před touto již dobře popsanou hrozbou přistupovat proaktivně. Reaktivní řešení lze obvykle získat už během několika hodin, samozřejmě v závislosti na složitosti a znalosti metodiky útoku. Ale vývoj proaktivní ochrany může často trvat celé měsíce a právě ta je pro spolehlivou obranu nezbytná. Musí ovšem být komplexně testována, aby se zajistilo, že nedochází k falešným poplachům a že je schopna odhalit i hrozby, které jsou záměrně zastřené a klamavé, což vyžaduje hodně času a značné úsilí.

Jak často se objeví skutečně nová hrozba, která není variantou nebo evolucí některé stávající metody útoků?
Tempo objevování nových hrozeb a metod útoků se v průběhu let dramaticky zpomalilo, když se pronikání do sítí stalo výdělečnou činností. Inovace dnes probíhají spíše v sociální rovině než v technické oblasti. Většina nových hrozeb se objevuje jako způsob, jak obejít stále sofistikovanější obranné technologie, a jejich vymyšlení vyžaduje hluboké technické znalosti. Řekl bych, že se s opravdu novými přístupy k využívání zranitelností setkáváme zhruba každých pět let.

V poslední době se vyšetřovatelům podařilo identifikovat a rozbít hned několik kyberzločineckých skupin. Znamená to, že se kyberzločinci mají začít bát, protože už nejsou tak nepolapitelní jako dříve? Nebo je to jen špička ledovce?
Trvalo mnoho let, než mezinárodní komunita orgánů činných v trestním řízení investovala a vybudovala účinné kybernetické policejní síly a vymyslela způsob přeshraniční spolupráce. Toto úsilí se začíná vyplácet, zvyšuje se tlak na kybernetické zločince i na zdroje a služby, které využívají ke koordinaci své trestné činnosti. I když se nám ne vždy podaří dopadnout samotné zločince, narušením jejich obchodních modelů a podkopáním jejich vzájemné důvěry dramaticky zvyšujeme náklady na jejich činnost.

Chester Wisniewski

globální technický ředitel, Sophos

Spolupracuje s výzkumníky týmu Sophos X-Ops po celém světě, aby porozuměl nejnovějším trendům a výzkumům v oblasti kyberkriminality a chování zločinců. To mu pomáhá s lepším pochopením stále se vyvíjejících hrozeb a chování útočníků i budováním účinné bezpečnostní obrany.

Když se zrovna nevěnuje boji s kyberzločinci, tráví svůj volný čas vařením, jízdou na kole a mentorováním nováčků v kyberbezpečnosti v rámci své dobrovolnické práce v organizaci InfoSec.

> Větší pokrok v používání umělé inteligence bude letos spíše na straně obránců než útočníků.

Mají vyšetřovatelé nové nástroje, postupy a znalosti, jak tento typ zločinců postihnout?
To si nemyslím. Podle mě jsme jen v pronásledování kyberzločinců efektivnější a zvýšená spolupráce vede k většímu počtu zatčení a narušení sítě kyberzločineckých skupin. Tato vyšetřování vyžadují starou dobrou policejní práci a často měsíce i roky pátrání a forenzních analýz.

Je snazší vypátrat amatérské útočníky, kteří využívají nástroje typu Ransomware as a Service nebo DDoS as a Service, nebo jim tyto služby poskytují dostatečnou míru ochrany a anonymity?
Čím méně je zločinec kvalifikovaný, tím snadnější je jeho identifikace a případné zadržení. Nejzkušenější kyberzločinci umí používat pokročilejší nástroje ke skrytí své identity a často mají kolem sebe vrstvy ochrany, které jejich vypátrání ztěžují. Udržet si úplnou anonymitu je ale téměř nemožné a pečliví vyšetřovatelé nakonec chyby najdou a odhalí jejich skutečnou identitu.

Angažuje se Sophos ve vyšetřování takových kyberzločinů? Poskytuje například vyšetřovatelům důkazy a další pomoc?
Pokud máme informace, které mohou být užitečné, pak samozřejmě s orgány činnými v trestním řízení při vyšetřování spolupracujeme. To se ale značně liší případ od případu. Jsme také členy mnoha organizací pro sdílení zpravodajských informací o hrozbách, ve kterých se angažují i zástupci orgánů činných v trestním řízení.

Jaký dopad bude mít umělá inteligence na kybernetickou bezpečnost v roce 2024?
Kdybych tak měl křišťálovou kouli… Ale vážně, domnívám se, že větší pokrok v používání umělé inteligence bude letos spíše na straně obránců než útočníků. Chcete-li z umělé inteligence vytěžit maximum, musíte zdokonalit způsob jejího využití jako rozšíření schopností lidí. Stroje umí dobře rozpoznávat opakující se vzorce a zpracovávat velké objemy dat, aby je v nich našly. Zatímco lidé mají instinkt k rozpoznání dobrého od špatného. Zločinci nemají datové vědce a pravděpodobně budou i nadále jednoduše zneužívat jakékoli veřejně dostupné nástroje. Je pravděpodobné, že budou pokračovat ve využívání umělé inteligence k vytváření přesvědčivějších spamových návnad a potenciálně i pro deepfake podvody s podvrženými hlasy a obrazem, protože jejich kvalita se rychle zlepšuje. Ale pravděpodobně se letos nepustí do něčeho úplně inovativního.

Je možné zmírnit negativní dopady umělé inteligence pomocí regulací, o kterých se v EU v souvislosti s AI často diskutuje?
Určitě ne. Předpisy se vztahují pouze na ty, kteří souhlasí s tím, že budou hrát podle pravidel. Džin technologie umělé inteligence už byl vypuštěn z lahve a nelze ho přesvědčit, aby se do ní vrátil. Podporuji použití regulace, která zabrání legitimním podnikům využívat AI k vytěžování informací o našem soukromí, ale zákony nebudou mít žádný vliv na kriminální zneužívání technologií umělé inteligence.

Deepfake podvody jsou obvykle odhalitelné pouze lidmi a vyžadují velkou ostražitost. Budeme mít v blízké budoucnosti k dispozici nějaké nástroje, které nám s obranou pomohou?
Pravděpodobně nebudeme. Jak to totiž vypadá, ani společnosti, které software na vytváření deepfake videí a hlasových záznamů vyvíjejí, nejsou schopny s jistotou určit, zda jejich vlastní nástroje daný zvukový nebo obrazový klip vygenerovaly, nebo ne. Budoucnost proto spočívá spíše ve schopnosti prokázat pravost zvuku a videa než v dokazování, že je něco falešné. Existují už i iniciativy, jako je například Content Credentials, které vám s tím pomohou.

