platform of invention

Informačné technológie pre podnikanie s nápadom

online pdf print

Užitočné v správnych hlavách

magazín pre CTO, CFO, CEO

číslo 10
ročník piaty | 2/2025



Kyberman:

Nový prístup k auditom kybernetickej bezpečnosti

Ako dlho si môže firma dovoliť nevyrábať?

Útok bol budíčkom

Magazín o informačných technológiách

Tlačená aj elektronická verzia zadarmo.
Kliknite na tlačidlo a čítajte.





PDF magazín

Online portál



#10

#9









#8

#7

#6

#5







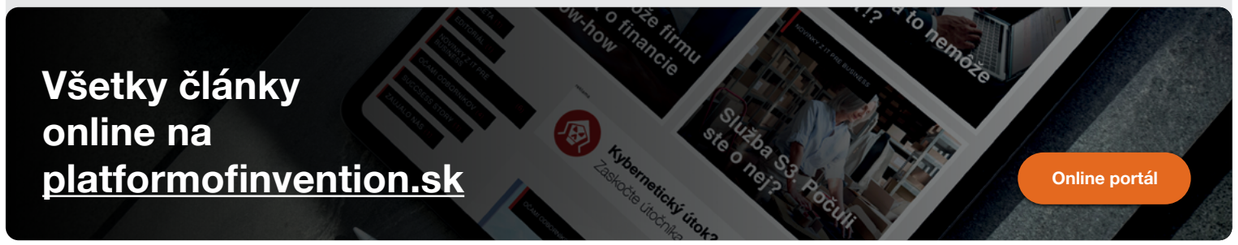


#4

#3

#2

#1



platform of invention
Informačné technológie pre podnikanie s nápadom

Magazín s ambíciou ukázať ako IT technológie ul'ahčujú firmám každodenný život, prinášať úspešné biznis riešenia, unikátne inovácie a trendy v IT, a pomáhať v uplatnení podnikatel'skej 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 do publika slovenských firiem.

Chcete zistiť viac a zapojiť sa?

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

www.platformofinvention.sk/profil-magazinu/

klikni alebo oskenuj QR

Čítajte nás online

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

www.platformofinvention.sk

klikni alebo oskenuj QR

EDITORIÁL



Pravda o vlastných rizikách

Kybernetická bezpečnosť už dávno nie je doménou IT oddelení. Dnes ovplyvňuje výrobu, jej chod, dôveru zákazníkov, reputáciu značky aj schopnosť inovovať.

Zároveň vstupujeme do éry, v ktorej je prirodzené využívať aj nástroje umelej inteligencie. Zrýchľuje rutiny, pomáha hľadať chyby, odporúča riešenia a generuje dáta, ktoré by človek spracovával celé dni.

No ako prináša efektivitu, tak prináša aj nové typy bezpečnostných rizík.

Finálny obsah je výsledkom ľudskej expertízy a zodpovednosti. Presne ako vo firemnej bezpečnosti: technológia pomáha, ale nerozhoduje.

Preto majú dnes audity, evidencia aktív či hodnotenie zhody zásadný význam. Digitalizácia a nástroje, ako náš Kyberman, dokážu sprístupniť aj zložité procesy širokému publiku a pritom zachovať presnosť, transparentnosť a dôveryhodnosť.

Firmy zároveň hľadajú rovnováhu medzi modernizáciou a kontrolou nad vlastným prostredím. Hybridné infraštruktúry spájajú cloud a on-premise tak, aby organizácie nemuseli voliť medzi rýchlosťou, flexibilitou a ochranou dát. Reagovať rýchlo, ale bezpečne. To je nová hranica konkurencieschopnosti.

A povedzme si úprimne: žiadna technológia nezabezpečí firmu, ktorá nepozná svoje riziká. Governance bez analýzy rizík je ako auto bez bŕzd. Možno sa pohne dopredu, ale nezastaví. Politiky a smernice majú význam len vtedy, keď znižujú dopady incidentov. A tie už dávno nie sú len technické. Často rozhodujú o tom, či firma prežije.

Kľúčová otázka, ktorú si mnohé podniky kladú až príliš neskoro, znie: Ako dlho si môžeme dovoliť nevyrábať? Odpoveď sa meria v hodinách či dňoch, a jej cena môže byť likvidačná.

Zmysluplné pravidlá vznikajú tam, kde organizácie vidia realitu vlastných rizík a majú odvahu povýšiť bezpečnosť medzi strategické priority.

Kyberbezpečnosť totiž nie je len o ochrane. Je o schopnosti fungovať, inovovať a prežiť aj v okamihu, keď sa stane neočakávané.


Zuzana Holý Omelková
Obchodná riaditeľka
zuzana.omelkova@gamo.sk

Nový štít proti ransomwaru v ére umelej inteligencie

Ransomware dnes útočí rýchlejšie ako stíhajú firmy reagovať. Útočníkom stačí jediné šťastné kliknutie, no IT oddelenia musia byť v strehu 24/7. A presne do tohto sveta vstupuje Veeam so svojou najnovšou platformou Veeam Data Platform v13, ambicióznym riešením, ktoré chce podľa tvorcov „zmeniť pravidlá hry“ v oblasti kybernetickej odolnosti.
Riešenie spája spoľahlivé zálohovanie s umelou inteligenciou, forenznou analýzou a okamžitou obnovou dát. Pre firmy to znamená viac než len technickú aktualizáciu. Veeam Data Platform v13 prináša pokoj do chaotického sveta kybernetických hrozieb a istotu, že ani najsofistikovanejší útok nebude znamenať koniec ich podnikania.
Nie je to len ďalšia verzia s pár novými funkciami. Je to zásadná zmena filozofie ochrany dát. V ére, kde tradičné nástroje zlyhávajú, Veeam stavia na inteligencii, automatizácii a odolnosti, aby firmy mohli inovovať bez strachu.

V čom je táto platforma výnimočná čítajte ďalej v magazíne.



Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



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



Azure Arc spája svet cloudu a on-premise

Moderné IT prostredie je rozptýlené medzi lokálne dátové centrá, verejný a privátny cloud či edge zariadenia. Kombinácia rôznych platforiem prináša komplexitu, ktorú je čoraz náročnejšie spravovať. Azure Arc od Microsoftu spája tieto svety do jedného celku. Poskytuje kompaktnú správu serverov, databáz a Kubernetes klastrov z jedného centrálneho miesta bez ohľadu na infraštruktúru. Spoločnosti tak získajú konzistentné zabezpečenie, jednoduchšiu compliance, aj možnosť modernizovať aplikácie bez nutnosti migrácie.

Chcete vedieť prečo je Azure Arc strategickým nástrojom pre budúcnosť IT? Buďte pripravení na budúcnosť hybridného IT už dnes. Prečítajte si celý článok.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Vladimír Krajkář
Business Development Manager Cloud
TD SYNNEX Czech s.r.o.



Používate ešte Windows 10? Neodkladajte modernizáciu

Definitívne ukončenie podpory Windows 10 predstavuje zásadný míľnik, ktorý má priamy dopad na bezpečnosť, plynulosť aj budúci rozvoj firemnej IT infraštruktúry. Bezpečnostné aktualizácie, opravy chýb ani technická podpora už nie sú pre tento systém dostupné.
Každým dňom preto rastie riziko kybernetických útokov, nekompatibility softvéru aj možných finančných strát. Bez bezpečnostných aktualizácií zostávajú firemné zariadenia zraniteľné, bez možnosti nápravy, a výkon kľúčových aplikácií môže postupne klesať.
Zistite aké dopady má koniec podpory na vašu firmu a aké riešenia máte k dispozícii — od prechodu na Windows 11 až po predĺžené bezpečnostné aktualizácie či výber nových zariadení.

Celý článok čítajte v online verzii a vyberte si bezpečnú cestu pre vašu IT infraštruktúru.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Gabriela Repatá
SOC špecialista
GAMO a.s.

Kyberútok nepríde s pozvánkou. Ako zistíte, či ho zvládnete?

Kybernetické útoky dnes neobchádzajú žiadnu firmu a často prichádzajú v najmenej vhodnom momente. Mnohé organizácie si síce uvedomujú riziká, no na reálne incidenty nebývajú dostatočne pripravené. Riešením je platforma TTX TableTop Exercises, ktorá prináša simulácie kybernetických útokov riadené umelou inteligenciou. Dokáže pre firmu okamžite pripraviť realistický scenár, prispôsobovať jeho priebeh reakciám tímu a vkladať nečakané udalosti, ktoré preveria rozhodovanie aj koordináciu v kríze. Firmy tak získajú jasný obraz o tom, ako sú na hrozby pripravené a čo potrebujú zlepšiť.

Ako môže vyzerať skutočný incident a čo rozhoduje v kritických chvíľach? Predstavte si, že je piatok 16:30, väčšina tímu už odchádza domov, a zrazu sa na zdieľanom disku objaví podozrivý súbor. Čo teraz?

Riešenie nájdete na online portáli platform of invention.



Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Diana Filadelfi
Produktový manažér
GAMO a.s.



AI mení spôsob, akým pracujeme. Čo prináša a načo si dať pozor

Umelá inteligencia mení pracovné prostredie rýchlejšie, než sme čakali. Dokáže automatizovať rutinu, odhaliť chyby v kóde, spracovať obrovské množstvo textu či vytvoriť kompletný výstup za pár sekúnd. S jej prudkým nástupom však prichádzajú aj riziká – halucinácie, zacyklenie či únik citlivých údajov, ak sa používa neuvážene. Firmy dnes nasadzujú vlastných AI agentov, ktorí vyhľadávajú informácie, odpovedajú na otázky a odbremeňujú ľudí od manuálnej práce. Ich schopnosti rastú exponenciálne. AI sa tak mení na super asistenta, no človek zostáva garantom kvality. Tempo inovácií sa navyše stále zrýchľuje a možnosti modelov rastú z mesiaca na mesiac. To všetko vytvára tlak na organizácie, aby držali krok s technológiou aj pravidlami jej bezpečného používania. Ako sa AI vyvíja a kde prináša najväčšiu hodnotu?

Prečo je dôležité zachovať si kritické myslenie? Zistíte v plnom znení článku.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

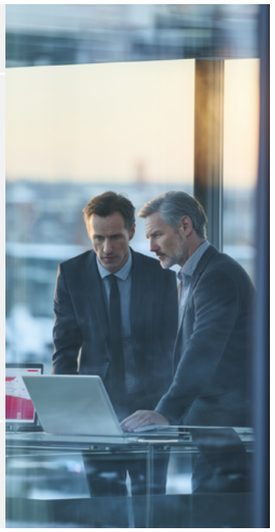


Roman Schmidt
Starší špecialista
GAMO a.s.

Kedy treba hlásiť kybernetický incident?

Hlásenie kybernetického incidentu do 24 hodín je povinnosťou regulovaných subjektov podľa Zákona o kybernetickej bezpečnosti, ktorý bol aktualizovaný v súvislosti s požiadavkami Európskej únie. Rýchle „včasné varovanie“ sa vyžaduje len pri závažných incidentoch, ktoré majú reálny dopad na dostupnosť, integritu alebo dôvernosť služieb. Kľúčové je vedieť rozlíšiť bežnú udalosť od incidentu a mať pripravené interné procesy, aby organizácia dokázala reagovať okamžite. Správne nastavený incident response, jasné zodpovednosti aj dostupná dokumentácia, ideálne aj v papierovej forme, výrazne skracujú čas medzi odhalením problému a jeho nahlásením. Nové pravidlá zároveň rozširujú okruh subjektov, ktorým vznikajú tieto povinnosti. Firmy by preto nemali odkladať preverenie toho, či do tejto kategórie patria.

Overte si, či sa na vašu organizáciu vzťahujú nové povinnosti a pripravte sa na incidenty skôr, než nastanú.



Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Martin Ondrušek
Manažér kybernetickej bezpečnosti, CISO
GAMO a.s.



Ako dlho si môže firma dovoliť nevyrábať?

O prežití rozhoduje RTO. Prečo ho musíte poznať ešte pred krízou

RTO, Recovery Time Objective, je v skutočnosti čas, počas ktorého dokáže firma zadržať dych. Keď sa systémy zastavia, podnik funguje v núdzovom režime a každá ďalšia hodina je drahšia a rizikovejšia.

Nie každý manažment si túto otázku položí včas, no práve on rozhoduje o tom, či podnik krízovú situáciu prežije alebo nie. Moderné kybernetické útoky dnes neznamenajú len únik dát, čoraz častejšie dokážu úplne zastaviť výrobu, dodávky a príjmy. V momente, keď stroje stoja, beží najdrahší čas v histórii firmy. Ak je RTO napríklad 72 hodín, tak to znamená, že po troch dňoch výpadku už podnik vstupuje do zóny ohrozenia: reputačného, právneho či existenčného, čiže finančného.

Práve preto je dôležité poznať hranicu, dokedy dokážete výpadok ešte ustáť. Tento čas neurčuje pocit ani intuícia, ale analýza vplyvu na podnikanie. Ukáže, ktoré procesy musia byť obnovené ako prvé, koľko času máte na bezpečnú obnovu a akú mieru straty dát si môžete dovoliť (RPO). Spolu to vytvára základnú toleranciu firmy na akýkoľvek výpadok.

RTO nevzniká odhadom, ale analýzou

Na určenie realistického RTO teda nestačí domnienka typu „asi by sme to ustáli“. Slúži na to analýza vplyvu na podnikanie. Analysis BIA presne určí, ktoré procesy sú kritické, ako rýchlo sa musia obnoviť a aké straty vznikajú pri ich odstávke.

Typický výstup BIA môže napríklad ukázať, že expedícia potrebuje obnovu do 4 hodín, výrobná linka do 12 hodín a účtovný systém do 48 hodín. Práve tieto rozdiely sú kľúčom k správnemu nastaveniu stratégie prežitia.

BIA už nie je len odporúčaním, ale aj požiadavkou legislatívy Zákona o kybernetickej bezpečnosti a európskej smernice NIS 2. Jej výsledky sú základom pre celú bezpečnostnú stratégiu, od zálohovania až po krízové scenáre. Ak firma vyhodnotí, že prežije maximálne týždeň bez výroby, všetky technológie, procesy aj zmluvné vzťahy musia byť postavené tak, aby bolo možné obnoviť prevádzku v priebehu siedmich dní. Nie teoreticky, ale v realite, keď bude situácia najhoršia.

Keď minúta stojí viac než celá ochrana

Výpadok výroby má priame a merateľné finančné dôsledky, často omnoho vyššie než akékoľvek pokuty či investície do prevencie. Nie je to abstraktná hrozba, ale okamžitý únik peňazí z firmy. Čím je podnik viac automatizovaný a previazaný s dodávateľskými reťazcami, tým rýchlejšie stráca.

Takáto je realita globálnych incidentov:

Jaguar Land Rover (2025)

Kybernetický útok zastavil výrobu na viac než päť týždňov, zasiahol 30-tisíc zamestnancov a až 200-tisíc ľudí v dodávateľskom reťazci. Mal vplyv na vyše 5-tisíc organizácií.

Straty presiahli 1,9 miliardy GBP, britskej libry šterlingov, pričom denne firma prichádzala o milióny. Straty v slovenskom nitrianskom závode presiahli 5 miliónov eur denne, tisíce zamestnancov zostalo doma. Incident ukázal, že aj globálne značky sú zraniteľné, ak nemajú oddelené IT a OT siete.

Kým IT systémy riadia informácie, OT systémy riadia samotnú výrobu – a ich prepojenie bez adekvátnej ochrany je jednou z najčastejších slabín priemyselných podnikov.

Norsk Hydro (2019)

Útok LockerGoga paralyzoval IT infraštruktúru Norsk Hydro a zastavil výrobu v divízii Extruded Solutions. Zasiahol viac než 35-tisíc zamestnancov v 40 krajinách.

Firma musela prejsť na manuálne procesy, zatvoriť niektoré závody a obnovovať systémy z offline záloh. Celková škoda sa vyšplhala až na 75 miliónov USD.

CFO spoločnosti Eivind Kallevik vtedy priznal: „Hodina odstávky nás stála viac než celodenné investície do kybernetickej bezpečnosti. Z praxe vidím, že firmy najčastejšie podceňujú práve to, koľko času skutočne potrebujú na plnú obnovu – a rozdiel medzi odhadom a realitou býva dramatický.“

Čo to znamená v realite

Predstavte si obyčajné pondelkové ráno. Operátor hlási, že linka nereaguje, no spočiatku to vyzerá len ako drobný výpadok. Po hodine už stoja tri výrobné úseky, expedícia čaká a zákazník volá prečo meška dodávka. Toto je okamih, keď sa nečakaný incident mení na reťazovú reakciu strát.

Podľa analýzy IBM a Ponemon Institute trvá obnova po takomto útoku v priemere 11 až 22 dní, pričom náklady rastú s každým dňom odstávky. Priemerná finančná škoda presahuje 1,8 milióna eur ešte pred zaplatením prípadného výkupného, a to len za straty spôsobené prerušením výroby a obnovou systémov.

Správa Check Point Threat Intelligence Report z júla 2025 uvádza, že výrobný sektor na Slovensku čelí v priemere 958 kyberútokom týždenne. Ransomvér je najväčšou hrozbou, schopnou úplne zastaviť prevádzku. Tu už nejde o IT rozpočet, ale o schopnosť firmy dýchať. Útočníci cielia najmä na dostupnosť systémov, pretože vedia, že zastavená výroba bolí viac než ukradnuté dáta.

