platform of invention

Informačné technológie pre podnikanie s nápadom

11
ročník šiesty | 1/2026

AI mení pravidlá útokov. Firmy musia zmeniť pravidlá obrany

OČAMI ODBORNÍKOV

Digitálne bojisko

Prečo testovať pripravenosť „nanečisto“?

OČAMI ODBORNÍKOV

Firmy menia stratégiu IT

Lokálny cloud získava na význame

SUCCESS STORY

Keď Excel nestačí

APIS vyvíja platformu webBox pre firmy

platform of invention

Magazín o informačných technológiách

Tlačená aj elektronická verzia zadarmo

platformofinvention.sk

platform of invention

Informačné technológie pre podnikanie s nápadom

Magazín s ambíciou ukázať ako IT technológie uľahčujú firmám každodenný život, prinášať úspešné biznis riešenia, unikátne inovácie a trendy v IT, a pomáhať v uplatnení podnikateľskej tvorivosti a invencie.

Výzva pre všetkých CEO, CTO a CFO

Ponúknite nám svoj príbeh využitia IT vo vašej firme a my vám bezplatne ponúkneme exkluzívnu možnosť prehovoriť k publiku slovenských firiem.

Chcete zistiť viac a zapojiť sa?

Navštívte náš web, vyberte si vhodnú rubriku a odošlite formulár.

www.platformofinvention.sk/profil-magazinu/

Čítajte nás online

Kompletný obsah platform of invention s rozšíreným obsahom a ďalšími článkami nájdete v elektronickej podobe magazínu.

www.platformofinvention.sk

Pripravenosť sa nerieši až v kríze

Po desiatich vydaniach otvárame ďalšiu kapitolu magazínu Platform of Invention. Jedenáste číslo prichádza v novom vizuálnom šate: s čistejšou kompozíciou, prehľadnejším zalomením článkov a výraznejším prepojením tlačeného magazínu s digitálnym obsahom.

Refresh však nevnímame len ako estetickú zmenu. Je pripomienkou, že v dynamickom prostredí, ktoré sa rýchlo mení, nestačí raz nastaviť systém a spoliehať sa, že bude fungovať navždy. To platí aj pre spôsob, akým pracujeme s informáciami, technológiami aj rizikami.

A platí to aj pre kybernetickú bezpečnosť.

Kybernetický incident nečaká kým bude aktualizovaný krízový plán, dostupní všetci členovia tímu alebo pripravené stanovisko pre partnerov a verejnosť. Prichádza nečakane, prináša neúplné informácie a núti organizáciu rozhodovať sa pod tlakom. Práve vtedy sa ukáže rozdiel medzi formálnou pripravenosťou a schopnosťou skutočne konať.

Umelá inteligencia mení pravidlá útokov a legislatíva zvyšuje nároky na organizácie. Incidenty ukazujú, že samotné smernice či dokumenty uložené v zásuvke nestačia. O to dôležitejšia je schopnosť včas rozpoznať riziko, koordinovať technické, právne aj komunikačné kroky a prijímať zodpovedné rozhodnutia na úrovni vedenia.

Kybernetickú bezpečnosť preto už nemožno vnímať iba ako tému pre IT oddelenie. Je otázkou fungovania celej organizácie, jej odolnosti a dôveryhodnosti.

Aj preto sa na ňu v tomto vydaní pozeráme z viacerých uhlov: cez meniace sa hrozby v ére umelej inteligencie, praktické simulácie incidentov, právne povinnosti v prvých hodinách po útoku aj novú úlohu manažmentu.

Náš nový dizajn má čítanie sprehľadniť a obsah otvoriť otázky, ktoré sa v organizáciách neoplatí odkladať. Pretože pripravenosť sa nedá dopísať v momente, keď už incident prebieha. Buduje sa skôr. V rozhodnutiach, procesoch aj v schopnosti vedenia konať včas.

Iveta Hlaváčová
Marketingová manažérka

Ochrana pre virtuálne počítače

Firmy dnes presúvajú čoraz viac aplikácií a dát do verejného cloudu, pretože im prináša flexibilitu, rýchlejšie nasadzovanie služieb a jednoduchšie škálovanie infraštruktúry. Zároveň však rastie potreba mať nad cloudovými virtuálnymi počítačmi rovnakú viditeľnosť, kontrolu a úroveň ochrany, ako nad endpointmi či servermi. Práve v hybridnom prostredí totiž bezpečnostné tímy často narážajú na vyššiu komplexnosť a riziko slepých miest.

Na túto potrebu reaguje ESET Cloud Workload Protection, nový modul platformy ESET PROTECT, ktorý rozširuje ochranu na virtuálne počítače vo verejných cloudových prostrediach AWS, Microsoft Azure a Google Cloud Platform a integruje ich správu do jednej platformy.

Článok pokračuje na **platformofinvention.sk**

Igor Kmiť
PR and Communications Specialist,
ESET Slovensko

Microsoft 365 E7: AI agenti menia správu bezpečnosti aj dát

Microsoft predstavuje novinku, reagujúcu na rastúce požiadavky v oblasti bezpečnosti, správy dát a využitia umelej inteligencie s rozšírením štandardu 365 balíkov E3 a E5. Ide o novú licenciu Microsoft 365 E7. Prináša integrovaný balík pokročilých nástrojov pre kybernetickú bezpečnosť, ochranu identity, riadenie dát a moderné pracovné prostredie, pričom veľký dôraz kladie na automatizáciu a zjednodušenie práce IT tímov využitím AI agentov podporujúcich nový spôsob práce s technológiami. Veľkou výhodou je ich prepojenie na nástroje ako Microsoft Copilot, Defender, Entra či Purview, vďaka čomu dokážu prepájať bezpečnostné, dátové aj používateľské scenáre. Firmy tak získavajú jednotnú platformu, kde AI agenti nielen asistujú, ale reálne zvyšujú produktivitu a znižujú operačnú záťaž.

Článok pokračuje na **platformofinvention.sk**

Marcela Gottwaldová
Obchodný konzultant
GAMO a.s.

Veeam ukazuje, ako môže obnova dát fungovať presnejšie

Veeam Intelligent ResOps posúva obnovu dát od technickej zálohy k presnejšiemu rozhodovaniu po incidente. Riešenie prepája dáta, používateľov, oprávnenia, aktivitu AI nástrojov a stav ochrany dát. Bezpečnostným a IT tímom pomáha rýchlejšie pochopiť, čo sa v dátach zmenilo, koho alebo čoho sa zmena týka, kam sa zásah rozšíril a ktoré položky je potrebné skutočne obnoviť.

Význam takéhoto prístupu rastie v prostredí, kde firmy čoraz viac využívajú AI asistentov a autonómnych agentov. Aj malá chyba, nesprávne nastavenie alebo škodlivá aktivita sa môžu rýchlo premietnuť do veľkého množstva súborov.

Intelligent ResOps preto prináša kontext, ktorý môže rozhodovať o rýchlosti, rozsahu aj kvalite obnovy firemných dát bez zbytočného zásahu do prevádzky – a ako prvý podporuje Microsoft 365.

Článok pokračuje na **platformofinvention.sk**

Boris Mittelmann
Senior System Engineer,
North|Eastern Europe,
Veeam Software

AI vo výskumných IT projektoch. Kde sú právne hranice?

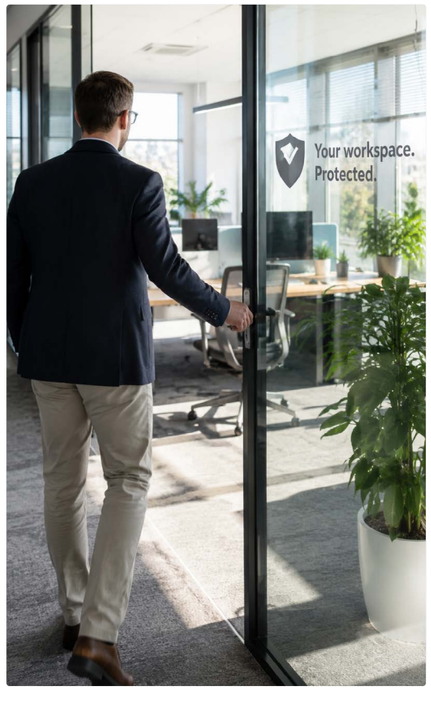
Pri vývoji umelej inteligencie vo výskumných IT projektoch často narážame na otázku, či môže byť AI model trénovaný na osobných údajoch, alebo si musíme vystačiť s anonymizovanými dátami. Odpoveď nie je čiernobiela.