Kvantové počítače jsou považovány za revoluční zbraň v rukou kyberzločinců. Měli bychom si s tím dělat starosti? A co vlastně může zneužití této technologie znamenat?
Do doby, než budou mít zločinci v rukou použitelné kvantové počítače, zbývá ještě dlouhá cesta. Ale možnost jejich využití nepřátelskými vládami už zase tak daleko není. Největším rizikem je jejich schopnost prolomit dnes nejčastěji používané šifrovací techniky. Už ale existuje několik návrhů šifrovacích metod, které tomu potenciálně zabrání. Když chráníme citlivé informace, musíme si být jisti, že je ochráníme po celou dobu, po kterou musí zůstat utajeny. To znamená, že už nyní je vhodná doba začít přecházet na kvantově bezpečné šifrování, aby informace, které je třeba chránit dnes, zůstaly utajené třeba i za 25 let, kdy tato technologie může být celkem běžná.

Co byste doporučil společnosti, která nemá mnoho prostředků na robustní kybernetickou ochranu? Jaká opatření jsou levná, ale současně velmi účinná?
Určitě školení uživatelů a protokolování. Zásadní je mít záznam o všem, co se stalo, a někoho, kdo ví, jak a co v něm hledat. Pro většinu organizací nedává z ekonomického hlediska smysl najímat si vlastní odborníky na kybernetickou bezpečnost, protože jsou poměrně drazí a často potřební pouze pro konkrétní úkoly. Přesto je nepřetržité monitorování infrastruktury – 24 hodin denně 7 dní v týdnu – pro účinnou obranu nezbytné. I proto jsou dnes mezi podniky tolik oblíbené služby řízené detekce hrozeb a reakce na ně. Získáte s nimi přístup k vysoce vyškoleným odborníkům na kybernetickou bezpečnost, kteří na vše dohlédnou a budou k dispozici v případě potřeby, aniž by se musely zvyšovat náklady na další zaměstnance. Vaše týmy IT sice musí dostatečně dobře rozumět zabezpečení a jeho vlivu na podnikání, ale mohou se spolehnout na externí odborníky, kteří nepřetržitě odhalují vzory útoků a pokusy o neoprávněný přístup do sítě.

Zmínil jste i školení – máte nějaká doporučení, jak se vyhnout určité únavě z opakovaných e-learningů a testovacích phishingových kampaní? Jak udělat školení účinnější?
Osobně nepovažuji většinu školení za zvlášť účinná. Smysl má ale především školení zaměřené na skutečné příklady, které se staly v rámci vaší organizace lidem, jež znáte. Například popsat phishingový útok na generálního ředitele nebo někoho z finančního oddělení má větší dopad než popisovat potenciální útok nebo vykládat obecný obsah, který bývá součástí většiny online školení. Ostatně, koncoví uživatelé nemohou být zodpovědní za odhalení útoků, musí je chránit technologie. Hrozby jsou dnes příliš sofistikované na to, aby bylo možné očekávat, že se uživatelé bez expertních znalostí v kyberbezpečnosti budou schopní účinně bránit.

Proč se podle vás podceňují i další, relativně levná a snadná opatření jako šifrování a vícefaktorová autentizace?
IT a bezpečnostní týmy jsou zahlceny množstvím práce, kterou musí vykonávat, a přidání nové komplikace, jako je šifrování a MFA, může vypadat jako další náročný úkol, který jim práci ještě ztíží. Já si sice nemyslím, že to tak opravdu je, ale když se vám skoro nedaří udržet hlavu nad vodou, může být těžké přijmout další práci. V konečném důsledku by tato dodatečná práce měla vést k celkově menšímu objemu úkolů, ale zdá se, že má vždy nižší prioritu, než by si zasloužila.

Lze nějak určit, jaký podíl obratu by měla společnost investovat do kybernetické ochrany? Jaká investice je „přiměřená“?
Toto není oblast, na kterou bych se soustředil, a navíc se obávám, že existuje příliš mnoho faktorů, které je třeba vzít v úvahu, než aby bylo možné poskytnout jednoznačnou odpověď. Obecně ale platí, že všechny organizace by měly jmenovat osobu odpovědnou za bezpečnost informací a také provést analýzu potenciálních rizik s kvantifikací jejich dopadu. Pak je nutné tuto analýzu předložit představenstvu, společně s návrhem řešení, jak možná rizika zmírnit. Výběr z možných řešení a míra akceptovaného rizika pak ovlivní výši výdajů na řešení těchto rizik, která se dnes týkají každé organizace.

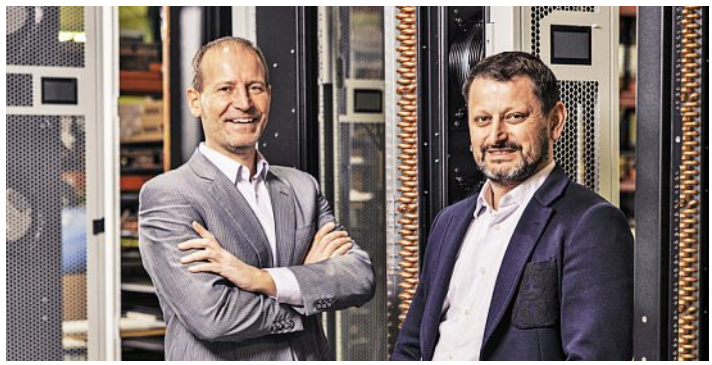
Je i vaší zkušeností, že organizace začnou skutečně přemýšlet nad kyberbezpečností a souvisejícími investicemi, až když dojde k jejich úspěšnému napadení?
Různé organizace se pohybují v celém spektru vyspělosti jejich kybernetické bezpečnosti. A ano, v organizacích na nejnižších stupních vyspělosti se často podceňuje riziko kybernetických útoků pro jejich fungování a zdá se, že zde reagují, až když už je příliš pozdě. Mnoho lidí odpovědných za bezpečnost IT pochází spíše z technického prostředí, než aby byli vyškoleni v tom, jak správně vyhodnocovat rizika. A právě to vede k takovému nesouladu mezi potenciálními riziky a opatřeními, která je mají omezit.