Ako vyzerá pripravená firma

Kým sa GDPR zameriava najmä na ochranu osobných údajov, kybernetické útoky v priemysle majú úplne inú dynamiku. Ich cieľom nie je krádež dát, ale zastavenie výroby, prerušenie prevádzky a spôsobenie finančnej či reputačnej škody. Moderná výroba je plne závislá od IT a OT systémov, logistiky, digitálnej komunikácie a skladového manažmentu v reálnom čase. Výpadok už nepreberie „papierový režim“ ako to bolo pred 30 rokmi. Bez systémov dnes výroba neexistuje.

Dobre pripravená firma pozná svoje RTO pre každý kritický proces, pravidelne testuje obnovu zo záloh, má jasné rozhodovacie postupy pre prvé hodiny incidentu, a nepočíta s tým, že IT vyrieši všetko samo. Pripravenosť znamená, že v čase krízy nevzniká panika, ale realizuje sa plán.

Najdrahší čas v každej firme je ten, v ktorom sa nič nevyrába.

Článok čítajte na platformofinvention.sk

klikní alebo oskenuj QR



Zuzana Holý Omelková
zuzana.omelkova@gamo.sk



5 najčastejších omylov firiem pri plánovaní obnovy

Veríme, že zálohy rovná sa obnova

Zálohovať neznamená vedieť obnoviť. Mnohé firmy zistia až pri útoku, že ich zálohy sú neúplné, neaktuálne alebo neprístupné. Správne nastavený systém zálohovania by sa mal riadiť pravidlom 3-2-1-1-0. Znamená to mať tri kópie dát, uložené na dvoch rôznych typoch médií, pričom jedna kópia sa uchováva mimo hlavnej lokality a ďalšia kópia musí byť offline, teda fyzicky odpojená od siete, aby bola chránená pred útokmi typu ransomware. Posledná nula v pravidle symbolizuje nulové chyby pri testovaní obnovy – teda pravidelné a automatizované overovanie, že zálohy sú nielen dostupné, ale aj skutočne obnoviteľné.

RTO si stanovíme sami

Čas obnovy sa často “odhadne” manažérsky, nie technicky. Realita je pritom takmer vždy dlhšia, než firma predpokladá.

Plán obnovy existuje, iba na papieri

Krízové scenáre bývajú pekne zdokumentované, no ešte nikdy neboli v praxi testované. Ak plán neprejde simuláciou, je len ilúziou bezpečia.

IT vyrieši všetko

Obnova výroby nie je len technický problém. Zahŕňa logistiku, komunikáciu so zákazníkmi, rozhodovanie manažmentu, dodávateľov aj právne kroky.

Nie sme zaujímaví, aby nás hackli

Útoky dnes nie sú cielené podľa prestíže, ale podľa zraniteľností. Automatizované ransomvérové kampane zasahujú aj malé a stredné podniky, často práve tie, ktoré „nemajú dôvod sa báť“.

Vráťme sa k otázke: Ako dlho?

Ak na ňu neviete odpovedať presne, nie je to len informačný nedostatok. Je to riziko, ktoré má svoju cenu a tá môže byť likvidačná. Túto odpoveď si firma nedokáže doplniť spätne po incidente. Hodnota RTO sa musí určiť v čase pokoja, keď je priestor na analýzu a plánovanie, nie v čase chaosu. Investícia do prevencie je vždy nižšia než cena odstávky. Rovnaké pravidlá neplatia len pre veľké korporácie, ale aj pre stredné a malé firmy. Tie sú často ešte zraniteľnejšie. Preto je teraz ten správny čas zistiť, aké je vaše RTO a či ste pripravení obnoviť prevádzku v reálnych podmienkach.



SUCCESS STORY

Kybernetický útok bol budíčkom

SIEM a SOC priniesli istotu tam, kde predtým vládla len nádej

Pred pár rokmi významný slovenský výrobný podnik žil v pocite, že jeho IT infraštruktúra je v dobrej kondícii. Logy existovali, administrátori robili čo bolo v ich silách, a bezpečnosť nebola akútne naliehavá. Až do momentu, keď prišiel útok – rýchly, rozsiahly a paralyzujúci. Výroba sa zastavila, dodávky sa prerušili, platby sa zablokovali.

Útok odhalil slabinu, ktorá sa síce dala tušiť, no dovtedy nebola vidieť. A kým problém nevidíte, máte dojem, že neexistuje. Realita vás však dobehne vtedy, keď je najhoršie – znie opakovaný vzorec naprieč priemyslom. V biznise sa to môže stať naozaj každému, dôležité je sa zo skúsenosti poučiť.

V konkrétnom podniku sa práve táto udalosť z roku 2023 stala impulzom, ktorá odštartovala zásadnú transformáciu. Podnik chcel získať reálnu kontrolu nad bezpečnostnými udalosťami. A urobiť to tak, aby nemusel budovať vlastný interný SOC tím – čo je dnes pre výrobnú firmu prakticky nemožné.

Neviditeľnosť bola najväčším problémom. Firma mala pocit, že je chránená, ale chýbali jej fakty. Logy síce boli, no roztrúsené naprieč systémami. Keď sa niečo stalo, riešenie každého incidentu začínalo od nuly: manuálne zisťovanie problému, zdĺhavé preverovanie, neistota, či sa na niečo nezabudlo. Chýbala centralizácia, automatické upozornenia, a aj spoľahlivý prehľad o bezpečnostných udalostiach. Bolo jasné, že ak záznamy nebudú zbierané centrálne, ich hodnota je minimálna.

Rozhodnutie: SIEM na Wazuh + SOC dohľad od GAMO

Po analýze viacerých možností, od drahých komerčných riešení typu QRadar či Splunk, sa pre manažment podniku ukázalo spojenie open-source SIEM technológie Wazuh a Managed SOC služby od GAMO ako flexibilné, dostupné, a najmä dlhodobo udržateľné.

Rozhodli sa pre platformu SIEM (Security Information and Event Management), systém, ktorý umožňuje centrálne zhromažďovanie, vyhodnocovanie a koreláciu záznamov a bezpečnostných udalostí naprieč celou IT infraštruktúrou.

Riešenie bolo postavené na verejne dostupnej bezpečnostnej technológii Wazuh, prepojené s dohľadovou službou Security Operation Center (SOC).

Firma získala jednotné miesto pre všetky záznamy, prehľad o dianí v infraštruktúre v reálnom čase a schopnosť rýchlo reagovať na hrozby, bez nutnosti budovania vlastného špecializovaného tímu. To všetko umožnilo centrálne zhromažďovanie a koreláciu logov zo serverov, siete, aplikácií aj endpointov, detekciu podozrivých aktivít, útokov a anomálií, reporting pre IT aj manažment, aj plnenie auditných a legislatívnych požiadaviek.

Kľúčoví však boli ľudia. „Technológia bez odborníkov nestačí. Môžete mať dáta, ale neviete, čo s nimi. SOC tím je nevyhnutný," zhodnotil danú situáciu zákazník.

„SIEM je základ, no jeho skutočná sila sa prejaví až vtedy, keď ho obsluhujú špecialisti. Našou úlohou je nielen zachytiť incidenty, ale aj pochopiť ich v kontexte, vyhodnotiť ich dopad a navrhnúť riešenia, ktoré zákazníka chránia dlhodobo," potvrdili špecialisti z GAMO.

Nasadenie a prvé výsledky: incidenty začali vychádzať na povrch

Po overení funkčnosti navrhnutého riešenia nasledovala pilotná fáza projektu, adaptácia do ostrej prevádzky a súčasne ladenie a dopĺňanie scenárov. Firma následne získala prakticky okamžite viditeľnosť do svojej infraštruktúry.

Najväčšou výzvou bolo zladenie záznamov zo starších systémov a nastavenie špecifických pravidiel použitia na mieru. Už počas prvých týždňov systém zachytil viacero incidentov, ktoré by predtým zostali nepovšimnuté:

- **Brute-force útoky na VPN a systémy**
Rýchle a opakované pokusy o uhádnutie hesla, ktoré SOC tím/operátor identifikuje podľa série neúspešných prihlásení z rovnakého zdroja alebo neobvyklej frekvencie pokusov.

- **Pokusy o komunikáciu so škodlivými C&C servermi**
Infikované zariadenie sa pokúša nadviazať spojenie s externým riadiacim serverom, čo SOC operátor odhalí vďaka nezvyčajnej komunikácii s podozrivými IP adresami mimo bežnej prevádzky.

- **Blokované Active Directory účty pri podozrivej aktivite**
Účty používateľov sú zablokované po sérii neúspešných prihlásení alebo pri inej podozrivej aktivite, to signalizuje pokus o neoprávnený prístup či reakciu vnútorného bezpečnostného opatrenia.

- **Detegované malvérové súbory**
Systém identifikuje škodlivé súbory podľa identifikačných znakov alebo správania. Často obsahujú backdoory, ransomware komponenty alebo špionážny kód. SOC ich označí, izoluje a preverí zdroj infekcie.

- **Prístupy na nedôveryhodné domény**
Detegované pripojenia na domény s pochybnou reputáciou, (ne)legálne platformy. V tomto prípade SOC blokuje a preveruje tieto spojenia.

