platform of invention

Informačné technológie pre podnikanie s nápadom

online | pdf | print

Užitočné v správnych hlavách

magazín pre CTO, CFO, CEO

číslo 9
ročník piaty | 1/2025



Ako nastaviť implementačný plán bezpečnostných opatrení podľa ZoKB

Prečo je priemyselná bezpečnosť iná liga?

Magazín o informačných technológiách



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

Čítajte 9. číslo

Venované opatreniam podľa ZoKB a téme OT bezpečnosti.



PDF magazín

Online portál









#8 #7 #6 #5

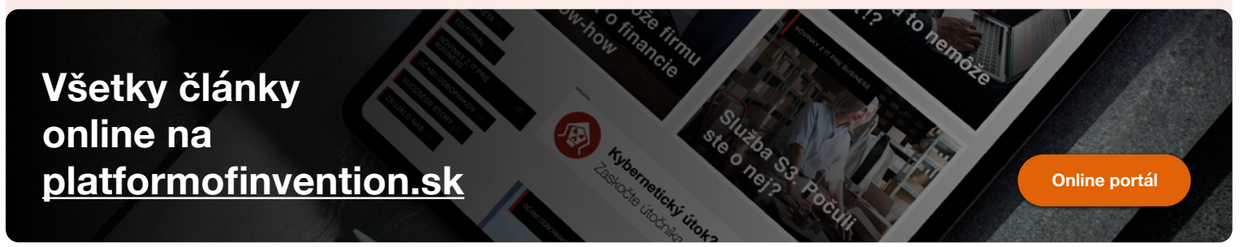








#4 #3 #2 #1



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



Bezpečnosť nemá univerzálny kód

Kybernetická bezpečnosť je súčasťou mojej každodennej práce – či už ide o diskusie na fórach, školenia u zákazníkov, alebo konzultácie vo firmách. Mnohé z nich prichádzajú samy, iné preto, že im to nariaďuje legislatíva cez novelizovaný zákon o kybernetickej bezpečnosti. Nech je dôvod akýkoľvek, dôležité je, že sa o bezpečnosť začínajú proaktívne zaujímať.

Zahraničné matky slovenských firiem často neriešia kybernetickú odolnosť svojich dcér, a už vôbec nevnímajú potrebu v zmysle legislatívy. Buď ju nepovažujú za prioritu alebo sa spoliehajú na centralizovaný model zabezpečenia. Ani jeden prístup dnes neobstojí. Moderné IT prostredie je rozptýlené, závislé od cloudu, IoT a práce na diaľku. Centrálne riešenia v ňom strácajú efektivitu, a najmä predstavujú riziko. Ak sa útočník dostane do jedného centrálneho bodu môže získať kontrolu nad celým systémom.

Segmentácia siete preto nie je len technické odporúčanie, ale je základným princípom odolnosti. Útokom sa nedá vždy zabrániť, ale útočníka môžeme spomaliť, obmedziť jeho pohyb a získať čas na reakciu.

Práve tu mi často pomáha jednoduchá analógia. Predstavte si, že by mala firma len jeden spoločný prístupový kód pre všetky miestnosti. To znie absurdne, však? V realite má každý prístup len tam, kde ho potrebuje. Ak niekto kód ukradne či prelomí, dostane sa len do jednej kancelárie alebo zasadačky. Každá ďalšia miestnosť je pre neho novou výzvou.

A presne to je podstatou segmentácie – vytvárať vrstvy ochrany, ktoré útočníka spomalia a prinútia zanechať stopy. Čím viac prekážok, tým väčšia šanca, že ho zachytia bezpečnostní operátori, alarm alebo strážny pes.

Firmy majú pripravené plány pre požiare či povodne a nacvičujú, ako reagovať v krízových situáciách. Rovnaký prístup by mal byť štandardom aj v kybernetickej bezpečnosti. Pretože odolnosť nevzniká z papierových podkladov, ale z pripravenosti konať.



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



Vďaka novej technológii ransomvér nezašifruje dáta ani keď sa dostane do systému

Niekedy sa stane, že útočníkom sa do firemnej siete podarí nasadiť ransomvér aj napriek silnému zabezpečeniu. Ani v takom prípade však citlivé údaje nemusia skončiť v rukách hackerov. Nová funkcia **Ransomware Remediation** (oprava po útoku ransomvérom) chráni vybrané dáta aj vtedy, keď sa spoločnosť stane obeťou útoku. Firmy tak dokážu výrazne znížiť riziko dlhodobého výpadku prevádzky.
Nástroj vytvára dočasné, zašifrované zálohy dôležitých údajov v izolovanom prostredí, ktoré je neprístupné pre nedôveryhodné aplikácie a procesy. Ransomware Remediation pritom využíva samostatne chránenú časť disku, v ktorej útočník nedokáže súbory upraviť, poškodiť ani vymazať.
Tým rieši jednu z najčastejších slabín tradičných záloh – ich zraniteľnosť počas aktívneho útoku.
Táto novinka inovatívnej ochrany je súčasťou riešení **ESET PROTECT,** ktoré poskytujú komplexné zabezpečenie firemných IT infraštruktúr.
Ako technológia Ransomware Remediation funguje v praxi sa dozviete na platformofinvention.sk.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Peter Blažečka
PR Manager Slovakia
ESET, spol. s r.o.