GDPR ani EDPB nevylučujú použitie oprávneného záujmu pri vývoji AI modelov. V mnohých prípadoch môže byť praktickejší než súhlas, najmä ak by spätné odstránenie údajov z natrénovaného modelu nebolo technicky realistické. Nejde však o automatický právny základ – procesu musí predchádzať riadny balančný test a primerané záruky. AI Act zároveň prináša špecifické výnimky pre výskum a testovanie.

Kľúčom je správne nastavenie projektu od začiatku. Vyjasniť si role v konzorciu, zvoliť primeranú formu dát (surové, pseudonymizované, anonymizované) podľa výskumného cieľa a pripraviť DPIA. Inak hrozí, že cenné výsledky výskumu skončia v právnej šedej zóne a nebudú monetizovateľné pre chýbajúcu compliance.

Článok pokračuje na **platformofinvention.sk**

JUDr. Tomáš Klinka, Mgr. Damián Palašta
SIGNUM legal s. r. o.,
Advokátska kancelária



Arrow Cloud Backup: Komplexná ochrana Microsoft 365 aj identity v Entra ID

Cloudové služby Microsoft 365 sú dnes základom každodennej spolupráce vo firmách. Menej sa hovorí o jednom zásadnom fakte. Microsoft nenesie zodpovednosť za zálohovanie zákazníckych dát ani identít. Ransomvérový útok, náhodné vymazanie či chyba administrátora môžu viesť k nevratnej strate dát alebo úplnému výpadku prístupu k firemným systémom.

Arrow Cloud Backup pre Microsoft 365 a Entra ID je plne cloudové SaaS riešenie, ktoré chráni nielen firemné dáta v Exchange Online, OneDrive, SharePoint a Teams, ale aj identity v prostredí Entra ID – používateľské účty, roly, prístupové práva a bezpečnostné konfigurácie. Obe služby spolu vytvárajú komplexnú stratégiu odolnosti, ktorá zahŕňa obsah aj prístupy, podporuje plnenie regulačných požiadaviek ako sú GDPR, DORA či ISO, a umožňuje rýchlu obnovu po incidente.

Prečo záloha dát bez zálohy identity nestačí?

Článok pokračuje na **platformofinvention.sk**

Rostislav Bořuta
Business Development Manager
Arrow Electronics

AI mení pravidlá útokov. Firmy musia zmeniť pravidlá obrany

Zuzana Holý Omelková
zuzana.omelkova@gamo.sk

Kyberbezpečnosť nie je odpoveďou na legislatívu. Je podmienkou bezpečného fungovania akejkoľvek firmy. V rozhovore hovoríme s TOMÁŠOM HETTYCHOM, členom predstavenstva a COO Kompetenčného a certifikačného centra kybernetickej bezpečnosti o tom, prečo nestačí mať dokumenty v zásuvke, čo má vedenie riešiť ešte pred samotným incidentom, a prečo je druhý najlepší čas začať práve teraz.

Ako by ste dnes opísali stav kyberbezpečnosti na Slovensku z pohľadu firiem a ich pripravenosti na aktuálne hrozby?

Objektívne môžem konštatovať, že stav sa zlepšuje. Ukazujú to nielen výsledky auditov, ale aj pribúdanie počtu spoločností v kyberkomunite a tiež počty vyškolených odborníkov.

V čom sa najviac zmenilo kybernetické riziko pre firmy za posledné dva, tri roky?

S dramatickým nárastom používania nástrojov umelej inteligencie prichádzajú riziká úniku firemných dát, väčšieho počtu automatizovaných útokov, zníženia ceny za objednanie útokov, a zlých rozhodnutí vedení spoločností na základe AI modelov.

Ktoré tri kybernetické riziká dnes považujete za najvážnejšie pre malé a stredné firmy?

Používanie nástrojov a modelov s AI bez jasných pravidiel. Nesystematické, čiže jednorazové riešenie požiadaviek kybernetickej bezpečnosti a falošný pocit bezpečia vyvolaný lacnými, takzvanými komplexnými riešeniami bez reálneho overenia ich účinnosti.

Prečo sú SME firmy často zraniteľnejšie? Prečo mnohé predpokladajú, že nie sú pre útočníkov zaujímavým cieľom?

SME firmy majú obmedzený rozpočet a väčšinou menšie množstvo procesov. Vôbec sa nezamýšľajú nad hrozbami totálneho výpadku informačných systémov či masívneho úniku svojich údajov. Zhrnuté: SME firmy zvyčajne podceňujú následky incidentov a nemajú plány kontinuity.

Čo v praxi znamená kyberincident pre bežnú firmu: z pohľadu prevádzky, financií, reputácie a vzťahov so zákazníkmi?

Kým sa vyhodnotí čo všetko uniklo alebo bolo zničené, je vedenie vystavené obrovskému stresu a pocitu neistoty. Pri riešení incidentu ide, samozrejme, aj o čas, sú potrebné rýchle a správne rozhodnutia. Takže je dôležité, aby všetci zachovali chladnú hlavu a nereagovali unáhlene.

S akými omylmi alebo falošným pocitom bezpečia sa vo firmách stretávate najčastejšie?

Rizikom je výber externých služieb či bezpečnostnej dokumentácie len podľa najnižšej ceny, bez overenia referencií. Častý je aj falošný pocit „papierovej“ bezpečnosti, keď firma má dokumenty, ale chýbajú jej technické opatrenia. Mnohé spoločnosti sa nesprávne domnievajú, že pre útočníkov nie sú zaujímavým cieľom. Práve tento omyl ich však môže urobiť zraniteľnejšími.

Ak by ste mali odporučiť päť priorít, na ktoré by sa malo vedenie SME firmy sústrediť ešte v tomto roku, ktoré by to boli?

Kľúčové je, aby firmy prestali vnímať kyberbezpečnosť ako nákladovú položku, ale vnímali ju ako integrálnu súčasť fungovania spoločnosti. S tým súvisí aj potreba pravidelne pozývať alebo trvale začleniť manažéra kybernetickej bezpečnosti do riadenia spoločnosti tak, aby bol súčasťou dôležitých rozhodnutí už v čase plánovania, nielen pri riešení incidentov.

Rovnako dôležité je riadiť svoje informačné aktíva, hrozby a riziká. Znamená to vykonávať reálnu a pravidelnú analýzu rizík a analýzu funkčných dopadov, ktorá firme ukáže kritické aktíva aj scenáre najviac ovplyvňujúce jej fungovanie. Na tieto zistenia by mali nadväzovať reálne scenáre kontinuity a obnovy po závažnom incidente, ktoré nestačí len pripraviť, ale treba ich aj otestovať.

Samostatnou prioritou je nastaviť si jasné interné pravidlá pre používanie AI nástrojov, najmä z pohľadu ochrany citlivých dát, osobných údajov a firemných informácií. A napokon je potrebné investovať do vzdelávania zamestnancov v kyberbezpečnosti na všetkých úrovniach, keďže práve ľudský faktor zohráva významnú úlohu pri incidentoch spojených s únikom dát.

Kde by mala firma začať, ak nemá veľký rozpočet ani interný bezpečnostný tím, ale chce urobiť prvé správne kroky?

Na stole sú dve jednoduché riešenia. Buď si zavolať externého odborníka,

Ďakujeme Danubiana Meulensteen Art Museum za poskytnutie nádherného priestoru k foteniu.

Foto: DESANA DUDÁŠOVÁ

ktorý biznisovým jazykom vysvetlí problematiku a riziká, aby sa vedenie mohlo rozhodnúť. Alebo absolvovať účasť na odbornej konferencii či školení, kde firma dostane základný informačný rámec.

Čo by malo tvoriť minimálne bezpečnostné minimum, bez ktorého by dnes nemala fungovať žiadna firma?

Stanovenie stratégie, zvládnutie základných politík kybernetickej bezpečnosti a nastavenie spôsobov riešenia incidentov. Implementovanie sieťovej bezpečnosti – firewallu, segmentácie, pravidiel. Zazmluvnenie interného alebo externého manažéra kybernetickej bezpečnosti.

Ktoré opatrenia prinášajú najlepší pomer medzi nákladmi, jednoduchosťou a reálnym efektom?

Príprava sady stručných a jasných politík kybernetickej bezpečnosti tak, aby im rozumeli všetci zamestnanci. Využitie služieb externého manažéra kybernetickej bezpečnosti s jasne nastavenými aktivitami a hodinovou sadzbou. Nasadenie cenovo efektívneho riešenia sieťovej bezpečnosti a open-source monitoringu.