- **Nežiaduca aktivita používateľov**
Objavené masívne alebo neočakávané zásahy do dát (napr. zmazanie), môžu signalizovať internú chybu, úmyselnú manipuláciu alebo prítomný ransomvér. SOC vníma udalosť ako kritický incident: prioritou je okamžitý zásah a zastavenie šírenia.

Predtým vs. teraz: Z nádeje sa stala istota

V súčasnosti má spoločnosť chránených viac ako 95 % infraštruktúry a SOC tím pracuje s desiatkami korelačných pravidiel prispôsobených prostrediu zákazníka. V reálnom čase a pravidelne poskytuje manažmentu prehľadné reporty aj odporúčania. Kritické incidenty sa riešia okamžite.

„Pred nasadením SIEM sme mali pocit, že IT je zabezpečené, ale chýbali nám fakty. Dnes vidíme incidenty v reálnom čase a máme istotu, že nad nami bdie profesionálny tím," vyjadril spokojnosť zákazník.

Zákazník tú zmenu vystihol presne: „Predtým sme dúfali. Dnes máme dôkazy." Rozhodovanie sa presunulo z roviny pocitov do roviny merateľných dát. Detekcia je rýchlejšia, reakcia je profesionálna, riziká sú pod kontrolou. A prevencia stojí menej než riešenie výpadkov! Firma to pocítila na vlastnej skúsenosti.

Podnik už plánuje rozšírenie monitoringu aj na operačné technológie (OT) a implementáciu automatizovaných reakcií pomocou orchestrácie, automatizácie a odozvy zabezpečenia (SOAR), ktorá výrazni zrýchli reakcie na incidenty. Cieľ je jasný: posunúť bezpečnosť na ďalšiu úroveň a minimalizovať čas potrebný na reakciu aj pri komplexnejších hrozbách.

Spojenie odvahy zákazníka a odbornosti tímu

Tento prípad ukazuje, že moderný SIEM a profesionálny SOC nie sú výsadou korporácií. Aj stredne veľká firma môže mať špičkový bezpečnostný dohľad bez extrémnych nákladov či potreby vlastného expertného tímu. Zákazník prijal odvážne rozhodnutie, investoval do bezpečnosti a otvorene pomenoval svoje slabiny. GAMO prinieslo odbornosť, technické know-how a schopnosť reagovať v kritických momentoch.

„Bez dôvery a spolupráce s tímom zákazníka by to nešlo. Každý krok, ktorý dnes vidíme ako úspech, je výsledkom spoločnej práce," uzatvára tím GAMO.

Je to dôkaz, že keď sa spojí technologická kompetencia s odhodlaním, výsledkom môže byť odolnejší, bezpečnejší a najmä sebavedomejší podnik.

Článok čítajte na platformofinvention.sk

klikni alebo oskenuj QR



Jana Kohárová
jana.koharova@gamo.sk





Kyberman: Nový prístup k auditom kybernetickej bezpečnosti

O riešení, ktoré odbremeňuje firmy aj audítorov, hovorí autor myšlienky

Audity kybernetickej bezpečnosti by nemali byť len formálnou povinnosťou, ale nástrojom, ktorý odhaľuje slabé miesta, dáva organizáciám jasný obraz o ich bezpečnostnom stave, a pomáha pri strategickom rozhodovaní. V praxi ich však často sprevádza administratívna záťaž, množstvo tabuliek a zdĺhavé procesy. Preto je tu nový slovenský systém Kyberman, ktorý garantuje audit bez chaosu.

Podľa aktuálnej novely Zákona o kybernetickej bezpečnosti sa povinnosť pravidelných auditov týka približne 6000 regulovaných subjektov. Napriek tomu sú audity stále vnímané skôr ako nepríjemná povinnosť. Na tieto výzvy reaguje slovenské riešenie Kyberman – aplikácia, ktorá spája evidenciu aktív, auditné procesy a riadenie kybernetickej bezpečnosti v jednom systéme. Jej ambíciou je uľahčiť prácu manažérom bezpečnosti, podporiť audítorov a priniesť do celého procesu vyššiu mieru transparentnosti a dôveryhodnosti.

O tom, ako Kyberman funguje, aké problémy rieši a akú pridanú hodnotu prináša používateľom aj audítorom sa Monika Vilimová rozprávala s ĽUBOMÍROM KOPÁČKOM, naším kolegom, autorom myšlienky a odborníkom na kybernetickú bezpečnosť.

Audity sú často vnímané ako „nutné zlo“. Zadefinujme to jednoznačne: Je bezpečnostný audit skôr administratívna záťaž alebo skutočný prínos pre organizácie?

Stále sa nachádzame v ére, kde je audit vnímaný ako niečo negatívne, ako mechanizmus kontrolovania, hľadania chýb, prípadne hľadania vinníkov. Tento pohľad je, žiaľ, hlboko zakorenený a pramení zo slabého povedomia o tom, čo audit v skutočnosti predstavuje. Chýba edukácia, nielen manažmentov, ale aj samotných manažérov kybernetickej bezpečnosti. Tí nie vždy dokážu audit odkomunikovať organizácii tak, aby bol vnímaný ako prínos, nie ako „strašiak“. Navyše, ani regulátori nepredstavujú audit verejnosti ako nástroj, ktorý má organizácii pomáhať v zlepšovaní riadenia a odolnosti. Legislatíva je postavená prísne, čo je v poriadku, ale komunikácia by mala byť mäkšia. Audit by mal byť niečo, čo organizácii pomôže, a tak by sa o ňom malo aj hovoriť. Toto je podľa mňa stále veľká výzva.

V praxi sa stretávame s tým, že organizácie majú problém najmä s evidenciou aktív, s dokumentáciou, s dôkazmi o plnení opatrení. Kde podľa teba vznikajú najčastejšie slabé miesta?

Sú prekvapivo rovnaké naprieč firmami. Najväčší problém je jednoznačne evidencia aktív. Stále žijeme v „dobe excelovej“. Mnohé organizácie – ak vôbec nejakú evidenciu majú, tak ju vedú v niekoľkých tabuľkách, ktoré nie sú konzistentné, nepracujú s rovnakými údajmi, majú desiatky verzií a nie sú dlhodobo udržateľné. Keď má niekto stovky alebo dokonca tisíce aktív, je prakticky nemožné udržať evidenciu v Exceli tak, aby bola použiteľná pre audit či pre analýzu rizík. Pokiaľ organizácia nevie aké aktíva má, tak jednoducho nevie, čo má chrániť. A to je zásadný problém, ktorý sa neustále opakuje. Vždy, keď prídeme robiť audit alebo rizikovú analýzu, prvé hodiny až dni trávime tým, že dávame dokopy databázu aktív. Je to základ, bez ktorého sa nedá pohnúť ďalej, a pre mnoho organizácií je to stále „nezvládnuteľná“ úloha.

Audítorská správa má význam iba vtedy, ak verne odráža skutočný stav bezpečnosti. Ako môže digitalizácia a automatizácia zabezpečiť, aby boli výsledky auditu naozaj presné, porovnateľné a relevantné?

Prvé, čo k tomu poviem, je slovo konzistencia. Pokiaľ nemáme jednotný rámec, podľa ktorého audit prebieha, výsledky sa budú vždy líšiť podľa toho, ktorý audítor ho robí. Pri rozdielovej analýze pracujem s tým, čo mi klient povie, čiže od neho nechcem dôkazy, lebo cieľom je rýchlo získať obraz o stave. Ale pri audite je povinnosť pracovať s dôkazmi, zákon to vyžaduje. A práve tam je digitalizácia nenahraditeľná: vytvorí jasný, pevný rámec, v ktorom sa pohybujeme. Z digitalizovaného audítorského setu sa nedá vybočiť. Systém presne definuje kontrolu, riziká, evidenciu dôkazov aj výstup. To zabezpečí opakovateľnosť a merateľnosť auditov. A čo je kľúčové – ak regulátor dostane päť správ generovaných cez jednotný systém, vie ich porovnať. Pri dnešnom stave, keď je každý audit „originál“, je porovnávanie prakticky nemožné.

Čiže do sveta chaosu prinášame poriadok. S touto myšlienkou vznikla aj aplikácia Kyberman. Čo bolo hlavným impulzom pre tvorbu riešenia?

Povedzme to na rovinu: vzniklo z čistej frustrácie. Keď som začal robiť audity vo veľkom, ohromovalo ma, aké je to pracné a ako veľmi to závisí od človeka. Desiatky dokumentov, stovky strán, Excelové tabuľky, ktoré nedávajú zmysel, nekonzistentné dáta… Bolo mi jasné, že toto nie je dlhodobo udržateľné. Prekvapilo ma aj to, že ani renomované audítorské firmy nemajú digitalizované riešenia, že všetko je postavené na Exceloch. Práve táto prax ma prinútila rozmýšľať ako to celé postaviť inak. A tak vznikol nápad vytvoriť systém, ktorý bude pevný, jednotný, odborný a použiteľný pre audítorov aj organizácie.