Ako kvantové technológie prepisujú pravidlá kybernetickej bezpečnosti

V predošlom článku, zameranom na kvantové technológie, sme rozobrali ako kvantové výpočty podlamujú súčasné šifrovacie metódy ochraňujúce kritické dáta podnikov, bánk či štátnej správy. Teraz zhodnotíme ako sa pripraviť na ich masové nasadenie, aké štandardy sa vyvíjajú, a čo hrozí organizáciám, ktoré túto transformáciu zanedbajú.
Kvantová výpočtová technika totiž zásadne mení pravidlá kybernetickej bezpečnosti. Odborníci z amerického Národného inštitútu pre štandardy a technológie (NIST) a britského Národného centra pre kybernetickú bezpečnosť (NCSC UK) varujú, že súčasná kryptografia neodolá útokom kvantových počítačov, a to skôr, než mnohí očakávajú.
Aké kroky odborníci odporúčajú a ako efektívne migrovať na post-kvantové šifrovanie, zistíte v plnom znení článku.



Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Diana Filadelfi
Produktový manažér
GAMO a.s.



AI gramotnosť podľa článku 4 AI Act: Praktický sprievodca pre compliance

Od vodičáku k algoritmom – a späť.

Vo februári 2025 vstúpila do platnosti ďalšia z významných povinností vyplývajúcich z nariadenia Európskeho parlamentu a Rady EÚ 2024/1689, ktorou sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie, známe pod názvom AI Act.

Zatiaľ čo väčšina pozornosti sa doteraz sústreďovala na zakázané systémy (čl. 5) a vysokorizikové AI (čl. 6 a nasl.), do praxe prichádza aj menej diskutovaný, no v compliance zásadný článok 4 o povinnosti zabezpečiť primeranú úroveň AI gramotnosti (AI literacy).

Stanovuje, aby všetci, ktorí sa podieľajú na navrhovaní, vývoji, implementácii alebo používaní AI systémov mali primeranú úroveň vedomostí a zručností v oblasti AI – a to v rozsahu primeranom ich úlohe a kontextu nasadenia systému.

Dlho však absentovali akékoľvek vysvetlenia, ako túto požiadavku napĺňať.

Ako si vybudovať program AI gramotnosti vo firme, čo sa stane, ak to necháte plávať, a tri kroky, ktoré môžete urobiť hneď zajtra, to všetko sa dozviete v celom článku na platformofinvention.sk.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



JUDr. Tomáš Klinka, JUDr. Štefan Pilár, JUDr. Peter Komínek, Mgr. Damián Palašta
SIGNUM legal s. r. o.
Advokátska kancelária



Reformný balík Omnibus prinesie zásadnú revíziu ESG reportingu: 80 percent firiem zrejme vypadne z povinnosti

Nedávno sa firmy začali vysporiadavať so zavedením povinného ESG reportingu do svojich vnútorných štruktúr, medzitým je už však na stole Európskej komisie nový reformný balík s názvom Omnibus, ktorý zásadne zmení pravidlá povinného nefinančného vykazovania v rámci EÚ.

Európska komisia predstavila vo februári návrh rozsiahleho balíka reformných opatrení s názvom Omnibus, ktorý zásadne zmení aj podmienky nefinančného ESG reportingu firiem. Návrh počíta s tým, že približne 80 % podnikov bude vyňatých z povinnosti vykazovať udržateľnosť podľa smernice CSRD. Zároveň navrhuje dvojročný odklad uplatňovania reportovacích povinností.

Reforma ešte nie je schválená, čaká ju legislatívny proces v Európskom parlamente a Rade EÚ. Tie môžu ovplyvniť jej finálnu podobu. Ide však o najzásadnejšiu zmenu ESG rámca od jeho zavedenia. Očakáva sa, že podnikateľské prostredie aj odborná verejnosť budú túto tému pozorne sledovať.

Aké konkrétne opatrenia Európska komisia navrhuje a ktorých firiem sa dotknú, sa ďalej dočítate na platformofinvention.sk.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Zuzana Peciarová
Manažér kvality a procesov
GAMO a.s.

AI ako nástroj kybernetických hrozieb: nová éra útokov

V posledných mesiacoch výrazne pribúda incidentov, pri ktorých útočníci využívajú AI na vykonávanie vysoko sofistikovaných kybernetických útokov. Až 78 % CISO dnes priznáva, že kybernetické hrozby poháňané umelou inteligenciou majú na ich organizáciu zásadný dopad.

Umelá inteligencia sa za posledných pár rokov stala neoddeliteľnou súčasťou digitálneho sveta. Podniky a organizácie s jej pomocou dokážu automatizovať procesy, zvyšovať efektivitu či analyzovať veľké objemy dát. Na druhej strane však zneužívanie AI začína značne ohrozovať kybernetickú bezpečnosť. Podľa prieskumu spoločnosti Darktrace označili odborníci za najväčšiu prekážku pri obrane proti AI útokom nedostatok kvalifikovaných expertov.

Kybernetickí útočníci rýchlo zistili, ako rôznymi spôsobmi z AI spraviť svojho spojenca. Jedným z najbežnejších je generovanie phishingových kampaní.

O aktuálnych kyber hrozbách a možnostiach obrany čítajte v rozšírenej verzii na www.platformofinvention.sk.



Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR



Diana Filadelfi
Produktový manažér
GAMO a.s.