Ako by ste zrozumiteľne vysvetlili legislatívne požiadavky - ZokB, NIS 2, vyhlášky - manažérom SME firiem?

Existujúca legislatíva celkom zrozumiteľným jazykom popisuje riadenie kybernetickej bezpečnosti vrátane organizačných a technických opatrení. Je to logická cesta známa ako Demingov cyklus PDCA:

1. Urobte / aktualizujte si zoznam svojich informačných aktív, aby ste vedeli, čo je pre firmu viac a čo menej dôležité.
2. Následne aktívam priraďte zraniteľnosti a hrozby, ktoré budú implikovať riziká.
3. Popíšte najväčšie riziká a pripravte plány kontinuity a obnovy.
4. Všetko pravidelne testujte a zlepšujte.

Čo by si firmy mali z legislatívy odniesť už dnes, aj keď nemusia byť priamo regulovaným subjektom?

Dôležitá rada znie: Neriešte kybersbezpečnosť kvôli legislatíve! Riešte ju kvôli zdravej, bezpečnej spoločnosti. Kyberhrozby existujú a budú určite pribúdať. Pripravené spoločnosti incidenty zvládnu lepšie a utrpia menšie škody.

Ak firma zistí, že čelí incidentu, čo by mala urobiť v prvých 24 hodinách?

V prvom rade konať okamžite a s chladnou hlavou. Infraštruktúru odpojiť od internetu, nevypínať ju! Zapojiť vedenie spoločnosti a postupovať podľa nacvičených scenárov. Podľa typu a závažnosti incidentu hlásiť na NBÚ. Informovať klientov a dodávateľov.

Ako spozná manažment, že firma má pripravený funkčný plán reakcie na incident a nejde len o formálny dokument?

Reakcie na incidenty a riadenie kontinuity by sa mali testovať a pravidelne prehodnocovať, inak to nebude fungovať. Funkčný plán sa spozná najmä podľa toho, že ho firma vie v krízovej situácii reálne použiť, nie iba predložiť ako dokument.

Ktoré témy budú v najbližšom období pre SME firmy najdôležitejšie?

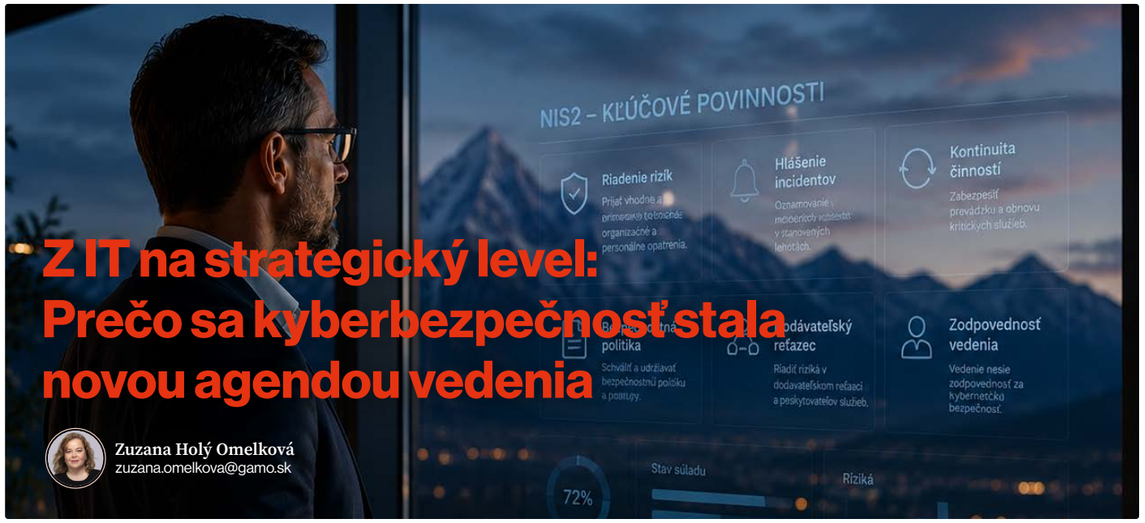
Použitie AI vo väčšine aplikácií, kybernetická odolnosť a vzdelávanie.

Aký odkaz by ste dali vedeniam firiem, ktoré kyberbezpečnosť stále odkladajú s tým, že ju začnú riešiť až „keď bude čas“?

Staré japonské príslovie hovorí o tom, kedy je najlepší čas zasadiť sakuru. Pred 50 rokmi.

A kedy je druhý najlepší čas? Teraz. Čiže: včera bolo neskoro. Nečakajte na incident, môže mať katastrofické následky – finančné, materiálne, reputačné. Príprava môže byť primeraná aj časovo a ľudsky efektívna. Nie je to žiadna raketová veda.

Plné a aktualizované verzie článkov nájdete na **platformofinvention.sk**



Z IT na strategický level: Prečo sa kyberbezpečnosť stala novou agendou vedenia

Zuzana Holý Omelková
zuzana.omelkova@gamo.sk

Éra, keď mohlo vedenie firmy nad kybernetickými rizikami mávnuť rukou so slovami „to rieši IT“, sa skončila. Kybernetická bezpečnosť sa presunula z technickej úrovne na úroveň strategického riadenia, dohľadu a právnej zodpovednosti.

Smernica NIS2 tento posun urýchlila, no dnes už nejde len o „prípravu na smernicu“. Keďže NIS2 nie je priamo uplatniteľné nariadenie, vyplývajú konkrétne povinnosti, dohľad aj sankcie najmä z národných transpozičných zákonov v krajinách, kde organizácia pôsobí. To je zásadný rozdiel oproti nariadeniam, akými sú GDPR alebo AI Act, ktoré sa uplatňujú priamo.

Pre riadiace orgány a vrcholové vedenie to znamená jediné: nestačí sa pýtať či má firma firewall, bezpečnostnú politiku alebo dodávateľa IT služieb. Dôležité je, či vedenie vie preukázať, že kybernetické riziká poznalo, schvaľovalo primerané opatrenia, dohliadalo na ich implementáciu a zanechalo dôkaznú stopu.

Pojmy „vedenie“, „riadiace orgány“ a „vrcholové vedenie“ používame všeobecne; ich konkrétny rozsah závisí od národnej legislatívy, právnej formy organizácie a vnútorného rozdelenia.

NIS2 bola začiatok. Dnes rozhodujú národné zákony

NIS2 priniesla zásadný posun v tom, ako sa v Európe chápe riadenie kybernetickej bezpečnosti. Kľúčovou zmenou je dôraz na úlohu riadiacich orgánov. Vedenie organizácie má schvaľovať opatrenia na riadenie kybernetických rizík, dohliadať na ich implementáciu a rozumieť rizikám, ktorým je organizácia vystavená. Kybernetická bezpečnosť sa tak stáva témou riadenia, nie iba technickej prevádzky.

V praxi však dnes nejde len o samotný text smernice. Firma pôsobiaca na Slovensku, v Česku, Rakúsku alebo v inom štáte EÚ musí sledovať nielen európsky rámec, ale aj konkrétnu lokálnu legislatívu. Na Slovensku je príkladom zákon o kybernetickej bezpečnosti. Pre medzinárodne pôsobiace organizácie to znamená, že jeden univerzálny „NIS2 checklist“ nestačí.

Menej formálnosti, viac dôkazov

Nový regulačný rámec posilňuje zodpovednosť riadiacich orgánov za kybernetickú bezpečnosť. Neznamená to, že každý člen vedenia bude osobne sankcionovaný za každý incident. Znamená to však, že pasívny prístup, formálne schvaľovanie bez diskusie alebo absencia kybernetickej bezpečnosti v agende vedenia sa stávajú ťažšie obhájiteľnými.

Dôležitá preto nie je len existencia bezpečnostných opatrení, ale aj dôkaz, že sa nimi vedenie reálne zaoberalo. Zápisnice z rokovaní, rozhodnutia, otázky položené manažmentu, schválené rozpočty, risk registre, výsledky auditov a následné kontroly vytvárajú dôkaznú stopu, ktorá môže byť pri kontrole alebo incidente rozhodujúca.

Externí dodávatelia, outsourcing IT služieb alebo cloudové riešenia môžu pomôcť s technickou realizáciou, no nenahrádzajú dohľad vedenia. Techniku možno delegovať, zodpovednosť za riadenie rizík, rozhodovanie a preukázateľný dohľad nie.

Ako sa táto zodpovednosť premieta do používania umelej inteligencie, riadenia incidentov, sankčných rizík a každodennej agendy vedenia? Téme sa venujeme podrobnejšie v online verzii.