Ako je Kyberman architektonicky navrhnutý? Ktoré moduly tvoria jeho základ?

Architektúra je jednoduchá, ide o zabezpečenú webovú aplikáciu typu klient–server. Ale podstatné sú moduly. Základom celého systému je asset management, kde si organizácia vytvorí kompletnú databázu aktív. Nad ním je postavený audítorský modul, ktorý obsahuje tzv. auditné sety, čiže digitalizované požiadavky legislatívy či noriem. Používateľ si jednoduchým klikom vyberie, voči čomu chce vykonať hodnotenie a spustí audit. Moduly sú previazané, to znamená v systéme vieme prelinkovať tie assety, ktorých sa auditná kontrola týka. Výstupom je tlačová zostava audítorskej správy a akčný plán úloh vyplývajúcich z auditu na riešenie. Hoci v tejto verzii nemáme plne rozvinutý modul analýzy rizík s váhami a číselnými modelmi, systém umožňuje pracovať s rizikami jednoducho – identifikované riziká previažeme s aktívami a prostredníctvom úloh s nimi štandardne pracujeme. Tento zjednodušený prístup je pre bežných používateľov, ktorými sú primárne manažéri KB, v praxi často efektívnejší. Systém je intuitívny, ale zároveň komplexný.

Ako Kyberman pomáha napĺňať slovenskú legislatívu?

Používateľ pracuje s auditným setom, ktorý presne vychádza z legislatívnej metriky. Poskytovatelia kritickej základnej služby (PKZS) majú povinný dvojročný auditný cyklus, resp. v prípade prevádzkovateľov základnej služby (ZS) päťročný s pravidelným samohodnotením. Ak si bude používateľ v Kybermanovi vykonávať priebežné interné audity rozdelené na menšie časti a samohodnotenia podľa auditného setu, vyhodnocovať ich, aplikovať opatrenia, porovnávať si navzájom stavy z auditov predošlých období, bude organizácia na konci obdobia veľmi dobre pripravená na povinný externý audit. A ak to budú robiť naozaj poctivo a rovnako budú pristupovať k opatreniam, budú sa približovať k vysokej miere zhody. Zároveň tým budú napĺňať požiadavky kybernetickej bezpečnosti a aj zvyšovať svoju kybernetickú odolnosť.

Legislatíva však nie je len slovenská. Ako ste riešili kompatibilitu s európskymi rámcami: NIS2, DORA, TISAX, NIST a ďalšími?

Veľmi jednoducho: nefixovali sme sa na žiadnu legislatívu ani výhradne na kybernetickú bezpečnosť. Vybrali sme univerzálne audítorské princípy podľa normy, ktoré sú spoločné pre všetky audity bez ohľadu na odvetvie. Audit je v podstate porovnávanie stavu voči nejakému štandardu. A tento princíp sa dá digitalizovať. Preto vieme vytvárať sety podľa európskych smerníc, národných legislatív alebo podľa interných noriem organizácií. Kým existuje dokument, ktorý definuje štandard, vieme ho digitalizovať. Záujem je dokonca aj z Česka, ktoré má nový zákon o kybernetickej bezpečnosti – a Kyberman je na to pripravený.

Čo presne sú auditné sety a ako fungujú v praxi?

Auditný set je digitalizovaný štandard prílohy 1 vyhlášky 227/2025 Z. z. o bezpečnostných opatreniach. Nie je to však len mechanické prepísanie požiadaviek. Vložili sme doň aj tzv. generické riziká, návrhy riešení a odporúčania, vysvetlenia a šablóny, ktoré pomáhajú používateľovi pochopiť čo má kontrolovať a aké riziká sú typické. Systém mu ponúkne riziká na výber, môže pridať vlastné, a celý audit tak prebieha jednotne. Cieľom je, aby aj menej skúsení audítori dokázali so systémom pracovať. Do budúcnosti plánujeme rozšíriť auditné sety o funkcie AI, ktorá bude schopná vyhodnocovať kontroly automaticky. To výrazne zrýchli celý auditný proces.

Ako Kyberman pracuje s dôkazmi? Integrita dôkazov je často problémom.

Pri každej auditnej kontrole si používateľ nahrá elektronický dôkaz – môže to byť dokument, fotografia, screenshot, výstup zo systému. Kyberman pri nahratí automaticky vytvorí kontrolný súčet dátového súboru. Všetky dôkazy sa evidujú s časovou pečiatkou aj kontrolným súčtom. Keď sa audit uzamkne, systém vytvorí veľký dátový súbor obsahujúci celý audit, vrátane dôkazov a kontrolných súčtov, a ten sa uloží do blockchainu. Tým pádom si každý vie kedykoľvek overiť, že s dôkazmi nikto nemanipuloval. Zmena jediného bajtu by zmenila kontrolný súčet a systém by to okamžite odhalil.

Používa Kyberman blockchain aj na archiváciu celého auditu?

Presne tak. Je to „svätý grál“, ktorý som chcel dosiahnuť od začiatku. Keď sa audit uzamkne, uloží sa jeho digitálny odtlačok do blockchainu. Ten je nemenný. Znamená to, že výsledky auditu sú validné a overiteľné aj po rokoch. Regulátor, audítor, manažér, ktokoľvek si vie overiť, či je auditný záznam hodnoverný a dáta konzistentné. Je to absolútny dôkaz, že audit nebol upravený, prispôsobený ani spätne menený.

Cieľom Kybermana je zjednodušovať rutinné činnosti a pomáhať šetriť čas manažérov a audítorov KB. Ktoré to sú?

Mnohé. Automatizácia spočíva najmä v udržiavaní prehľadu o tom, čo sa robí. V rámci úloh, ktoré manažérovi KB vyplývajú, sú procesy úplne zautomatizované a on v každom momente vie, čo má robiť alebo čo kde nefunguje Napríklad asset manažment eviduje dátumy end-of-life a exspirácie aktív, kedy bol vykonaný maintenance, aké má licencie. Pre manažéra kybernetickej bezpečnosti je často najväčší problém prehľad, a aj ten Kyberman rieši. Všetko je v jednom systéme: aktíva, kontroly, riziká, dôkazy, úlohy. Už to nie je stovka Excelov či Wordov na disku. Každý krok má presné miesto, proces je automatizovaný a zrozumiteľný.

Ako môže Kyberman pomôcť z pohľadu vrcholového manažmentu pri strategickom riadení bezpečnosti?

Manažment dostáva merateľné údaje. Nie odhady, nie pocitové hodnotenia. Každá kontrola je hodnotená CMMI metrikou od 0 do 5. Len exaktne zmerané výsledky sa dajú skutočne riadiť. Výsledky sa dajú porovnávať v čase. Medzi auditmi, medzi organizáciami, medzi jednotlivými oblasťami. Manažment tak vidí, kde sa zlepšuje, kde stagnuje, kde je problém a kam treba presunúť zdroje. Pre korporátne organizácie, ktoré majú viacero dcérskych spoločností alebo prevádzok, je to obrovská výhoda, pretože tieto súčasti sú v systéme upratané. To znižuje časovú náročnosť administrovať jednu konkrétnu zložku a organizácia získava absolútny prehľad nad všetkým na jednom mieste.

Hovoríme teda o multitenantnom režime. Ako funguje?

Najvyššia rola v systéme je manažér kybernetickej bezpečnosti. Ten môže spravovať desiatky firiem alebo organizačných jednotiek, čiže tenantov. Manažér KB má založený účet a tenant je aktivovaný zakúpením licencie. Každý tenant má svoje dáta, svoje licencie, svoj auditný cyklus. Ak manažér prestane organizáciu spravovať, jej dáta zostanú zachované a prenesú sa inému manažérovi. Nič sa nevymaže. Je to veľmi praktické, najmä keď jeden manažér zastrešuje desiatky organizácií, plus v bežnej praxi sa manažéri v organizáciách menia.

> Kybernetická bezpečnosť už dávno nie je témou len pre IT oddelenia. Stále vo vyššej miere sa stáva súčasťou strategického riadenia, podnikovej kultúry a reputácie organizácie. Projekty ako Kyberman ukazujú, že automatizácia, integrácia dát a dôveryhodná evidencia môžu zmeniť celý prístup k bezpečnostným procesom. Že aj komplexné oblasti akými sú audity, evidencia aktív a legislatívna zhoda sa dajú sprístupniť a automatizovať bez toho, aby sa stratil ľudský rozmer rozhodovania. Predstavuje krok smerom k novej generácii riešení, ktoré aktívne pretvárajú legislatívu do praktickej a technologicky podporenej reality. A práve vtedy sa z povinnosti stáva pridaná hodnota a z auditu skutočný nástroj rozvoja.

Ako podľa teba riešenia ako Kyberman menia kultúru kybernetickej bezpečnosti v organizáciách?