> “
> Smysl má především školení zaměřené na skutečné příklady, které se staly v rámci vaší organizace lidem, jež znáte.

text: redakce, foto: Conteg

Češi dodávají datacentra i pro NATO

Datacentra v posledních letech zažívají boom, který ovlivňují rostoucí požadavky na jejich kvalitu. Reflektují to i české firmy patřící k důležitým hráčům na světovém trhu. Roste poptávka po úsporných řešeních.



Spolumajitelé společnosti Conteg – ředitel Vít Voláček (vpravo) a obchodní ředitel Vojtěch Voláček

Energetické úspory jsou v posledních letech důležitým tématem ve všech oborech napříč ekonomikou a stejné je to i v byznysu s datovými centry. Chlazení je jednou ze základních komponent, které zákazníci po firmách požadují. „Zvyšují se požadavky na úspory i v malých a středních datacentrech, kde se dříve uplatňovaly jednotky s čistě kompresorovým chlazením. Dokážeme realizovat dvoukapalinové řešení využívající nepřímé volné chlazení. Díky tomu v Česku uspoříme až 60 procent elektrické energie, v severských podmínkách to může být i výrazně více," říká ředitel a spolumajitel společnosti Conteg Vít Voláček.

Úspory energií musí výrobci datových center hledat i při velkých zakázkách. „Kvůli tomu přizpůsobujeme jednotky s využitím počítačové simulace proudění vzduchu. Snižujeme tak příkon ventilátorů," říká Voláček.

Conteg se za 25 let existence stal silným evropským dodavatelem datových center. Svědčí o tom i to, že tato česká firma vyhrála tendr na kompletní dodávku rozvaděčů pro datová centra i celkovou infrastrukturu sídla NATO v Bruselu. I když většinu byznysu dělá Conteg v cizině, myslí i na tuzemské kořeny. V Česku stojí například za datovým centrem pro Státní pokladnu či za Centrem sdílených služeb, které za čtvrt miliardy korun vyrostlo v Zelenči u Prahy.

> „V Česku uspoříme až 60 procent elektrické energie.

Páteř datacenter

Stěžejním stavebním kamenem datacenter je koncept horké a studené uličky. Rozvaděče jsou k sobě otočeny čelními stranami. Studený vzduch míří do datacentra skrz dvojitou podlahu, která slouží jako dopravní cesta pro studený vzduch. „Ideální je, aby studená ulička byla široká 1,2 metru. Před každým rozvaděčem pak může být perforovaný panel, díky němuž lze přivést studený vzduch před skříň. Maximální účinnost zajistí vysoce perforované dveře," vysvětluje specialista na datová centra Tomáš Kroupa.

Klíčová je v datacentrech účinnost. „Pro co nejlepší využití studeného vzduchu doporučujeme zakrýt nevyužitý prostor v rozvaděči pomocí zaslepovacích panelů. Ke snížení nákladů také pomáhá použití separačního rámu v přední části rozvaděče, díky čemuž se zamezí nežádoucímu mísení studeného vzduchu a horkého vzduchu," přidává další technické finesy Tomáš Kroupa.

Proud vzduchu se řídí na úrovni rozvaděče, uvnitř datacentra je potřeba minimalizovat překážky v cestě toku studeného i horkého vzduchu. „Pro tradiční architekturu horké a studené uličky je jedním z efektivních řešení systém přesné klimatizace s jednotkami umístěnými po obvodu sálu," dodává Tomáš Kroupa.

Přizpůsobit se místním podmínkám

Conteg těží z toho, že datacentra vyrábí na zakázku. Dokáže tak flexibilně vyhovět požadavkům zákazníků na rozměry datacentra či vzít v potaz geografické odlišnosti jednotlivých zemí. Zatímco ve Skandinávii jsou teplotní podmínky pro provoz datacenter velmi vhodné, na Blízkém východě je tomu přesně naopak. Datacentra tak musí pracovat i v teplotách přesahujících 50 stupňů Celsia.

V místech s vysokou tepelnou náročností například spolehlivě funguje systém s uzavřenou studenou uličkou, kde chladný vzduch směřuje z dvojité podlahy přímo k rozvaděčům. Pokud není možné využít dvojitou podlahu, je praktickým řešením uzavřená horká ulička s chladicími jednotkami integrovanými přímo mezi rozvaděči. Pro zónu s vysokou výkonovou hustotou lze zvážit i navenek teplotně neutrální sestavu uzavřených IT rozvaděčů a klimatizačních jednotek. V poslední době je populární také volné chlazení datacenter využívající vzduchu z vnějšího prostředí.

Text vznikl ve spolupráci se společností Conteg

ADVERTORIAL

Jak ve firmách zavádět AI?
Nebát se experimentovat

Stratox ENTERPRISES

Trh s AI připomíná trochu Divoký západ. Produktů je mnoho a firmy se v nich často mají problém vyznat. Podle expertů ale nezáleží ani tak na volbě správného produktu, jako spíše na dovednosti rychle zavádět jakoukoliv inovaci. Jak tento přístup ve firmě podpořit? Nebát se experimentovat a jednat, radí Petr Svoboda ze společnosti Stratox, která má i vlastní platformu CodeNOW® pro snazší začleňování AI do podnikových aplikací.

Implementovat umělou inteligenci a nenechat si ujet vlak. To poslouchají firmy denodenně. Jak se jim daří zavádět AI do svých procesů?
Trh s AI je velmi heterogenní. Existuje sice spoustu možností, ale lidé pak mají problém se v nich orientovat. Nejde jen o jednorázové pořízení hotového produktu. Zavedením AI do firmy totiž vyrábíte interně nový produkt, který s vámi bude žít roky. Abyste AI ve firmě oživili, musíte ji integrovat do zbytku IT systémů. Zkrátka ji nakrmit daty. A ne jen jednou, ale kontinuálně. Koupě produktu je tedy pouze jedním krokem.

Obecně tedy firmám chybí strategie?
Přesně tak. Firmy mají dvě možnosti, jak k ní přistoupit. Buď půjdou cestou klasického plánování. A to trvá relativně dlouho. Druhá – více agilní – možnost je, že začnou experimentovat. Vytvoří si pro každé své byznysové produkty prostředí, které je řízené. Tak firmy dostanou implementaci AI pod kontrolu.

Předpokládám, že druhá cesta je ta správná.
Ano. Firmy potřebují hrací pole, které bude bezpečné, ale zároveň nebude omezovat byznys stakeholdery. Důležité je experimentovat, vytvářet krátké, rychlé iterace a mít okamžité výstupy – Proof of Concept, Proof of Technology, piloty. Jen tak rychle a efektivně zjistíte, co je pro vaši firmu nejlepší. Je potřeba neotálet a hned začít.