Plné a aktualizované verzie článkov nájdete na **platformofinvention.sk**

Digitálne bojisko: Prečo testovať pripravenosť „nanečisto“?

Diana Filadelfi
diana.filadelfi@gamo.sk

Pondelok ráno, dispečing vodárenskej spoločnosti. Časť interných systémov reaguje nezvyčajne pomaly, na pracovných staniciach sa objavuje výkupná správa a monitoring technologickej časti prevádzky je nedostupný. Bezpečnostný tím preveruje nočné prihlásenia cez VPN.

Nikto ešte nevie, či ide o technický problém, ransomware alebo incident, ktorý sa môže dotknúť aj prevádzkových technológií. Prevádzka zatiaľ beží, ale tlak rastie. Technický tím potrebuje čas na analýzu. Vedenie chce vedieť či sú ohrozené služby. Právne oddelenie sa pýta na oznamovacie povinnosti. Komunikačný tím pripravuje stanovisko.

Potom príde ďalší vstup: na internete sa objavuje zmienka o možnom úniku zákazníckych údajov. Útočník tvrdí, že organizácia má 72 hodín.

V tomto prípade však nejde o skutočný útok. Ide o simuláciu. Bez ohrozenia prevádzky, no s reálnym tlakom na rozhodovanie.

Práve v tom je význam TTX: mení tabletop cvičenie z diskusie pri stole na interaktívnu AI-driven simuláciu. Organizácia si v bezpečnom prostredí vyskúša ako by jej rozhodnutia ovplyvnili incident, prevádzku, komunikáciu aj povinnosti. Nie až vtedy, keď útok príde, ale skôr, než bude neskoro.

Keď plán narazí na realitu

Mnohé organizácie majú incident response plán, kontaktný zoznam, krízový tím a formálne definované postupy. Skutočný incident však málokedy prebieha podľa dokumentu. Informácie prichádzajú postupne, sú neúplné a často si odporujú. Technický tím zisťuje rozsah kompromitácie, zatiaľ čo vedenie už musí rozhodovať o prevádzke, komunikácii, právnych povinnostiach a reputácii.

Plán ukazuje čo by sa malo stať. Simulácia ukáže, či to organizácia dokáže aj urobiť. TTX vytvára bezpečné prostredie na preverenie reakcie bez zásahu do skutočnej prevádzky. Scenár nie je univerzálny príklad z prezentácie. Generuje sa podľa parametrov klienta, typu organizácie, kritických služieb, IT/OT prostredia a cieľov cvičenia. Tím tak nerieši abstraktný útok, ale vlastnú realitu.

AI-driven simulácia, nie statický workshop

Tradičné tabletop cvičenia často stoja na vopred pripravenom scenári. Moderátor číta udalosti, účastníci diskutujú čo by urobili, a na konci vznikne zápis. Scenár je však statický, reakcie tímu nemenia vývoj situácie a veľa závisí od skúsenosti facilitátora.

TTX posúva cvičenie ďalej. AI pomáha vytvárať scenáre a incidentové vstupy podľa kontextu organizácie. Do simulácie možno vkladať nové udalosti – zistenie exfiltrácie dát, výpadok dodávateľa, mediálny tlak, reakciu zákazníkov, alebo nové technické zistenia. Tieto vstupy menia dynamiku cvičenia a nútia tím rozhodovať sa pod tlakom.

Účastníci tak neodpovedajú len na otázku „Čo by sme urobili“. Vidia, ako ich rozhodnutia ovplyvňujú ďalší vývoj simulácie. Neskorá eskalácia môže oddialiť právne posúdenie. Neoverené informácie môžu viesť k nejednotnej komunikácii. Technické rozhodnutie bez koordinácie s prevádzkou môže zasiahnuť kritickú službu.

Táto spätná väzba robí zo simulácie tréning rozhodovania, nielen diskusiu o bezpečnosti.

Vlastné riziká, vlastné rozhodnutia

Najväčšia hodnota cvičenia vzniká vtedy, keď sa čo najviac približuje realite firmy. Pre vodárenskú spoločnosť môže simulácia pracovať s dispečingom, technologickou prevádzkou, prístupmi dodávateľov, zákazníckymi dátami a reguláciou. Pri výrobnom podniku môže ísť konkrétne o výpadok linky alebo kompromitáciu vzdialeného prístupu.

Zmyslom nie je vytvoriť dramatický príbeh. Zmyslom je ukázať ako sa rozhodnutia tímu premietajú do prevádzky, právnych povinností, reputácie a schopnosti obnovy. V ďalšej fáze môže prepojenie s modelom alebo digitálnym dvojčaťom infraštruktúry priniesť ešte vyššiu mieru interaktivity.

Prvé rozhodnutia ukážu najviac

V úvodnej fáze simulácie sa preveruje, ako rýchlo organizácia pochopí, čo sa deje. Kto incident identifikuje? Kto ho eskaluje? Kto rozhoduje či ide o významný kybernetický incident? Kedy sa zapája vedenie, právne oddelenie, komunikácia alebo prevádzkový manažment?

Pri scenári zasahujúcom IT aj OT prostredie prichádzajú ďalšie otázky. Treba oddeliť určité časti siete? Môže izolácia IT systémov ovplyvniť prevádzkovú technológiu? Ktoré služby sú kritické? Kto rozhodne či sa obnovuje systém, kontaktuje dodávateľ alebo aktivuje krízový režim?

TTX tieto rozhodnutia zaznamenáva a umožňuje ich spätne vyhodnotiť. Sleduje ako rýchlo sa tím rozhodol, kto bol zapojený, ktoré informácie chýbali a či boli kroky zdokumentované. Práve tu sa často ukáže, že najväčšie riziko nie je v technológii, ale v nejasných kompetenciách.

Nečakaný zvrat ako skúška koordinácie

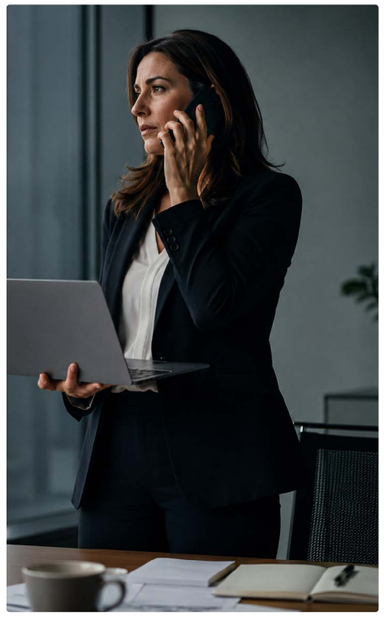
Dobre navrhnuté cvičenie nemá byť lineárne. Preto sa situácia v TTX posúva prostredníctvom nových vstupov. Počas riešenia incidentu môže prísť informácia, že útočník pravdepodobne získal prístup k zákazníckej databáze. Krátko na to sa na sociálnych sieťach objavia reakcie zákazníkov a médiá žiadajú stanovisko. Technický problém sa zrazu mení na právnu, reputačnú a komunikačnú krízu.

Technický tím pokračuje v analýze. Právny a compliance tím posudzuje oznamovacie povinnosti podľa kybernetickej regulácie, ochrany osobných údajov alebo sektorových pravidiel. Vedenie rozhoduje o prioritách, zdrojoch a komunikácii. Zákaznícka podpora potrebuje jednotné inštrukcie. V tejto fáze sa ukazuje, či organizácia funguje ako jeden tím alebo ako súbor oddelení, ktoré riešia krízu každý po svojom.

Povinnosti sa netrénujú v pokoji

Pri významnom kybernetickom incidente nejde len o technickú reakciu. Organizácia musí vedieť posúdiť, či vzniká oznamovacia povinnosť, komu sa incident oznamuje, v akej lehote, aký obsah má oznámenie obsahovať a kto zaň zodpovedá. Po transpozícii NIS2 sa tieto povinnosti posudzujú podľa legislatívy členského štátu. Pri úniku osobných údajov treba zároveň posúdiť povinnosti podľa GDPR.

TTX umožňuje preveriť, či organizácia tieto pravidlá pozná nielen teoreticky, ale aj prakticky. Vie určiť moment, keď sa incident stáva významným? Vie pripraviť včasné varovanie, aj keď ešte nemá všetky informácie? Vie oddeliť technickú analýzu od právneho posúdenia?



Report, ktorý ukáže viac než dobrý pocit

TTX zaznamenáva priebeh simulácie, prijaté rozhodnutia, reakčné časy, zapojenie tímov a kľúčové momenty, v ktorých sa incident mohol vyvíjať inak. Po skončení cvičenia vzniká report, ktorý ukazuje slabé miesta v procesoch, nejasné kompetencie, oneskorené eskalácie, komunikačné riziká aj odporúčania na zlepšenie.