Umožňujú vznik poriadku. Znie to banálne, ale je to kľúčové. Veľa organizácií fungovalo tak, že mali všetko tzv. „nejako“ zaznamenané, niekde roztrúsené, niekde zabudnuté. Keď prídeme robiť audit, niekedy je zázrak, že firma funguje bez incidentov. Kyberman dáva organizáciám štruktúru, procesy, meranie, transparentnosť. Je to veľmi silný nástroj na budovanie kultúry bezpečnosti. Samozrejme, systém sám o sebe nič nezachráni, musí byť používaný zodpovedne. Ale ak organizácia pracuje poctivo, Kyberman jej dá veľmi silný rámec.

Na záver: Ako vidíš budúcnosť auditov, compliance a regulačných procesov? Stane sa digitalizácia štandardom?

Verím, že áno. A veľmi by som si to prial. Dnes sa na strane regulátora deje niečo absurdné: dostávajú desiatky auditov, ktoré nie sú porovnateľné. Každý audítor má vlastný štýl, vlastné metriky a výstupy. Potom je pre regulačný orgán extrémne náročné skonsolidovať výsledky do údajov, ktoré je možné merať a porovnávať. Namiesto toho by mal vzniknúť jednotný systém, ktorý sa stane štandardom, ideálne na úrovni Európskej únie. Digitalizácia prináša porovnateľnosť, merateľnosť a kvalitu. A ak to má zabezpečiť Kyberman – prečo nie? Sme otvorení spolupráci. A bolo by to efektívne riešenie pre všetkých.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Monika Vilimová
monika.vilimova@gamo.sk





Incident nestačí odhaliť, treba ho aj nahlásiť

V septembri 2025 nadobudla účinnosť vyhláška, ktorá zásadne mení spôsob ako organizácie na Slovensku pristupujú k hláseniu kybernetických incidentov. Korektné nahlásenie môže byť výzvou.

Vyhláška Národného bezpečnostného úradu SR nadväzuje na novelu zákona o kybernetickej bezpečnosti. Pre potreby praxe presne určuje, čo sa považuje za závažný incident a aké sú povinnosti prevádzkovateľov základných služieb pri jeho hlásení.

Identifikačné kritériá pre incident

Pri posudzovaní jeho vážnosti sú stanované kľúčové identifikačné kritériá. Patria tu napríklad úplný výpadok služby nad stanovený čas, ohrozenie dôvernosti, integrity či dostupnosti údajov, alebo incidenty s dopadom na viac ako 25-tisíc osôb.

Každý subjekt, na ktorý sa vzťahuje zákon o kybernetickej bezpečnosti, musí v prípade splnenia kritérií incidentu odoslať hlásenie cez Jednotný informačný systém kybernetickej bezpečnosti. Samotné hlásenie však nie je voľná textová správa a vyhláška presne stanovuje, aké parametre musí obsahovať.

V hlásení musia organizácie uviesť základné údaje, akými sú čas detekcie a opis incidentu a aj následné doplnenia, čiže časový priebeh, prijaté opatrenia a aktuálny stav riešenia. Vyhláška zároveň prináša jasné pravidlá, ktoré zabezpečujú jednotnú a rýchlu komunikáciu s NBÚ. V praxi to znamená, že organizácie musia byť schopné incidenty nielen včas odhaliť, ale aj efektívne zdokumentovať a nahlásiť.

Korektné hlásenie

Výzvou pre korektné nahlásenie incidentu sa však stáva samotný proces ako získať všetky potrebné vstupy. Technicky zdatní administrátori dokážu zozbierať vyžadované údaje z viacerých zdrojov postupne pomocou logov, ide však o zdĺhavý a komplikovaný proces.

Dobrou správou je, že IT správcom môže pri nahlasovaní významne pomôcť technológia. Riešenie rozšírenej detekcie a reakcie (XDR) od spoločnosti ESET umožňuje pokročilú detekciu hrozieb v reálnom čase prostredníctvom korelácie dát. Dáta sa v tomto prípade zbierajú z rôznych zdrojov od koncových zariadení až po cloudové služby.

Automatizácia je zásadná

Súčasťou XDR riešenia je nástroj Incident Creator, ktorý zozbierané dáta automaticky premieňa na prehľadné informácie o incidente.

Incident Creator reportuje všetky potrebné detaily od technických údajov až po opis prijatých opatrení. Tieto dáta môžu následne správcovia využiť na korektné hlásenie do Jednotného informačného systému kybernetickej bezpečnosti.

Ak organizácie nemajú vlastné kapacity na vyhodnotenie závažnosti incidentov, v rámci zmluvných služieb riadenej detekcie a reakcie im pomáha ESET tím. Experti spracujú nielen analýzu závažnosti a dopadov, ale aj návrh opatrení.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Július Selecký
Solution Architect
ESET, spol. s r.o.

Pohľad na aktuálnu kyberbezpečnostnú vyhlášku NBÚ. Posun dozadu či dopredu?

Vyhláška č. 227/2025 Z. z. v kontexte „starej“ vyhlášky č. 362/2018 Z. z.



Slovenská kybernetická bezpečnosť dostala od 1. 9. 2025 nové „pracovné prostredie“. Z pohľadu práva, ale už aj existujúcej praxe v oblasti kybernetickej bezpečnosti, nejde rozhodne o kozmetickú zmenu. Mení sa predovšetkým filozofia a s tým súvisiaca štruktúra aj „mikronastavenie“ mnohých požiadaviek so spoločným a jediným správnym začiatkom.

Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach („227/2025“) nahrádza doterajšiu vyhlášku č. 362/2018 Z. z. („362/2018“) a spolu so skoršou transpozíciou smernice NIS2 vo forme novely zákona o kybernetickej bezpečnosti, ktorej účinnosť datujeme k prvému dňa roka 2025, mení pravidlá hry nielen pre starých známych prevádzkovateľov základných služieb.

Pozrime sa spolu ako.

Od „checklistu“ k risk-based

Vyhláška 362/2018 bola v čase prijatia dôležitým krokom, vytvorila značne detailný katalóg bezpečnostných opatrení viazaných na oblasti podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti, doplnený o klasifikáciu informácií, kategorizáciu IS a minimálne požiadavky pre jednotlivé kategórie IS I–III. Textácia vyhlášky 362/2018 povinné osoby často motivovala ku tendenciám a „compliance“ prístupu mať značný rozsah bezpečnostných požiadaviek spracovaný len formálne, prostredníctvom dokumentácie, bez skutočného prepojenia na reálnu analýzu rizík či kontinuitu činností. Hoci je potrebné jedným dychom dodať, že práve formalizácia a dokumentácia boli často auditmi identifikované ako nedostatkový „tovar“ u povinných osôb.

Bez ohľadu na uvedené, s vyhláškou 362/2018 nám v reáliách slovenskej kyberbezpečnosti čiastočne končí aj konštatovaný formálny prístup a tento je nahradený odlišnou filozofiou a prístupom na podklade vyhlášky 227/2025. Hoci sa to na prvý, a možno ani na druhý pohľad, nemusí takto hneď javiť.

Bezpečnostné opatrenia sa podľa ostatného znenia zákona o kybernetickej bezpečnosti delia na minimálne opatrenia podľa § 20 ods. 4 zákona a všeobecné bezpečnostné opatrenia (oblasti, pre ktoré sa prijímajú bezpečnostné opatrenia) podľa § 20 ods. 2 zákona s tým, že obsah oblastí bezpečnostných opatrení podľa § 20 ods. 2 zákona stanovuje práve vyhláška 227/2025 v rámci rozsiahlej 151 riadkovej prílohy č. 1. Zatiaľ nič nové, takto obdobne bol vyskladaný aj zákon pred novelou v spojení s vyhláškou 362/2018.

Kľúčovou je však skutočnosť, že rozsah bezpečnostných opatrení sa v zmysle nových pravidiel viaže len na výsledky analýzy rizík. Argumentom by mohlo byť, že analýza rizík predsa bola vyžadovaná aj v zmysle vyhlášky 362/2018, no pravda je taká, že primárna identifikácia bezpečnostných opatrení bola založená na klasifikácii informačných aktív a kategorizácii sietí a informačných systémov (minimálne opatrenia boli fixné podľa kategórie I / II / III) s tým, že analýza rizík bola častokrát vykonaná len formálne, naoko, voči katalógu aktív nekorešpondujúcemu s už klasifikovanými aktívami.

Výstup sa teda volal analýza rizík, aj sa tak obsahovo tváril, no prevažne sa jednalo o izolovaný dokument, ktorý nereflektoval všetky aktíva prevádzkovateľa základnej služby, „pracujúceho“ so štandardnými katalógmi hrozieb, výnimočne aj zraniteľností, bez reflexie na skutočný rizikový profil organizácie, jej aktíva, kritické činnosti a v neposlednom rade biznisové a iné potreby. Šlo v zásade len o formalitu predloženú audítorovi, lebo checklist si ju „pýta“.