Proč se tomu v českých firmách zatím tak neděje?
Většina firem měla bariéru v tom, že vytvoření prostředí pro experimentování pro ně byl běh na dlouhou trať. A také velký náklad, který se nemusí vyplatit. Interní IT oddělení bývají často už tak přetížená různými požadavky. Rozpočty na další specialisty chybí. Když ale nemáte jasný byznys case, tak nevíte, jestli se vám investice vrátí.


Petr Svoboda

Petr Svoboda je bývalý IBM, IT architekt a zakladatel několika technologických firem. Momentálně vede skupinu Stratox, jejímž cílem je demokratizovat inovace v cloudovém prostředí. S tím pomohl Stratox například logistické společnosti Packeta. „Během pandemie zaznamenala Packeta raketový růst. Počet jejích výdejních míst se blížil k 9 tisícům a čekala ji další expanze. V té ji však omezovala monolitická struktura jejího IT. Se zvyšujícím se počtem výdejních míst navíc běžely widgety na tabletech a mobilech stále pomaleji," vysvětluje Petr. „Tým Packety nakonec přemigroval svou monolitickou strukturu do platformy CodeNOW®, cloud-native prostředí, které je responzivnější a agilnější. I bez větších dovedností s cloudem zvládl tým ve svém malém složení dosáhnout výrazně větší škálovatelnosti ke 100 milionům transakcí."

Co dalšího trápí firmy při zavádění AI?
Velkým tématem je také autonomie vývojářských týmů. Často nemají dostatečná oprávnění, aby se mohli sami posouvat dopředu. Přitom právě autonomie přispívá k efektivnějšímu vývoji a inovacím. Pro firmy bývá také náročné zavedení nového dodavatele do organizace, tedy vendor management.

S tím souvisí i ochrana dat.
To je často velká překážka. Abych jakýkoliv produkt v oblasti AI efektivně využil, tak ho musím propojit s interními daty. Je třeba si ohlídat, komu všemu a k jakým datům je přístup poskytnut, aby se vývojáři třetích stran nedostali k citlivým informacím.

Na první pohled to vypadá, že pro zavedení AI je potřeba spoustu změn. Je to tak?
Změna souvisí především s přístupem. Firmy, které jsou na trhu například už 20 let, provozují hromadu softwaru. Kvůli AI se hned nezbaví třeba SAP a nenahradí ho různými mikroslužbami. Pokud chtějí firmy zavést AI co nejdříve, tak s tím nemohou spojovat změnu svých core systémů. Musí akorát změnit svůj přístup a osvojit si kritickou dovednost, jak AI vůbec implementovat. Otázkou není, jak například rychle adaptovat open AI, ale jak se rychle adaptovat na cokoliv. Dnes nám může přijít jako nejlepší LLM model GPT, zítra to ale může být Gemini od Googlu nebo llama2 od Mety. A firmy se musí naučit, jak rychle změnit směr.

Jakou radu na závěr byste ještě dal českým firmám při zavádění AI?
Nebát se a hlavně začít co nejdříve. Jen tak si firmy si udrží náskok před konkurencí. Zahraniční společnosti už pracují na tom, aby si vybudovaly schopnost rychlého zavádění AI do všech svých procesů. Takže: Stop talking, start doing.

Aktuálně.cz

CO JSOU

DEZ INFOR MACE

ROZDĚLENÍ

PROČ FUNGUJÍ

KDE SE ŠÍŘÍ

PROČ A JAK SE ŠÍŘÍ

CELÝ SPECIÁL

Řiďte vaši firmu díky jedné aplikaci na míru.

Nemusíte měnit své firemní procesy.
Vytvoříme řešení, které se plně ***přizpůsobí vám***.

www.koala42.com

Jan Jelínek
CEO, KOALA42
+420 728 488 116
jelinek@koala42.com

KOALA42

Hodnoceno 5.0 ★ Clutch

EK015631

text: Marek Zouzalík, foto: Shutterstock

Digitální správa dokumentů zvyšuje efektivitu jejich zpracování

Digitalizace a následná automatizace procesů prostřednictvím DOCU-X zkrátila v ASB Group schvalování dokumentů na čtvrtinu původního času.

Společnost ASB Group je přední poskytovatel poradenských a outsourcingových služeb určených pro firmy všech velikostí. Svým klientům z Česka, Slovenska, Polska a Maďarska nabízí účetní a daňové poradenství, zpracování mzdové agendy a řadu dalších korporátních služeb.

Výchozí stav před digitalizací

Zpracování faktur a dalších dokladů prováděli zaměstnanci ASB Group ručně a zadávali je do jednotlivých oddělených systémů. Při vysokém objemu zpracovávaných dokladů byly kladeny vysoké nároky na výkon těchto pracovníků, což se negativně odrazilo ve vysoké chybovosti. Samotná kontrola faktur zabrala přibližně 60 minut a jejich následné manuální schvalování dalších 20 minut.

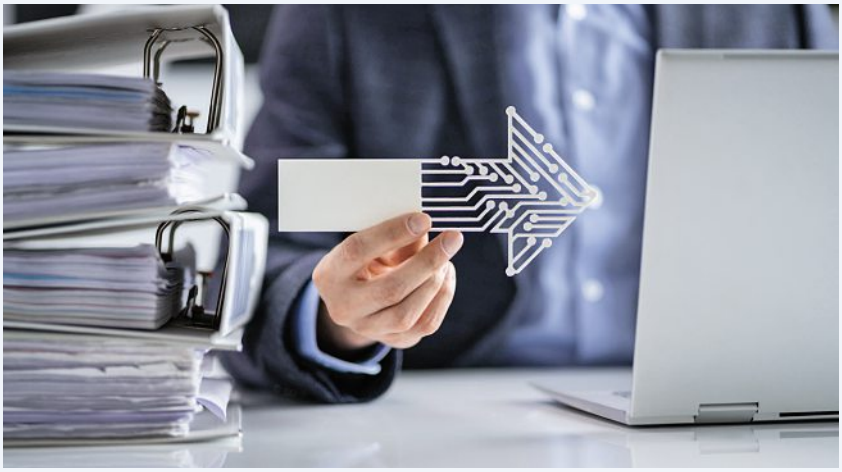
Do procesu zpracování dokladů se navíc nabalovaly i další problémy spojené s neefektivním schvalováním jednotlivých dokladů a jejich kontrolou. Zároveň nebylo možné bezpečně sdílet data se zákazníky. Vzniklá situace vyžadovala buď výrazné zvýšení počtu zaměstnanců, nebo nalezení účinného a přitom cenově výhodného řešení v podobě automatizované digitalizace dodaných podkladů.