Organizácia tak nezíska len zážitok zo simulácie. Získa mapu toho čo treba opraviť skôr, než príde skutočný incident.

Tréning ako nástroj riadenia

Tabletop cvičenia už nemusia byť jednorazovým workshopom raz za rok. Vďaka SaaS platforme a AI-generovaným scenárom sa môžu stať pravidelným nástrojom riadenia kybernetickej odolnosti. TTX umožňuje scenáre opakovať, meniť a prispôsobovať podľa aktuálnych hrozieb, sektora a vývoja organizácie.

Zopakujme si: skutočný incident nepríde s pozvánkou do kalendára. Príde v najnevhodnejšom čase, s neúplnými informáciami a pod tlakom. Organizácia, ktorá svoje rozhodovanie nikdy netestovala, často zistí až počas útoku, že jej plán nehovorí kto má rozhodnúť, kto má komunikovať a ktoré služby sú skutočne kritické.

TTX dáva organizácii možnosť zistiť to skôr. V simulovanom prostredí. Bez ohrozenia prevádzky. S jasnou spätnou väzbou.

Lebo v kríze nerozhoduje len technológia. Rozhoduje schopnosť konať. A tá sa nedá deklarovať v politike ani dokázať v prezentácii. Musí sa trénovať.

Plné a aktualizované verzie článkov nájdete na **platformofinvention.sk**

Firmy menia stratégiu IT: Lokálny cloud získava na význame

Jana Kohárová
jana.koharova@gamo.sk

Hardvérové železo, dedikovaný server, ktorý nepríde tri mesiace. Faktúra za cloud, ktorá rastie rýchlejšie ako biznis. Dáta uložené kdesi v zahraničí, pod cudzou legislatívou. A výpadok, ktorý nik nečakal, a ani nevie, kde presne nastal a kedy ho globálny poskytovateľ odstráni. Toto nie je scenár budúcnosti. Je to realita, ktorú dnes rieši čoraz viac slovenských firiem.

Prečo sa mení prístup k IT infraštruktúre

Je pondelkové ráno a IT manažér technologickej firmy rieši problém, ktorý môže ohroziť chod celej spoločnosti. Dedikovaný server, na ktorom bežia kľúčové firemné aplikácie, dosahuje limity výkonu. Firma rastie, zákazníkov pribúda, a infraštruktúra nestíha držať krok. Riešenie sa zdá byť jednoduché – objednať nový server.

Lenže realita je v dnešnej geopolitickej situácii iná. Dodávateľ oznámi termín na dodanie až o niekoľko mesiacov. Cena hardvéru je zároveň výrazne vyššia než pred rokom, náklady na prevádzku a správu infraštruktúry sú takisto vyššie. Plus firma potrebuje kapacitu okamžite.

Podobné situácie dnes rieši čoraz viac podnikov. Tradičný model IT infraštruktúry, postavený na vlastných serveroch, začína narážať na limity. Hardvér tak obmedzuje rast.

Modelová situácia 1. Výrobný podnik v Trnave

Stredne veľká spoločnosť s 80 zamestnancami potrebuje rozšíriť IT infraštruktúru, rastie jej objem dát z výrobných liniek. Objednajú nové servery. Dodacia doba je 22 týždňov a cena medzitým stúpla o 18 percent. IT manažér stojí pred vedením a vysvetľuje: prečo firma, ktorá rastie, musí čakať pol roka na kus hardvéru. Nikto v miestnosti to nechce počuť.

💡 Lokálny cloud má infraštruktúru už postavenú a škálovateľnú. Firma platí za kapacitu, nie za fyzický majetok, a nečaká na kontajner z Ázie.

Cloud ako ďalší logický krok

Práve v takýchto situáciách firmy začínajú prehodnocovať spôsob akým budujú svoju IT infraštruktúru. Model Infrastructure as a Service (IaaS) umožňuje využívať výpočtový výkon, úložisko aj sieťové zdroje bez nutnosti investovať do vlastného hardvéru. Kapacitu je možné zvýšiť prakticky okamžite a platiť len za to, čo sa skutočne využíva. Navyše, problém alebo úplný výpadok služby rieši lokálny poskytovateľ takmer okamžite.

Cloud sa tak stáva štandardnou súčasťou podnikovej infraštruktúry. Podľa údajov Eurostatu v roku 2025 už viac ako polovica stredne veľkých podnikov využívala cloudové služby a tento podiel každoročne rastie.

Geopolitika vstupuje do legislatívneho sveta IT

Väčšina globálneho cloudového trhu je dnes v rukách amerických technologických spoločností. Pre mnohé firmy to dlho nebol zásadný problém. V posledných rokoch sa však situácia mení. Geopolitické napätie, regulačné zásahy štátov či diskusie o prístupe k dátam spôsobujú, že podniky začínajú viac riešiť otázku digitálnej suverenity.

- Kde sú dáta uložené?
- Pod akou legislatívou sa spravujú?
- Kto k nim môže mať prístup?
- Je nový prístup v súlade so ZoKB?

Aj preto Európska únia podporuje rozvoj vlastného cloudového ekosystému aj opatrenia, ktoré majú posilniť kontrolu nad dátami a znížiť závislosť od globálnych technologických hráčov. Práve v tomto kontexte získavajú na význame lokálni cloudoví poskytovatelia.

Modelová situácia 2. Právnická kancelária v Bratislave

Kancelária spracúva citlivé zmluvné dokumenty pre klientov z finančného sektora. Všetko beží na zahraničnom cloude. Pri audite sa klient z bankovníctva spýta priamo: „Kde fyzicky sú naše dokumenty a kto k nim môže mať prístup“? Kancelária stíchne, odpoveď neexistuje. Alebo existuje, ale klientovi sa nepáči.

💡 Lokálny slovenský provider má dáta fyzicky na Slovensku, pod slovenským a európskym právom, bez extrateritoriálneho dosahu US Cloud Act. Digitálna suverenita prestáva byť buzzword – stáva sa obchodnou podmienkou.

Licenčná politika veľkých hráčov: skrytá brzda rastu

Ďalším faktorom, ktorý ovplyvňuje rozhodovanie firiem pri prechode do cloudu, je licenčná politika veľkých cloudových hráčov.

Niektoré globálne cloudové platformy majú komplexné licenčné modely, ktoré môžu výrazne zvýšiť náklady na prevádzku aplikácií. S rastom infraštruktúry rastú aj licenčné poplatky a firmy sa môžu dostať do situácie, keď je zmena poskytovateľa technicky alebo finančne komplikovaná.

Aj preto Európska únia prijala legislatívne opatrenia, ktoré majú firmám uľahčiť presun dát medzi cloudovými poskytovateľmi a znížiť riziko tzv. vendor lock-inu. Tento vývoj zároveň otvára priestor pre regionálnych cloudových providerov, ktorí ponúkajú transparentnejšie nákladové modely a väčšiu flexibilitu.

Modelová situácia 3. E-commerce startup z Košíc

Mladá firma s 12 ľuďmi spúšťa B2B marketplace na zahraničnom cloude. Po šiestich mesiacoch príde prvý väčší klient, traffic narastie štvornásobne, faktúra za cloud šesťnásobne, napríklad kvôli egress poplatkom, managed databázam a support tier. Náklady na cloud nakoniec tvoria 34 percent prevádzkových výdavkov. CFO otvorí faktúru a zatvorí ju. Otvorí znova. Zistí, že čísla sa nezmenili: cloud, ktorý mal rast umožniť, ho začína brzdiť.

💡 Lokálny provider ponúka predvídateľné paušálne ceny bez skrytých poplatkov. Firma vie plánovať cashflow a neštuduje 47-stranovú cenovú dokumentáciu hyperscalera.

Lokálny cloud: nie ako kompromis, ale strategická voľba

Pre mnohé firmy tak vzniká logická otázka: Existuje riešenie, ktoré kombinuje flexibilitu cloudu s transparentnými nákladmi a zároveň kontrolou nad dátami? Jednou z odpovedí je lokálny cloud.

Modelová situácia 4. Regionálna sieť ambulancií

Skupina ôsmich lekárskych ambulancií prechádza na digitálny systém zdravotnej dokumentácie. Pri audite sa ukáže, že nevedia garantovať, kde presne sú dáta pacientov replikované. Štyri hodiny zostanú bez prístupu ku zdravotnej dokumentácii. Nie pre hackerský útok, ale pre výpadok datacentra niekde v zahraničí, o ktorom nikto v ambulancii vopred nevedel.