Ako nastaviť implementačný plán bezpečnostných opatrení podľa ZoKB

Ak sa chcú organizácie vyhnúť chybám, je nevyhnutné pristupovať k implementácii novely ZoKB systematicky a zodpovedne, s dôrazom na pravidelné hodnotenie bezpečnostných opatrení, školenie zamestnancov, a spoluprácu s odborníkmi v oblasti kybernetickej bezpečnosti. Čo je osvedčeným postupom?

Pre účinné zorientovanie sa v zložitých otázkach dodržiavania požiadaviek ZoKB a transponovanej smernice NIS 2 je dôležité vyčlenenie primeraných zdrojov, zapojenie vedenia, spolupráca s externými odborníkmi s cieľom zvýšiť ich kybernetickú odolnosť.

Novela Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, účinná od 1. januára 2025, zavádza zmeny vyplývajúce z transpozície smernice NIS 2. Zásadnou zmenou je prechod od regulácie služieb k regulácii celých subjektov alebo sektorov s cieľom zvýšiť ich kybernetickú odolnosť. Novela zároveň ruší a nahrádza viaceré vykonávacie predpisy, vrátane vyhlášok 164/2018 Z.z. a 165/2018 Z.z. Do nadobudnutia účinnosti novej vyhlášky o bezpečnostných opatreniach (predbežne 1. 7. 2025) ostáva v platnosti vyhláška 362/2018 Z.z.

V súlade s NIS 2 sa kybernetická bezpečnosť už nevzťahuje len na konkrétnu službu, ale na celý subjekt alebo sektor. Zákon sa tak orientuje na ochranu hlavných činností subjektu. Subjekty podliehajúce regulácii sú po novom definované podľa príloh 1 a 2 zákona, na základe NACE kódov, pričom príloha 1 sa vzťahuje na sektory s vysokou úrovňou kritickosti (Essential), príloha 2 na iné kritické sektory (Important). Hlavným kritériom pre zaradenie medzi regulované subjekty je veľkosť organizácie – viac ako 50 zamestnancov a obrat nad 10 miliónov eur. Niektoré subjekty však môžu byť regulované aj bez splnenia tejto podmienky.

Proces auditu je nastavený tak, aby štatutár bol priamo zapojený: musí podpísať auditnú správu a vyjadrenie k nej vrátane plánu implementácie opatrení, a hoci dokumenty môže dať vypracovať niekomu inému ich verifikácia je na ňom.

Novela zavádza povinnosť implementácie rozšírených bezpečnostných opatrení vrátane monitorovania sietí, správy zraniteľností, a včasného hlásenia incidentov a hrozieb. Netreba zabúdať aj na trestnoprávnu zodpovednosť štatutára, ktorý je povinný oboznamovať sa o stave kybernetickej bezpečnosti.

Odoslaním finálnej správy na NBÚ, ktorá obsahuje jeho podpis, potvrdzuje svoju oboznámenosť a súhlas. Zodpovednosť nesie aj za výber kompetentného manažéra kybernetickej bezpečnosti, hoci praktickú zodpovednosť za riadenie incidentov a komunikáciu s NBÚ nesie manažér, trestnoprávna zodpovednosť ostáva na štatutárovi.

Identifikovali sme sa, a čo teraz?

Ak ste už zistili, že patríte medzi subjekty, na ktoré sa zákon vzťahuje – teda ste poskytovateľ Essential alebo Important služieb, prípadne patríte do inej zákonom zadefinovanej kategórie, potom vás čaká séria krokov, ktoré si vyžadujú odborný, ale zároveň pragmatický prístup.

Na úvod je dôležité pochopiť, že celý proces nezačína auditom. Audit je až jedným z neskorších krokov. Prvým reálnym krokom, ktorý by mala firma spraviť, je vstupná analýza. Odborne sa nazýva GAP analýza, teda rozdielová analýza. Jej cieľom je zistiť, kde sa vaša organizácia v oblasti kybernetickej bezpečnosti nachádza dnes a čo všetko jej chýba k tomu, aby spĺňala požiadavky zákona.

GAP analýzu si môžete vykonať aj sami, ak máte ľudí, ktorí dokážu čítať a interpretovať zákon a príslušné metodiky. V princípe je veľmi podobná auditu – kladú sa pri nej tie isté otázky, sledujú sa rovnaké oblasti. Hodnotí sa napríklad to, či máte zavedené technické opatrenia ako bezpečnostný monitoring, hardening systémov, alebo systémy na správu privilegovaných účtov. Posudzuje sa aj existencia bezpečnostných politík, smerníc a organizačných opatrení.

Výsledkom tejto analýzy je obraz o tom, kde sa nachádzate – napríklad zistíte, že máte pokrytých 40 % požiadaviek zákona, no v niektorých oblastiach ste úplne na začiatku. A tu prichádza na rad ďalší kľúčový krok: plánovanie.

Plánovanie bezpečnostných opatrení

Na základe zistených nedostatkov je potrebné vypracovať návrh implementácie bezpečnostných opatrení – časový plán, ktorý berie do úvahy vaše reálne možnosti, zdroje aj priority. Nie všetky opatrenia si vyžadujú vysoké náklady. Niektoré sú čisto organizačné a procesné, iné si vyžadujú investície do technológií alebo externých služieb. Preto je dôležité, aby ste stanovili, čo chcete a môžete urobiť v horizonte jedného, dvoch či troch rokov. Dôležité pritom je, že zákon ani audítor od vás nežiadajú okamžité splnenie všetkého, nejde teda o to, aby ste boli na 100 percent v súlade hneď od začiatku. Oveľa dôležitejšie je, že máte plán, že pracujete na zlepšení a že viete preukázať pokrok.