Řešením se stal systém DOCU-X

Systém DOCU-X vyvinutý českou společností SOCOS IT je komplexní řešení pro správu firemních dokumentů. Základem tohoto řešení jsou dva moduly, DOCU-X DMS a DOCU-X OCR.

První z těchto modulů zajišťuje efektivní a bezpečnou správu dokumentů, přičemž nabízí i automatizaci řady procesů. Druhý modul pak představuje pokročilé řešení pro optické rozpoznávání znaků, které umožňuje automatické vytěžování dat z naskenovaných či elektronických firemních dokumentů, což zrychluje proces jejich digitalizace a snižuje chybovost, ke které dochází při ručním přepisování dat.

Modul DOCU-X OCR je možné snadno integrovat i s mnoha dalšími podnikovými systémy. Vzhledem k robustnosti celého systému je možné tímto způsobem zpracovávat dokumenty z neomezeného počtu zdrojů a zároveň s prakticky neomezeným počtem uživatelů. Naskenované dokumenty jsou pomocí optického rozpoznávání znaků zapisovány do systému čtyřikrát rychleji než při ručním zadávání. Nasazení systému DOCU-X u ASB Group navíc představuje úsporu přibližně jednoho sta listů papíru ročně.



Digitalizace nabízí oproti práci s papírovými dokumenty mnoho výhod. Umožňuje snadný přístup k informacím, rychlé vyhledávání a sdílení dat. Navíc digitální dokumenty nezabírají fyzický prostor a jsou ekologicky šetrnější.

Nasazení systému DOCU-X v ASB Group

Automatickou digitalizací účetních dokladů se podařilo zrychlit a zefektivnit všechny procesy spojené se zadáváním a schvalováním v rámci účetního systému Helios, který ASB Group pro zpracování účetní agendy využívá. Po přijetí faktura prochází třemi systémy, přičemž je uložena stále jen na jednom místě, kde zároveň probíhají i všechny úpravy. Kontrola přijatých faktur nyní zabere pouhé dvě minuty, přičemž schvalování prostřednictvím systému DOCU-X zabere jen pět minut. ASB Group tak může svým klientům garantovat zpracování dokladů do 48 hodin od jejich zaslání, což představuje nespornou konkurenční výhodu.

„DOCU-X poskytuje bezpečnou platformu pro sdílení dat a informací s našimi klienty. Toto řešení umožňuje rychlé schvalování faktur odpovědnými manažery, přičemž data jsou z fyzických dokumentů získávána automatickým systémem optického rozpoznávání znaků. DOCU-X je zároveň platformou i pro sdílení našich výstupů s jednotlivými klienty. Veškeré účetní operace se přitom odehrávají v bezpečném prostředí," říká Petr Studnička, výkonný ředitel ASB Group.

Význam má jen ta záloha, ze které lze data obnovit

Asi jen těžko bychom narazili na firmu či organizaci, která vůbec nezálohuje svá data. Často se ale ukazuje, že kvůli nevhodně zvolené strategii zálohování není obnova dat v případě potřeby možná.

R

Ransomwarovým útočníkům trvá jen minuty, nanejvýš jednotky hodin, než po úspěšném proniknutí do sítě své oběti zašifrují důležitá data a tím prakticky vyřadí podnik nebo jakoukoli jinou organizaci z provozu. O data jde ale přijít i mnohem rychleji – lidskou chybou, selháním hardwaru nebo ztrátou či zničením zařízení, jehož obsah nebyl zálohovaný.

Lékem na všechny tyto potíže by samozřejmě mělo být pravidelné zálohování důležitých dat. Jak se ale ukazuje, samotná existence záložních dat ještě neznamená, že se data také podaří obnovit. Zčásti je to kvůli změně v taktice útočníků. Podle studie společnosti Veeam se při 93 procentech kybernetických incidentů útočníci pokusí napadnout i záložní úložiště. Výsledkem je, že 75 procent organizací během útoku ztratí alespoň část záložních úložišť a více než třetina (39 procent) záložních úložišť je zcela ztracena. Ale ani když zálohy během útoku odolají, není zdaleka vyhráno – nevhodně zvolená strategie zálohování může znamenat, že budou rezervní data zastaralá (nezálohuje se dostatečně často) nebo nepoužitelná (nekontroluje se čitelnost záloh). A důležitou roli hraje i čas. K čemu jsou bezpečné a čitelné zálohy, když z nich obnova dat nezbytných k provozu trvá dlouhé dny nebo celé týdny?

Zálohování jako povinnost

Zcela chybějící strategie zálohování a obnovy dat (která pochopitelně přímo souvisí se zachováním kontinuity provozu) už brzy přestane být čistě interní záležitostí organizací – alespoň tedy těch, které budou spadat do kategorie poskytovatelů regulovaných služeb podle nového zákona o ky-

> Zálohování probíhá nesystematicky, data se netestují a už vůbec se pravidelně netrénuje obnova.

text: Radek Kubeš, foto: Shutterstock

bernetické bezpečnosti, který do české legislativy přenáší povinnosti dle celoevropské směrnice o kybernetické bezpečnosti NIS2. Procesy na ochranu dat budou také důležitým tématem při sjednávání kybernetického pojištění, respektive při případném vyplacení pojistného plnění.

„Praxe ukazuje, že nějaké zálohy najdeme prakticky v každé společnosti. Problém je, že jejich vytváření probíhá nesystematicky, zálohovaná data se netestují a už vůbec se pravidelně netrénuje jejich obnova, aby bylo jasné, co a jak rychle je možné v případě chyby, kybernetického útoku nebo havárie obnovit," vysvětluje Ivo Šmerda, Team Leader ve společnosti SoftwareOne. Častých chyb a omylů při zálohování je ale ještě mnohem víc. A začít můžeme už tím, že v mnoha organizacích není jasné, co se má vlastně zálohovat.

Podle studie společnosti Veeam se naprostá většina útočníků pokouší napadnout i záložní úložiště. Především kvůli ransomwarovým útokům experti doporučují přidat další kopii dat, která nebude dostupná v rámci podnikové síťové infrastruktury.