Pokiaľ sa však jedná už o vyhlášku 227/2025, povinný je ňou ukotvený systematický proces riadenia rizík so zrejmým mapovaním na metodiku NBÚ (hoci metodika nie je záväzná) a s jasným rozlíšením prijatých, neprijatých a zvyškových rizík. Vyhláška 227/2025 výslovne vyžaduje preukázateľné schvaľovanie výsledkov analýzy rizík osobou podľa § 20 ods. 4 písm. h) zákona.

Z pohľadu praxe je to krok dopredu, posúva od „odfajknutia opatrení“ k diskusii, čo je pre konkrétneho prevádzkovateľa základnej služby potrebné, dôležité a obhájiteľné.

Bezpečnostná dokumentácia: menej rozprávania, viac obsahu

Vyhláška 362/2018 definovala bezpečnostnú dokumentáciu pomerne široko a miestami opisne – so záberom aj na súvisiacu organizačnú kultúru, rámce riadenia operačných rizík či bezpečnostné návody.

Vyhláška 227/2025 tento rámec síce obsahovo nepribližuje (dokonca je tu prítomná nižšia miera detailu v porovnaní s vyhláškou 362/2018), avšak čo do objemu rámec rozširuje. A to napr. požiadavkou o existenciu bezpečnostných politík pre jednotlivé oblasti bezpečnosti (novelou zákona došlo k rozšíreniu oblastí), výkon analýzy rizík, určenie úrovne identifikovaných rizík, akceptovaných rizík a zvyškových rizík pre aktíva spolu so zoznamom aktív alebo zadokumentované určenie rozsahu a spôsobu prijatia, dodržiavania a vykonávania bezpečnostných opatrení vrátane odôvodnenia neprijatia bezpečnostného opatrenia.

Okrem uvedeného je možné posun vnímať aj v tom, že dokumentácia je podľa vyhlášky 227/2025 jasnejšie previazaná na riadenie rizík a na reálnu architektúru prostredia. Pre organizácie, ktoré už v praxi používajú napr. ISO 27001 alebo iné rámce, je výslovne umožnené mapovanie existujúcich metodík výkonu analýzy rizík na (hoci nezáväznú, ale dobrú) metodiku zverejnenú Národným bezpečnostným úradom SR.

Uvedené teda vytvára tlak na tých, ktorí doteraz fungovali „papierovo“. Bezpečnostná dokumentácia nemôže byť len univerzálny šablónový balík. Musí reálne odrážať aktíva organizácie, jej architektúru a riziká.

OT „naozaj“ na scéne

Jedným z najväčších posunov je explicitné zakotvenie operačných technológií (OT) v texte vyhlášky 227/2025, kde pracuje s pojmom operačné technológie priamo napr. v § 1 a § 4 a v prílohe č. 1 rozdeľuje opatrenia podľa relevancie pre IKT a OT a stanovuje bezpečnostné požiadavky v reflexii na špecifiká OT (napr. núdzové napájanie, oddelené zálohovacie systémy, fyzická a logická segmentácia OT vs. IT, vrstvy OT, nezávislé firewally pre OT).

Z hľadiska kybernetickej bezpečnosti ide o výrazný posun. Regulačný rámec konečne explicitne reflektuje, že PLC, SCADA či DCS sa nedajú riadiť podľa rovnakých zásad ako „kancelárske“ IT, a zároveň, že narušenie OT môže mať skutočné dopady.

Uvedeným jednoznačným rozšírením pôsobnosti zákona však zároveň otvárame aj novú pandorinu skrinku. Spomedzi už teraz úzkej skupiny IKT odborníkov pre oblasť kybernetickej bezpečnosti je potrebné nájsť aj takých, ktorí disponujú reálnou znalosťou a špecializáciou pre svet OT.

Pri napĺňaní nových povinností je dôležité riešiť kybernetickú bezpečnosť nielen technicky, ale aj z právneho hľadiska. Ak organizácia potrebuje vyhodnotiť svoje záväzky podľa rozšíreného regulačného rámca, právna istota je kľúčová. Advokátska kancelária SIGNUM legal s. r. o. dlhodobo pôsobí v oblasti regulačného a technologického práva a pomáha pri implementácii požiadaviek kybernetickej bezpečnosti – od identifikácie rizík až po nastavenie procesov a zmluvných vzťahov v súlade so zákonom.

Na právne nastavenie však musí nadviazať aj technická realizácia. Pre efektívne zvládnutie požiadaviek zákona je vhodné spolupracovať s partnerom, ktorý rozumie bezpečnosti OT aj IT. GAMO a.s. ponúka implementáciu požiadaviek zákona, IT/OT audity, bezpečnostný monitoring aj služby manažéra kybernetickej bezpečnosti. Vďaka kombinácii technického know-how a praktických skúseností dokáže organizáciám ponúknuť riešenia, ktoré sú udržateľné, funkčné a v súlade s legislatívou.

Záverom

Kam sa teda posúvame prostredníctvom vyhlášky 227/2025? Či dopredu alebo dozadu bude závisieť predovšetkým od toho, ako si budú svoju prácu robiť kontrolóri, audítori a manažéri kybernetickej bezpečnosti. Prax vytvorená týmito subjektmi ukáže, či sa budeme v kybernetickej bezpečnosti uchyľovať ku vzorovosti a formalizmu, alebo k reálnemu plneniu bezpečnostných požiadaviek, na ktorého začiatku je výkon analýzy rizík a mapovanie bezpečnostných opatrení, ktoré reálne mitigujú identifikované riziká.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR



JUDr. Štefan Pilár
advokát SIGNUM legal s.r.o.
a certifikovaný audítor
kybernetickej bezpečnosti



Hybridný cloud ako nový štandard moderného IT



Digitálna transformácia už dávno nie je voľbou, ale nevyhnutnosťou. Väčšina organizácií, bez ohľadu na charakter a veľkosť, stojí pred zásadnou otázkou: Ako vybudovať moderné, flexibilné a najmä bezpečné IT v dlhodobom horizonte? Jednou z odpovedí je hybridný prístup.

Existuje mnoho dôvodov, kedy je lokálna infraštruktúra pre organizáciu nevyhnutná. Môže to byť ochrana dát a regulácie v odvetviach ako napríklad financie či štátna správa, kde je nutné, aby dáta zostali pod kontrolou organizácie. Prioritou iných organizácií, najmä výrobných alebo zdravotníckych zariadení, je zabezpečenie nízkej latencie.

Hybridný cloud prepája svet lokálnych dát a cloudových služieb. Inými slovami ide o kombináciu lokálnej infraštruktúry so širokými možnosťami cloudu. V tomto modeli zohrávajú kľúčovú úlohu dve technológie od Microsoftu Azure Local a Azure Arc.

Azure Local a Azure Arc: Spojenie výkonu a riadenia

Služba Azure Local je niečo ako „mini cloud“ implementovaný do on-premise infraštruktúry. Laicky povedané, je to moderná infraštruktúra, ktorá funguje podobne ako verejný cloud (napr. Azure), ale fyzicky sa nachádza v dátovom centre organizácie.

Pri tradičnej on-premise infraštruktúre, ktorá beží na klasických serveroch, je potrebné zabezpečiť jej správu, pravidelné aktualizácie a zálohovanie. To si vyžaduje veľa manuálnej práce zo strany administrátorov. Využitím riešenia Azure Local získate zariadenie, ktoré na prvý pohľad pripomína bežný server, no prináša oveľa viac. Dokáže automatizovať množstvo rutinných činností, ktoré by inak museli vykonávať IT pracovníci. Navyše ponúka rozšírené funkcie ako sú monitoring, zálohovanie či pokročilé bezpečnostné mechanizmy. Výsledkom je výrazné zníženie prevádzkovej záťaže IT oddelenia a efektívnejšia správa celej infraštruktúry.

Dáta zostávajú v lokálnej infraštruktúre organizácie, tá má nad nimi kontrolu. Tým, že dáta sú blízko, aplikácie reagujú okamžite, t.j. majú okamžitú odozvu. Rýchlosť je zásadná napríklad vo výrobe alebo v zdravotníctve.

Prostredníctvom Azure Local sa otvára cesta k inováciám. Bez investícii do zložitejšej infraštruktúry a nutnosti migrácie do cloudu je možné nasadzovať moderné služby vrátane umelej inteligencie alebo automatizácie.

Služba Azure Arc funguje ako most, ktorý spája lokálne servery a cloud do jedného celku. Umožňuje jednotnú správu IT prostredí aj v prípadoch, keď je infraštruktúra organizácie dislokovaná na rôznych miestach, napríklad v dátovom centre, v cloude alebo u iného poskytovateľa. Ide o celkom nový spôsob ako riadiť servery, databázy, kontajnery a ďalšie prvky naprieč všetkými prostrediami z jedného miesta.

Azure platforma sa stáva centrálnym riadiacim bodom, ku ktorému sa cez Arc pripájajú rôzne dislokované objekty: on-premise servery, edge zariadenia, dokonca aj systémy v multicloude. Správa serverov a aplikácii z ich vlastnej konzoly a s vlastnými pravidlami sa stáva minulosťou. Všetko sa ovláda z jedného miesta. Zjednodušene povedané ako na „diaľkové ovládanie“ pre celé IT.