Súčasťou tohto plánovania je aj vypracovanie stratégie kybernetickej bezpečnosti. Ide o dokument, ktorý nie je len formalitou. Naopak, stratégia by mala byť



schválená vedením organizácie a mala by jasne určovať aké sú vaše ciele v oblasti bezpečnosti, ako ich plánujete dosiahnuť, a ako budete ich plnenie vyhodnocovať. Pre audítora alebo kontrolný orgán, napríklad NBÚ, je existencia stratégie jasným signálom, že organizácia pristupuje k bezpečnosti systémovo a s vedomím vedenia.

Aby však boli zvolené opatrenia naozaj primerané nestačí plánovať ‚od stola'. Firma musí vychádzať z analýz, ktoré odhalia čo skutočne potrebuje. Tu prichádzajú na rad dve kľúčové analýzy: analýza vplyvu na podnikanie (BIA – Business Impact Analysis) a analýza rizík. Ich cieľom je určiť, ktoré procesy sú pre firmu najdôležitejšie, aké výpadky si môže (alebo nemôže) dovoliť, aké hrozby a slabiny jej hrozia, a aký by bol ich dopad.

Ako by to fungovalo v praxi?

Predstavme si firmu, ktorá prevádzkuje cloudové služby. V rámci BIA si stanoví, že jej kľúčovým procesom je poskytovanie cloudu. Potom si položí otázku: Ako dlho si môžeme dovoliť, aby tento proces nefungoval? Týždeň? Deň? Odpoveď znie: Ani minútu. Na základe tej odpovede firma vie, že musí mať zavedený monitoring, ktorý výpadok okamžite identifikuje, musí mať technológie a ľudí pripravených obnoviť službu v krátkom čase, musí mať pripravené záložné systémy a krízové scenáre.

Z týchto požiadaviek potom logicky vyplývajú bezpečnostné opatrenia – od technických (napr. sieťová redundancia, zálohovanie), cez organizačné (pohotovostné tímy, interné procesy), až po investičné (licencie, služby SOC a pod.).

Výstupy z týchto analýz nie sú len podkladom pre rozhodovanie – sú aj dokumentmi, ktoré si pri kontrole vyžiada audítor alebo NBÚ. Tieto dokumenty dokazujú, že vaše opatrenia nie sú náhodné, ale založené na hodnotení rizík a reálnych potrieb vašej firmy.

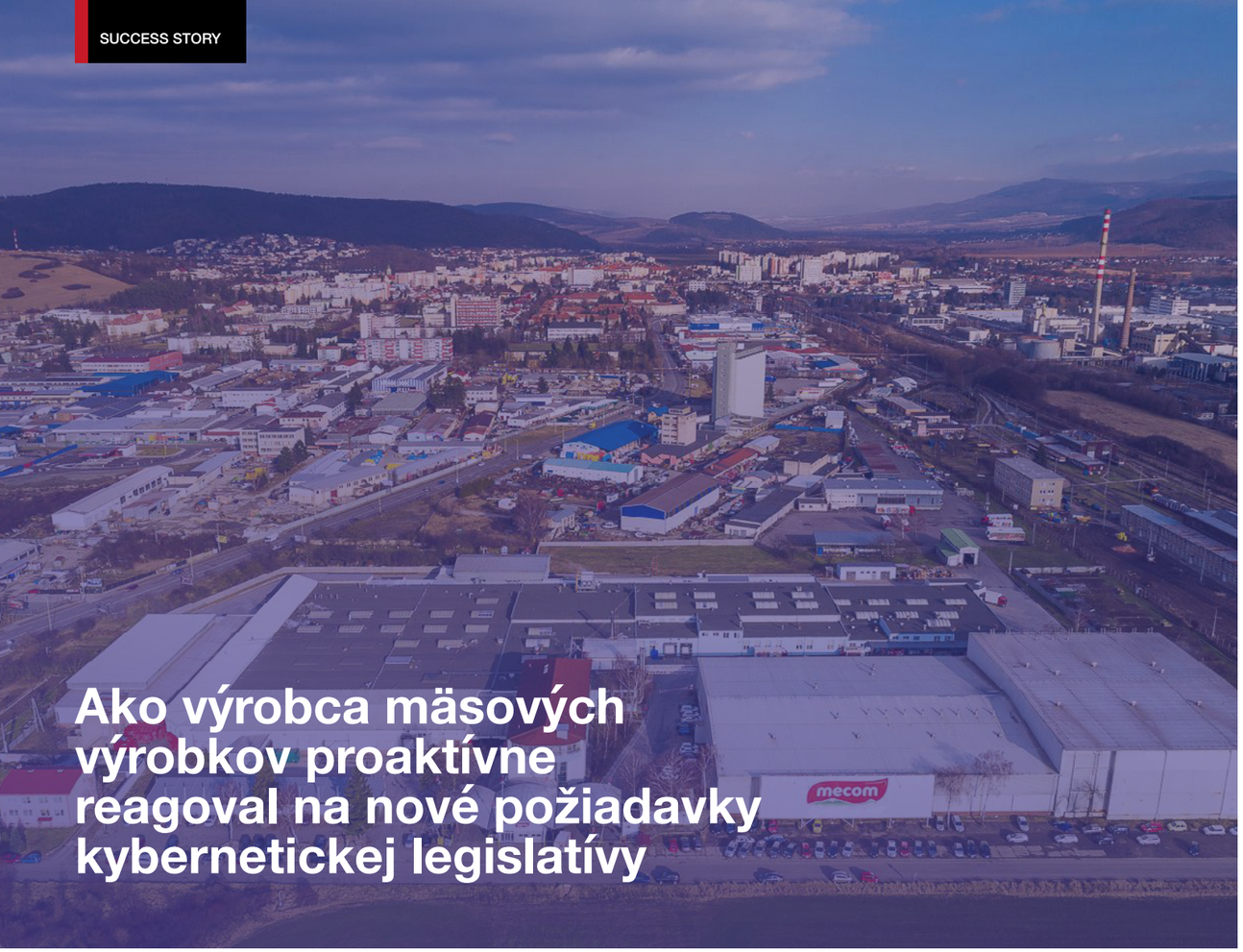
Celý tento proces sa napokon uzatvára auditom – buď interným alebo externým. Audit preverí ako máte nastavený systém kybernetickej bezpečnosti, do akej miery plníte plán a stratégiu, a čo ešte ostáva urobiť. Výsledky auditu slúžia ako spätná väzba a zároveň ako dôkaz, že firma pracuje na zvyšovaní svojej odolnosti.