Začněte klasifikací dat

Data jsou dnes pro stále více firem jejich nejcennějším majetkem, a proto by o ně měly odpovídajícím způsobem pečovat. Je ale jasné, že ne všechna data si zasluhují stejnou úroveň zabezpečení před případným odcizením a ztrátou. Bylo by extrémně neekonomické aplikovat na všechna data nejvyšší úroveň ochrany – už proto, s jak značnou rychlostí se zvyšuje objem dat, která musí organizace zpracovávat a ukládat.

Proto je základním krokem při správě podnikových dat jejich klasifikace, ze které pak vychází úroveň jejich důvěrnosti a také stupeň jejich ochrany před odcizením či ztrátou. Pro každou kategorii informací je nutné definovat pravidla, jak s těmito dokumenty zacházet, kdo s nimi může nakládat a jak budou uloženy a zá-

lohovány. „Klasifikace informací je v některých odvětvích vyžadována i legislativou a je také nezbytným předpokladem splnění požadavků na zvýšenou ochranu osobních dat podle regulace GDPR. A stejně jako kontinuita provozu se řeší i v rámci novely zákona o kybernetické bezpečnosti dle směrnice NIS2," dodává Ondřej Smíšek, Information Security Consultant v SoftwareOne.

Klasifikace dat pomáhá organizacím nejen lépe chránit citlivé informace, ale také lépe pochopit a efektivněji řídit jejich oběh a zpracování. V souvislosti se zálohováním se klasifikace využívá především pro plánování potřeby a škálování úložných kapacit, definování plánů obnovy po havárii a ve výsledku také ke kalkulaci nákladů na ukládání, automatizaci a archivaci dat. Požadavek na ochranu citlivých dat před odcizením a ztrátou přitom vyplývá již ze samotné regulace GDPR, a proto je nutné označit a zabezpečit přinejmenším osobní data, která spravuje každá organizace (typicky o svých zaměstnancích, ale často také o zákaznících). Klasifikaci dat dnes řeší řada podnikových systémů a lze ji realizovat i pomocí funkcí sady cloudových služeb Microsoft 365.

Modely záloh pro spolehlivou ochranu dat

Pokud už máme stanovenou potřebnou úroveň ochrany dat, zbývá nastavit strategii jejich zálohování. Ta zahrnuje nejen frekvenci pořizování záloh, ale také počet verzí, které budou od konkrétních souborů postupně uchovávány. A rozhodnout je třeba také o použitém způsobu zálohování – především na základě určení, jak rychle potřebujeme mít data v případě ztráty obnovená. Rozsah možných úložišť dnes sahá od velmi rychlých flash úložišť pro data, která je nutné obnovit v řádu minut, až po páskové knihovny na velké objemy dat, jejichž případná obnova tolik nespěchá. Rychlost obnovy je často přímo úměrná nákladům na zálohování – nejrychlejší úložiště jsou ta nejdražší a naopak.

Nabízí se samozřejmě také cloudové zálohovací služby, u kterých je nutné zvážit nejen cenu za potřebnou kapacitu, ale také závislost obnovy na rychlosti (a dostupnosti) internetového připojení. V případě kyberútoku může být lokálně dostupná záloha výhodou, ale také potenciálním rizikem.

I proto, že se záložní data stala jedním z primárních cílů kyberútočníků, je nutné revidovat současné zálohovací strategie. Ty většinou staví na pravidlu označovaném jako 3-2-1, tedy existenci tří kopií dat na dvou různých médiích, s jednou z kopií uloženou na jiném místě. Tento model se, především kvůli ransomwarovým útokům, doporučuje rozšířit o další kopii dat, která nebude dostupná v rámci podnikové síťové infrastruktury. Tato offline (nebo také neměnná) kopie nemůže být zašifrována ani jinak zničena, protože se k ní útočníci nemohou dostat. Ale pak je zde ještě jeden faktor, který je nutné zohlednit.

> Po kybernetickém útoku musí být celé prostředí zkontrolováno a očištěno od případného malwaru, jinak riskujeme opětovné infikování.

Jsou zálohy použitelné?

Velmi častým problémem strategií zálohování dat je chybějící plán jejich obnovy v případě napadení nebo havárie. Součástí zálohovací strategie proto nutně musí být i přesný popis, kde a na jakých médiích jsou zálohy uloženy, jaká je doba nutná k obnově různých systémů a dat a kde jsou případná úzká hrdla procesu obnovy (je potřeba spustit jiné systémy, je obnova závislá na dostupnosti a rychlosti internetového připojení, musí se data dešifrovat a podobně). To vše musí být popsáno v postupech, společně s identifikací lidí, kteří jsou do obnovy dat zapojeni.

Často se také nepočítá s tím, že po kybernetickém útoku musí být celé prostředí zkontrolováno a očištěno od případného malwaru, aby bylo možné provést obnovu do „čistého prostředí". Jinak podnik riskuje opětovné infikování svého produkčního prostředí. Samozřejmě to ale prodlužuje dobu odstávky a zvyšuje ztráty.

Ještě horší je ale situace, kdy sice existuje záloha dat, ale nelze ji použít k úspěšné obnově. Taková situace vůbec není výjimkou, jelikož zálohovacím strategiím často chybí pravidla a procesy pro ověřování funkčnosti záloh. Přestože bývají funkce na jejich kontrolu běžnou součástí zálohovacích řešení, často se na ně zapomíná. Je to práce navíc, a tak se spolehlivost obnovy a skutečný čas potřebný k obnově dat testuje spíše výjimečně.

Cloud neznamená automatické zálohování

Využívání cloudových služeb je ve firmách stále častější a nepochybně přináší řadu výhod. Často se ale zapomíná na velmi důležitou věc – nelze se spoléhat na uložení dat v rámci cloudových služeb jako na způsob zálohování. Všichni seriózní poskytovatelé cloudových služeb ve svých podmínkách použití jasně uvádějí, že data uložená v rámci služeb typu Microsoft 365 a podobných nejsou zálohována. O jejich zálohování se na základě principu sdílené odpovědnosti musí postarat vlastník těchto dat. I proto vzniká řada specializovaných řešení určených právě pro zálohování a archivaci dat z cloudových služeb.