Hybridný model a nová úloha IT oddelení

Zavedenie hybridného prostredia mení aj rolu IT oddelení v organizácii. V klasickej on-premise infraštruktúre sú doposiaľ IT tímy primárne orientované na rutinnú prevádzku: inštalácie, patchovanie, riešenie incidentov, hybridný model tieto činnosti výrazne automatizuje. Správa sa presúva do jednotnej platformy, kde je možné centrálne riadiť konfigurácie aj bezpečnostné pravidlá.

IT oddelenie sa stáva strategickým partnerom biznisu. Jeho ťažisko sa z „udržiavania systémov v chode“ presúva na inovácie, rozvoj služieb a podporu rastu organizácie. Čas pre nasadenie novej aplikácie či služby sa výrazne skracuje, čo dáva firmám konkurenčnú výhodu.

Práca s hybridom: Ako začať a kam smerovať

Transformácia on-premise infraštruktúry na hybridný model nevyžaduje zásadné zmeny. Modernizáciu IT môžete robiť postupne malými krokmi a priebežne sa zoznamovať s možnosťami hybridného modelu, získavať zručnosti, a v neposlednom rade aj dôveru v riešenie.

Ak chcete začať využitím hybridného cloudu, prvým krokom je vyhodnotenie priorít. Je nutné zamyslieť sa nad tým, ktoré aplikácie musia zostať blízko vašich dát – napríklad výrobné systémy, ktoré vyžadujú rýchlu odozvu a je možné ich presunúť do cloudu, kde získajú väčšiu flexibilitu.

Ďalším krokom je výber správneho prostredia. Pre kritické aplikácie, ktoré potrebujú stabilitu a okamžitú reakciu, je vhodná lokálna infraštruktúra. Naopak, cloud je ideálny pre škálovanie a nasadzovanie inovácií ako sú moderné aplikácie či umelá inteligencia.



Až teraz prichádza na rad technológia Azure Arc, spájajúca oba svety a umožňujúca spravovať všetky prostredia jednotne – od serverov cez aplikácie až po kontajnery.

Príležitosti a strategické výhody

Hybridný model prináša modernizáciu bez zbytočných rizík. Organizácie naďalej zostávajú vo svojej lokálnej infraštruktúre, nie sú nútené migrovať a pritom majú k dispozícii cloudové benefity. Začať môžu tam, kde vidia najväčší a najrýchlejší prínos. Tento prístup umožňuje využívať AI aj v prostrediach, kde cloud nie je plne dostupný, a zároveň optimalizovať náklady vďaka jednotnej platforme a automatizácii.

Z pohľadu vedenia spoločností ide o strategické rozhodnutie, ktoré priamo ovplyvňuje konkurencieschopnosť. Organizácie, ktoré dokážu rýchlo reagovať na zmeny a zároveň chrániť svoje dáta získavajú výrazný náskok. Azure Local a Azure Arc zrýchľujú inovácie, znižujú náklady a prinášajú jednotné bezpečnostné mechanizmy naprieč prostrediami.

Potenciál Azure Arc

Z predchádzajúcich riadkov jasne a jednoznačne vyplýva, že implementovanie Azure Arc do vlastnej lokálnej infraštruktúry predstavuje pre organizácie reálnu príležitosť znížiť náklady, zvýšiť flexibilitu a posilniť kybernetickú bezpečnosť.

Práve v podpore a riadení kybernetickej bezpečnosti sa skrýva ďalší významný potenciál Azure Arc. Agent Azure Arc dokáže zabezpečiť automatické monitorovanie rizík a nasadzovanie bezpečnostných politík v celom IT ekosystéme, zbierať logy, metriky a upozornenia z rôznych prostredí.

Licencovanie pomocou Azure Arc je ďalšou nezanedbateľnou vlastnosťou. Flexibilný „pay-as-you-go“ spôsob licencovania SQL Serverov a Windows Serverov 2025 s platbou podľa použitia je alternatívou ku konvenčnému trvalému licencovaniu.

Pravidlá licencovania sú jednoduché a transparentné: 1 jadro = 1 licencia s platbou na dni alebo hodiny. Počet licencii je možné kedykoľvek upravovať podľa reálnej potreby. K licenciám z Azure Arc je k dispozícii neobmedzený počet User CAL.

Ak chcete mať svoje servery pod kontrolou, dosiahnuť predvídateľné náklady, zjednodušiť plánovanie a vytvoriť pevný základ pre modernizáciu infraštruktúry, Azure Arc je riešenie, ktoré sa oplatí zvážiť. Získate hybridné cloudové prostredie s jednotnou správou aj bezpečnostným monitoringom celej infraštruktúry. Obráťte sa na Microsoft partnera, spoločnosť GAMO a jej špecialistov. Pripravia analýzu, prepočty a ukážu vám konkrétnu hodnotu, ktorú môže Azure Arc priniesť práve vašej organizácii.

Článok čítajte na platformofinvention.sk

klikni alebo oskenuj QR



Jakub Müller
CEMA Partner Solution Sales Manager for Azure Microsoft



Mladí slovenskí hekeri dobýjajú Európu

Kyberbezpečnosť dnes nie je len o kóde a technológiách. Je to svet, kde rozhoduje zvedavosť, rýchle myslenie, vytrvalosť a tímová súhra. Presne taký je Slovak Cyber Team.

Komunita mladých talentov ukazuje, že Slovensko má v kybernetickom priestore silný hlas. Sú odvážni, pripravení na výzvy a motivovaní byť súčasťou riešení, ktoré chránia modernú spoločnosť.

Ako vzniká národný SCT kybertím? Začiatok cesty vôbec nie je jednoduchý. Z účastníkov národnej súťaže CyberGame sa vyberie dvadsiatka najlepších. Tí následne niekoľko mesiacov prechádzajú intenzívnym tréningom – od víkendových bootcampov v kaštieli v Brunovciach až po medzinárodný tréningový kemp vo Viedni.

Tím tvoria mladí ľudia od 16 do 23 rokov vedení manažérmi Alexandrou Húskovou a Tomášom Hettychom z Kompetenčného a certifikačného centra kybernetickej bezpečnosti. Technickú prípravu tímu vedie Adam Gajdošík (NBÚ). V roli kapitána tímu je 23-ročný Marek Geleta. V roku 2025 dosiahli viaceré úspechy, ten najväčší prišiel v októbri na European CyberSecurity Challenge vo Varšave, kde slovenská finálová desiatka získala fantastické 4. miesto spomedzi 39 národných tímov.

Okrem technických vedomostí sa učia pracovať pod tlakom, myslieť ako útočník aj obranca, riešiť problémy kreatívne, a, čo je nemenej dôležité, koordinovať sa. Pri riešení úloh z oblastí ako forenzná analýza, kryptografia, binárna exploitácia či reverzné inžinierstvo získavajú praktické IT zručnosti, ktoré sú inde dostupné len ťažko.

Ide o budovanie komunity, ktorá zdieľa skúsenosti a vytvára priateľstvá. Slovak Cyber Team rozvíja ich kľúčové soft skills, potrebné pre kariérny rast a uplatnenie sa pri ochrane spoločností a podnikania v budúcnosti.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR



Iveta Hlaváčová
iveta.hlavacova@gamo.sk

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autorov(-iek) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK

ECCC

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

platform of invention

Informačné technológie
pre podnikanie s nápadom

Redakcia



Zuzana Holý Omelková
Obchod, Kybernetická bezpečnosť
zuzana.omelkova@gamo.sk



Branislav Lupták
Obchod
branislav.luptak@gamo.sk



Zuzana Peciarová
Kvalita a procesy
zuzana.peciarova@gamo.sk



Diana Filadelfi
Obchod
diana.filadelfi@gamo.sk



Jana Kohárová
Obchod
jana.koharova@gamo.sk



Martin Ondrušek
Kybernetická bezpečnosť,
Biznis kontinuita
martin.ondrusek@gamo.sk



Iveta Hlaváčová
Marketing
iveta.hlavacova@gamo.sk

Spracovanie textov a štylistická úprava
TIME.is COMMUNICATION
www.time-is.eu

Grafická úprava a sadzba
Morse s. r. o.
www.morse.click

Vydavateľ
GAMO a. s.
www.gamo.sk

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

Preberanie textov, ilustrácií a ich častí, rozširovanie prostredníctvom tlače a elektronických médií je možné len so súhlasom redakcie.

Ozvite sa skôr ako

Phishing

Len jeden klik,

... a bolo po všetkom!

Vybielený účet

Zneužitá kreditka

Infikovaný systém

GAMO
INFORMAČNÉ TECHNOLÓGIE

Spoznajte odpoveď na neproduktívnu administratívnu záťaž

Chcem zistiť viac



GAMO
INFORMAČNÉ TECHNOLÓGIE