💡 Lokálny slovenský cloud provider ponúka SLA s garantovanou lokalitou dát, fyzickou redundanciou na území SR a priamou podporou v slovenčine – čo pri regulovaných odvetviach nie je detail, ale podmienka licencie a súladu s GDPR a NIS2.

Priateľské SK prostredie, technológie a bezpečnosť ako základ

Presne na uvedený typ výziev reagujú lokálni poskytovatelia ako GAMO Cloud, infraštruktúra prevádzkovaná priamo na Slovensku, bez kompromisov v dostupnosti a v bezpečnosti.

Podniky, ktoré prechádzajú na GAMO Cloud, najčastejšie hľadajú:

- škálovateľnosť infraštruktúry,
- optimalizáciu nákladov,
- vysokú dostupnosť systémov,
- maximálnu bezpečnosť firemných dát,
- flexibilitu.

Služby GAMO dnes využívajú spoločnosti ako Mraziarne CHRIEN, ELBA, Oftal, Sashe.sk, Biometric či IDS BBSK, pričom ich dlhodobá dôvera potvrdzuje stabilitu poskytovaných riešení.

Cloudová infraštruktúra GAMO využíva modernú virtualizačnú platformu a je prevádzkovaná v dátovom centre DATACUBE, ktoré spĺňa kritériá TIA-942 Tier III. Riešenie zároveň spĺňa bezpečnostné štandardy ISO 27001 a ISO 27018, ktoré definujú prísne pravidlá ochrany dát a prevádzky cloudových služieb.

Jednou z najväčších výhod danej cloudovej infraštruktúry je aj flexibilita a schopnosť rýchlo reagovať na technické, legislatívne či biznis požiadavky slovenského prostredia.

Súčasťou riešenia sú tiež:

- **Zálohovanie a obnova dát**
  Automatické zálohovanie v denných alebo hodinových intervaloch a rýchlu obnovu dát po incidente.
- **Virtuálne privátne servery a cloudové úložiská**
  Bez obmedzenia počtu používateľov či objemu dát, ideálne pre moderné firemné prostredie.
- **Monitoring a bezpečnostné služby**
  Nepretržité sledovanie infraštruktúry a rýchlu reakciu na incidenty.
- **Škálovateľné prostredie pre vývoj aplikácií**
  Optimálne podmienky pre vývoj, testovanie aj produkčnú prevádzku digitálnych riešení.

Cloud ako strategické rozhodnutie

Pre firmy sa cloud postupne stáva nielen technologickou voľbou, ale aj strategickým rozhodnutím. Rast cien hardvéru, tlak na optimalizáciu nákladov, geopolitické riziká a rastúce požiadavky na bezpečnosť dát vedú organizácie k tomu, aby namiesto vlastnej infraštruktúry využívali profesionálne cloudové služby.

Lokálny cloud tak ponúka kombináciu, ktorá je pre podniky mimoriadne atraktívna – modernú technológiu, vysokú bezpečnosť a dostupnosť partnera, ktorý rozumie ich podnikaniu aj prostrediu, v ktorom pôsobia.

Plné a aktualizované verzie článkov nájdete na **platformofinvention.sk**

Keď Excel nestačí

webBox pre firmy, ktorým administratíva začala prerastať cez hlavu.

Stroje vo výrobných firmách často pracujú na maximum. Linky bežia, logistika sa zrýchľuje, manažéri potrebujú rozhodovať v reálnom čase. No keď chcú zistiť, kto je dnes na smene, kde viazne schvaľovanie služobnej cesty alebo ako vyzerá dochádzka väčšieho tímu, stále sa v mnohých firmách dostanú k papierom, tabuľkám a nespojeným systémom.

Ján Kostor, CTO
APIS spol. s r.o.
jkostor@apis.sk

Práve tam sa digitalizácia začína oveľa častejšie, než by sa mohlo zdať. Nie pri veľkých transformačných stratégiách, ale pri každodennej administratíve, ktorá prestane stíhať tempo prevádzky. S rastom firmy sa z manuálnych procesov stáva brzda, ktorá si pýta buď ďalších ľudí na administratívu alebo zmenu spôsobu práce.

Slovenská spoločnosť APIS sa tejto oblasti venuje už 35 rokov. Jej platforma webBox dnes pomáha firmám digitalizovať dochádzku, zmeny, prístupy, služobné cesty, návštevy, stravovanie aj ďalšie schvaľovacie procesy. Nie ako jeden izolovaný nástroj, ale ako systém, ktorý má ambíciu spraviť z administratívy riadený, merateľný a bezpečný proces.

Pri cloudovej prevádzke pritom APIS stavia aj na technologickom zázemí spoločnosti GAMO, ktoré do riešenia prináša stabilitu, dostupnosť a bezpečnostnú vrstvu potrebnú pre firemné dáta.

Keď fabrika beží a kancelária nestíha

Dobre to vidieť na príklade SANOVO TECHNOLOGY NIKRO s. r. o., ktorá sa špecializuje na technologické riešenia pre potravinársky priemysel, najmä v oblasti spracovania vajec.

Pred implementáciou systému webBox prebiehal proces objednávania a výdaja stravy v papierovej forme. Zamestnanci si stravu objednávali prostredníctvom lístkov, ktoré následne personálne oddelenie sumarizovalo, spracovávalo objednávky a zabezpečovalo ich distribúciu.

Nasadením systému webBox došlo k úplnej automatizácii tohto procesu. Personálne oddelenie sa výrazne odbremenilo od rutinných činností a zároveň sa zvýšil komfort pre zamestnancov. Tí majú možnosť spravovať svoje stravovanie jednoducho – prostredníctvom terminálu v jedálni alebo pohodlne na diaľku cez mobil či počítač.

Na základe pozitívnej skúsenosti so stravovacím modulom spoločnosť postupne rozšírila využitie webBoxu aj o ďalšie funkcionality, konkrétne o evidenciu dochádzky a správu prístupov do budov firmy.

„Veľkú výhodu webBoxu vidím v modularite riešenia, ktoré sme mohli postupne rozširovať podľa našich potrieb. Vďaka jednému centralizovanému systému pre viacero oblastí sme výrazne zefektívnili procesy a eliminovali duplicitné činnosti," potvrdzuje Peter Škvarka, finančný riaditeľ SANOVO TECHNOLOGY NIKRO s. r. o.

320
ušetrených hodín mesačne
SANOVO TECHNOLOGY NIKRO

300+
riadených zamestnancov
DPD Slovakia

88 %
úspora času pri správe stravy
Fakultná nemocnica Nitra

Nie hotový balík, ale vlastný vývoj

Za týmto typom riešenia nie je len nasadenie softvéru. APIS zdôrazňuje rozdiel medzi integrátorom, ktorý kúpi, predá a implementuje hotové riešenie, a softvérovým domom, ktorý má vlastný vývoj pod kontrolou.

„Byť integrátorom a byť softvérovým domom sú dva odlišné svety. Pri webBoxe máme pod kontrolou celý životný cyklus produktu, od analýzy požiadaviek cez architektúru a vývoj až po prevádzku a podporu. Vďaka tomu vieme platformu prispôsobiť realite klienta, nie naopak," vysvetľuje Ján Kostor, CTO spoločnosti APIS.

Sila platformy preto nestojí iba na počte modulov. Stojí na schopnosti prispôsobiť sa reálnej prevádzke, jej pravidlám, zmenovým kalendárom, schvaľovacím postupom a hardvérovým integráciám.

Sto ľudí, rôzne krajiny, jeden proces

Iný typ problému riešila DPD Slovakia. Tu nešlo o výrobnú linku, ale o ľudí v pohybe.

Viac ako 300 zamestnancov, geograficky distribuovaný tím a pracovné cesty v rámci Európy vytvárali prostredie, v ktorom papierové alebo e-mailové schvaľovanie prirodzene narážalo na svoje limity.

Nasadením modulu webDrive prešla DPD Slovakia na digitálny, cloudový model schvaľovania cestovných príkazov. Manažér dnes môže schváliť pracovnú cestu v reálnom čase cez mobil, aj keď sa nachádza na inej pobočke alebo v inej krajine. Výsledkom je menej čakania, menej manuálneho spracovania a rýchlejší tok informácií.

„webBox nám poskytol ucelené riešenie dochádzky za najvýhodnejšiu cenu. V DPD tak z jedného programu používame dochádzku, ale tiež napríklad schvaľovanie a vyúčtovanie služobných ciest," hovorí Peter Radačovský, IT & Project Director, DPD Slovakia.