Ponechat data v cloudových službách bez zálohy představuje obrovské riziko. O data svých zákazníků může vlivem havárie nebo kyberútoku přijít poskytovatel cloudové služby, ale může se například také stát, že svou e-mailovou schránku a data na firemním SharePointu v cloudu nebo v úložišti OneDrive zlikviduje odcházející zaměstnanec. Bez možnosti obnovy důležitých kontaktů, dokumentů, objednávek a dalších informací. A samozřejmě také za ztrátou důležitých dat nemusí být zlý úmysl, ale jen nepozornost – výsledek je každopádně stejný.

Připravte se na nejhorší

Podle aktuální studie společnosti Check Point byl v roce 2023 v průměru proveden ransom-

warový útok na každou desátou organizaci po celém světě. To představuje meziroční nárůst o 33 procent. Organizace po celém světě pak průměrně zaznamenaly 1158 různých kyberútoků týdně. Neustále se zhoršující situace v kyberbezpečnosti musí nutně znamenat posun ve způsobu, jakým budou podniky a další organizace uvažovat o svém zabezpečení.

Jedním z moderních přístupů je také metoda assumed breach – tedy předpoklad prolomení obrany a úspěšného napadení podnikové infrastruktury. Cílem tohoto přístupu je zajistit co nejrychlejší detekci takového napadení a minimalizaci škod. Proto se soustředí především na procesy a nástroje, které ochrání to nejdůležitější – tedy typicky data – a povedou k co nejrychlejšímu návratu k běžnému provozu.

Klíčovou součástí přípravy na úspěšný kybernetický útok jsou právě aktuální a funkční zálohy podnikových dat. Tím se vracíme k předpokladu, že účinnou zálohu pro případ ransomwarového útoku je nezbytné udržovat mimo podnikové síť jako neměnnou kopii, kterou nelze zničit nebo zašifrovat. Častou chybou je ale naopak zahrnutí zálohovacího serveru do podnikové struktury Active Directory – adresářové služby, která umožňuje efektivně uspořádat síťové prostředky. Tím se útočníkům otevře prostor pro zničení všech dat, včetně záložních.

Zálohování jako pojistka v nouzi

Většina problémů a nedostatků spojených se zálohováním má svoje příčiny už v samotném vnímání důležitosti a smyslu tohoto způsobu ochrany důležitých dat. Podceňuje se především úvodní analýza rizik, která má identifikovat následky případné ztráty nebo odcizení cenných dat a kvantifikovat jejich dopad. Na základě této analýzy je pak možné nejen určit nutnou úroveň ochrany různých typů dat, ale také si stanovit objem finančních prostředků, který má smysl na jejich zálohování vynaložit.

Management má navíc často tendenci vnímat náklady na zálohování dat jako investici do podnikové infrastruktury IT, která by měla vykazovat nějakou návratnost. Ve skutečnosti jde ale především o formu pojištění, které oceníme ve chvíli, kdy skutečně dojde k havárii nebo třeba kyberútoku. Tak jako pojištění proti požáru nebo záplavám, ani zálohování dat samo o sobě žádný zisk generovat nemůže a také nezabrání příčině havárie. Může ale minimalizovat následky a rychle vše vrátit do správných kolejí. „Zálohovací strategie musí reflektovat různé úrovně důležitosti dat z hlediska požadavku na jejich dostupnost a rychlosti obnovy. Často se přitom ukáže, že není nutné využívat velkou kapacitu nejrychlejších, a tedy i nejdražších úložišť. Na základě klasifikace dat lze najít takovou kombinaci úložišť, která zajistí spolehlivou ochranu záloh a současně nebude tolik zatěžovat rozpočet organizace," uzavírá Ivo Šmerda ze společnosti SoftwareOne.

Pokud se má zálohování dat provádět správně, jde o poměrně náročnou disciplínu, která má ale naprosto zásadní dopad na fungování a kontinuitu provozu firmy nebo jiné organizace. Ztráta důležitých dat může být pro podnik i likvidační a nelze podceňovat ani dopad na reputaci podniku nebo případný postih kvůli porušení smluvních či legislativních podmínek. Plány obnovy po havárii (Disaster Recovery Plan – DRP) a řízení kontinuity provozu (Business Continuity Management – BCM) jsou navíc nezbytnou součástí bezpečnostních opatření v organizacích, které spadají mezi povinné osoby dle připravované novely zákona o kybernetické bezpečnosti.

> Management má často tendenci vnímat náklady na zálohování dat jako investici do podnikové infrastruktury IT, která by měla vykazovat nějakou návratnost.

Inzerce

EK015629

eset® Digital Security
Progress. Protected.

TECHNOLOGIE POMÁHAJÍ MĚNIT SVĚT K LEPŠÍMU. ESET JE TADY, ABY JE CHRÁNIL.

Unikátní technologie ESET efektivně chrání bezpečnost firem všech velikostí. Díky detailním reportům z výzkumných center po celém světě získáte přehled o aktuálních kybernetických hrozbách, a navíc budete vždy v obraze ohledně zavádění nejnovější legislativy NIS2.

NIS2 info

Vyplňte krátký dotazník s využitím QR kódu a získejte zdarma příručku **Nejnovější legislativa EU pro oblast kybernetické bezpečnosti**.

text: Marek Zouzalík, foto: GIRITON Systems

Objevte klíč ke snadné a efektivní správě lidských zdrojů

Moderní systémy pro správu lidských zdrojů jsou klíčem k zjednodušení práce a administrativní zátěže v rámci personálních oddělení. Škálovatelný cloudový systém GIRITON umožňuje digitalizaci personální agendy jak u malých, tak u středních a velkých firem.

Nástup nových zaměstnanců je zpravidla spojen s poměrně velkým objemem dokumentace. Od evidence pracovních smluv a souhlasů se zpracováním osobních údajů (GDPR) přes akceptaci interních směrnic a nařízení až po ukládání protokolů o povinných školeních. Systém pro správu agendy lidských zdrojů GIRITON umožňuje správu všech potřebných dokumentů digitálně, což eliminuje nutnost vedení papírové dokumentace a složitého hlídání důležitých termínů. Vzhledem k faktu, že se jedná o cloudovou aplikaci, je možné veškerou agendu spravovat i bez nutnosti přítomnosti v prostorách společnosti nebo připojení do firemní sítě pomocí VPN. Díky cloudovému řešení je možné systém neustále doplňovat o nové funkce a zároveň pružně reagovat na měnící se legislativu.

„Naše společnost se specializuje na systémy pro správu agendy lidských zdrojů, evidenci docházky a agendu whistleblowingu. Některý z našich systémů aktuálně využívá přibližně tisíc firem, a to jak v Česku, tak i na Slovensku," říká Jan Gřeš, jednatel společnosti GIRITON Systems, s. r. o.