„Zosúladenie so ZoKB nie je jednorazový projekt, ale dlhodobý proces. Nejde o to rýchlo ‚splniť povinnosť', ale o to, aby organizácia systematicky budovala bezpečnostnú kultúru, chrániacu jej najcennejšie aktíva: dáta, služby, infraštruktúru a dôveru klientov. S dobrým plánom, reálnymi cieľmi a odborným vedením sa aj zdanlivo zložitý zákon môže stať nástrojom pre posilnenie vašej firmy.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR


Zuzana Holý Omelková
zuzana.omelkova@gamo.sk

SUCCESS STORY



Ako výrobca mäsových výrobkov proaktívne reagoval na nové požiadavky kybernetickej legislatívy

Novelizácia zákona o kybernetickej bezpečnosti transponujúca smernicu NIS 2 priniesla nové povinnosti aj pre podniky venujúce sa spracovaniu a distribúcii potravín. Líder slovenského mäsospracujúceho priemyslu sa rozhodol reagovať včas a systematicky. V spolupráci so spoločnosťou GAMO a.s. prešiel komplexným procesom hodnotenia, analýzy a posilňovania svojej kybernetickej odolnosti.

Výsledkom systematického prístupu, ktorý MECOM GROUP spustil už v roku 2023 a rozvinul v priebehu roka 2024, bolo úspešné splnenie nových zákonných požiadaviek. Vo februári 2025 sa spoločnosť zaregistrovala ako prevádzkovateľ kritickej základnej služby v oblasti výroby a distribúcie potravín. Disponuje jasným prehľadom o úrovni svojej kybernetickej bezpečnosti, má zmapované riziká a ich dopady a vypracovaný plán konkrétnych opatrení s jasne stanovenými prioritami a zodpovednosťami.

Manažment spoločnosti si uvedomuje, že kybernetická bezpečnosť nie je jednorazový projekt, ale dlhodobý proces vyžadujúci si pravidelné prehodnocovanie a aktualizáciu. Vďaka tomuto prístupu získala spoločnosť nielen súlad s legislatívou, ale aj zvýšenú odolnosť voči incidentom a dôveru partnerov, pre ktorých je spoľahlivosť v dnešnom digitálnom prostredí kľúčová.

Nové zákonné povinnosti pre potravinársky sektor

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v novele z roku 2025 zaviedol sprísnené pravidlá pre viaceré sektory z oblasti priemyslu, distribúcie alebo poskytovania služieb vrátane kritickej infraštruktúry. Medzi ne patrí aj „výroba, spracovanie a distribúcia potravín“ – teda podniky zaoberajúce sa veľkoobchodnou distribúciou a priemyselnou výrobou a spracovaním potravín.

Spoločnosť MECOM GROUP s.r.o. sa tak stala subjektom, na ktorý sa vzťahujú povinnosti zákona a vzhľadom na svoje postavenie na trhu je určený ako poskytovateľ kritickej základnej služby. Spoločnosť sa rozhodla nečakať na 1.1.2025, odkedy mal začať platiť novelizovaný zákon o kybernetickej bezpečnosti, ale konať proaktívne a odborne.

Strategický prístup: zapojenie vedenia a odborná pomoc

Kybernetická bezpečnosť nie je len technická úloha pre IT oddelenie – je to strategická otázka s dopadom na chod firmy, dodávateľský reťazec aj reputáciu. MECOM GROUP s.r.o. preto od začiatku zapojil do procesu prípravy aj manažment a prizval si na spoluprácu odborníkov zo spoločnosti GAMO.

Prvým krokom bola GAP analýza – nezávislé zhodnotenie stavu a úrovne bezpečnostných opatrení vo firme s požiadavkami zákona a súvisiacich vyhlášok. Analýza ukázala, kde sú silné stránky, a zároveň identifikovala oblasti, ktoré si vyžiadajú doplnenie alebo úpravu. Výsledky GAP analýzy obsahovali detailné návrhy v oblasti bezpečnostných procesov, postupov, čiastočne aj návrhy nových technológií.