Cloud, mobilita

webBox vznikol v roku 2014 ako natívne cloudové riešenie a neskôr prešiel aj na architektúru PWA. Pre používateľov to znamená plnohodnotný prístup k systému cez počítač, tablet aj mobil.

Schváliť dochádzku, dovolenku, návštevu alebo pracovnú cestu tak už nemusí znamenať sedieť pri kancelárskom počítači. V distribuovaných tímoch je práve mobilita rozdielom medzi systémom, ktorý ľudia obchádzajú, a systémom, ktorý používajú.

Ak cez systém prechádzajú prevádzkové dáta, dochádzka, prístupy alebo schvaľovacie procesy, technológia musí stáť na infraštruktúre, ktorá je stabilná, bezpečná a pripravená na každodennú firemnú záťaž. Cloudová dostupnosť nie je iba otázkou pohodlia. Aj preto je pri SaaS modeli webBoxu dôležitá spolupráca APIS so spoločnosťou GAMO.

Od administratívy k riadenému procesu

webBox nestojí na logike „všetko naraz". Firma môže začať jedným procesom a ďalšie moduly pridávať postupne podľa rastúcich potrieb.

Jednou z najčastejších chýb pri digitalizácii je preniesť pôvodný papierový proces do digitálnej podoby. „Bez otázky, či to ešte dáva zmysel, nejde o správne riešenie. Digitalizácia nemá zakonzervovať chaos. Má ukázať, kde firme uniká čas, a proces nastaviť tak, aby sa dal riadiť, merať a ďalej rozvíjať," zdôrazňuje Ján Kostor, CTO spoločnosti APIS.

Budúcnosť firemnej digitalizácie nebude len v tom, že manažér uvidí či stroj vyrába. Rovnako dôležité bude vedieť, či sú na správnom mieste správni ľudia, procesy schválené, dáta aktuálne a prevádzka pod kontrolou.

webBox ukazuje, že aj zdanlivo bežné administratívne agendy majú strategický význam. Digitalizácia totiž nie je o tom, že papier nahradí obrazovka. Je o tom, že firma získa nad svojimi procesmi prehľad, kontrolu a možnosť ďalej rásť.

Softvér potrebuje bezpečné zázemie

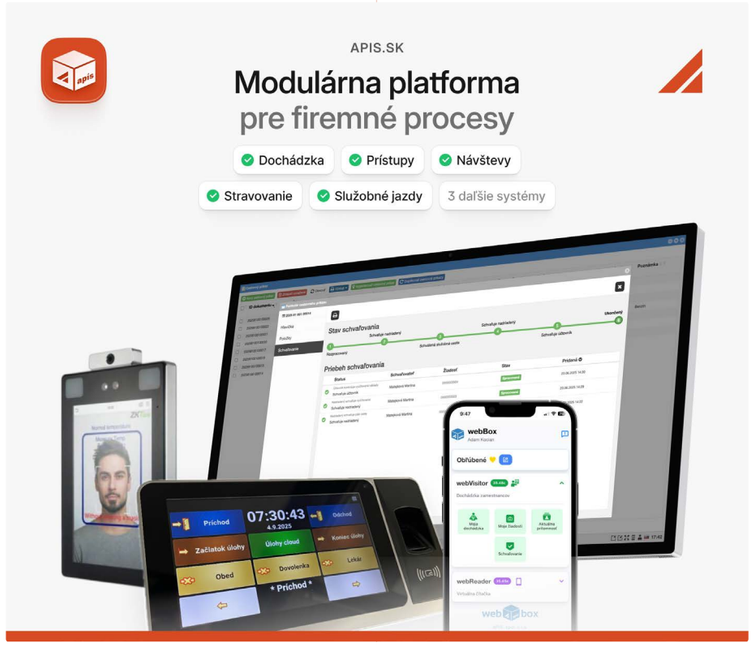
Ak systém riadi dochádzku, prístupy, pracovné cesty alebo iné prevádzkové dáta, musí byť nielen funkčný, ale aj bezpečný, dostupný a spoľahlivý.

APIS dodáva softvérovú platformu, vlastný vývoj a znalosť firemných procesov. GAMO prináša infraštruktúrne a bezpečnostné zázemie, ktoré je pri cloudových službách kľúčové.

„webBox môže fungovať ako samostatná platforma, ale pri cloudových službách je technologické zázemie kľúčové. V spolupráci s GAMO vieme klientom poskytnúť stabilné a bezpečné prostredie s vysokou dostupnosťou a zálohovaním na úrovni, ktorú firemné procesy potrebujú," uzatvára Ján Kostor, CTO spoločnosti APIS.

Pre SaaS klientov webBoxu to znamená prevádzku na certifikovanej infraštruktúre a bezpečnosť na úrovni TIER III.

Dôležité je aj to, že GAMO webBox samo používa. Partnerstvo tak nestojí iba na dodávateľskom vzťahu, ale aj na každodennej skúsenosti.



Plné a aktualizované verzie článkov nájdete na **platformofinvention.sk**

72 hodín, ktoré rozhodujú: kybernetický incident očami práva po transpozícii NIS2

Zuzana Holý Omelková
zuzana.omelkova@gamo.sk

Prvé hodiny po kybernetickom incidente nie sú len IT krízou. Sú právnou, manažérskou a reputačnou udalosťou, pri ktorej každé rozhodnutie zanecháva stopu alebo medzeru, ktorú bude regulátor neskôr hľadať. NIS2 nastavila európsky rámec, no konkrétne oznamovacie povinnosti dnes vyplývajú z národných zákonov.

Je piatok, 17:43. Bezpečnostný systém spúšťa alarm a súbory sa začínajú šifrovať. Zrejme ide o ransomware. Technický tím útok potvrdí o dve hodiny neskôr. A práve v tej chvíli sa začína nielen boj o dáta, ale aj odpočítavanie lehôt, ktoré môžu rozhodovať o pokutách, dôvere partnerov a schopnosti organizácie zvládnuť krízu.

Kybernetický incident si totiž vyžaduje koordinovanú reakciu viacerých organizačných zložiek naraz. Technický tím potrebuje zastaviť útok. Právne oddelenie musí sledovať oznamovacie povinnosti. Vedenie musí prijímať rozhodnutia, ktoré majú strategický, reputačný aj právny význam. Komunikácia musí byť koordinovaná a každý krok musí byť zdokumentovaný.

Smernica NIS2 tento tlak výrazne zvýšila. Pri konkrétnom prípade však organizácia nevychádza iba zo samotného textu smernice. NIS2 je európsky rámec, ktorý členské štáty premietli alebo premietajú do národných právnych predpisov. Povinnosti pri incidente preto treba posudzovať podľa národnej legislatívy, sektorovej regulácie a pravidiel dohľadového orgánu.

Čo vyžaduje právny rámec po transpozícii NIS2

Európsky rámec NIS2 zaviedol prísnejší mechanizmus oznamovania významných kybernetických incidentov. Nejde však o každý technický problém ani každý bezpečnostný alarm. Oznamovacie povinnosti sa viažu na incident, ktorý napĺňa kritériá stanovené príslušnou právnou úpravou.

Základná logika je trojstupňová. Najskôr prichádza včasné varovanie. Cieľom nie je úplná forenzná analýza, ale rýchly signál príslušnému orgánu, že incident nastal alebo pravdepodobne nastal, a môže mať širšie bezpečnostné dôsledky.

Nasleduje podrobnejšie oznámenie s prvotným hodnotením incidentu, odhadovaným rozsahom dopadu na služby, systémy alebo dáta a prehľadom prijatých opatrení. Napokon prichádza záverečná správa s analýzou príčin, priebehu útoku, dopadov a nápravných opatrení. Konkrétne lehoty, obsah a forma oznámení sa môžu líšiť podľa národnej legislatívy.

Podstata je však rovnaká: regulátor neočakáva, že organizácia bude v prvých hodinách vedieť všetko. Očakáva však, že bude konať včas, primerane, koordinovane a zdokumentovane. Neúplnosť informácií preto nie je ospravedlnením pre meškanie.

Odpočítavanie: ako vyzerá prvých 72 hodín v praxi

V piatok podvečer bezpečnostný systém detekuje šifrovanie súborov. Alarm sa spúšťa automaticky, no nikto ešte nevie, či ide o izolovaný problém, technickú chybu alebo rozsiahly útok.