Rychlá implementace a přizpůsobení

Základní agendy jsou v rámci systému GIRITON připraveny tak, aby digitalizace stávajících dokumentů mohla proběhnout co nejrychleji a zároveň s minimem starostí. V rámci systému je možné spravovat všechny běžné agendy – od evidence uchazečů o zaměstnání přes správu majetku a vozového parku až po zpracování agendy BOZP či knihy úrazů.

Jednotlivé agendy je možné přidávat a nastavovat dle vlastních potřeb, a to pomocí jednoduchého editoru. Vkládat je možné vlastní textová pole, data, dokumenty nebo i obrázky. Tímto způsobem je možné během chvíle vytvořit v rámci systému GIRITON prakticky jakoukoliv agendu dle specifických potřeb společnosti. Systém umožňuje použít i vlastní tiskové sestavy. Vaše současné dokumenty typu Word doplníte o datová pole dané agendy a nahrajete do systému jako šablony. GIRITON pak při exportu vyplní vaši šablonu vybranými daty.

Zabezpečení a důvěryhodnost dokumentů

Vygenerované dokumenty s konkrétními daty je možné buď vytisknout, nebo jej odeslat k digitálnímu podpisu danému zaměstnanci. K dispozici je podpis pomocí SMS, e-mailu nebo prostřednictvím bankovní identity. Takto digitálně podepsané dokumenty splňují požadavky na zaručený elektronický podpis dle klasifikace eIDAS, takže je možné tímto způsobem elektronicky podepisovat například i pracovní smlouvy a další právně závazné dokumenty.

Digitálně podepsané datové soubory jsou opatřeny časovým razítkem, které se v prostředí systému GIRITON automaticky prodlužuje a neztratí tak svoji platnost. Veškerá data uložená v cloudu jsou chráněna s využitím nejnovějších bezpečnostních technologií a integrována je i plná kontrola nad přístupem k osobním údajům v rámci společnosti. Uživatelům je možné omezit přístup k jednotlivým agendám, nebo jim naopak přidělit oprávnění jen k určitým agendám či dokumentům.

Termíny pod kontrolou

Samozřejmostí je sledování všech důležitých termínů, jako jsou například konce pracovních smluv, platnost různých školení nebo lékařských prohlídek. U lékařských prohlídek umí systém ohlídat i to, zda zaměstnanec již nedosáhl věku, kdy musí prohlídky absolvovat častěji. Záznamy agendy, které jsou svázány s nějakým datem, je možné jednoduše propisovat do integrovaného kalendáře nebo exportovat do sdílených kalendářů Googlu a Microsoft Office. Automatické notifikace zajišťují upozornění na důležité termíny či významná pracovní výročí. Systém řeší i plánování směn a žádosti o dovolenou, přičemž hlídá různé limity a zároveň i řadu dalších parametrů.

onpoint

www onpointserv.cz

ERP, CRM nebo účetní systém?

Váháte, co vaše firma potřebuje? Povedeme vás ideální cestou k digitalizaci a automatizaci procesů.

Podnikové systémy usnadňují řízení společnosti a zvyšují její hodnotu. Jako ty na míru pro naše klienty:

Přečtěte si detailní příběhy našich klientů

Kentico

Šest lokálních účetních systémů poboček Kentico nahradil jeden ERP systém. Ten jsme propojili s bankou a CRM systémem a sjednotili veškeré procesy.

MOROSYSTEMS

Nový ERP i CRM systém, Power BI pro reporting, on-line podepisování, automatizace a řada integrací. V MoroSystems jsme se postarali o technologickou (r)evoluci.

FIDUROCK

Že ERP systém na míru pro realitní společnosti neexistuje? Už ano! Vyvinuli jsme jej pro FIDUROCK. A k tomu i s ním propojený portál pro jejich nájemníky.

Vyvíjíme moduly, funkce, add-ony, vlastní produkty

Upgradujeme, migrujeme do cloudu, integrujeme

Konzultujeme, jsme s vámi v kanceláři, školíme

> Postup práce se neplánoval jen podle našeho zadání, ale na základě doporučení, jaké procesy by ERP systém mohl ještě zjednodušit. Petr a jeho tým dali produktu přidanou hodnotu a cením si toho, že vidí naše potřeby v celkovém obrázku.
>
> GABRIELA JAKABOVÁ, KENTICO SOFTWARE

Ozvěte se nám pro nezávaznou konzultaci

info@onpointserv.com
+420 704 122 326

onpoint

Microsoft Partner

Microsoft Dynamics 365 **Business Central**

Brněnský i mezinárodní poskytovatel ERP a softwarových řešení

On Point Services s.r.o., Rokycanova 823, 615 00 Brno-Židenice

EK015644

EK015525

ATS TELCOM

ATS TELCOM POSKYTUJE SPOLEHLIVOU POMOC PŘI PLNĚNÍ KYBERNETICKÝCH POŽADAVKŮ

Brzy vstoupí v platnost **směrnice Evropského parlamentu a Rady Evropské unie NIS 2**, která se zaměřuje na kybernetickou bezpečnost.

Směrnice NIS 2 přináší nové požadavky pro podnikya organizace, ale také obavy a nejistotu v rámci IT oddělení.

Je nutné ujasnit si vztah práva a technicko-administrativního zabezpečení informačních systémů. **Lze se připravit na NIS 2 bez NIS 2?**

Odpověď vám poskytneme na odborné konferenci

ISSS V HRADCI KRÁLOVÉ 13. – 14. KVĚTNA 2024.

KOMPLEXNÍ BEZPEČNÁ ŘEŠENÍ A SLUŽBY

- BEZPEČNOSTNÍ PORADENSTVÍ
- SPECIÁLNÍ TECHNOLOGIE
- BEZPEČNÁ OCHRANA DAT
- INFRASTRUKTURA ROZSÁHLÝCH SÍTÍ

SÍDLO FIRMY: ATS-TELCOM PRAHA a. s., Nad elektrárnou 1526/45, 106 00 Praha 10 – Michle, +420 283 003 111 • IČ: 61860409
KANCELÁŘ BRNO: Vídeňská 122, 619 00 Brno • **KANCELÁŘ HRADEC KRÁLOVÉ:** Pohřebačka 110, 533 45 Opatovice nad Labem
KANCELÁŘ PRAHA: Milíčova 14, 130 00 Praha
WWW.ATSTELCOM.CZ