Inventarizácia IT aktív a ich kategorizácia

Na základe výsledkov GAP analýzy nasledovalo zmapovanie IT aktív využívaných v MECOM GROUP s.r.o., čiže inventúra toho, čo má byť predmetom kybernetickej ochrany. Nielen fyzické servery, počítače, sieťová infraštruktúra, ale aj softvér, dáta, ľudské zdroje a samotné priestory v MECOM GROUP. Zároveň boli určené priority – kritické aktíva z pohľadu hodnoty pre firmu, na základe bezpečnostných atribútov: dôvernosť, integrita, dostupnosť.

Do katalógu aktív boli zaznamenané aj nadväznosti medzi aktívami. Súbežne s touto činnosťou bola IT oddelením aj zaktualizovaná mapa topológie IT infraštruktúry, z ktorej katalóg aktív vychádza.

Analýza rizík: Praktické scenáre a konkrétne opatrenia

Po identifikácii kľúčových aktív a procesov nasledovala analýza rizík, ktorá identifikovala tie najzávažnejšie riziká voči jednotlivým IT aktívam. Pre každý identifikovaný prvok – servery, aplikácie, dáta či procesy – sa určila pravdepodobnosť výskytu konkrétnej hrozby a jej potenciálny dopad. Zároveň sa pre každé riziko určil jeho vlastník, zodpovedajúci za jeho riadenie a ošetrenie. Výsledkom bol zoznam rizík, ktoré:

- Môžu byť iba monitorované,
- Je nevyhnutné ošetriť.

Analýza dopadu na podnikanie BIA: Čo je pre firmu najcennejšie

Katalóg aktív bol zároveň východiskom pre vykonanie BIA, analýzy dopadu na podnikanie (Business Impact Analysis). Cieľom bolo zistiť, ktoré procesy a služby sú pre firmu najkritickejšie a ktorý výpadok by znamenal významné ohrozenie plynulosti výroby a následnej distribúcie výrobkov.

MECOM GROUP identifikovala kľúčové procesy z pohľadu plánovania, obchodu, nákupu, výroby, expedície a ďalších oblastí, pričom stanovila:

- Kľúčové procesy a ich vlastníkov,
- IT aktíva nevyhnutné pre plnú funkčnosť procesu.

Následne vlastníci procesov spolu s IT managerom určili:

- Úroveň dopadu pri výpadku – v oblasti financií, interných procesov, reputačných následkov, porušení zmluvných alebo právnych povinností,
- Požiadavky na RTO (Recovery Time Objective) a RPO (Recovery Point Objective),
- Vitálne osoby, ktoré sú v prípade incidentu nevyhnutné pre obnovu prevádzky.

Týmto krokom si spoločnosť určila priority v tom aké procesy, respektíve ktoré IT aktíva, sú kritické a majú najvyššiu dôležitosť pre udržanie plynulosti výroby.

Analýza zraniteľností systémového a sieťového prostredia

Analytická činnosť bola podporená aj praktickým preskúmaním stavu IT a OT technológií, zameraných na detekciu sieťových kybernetických hrozieb neinvazívnym spôsobom. Na základe automatizovanej analýzy sieťovej prevádzky a tokov dát s využitím AI bolo cieľom vyhľadať kybernetické hrozby a bezpečnostné anomálie, čiže potenciálne nebezpečné udalosti.

Zo zistení, ktoré vyplynuli z detekcie sieťových kybernetických hrozieb, bol spracovaný zoznam kritických IT aktív spolu s návrhom na vyriešenie najzávažnejších detekcií. Pripravené boli konkrétne návrhy ako zvýšiť odolnosť voči kybernetickým rizikám – či už aplikovaním pravidiel pre hardening, nastavením sieťových prvkov, vynútenou aktualizáciou, vypnutím slabo zabezpečených protokolov, ak nie sú využívané, a ďalšími.

Zároveň bol získaný obraz o tom aké zraniteľnosti a s akou úrovňou závažnosti sú nedostatočne ošetrené.

Kybernetická bezpečnosť ako súčasť biznis stratégie

Tento prípad ukazuje, že aj výrobná firma mimo IT sektora môže (a musí) aktívne pracovať na zvyšovaní svojej odolnosti. Včasná reakcia, zapojenie vedenia a odborné spracovanie celého procesu zabezpečili, že spoločnosť sa pripravila nielen na nové povinnosti, ale aj na reálne hrozby.

Kybernetická bezpečnosť sa stáva konkurenčnou výhodou – nie len z hľadiska regulácie, ale najmä z pohľadu dôveryhodnosti pre zákazníkov, partnerov aj verejnosť.



Článok čítajte na platformofinvention.sk

klikni alebo oskenuj QR



Martina Kormaník
martina.kormanik@gamo.sk



Prečo je priemyselná bezpečnosť iná liga?

Kyberbezpečnosť v OT je atribútom kvality, hovorí expert Martin Fábry

S rozmachom digitalizácie, nástupom IIoT a prepájaním IT a OT systémov je kybernetická bezpečnosť priemyselných technológií doménou súčasnosti. Každodenne sú na stole nové zraniteľnosti vyžadujúce špecifické bezpečnostné opatrenia a vznikajúce riešenia. V rozhovore s Martinom Fábrym hovoríme o rizikách, prioritách a reálnych incidentoch v priemysle.

Kybernetická bezpečnosť Operational Technology (OT) sa zaoberá ochranou systémov prevádzkových technológií, ktoré sú často súčasťou kritickej infraštruktúry. Na rozdiel od IT systémov spravujúcich predovšetkým biznis procesy a dáta riadia OT tzv. mission-critical operácie, ktorých výpadok môže mať okamžité a vážne následky pre fungovanie spoločnosti, kritickej infraštruktúry a priemyslu.