O dve hodiny neskôr IT tím potvrdí ransomware a identifikuje prvé postihnuté systémy. Incident je okamžite eskalovaný na úroveň vedenia, právneho tímu a zodpovedných osôb podľa interného Incident Response Planu. Nie preto, aby sa hľadal vinník, ale preto, že ďalšie rozhodnutia presahujú kompetencie technického tímu.

Začína sa posudzovať či incident napĺňa kritériá významného kybernetického incidentu. Dôležité je správne určiť, kedy organizácia nadobudla vedomosť o incidente, ktorý môže spúšťať oznamovaciu povinnosť. Nie každý technický alarm automaticky znamená začiatok plynutia právnej lehoty. Nemôže však čakať na úplnú istotu, ak už okolnosti naznačujú významný incident.

Osemnásť hodín po potvrdení útoku technici ešte nepoznajú plný rozsah škôd. Právne oddelenie však v spolupráci s technickým tímom a vedením pripravujú včasné varovanie. Správa obsahuje to, čo organizácia v danom momente vie, aké opatrenia prijala a aké riziká predbežne identifikovala.

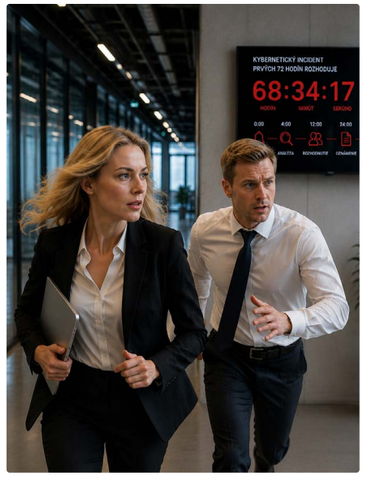
Po šesťdesiatich hodinách tím zisťuje, že pri útoku mohlo dôjsť aj k úniku osobných údajov klientov. Do procesu preto vstupuje posúdenie povinností podľa GDPR. Organizácia pripravuje podrobnejšie oznámenie podľa kybernetickej regulácie a paralelne posudzuje, či vzniká povinnosť oznámiť porušenie ochrany osobných údajov.

Tento scenár má relatívne dobrý koniec nie preto, že organizácia mala šťastie. Ale preto, že niekto vopred vedel čo robiť, koho informovať, ako dokumentovať rozhodnutia a kedy komunikovať s príslušným orgánom.

Kde organizácie zlyhávajú

Organizácie často nezlyhávajú preto, že by útok technicky nezvládli. Zlyhávajú preto, že porušia procesné povinnosti. Najnebezpečnejší prístup je ten, keď sa organizácia rozhodne najprv útok „vyriešiť“, a až potom ho oznámiť. Ak medzičasom zmešká oznamovaciu lehotu, technický úspech neodstráni právny problém.

Ďalším častým zlyhaním je oneskorená eskalácia na úroveň vedenia.



Incident zostane príliš dlho uzavretý v technickom tíme, hoci už má právne, reputačné alebo prevádzkové dopady. Rizikom je aj nekoordinovaná komunikácia, keď rôzne oddelenia hovoria navonok rôzne veci alebo komunikujú bez overených informácií.

Osobitnou slabinou býva dokumentácia. Ak organizácia nedokáže spätne preukázať čo vedela, kedy to vedela, kto rozhodol, aké opatrenia boli prijaté a prečo, jej postavenie pri kontrole je oslabené. Dokumentácia nie je byrokracia. Je to najdôležitejší dôkazný prostriedok.

Prečo musí byť rozdelenie práce jasné vopred

Incident Response Plan nie je len interný dokument pre IT oddelenie. V regulovanom prostredí je praktickým predpokladom toho, aby organizácia vedela splniť oznamovacie, dokumentačné a riadiace povinnosti.

Mal by určovať kto má právomoc incident eskalovať, kto posudzuje jeho závažnosť, kto komunikuje s príslušným orgánom, kto informuje vedenie a kto koordinuje reakciu naprieč tímami. V slovenskom prostredí môže ísť napríklad o komunikáciu podľa zákona o kybernetickej bezpečnosti, typicky voči NBÚ alebo príslušnému CSIRT. V iných štátoch bude príslušný orgán vyplývať z lokálnej legislatívy.

V prvých hodinách musia fungovať minimálne tri línie reakcie: technický tím, právne a compliance tímy a vedenie. Technický tím izoluje systémy, zastavuje šírenie útoku a pripravuje podklady. Právne a compliance tímy sledujú oznamovacie lehoty a pripravujú oznámenia. Vedenie prijíma strategické rozhodnutia o prevádzke, komunikácii, zdrojoch a kontinuite služieb.

Tieto línie nemôžu fungovať izolovane. Prvé hodiny po incidente sú testom schopnosti organizácie konať ako jeden koordinovaný celok. Každé rozhodnutie, zistenie a prijaté opatrenie musí mať záznam, aby organizácia dokázala spätne preukázať, že reagovala primerane, včas a na základe dostupných informácií.

Príprava rozhoduje. Nie šťastie

Prvých 72 hodín po významnom kybernetickom incidente nie je len testom technickej obrany. Je to test toho, či organizácia vie konať, rozhodovať, dokumentovať a komunikovať v súlade s právnymi povinnosťami.

V digitálnom prostredí už príprava na incident nie je prejavom pesimizmu. Je základnou súčasťou riadenia rizík. Ak má organizácia vopred nastavený Incident Response Plan, jasné kompetencie, komunikačné scenáre a testované procesy, dokáže premeniť kritických 72 hodín na kontrolovaný postup. Ak ich nemá, technický problém sa rýchlo zmení na právnu, reputačnú a manažérsku krízu.

Nečakajte na prvý útok. Určite si už dnes kto má právo incident eskalovať, komunikovať a riešiť ho. Pretože pri kybernetickom incidente nerozhoduje len to, čo organizácia urobí. Rozhoduje aj to, či vie preukázať kedy, prečo a ako konala.

Plné a aktualizované verzie článkov nájdete na **platformofinvention.sk**

Anti-slop: návrat ľudskej stopy

Prečo nás opäť zaujíma nedokonalé umenie?


Iveta Hlaváčová
iveta.hlavacova@gamo.sk

V čase, keď dokáže umelá inteligencia generovať obrazy, videá, hudbu v priebehu sekúnd, sa mení aj náš vzťah k tvorbe. To, čo ešte nedávno pôsobilo technicky ohromujúco, dnes veľmi rýchlo splýva s nekonečným prúdom podobných výstupov.

Dokonalosť sa stala dostupnou, a práve preto začína byť zaujímavé niečo iné: stopa človeka.

Ak sa dajú pekný a bezchybný obraz, hudobný motív alebo krátke video vytvoriť takmer okamžite, otázka neznie tak, či výsledok spĺňa všetky normy kvality. Dôležitejšie začína byť, prečo vznikol, kto za ním stojí a akú skúsenosť doň vložil.

V kultúrnej debate sa pre presýtenie masovo generovaným AI obsahom udomácňuje pojem „slop“ = digitálna kaša. Čiže obsah, ktorý môže byť vizuálne pôsobivý, ale často pôsobí zameniteľne, lacno a bez osobnosti.

Anti-slop je reakciou na tento stav. Nie ako odmietnutie technológií, ale ako hľadanie protiváhy. V umení to znamená návrat k ručnej práci, materiálu, chybe, náhode, procesu a nedokonalosti.

Čím viac obsahu vzniká bez odporu, tým väčšiu hodnotu môže mať tvorba, v ktorej odpor ešte cítiť. Drsná línia, stopa ruky, nepresnosť, pomalosť či viditeľná námaha môžu byť v čase umelej dokonalosti tým, čo pôsobí najľudskejšie.

Pričom je dôležité podotknúť, že anti-slop nám (nostalgicky) nepripomína minulosť. Skôr ukazuje, že aj v digitálnom svete môže byť najvzácnejšia práve ľudská stopa.

Bude zaujímavé sledovať meniaci sa pomer hodnoty aj hodnôt tých dvoch svetov.

Plné a aktualizované verzie článkov nájdete na **platformofinvention.sk**

Ručne maľovaný akvarel z ciest po Slovensku.

Autor: Rastislav Ekkert, Názov: Čachtický hrad so stromom

platform
of invention

Informačné technológie
pre podnikanie s nápadom

Vydavateľ
GAMO a.s.
www.gamo.sk

Sídlo redakcie
Kyjevské námestie 6
974 04 Banská Bystrica
redakcia@platformofinvention.sk
www.platformofinvention.sk

Spoznajte odpoveď na neproduktívnu administratívnu záťaž

GAMO
INFORMAČNÉ TECHNOLÓGIE