Podľa experta na OT bezpečnosť Martina Fábryho, priemyselné riadiace systémy (ICS) kedysi fungovali ako uzavreté, analógové riešenia, ktoré boli prakticky ‚neheknuteľné'. Ich vývoj smerom k digitalizácii však priniesol zásadný zlom. Všetko, čo dnes obsahuje procesor a sieťové pripojenie sa môže stať potenciálnym cieľom útoku. Príchod IIoT a inteligentných senzorov navyše rozšíril plochu útoku natoľko, že ochrana ICS systémov sa stala výzvou.

Aké sú najčastejšie typy kybernetických útokov, ktorým priemyselné riadiace systémy v súčasnosti čelia?

Rozlišujeme tri hlavné vektory. Najčastejšie ide o ransomvérové útoky z IT do OT – najmä kvôli tomu, že mnohí prevádzkovatelia majú riadiace systémy pripojené na internet. Útočníci sa dostanú dovnútra cez zraniteľné komunikačné kanály alebo exponované porty. Riadiace systémy sú veľakrát neaktualizované a ‚viditeľné' z online priestoru, takže sú ľahko zraniteľné. Ďalšou častou hrozbou sú nezaškolení používatelia, ktorí do prevádzky prinesú vlastné USB kľúče a tie pripájajú do siete. Podobne rizikoví sú aj dodávatelia. Tí prichádzajú s vlastnými notebookmi kvôli údržbe či integrácii, no často ide o nezabezpečené zariadenia, ktoré môžu do systému zavliecť škodlivý kód.

Zabezpečenie ICS je výrazne zložitejšie než zabezpečenie bežného IT prostredia. Prečo je to tak?

Pretože ICS má úplne iné priority než IT.

V priemyselných systémoch je na prvom mieste dostupnosť, potom integrita, spoľahlivosť, až nakoniec dôvernosť. V IT je to presne naopak. V OT prostredí je kľúčové, aby systém bežal nepretržite a stabilne, pretože ak zlyhá, môže to mať vážne následky. Nielen ekonomické, ale aj na zdravie ľudí. Vo výrobe sa často pracuje s nebezpečnými chemikáliami, robotmi, v prostredí s vysokým rizikom výbuchu, ako napríklad v ropnej rafinérii. Nie je to ako spravovať kancelársku sieť, ide o bezpečnosť aj životy.

Pozrime sa na OT aj z opačnej strany. Aké sú základné piliere ochrany ICS systémov a na čom by mala bezpečnostná stratégia v OT prostredí stáť?

Základom sú vždy tri piliere: ľudia, procesy a technológie. Ak manažment nedisponuje informáciami o rizikách, žije v predstave, že všetko funguje. Veľakrát nemá vo výrobe nikoho, kto by mu hrozby reálne hlásil. Tým pádom sa ani neprijímajú potrebné opatrenia. Z druhej strany už ale prichádza tlak z legislatívy – novelizovaný zákon o kybernetickej bezpečnosti s transponovanou smernicou NIS2 núti štatutárov konať. Či sa im to páči alebo nie, aj malé a stredné podniky budú musieť riešiť kybernetickú bezpečnosť, pretože budú podliehať pravidelným auditom.

Existuje nejaký overený postup, ktorý odporúčate klientom pri budovaní bezpečnostnej stratégie?

V praxi odporúčame zamerať sa na päť kritických opatrení. Prvým je bezpečný prístup do IT a OT prostredia, teda kontrolované pripojenie a eliminácia priamych vstupov z internetu do riadiaceho systému. Druhým pilierom je bezpečná architektúra: segmentácia siete, firewall medzi IT a OT, nasadené IDS/IPS systémy. Tretím je monitoring – bez neho neviete, čo sa deje. OT svet si vyžaduje špecializované nástroje na detekciu hrozieb.

Štvrtým pilierom sú ľudia. Vo výrobe často chýbajú odborníci na bezpečnosť, a ak aj sú, firmy ich nechcú platiť. Kybernetická bezpečnosť sa ešte stále berie ako náklad, nie ako súčasť kvality. A piatym bodom je mať pripravený incident response plán a biznis kontinuity plán, teda vedomosť čo robiť keď dôjde k útoku a koho kontaktovať. Dobré je mať externého partnera, ktorý pomôže obnoviť prevádzku. Dnes už platí, že kybernetická bezpečnosť je jeden z atribútov kvality výroby, bez nej vám všetky stroje a ľudia nestačia.

Čo v prípade, ak som konateľ firmy a rozhodujem sa pre externého dodávateľa kybernetickej bezpečnosti. Podľa čoho rozlíšim, že ide o spoľahlivého partnera?

Určite je potrebné spraviť dôkladný background check. Pýtať si referencie, ideálne z OT projektov posledných piatich rokov. Overiť si, s akými technológiami pracuje, akých má vendorov, a, hlavne, či má certifikovaný personál. Malo by byť samozrejmosťou, že vie doložiť odborné certifikáty svojich ľudí. Na Slovensku sa často rozhoduje podľa ceny, no tu je dôležité pozerať sa na kvalitu, reputáciu a reálne skúsenosti.

Zažili ste situácie, keď zavedenie bezpečnostných opatrení pomohlo útok odvrátiť alebo aspoň výrazne zmierniť jeho dopady?

V skutočnosti to v praxi funguje presne opačne. Firmy začnú riešiť opatrenia na minimalizovanie dopadov incidentu, až keď k nemu dôjde. Väčšinou až potom, keď útočník žiada výkupné 100 000 eur v bitcoinoch, si štatutár uvedomí, že mohol radšej vložiť prostriedky do opatrení a ľudí.

Na druhej strane sú aj firmy, ktoré investujú do bezpečnosti preventívne a majú kybernetickú hygienu v OT pod kontrolou. Vďaka monitorovacím nástrojom dokážu napríklad identifikovať infikovaný notebook dodávateľa a izolovať ho skôr, než spôsobí problém. Incident sa síce začne, ale vďaka pripravenosti sa nešíri ďalej.

Cloud a AI prenikajú aj do sveta OT. Čo to znamená pre firmy a bezpečnosť?

V OT svete sa čoraz viac objavuje prepojenie výrobných systémov s cloudom – kvôli analytike, AI spracovaniu dát, prediktívnej údržbe a podobne. Je to trend, ktorý bude rásť. Podobne ako kedysi banky váhali s prechodom do cloudu, ktorý sa dnes stal štandardom, teraz to čaká aj priemysel a OT systémy, ktoré budú čoraz častejšie integrované s cloudovým prostredím.

Práve preto je mimoriadne dôležité, aby sa tieto zmeny odrazili aj v oblasti kybernetickej bezpečnosti. Prepojenia do cloudu musia byť realizované s maximálnym dôrazom na zabezpečenie, aby nedošlo k ohrozeniu citlivých výrobných systémov.

Špecialisti na OT bezpečnosť sú stále vzácnejší. Myslíte si, že by mohla do budúcnosti pri ich zaškoľovaní zohrať významnejšiu rolu umelá inteligencia?

Určite áno. V oblasti OT bezpečnosti však vidím väčší prínos AI najmä pri detekcii hrozieb – ako súčasť intrusion detection systémov. Nečakajme však, že AI nahradí odborníka, ktorý navrhuje zabezpečenie celej prevádzky. Singularita je v OT ešte ďaleko, minimálne najbližších 10 rokov.

Kde vidíte hlavné príčiny nedostatku manažérov kybernetickej bezpečnosti, je to o nízkom záujme mladých ľudí, poddimenzovanom vzdelávaní, alebo o slabých pracovných podmienkach a platoch?

Mnohí sú prepracovaní, finančne podhodnotení, často menia zamestnania a idú za lepšími ponukami. Na trhu ich je málo a mnohé firmy si ich ani nemôžu dovoliť. Čísla, ktoré sa uvádzajú, že Slovensku chýbajú tisíce manažérov kybernetickej bezpečnosti, sú však mimo reality. Na pracovných portáloch ich hľadá možno jedna, dve firmy. Reálne riešenie je outsourcing - jeden takýto manažér pre viacero firiem, inak sa to kapacitne nedá zvládnuť. A problémom je aj vzdelávanie. Na technické odbory sa hlási málo študentov, dve tretiny štúdium ani nedokončí. Ak štát nezačne systematicky podporovať technické vzdelanie a univerzity, tak zostaneme bez odborníkov.

Keď porovnáme so Slovenskom ČVUT alebo Masarykovu univerzitu v Brne, pozrieme sa, aké kapacity odtiaľ vychádzajú a koľko startupov v Čechách je, vidíme, že u nás budeme mať v budúcnosti problém. Zopakujem: Kým štát nebude investovať do vzdelávania a nepodchytí študentov na univerzitách, situácia bude alarmujúca.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR



Diana Filadelfi
diana.filadelfi@gamo.sk



Claroty ochraňuje kritickú infraštruktúru

Význam bezpečnosti informačných systémov rastie priamo úmerne s rýchlo sa zvyšujúcim počtom útokov na informačné systémy a neustále sa zvyšujúcim objemom škôd, ktoré tieto útoky spôsobujú.

Priemyselné riadiace a kontrolné systémy tvoria z pohľadu bezpečnosti rozsiahlu a najviac podceňovanú oblasť. V posledných rokoch je pritom jednoznačne pozorovateľný exponenciálny nárast počtu kybernetických útokov práve na prvky priemyselných riadiacich a kontrolných systémov. V prípade základných služieb a kritickej infraštruktúry predstavujú tieto typy útokov vážnu hrozbu s rizikom mimoriadne vysokých ekonomických škôd a dopadu na celú spoločnosť.

Je preto nevyhnutné prijímať vhodné bezpečnostné opatrenia, ktoré reflektujú aktuálne bezpečnostné hrozby a trendy v oblasti informačnej aj priemyselnej bezpečnosti s možnosťou priameho dopadu na konkrétnu spoločnosť alebo jej informačný systém. Efektívnosť a primeranosť prijatých opatrení priamo súvisí s analýzou rizík informačného systému.

Bezpečné, spoľahlivé a efektívne operácie

Riešenie Claroty je nakonfigurované tak, aby poskytovalo bezpečné a spoľahlivé operácie na zber logov a dát vo veľkých komplexných priemyselných sieťach. Je plne vyladené k podpore a porozumeniu komponentom OT infraštruktúry, ich technickým obmedzeniam, vrátane prevádzok s obmedzeným výpočtovým výkonom a komunikáciou cez spojenia s úzkou šírkou pásma.

Nasadením Intrusion Detection System do výrobnej prevádzky získava podnik okamžitý prehľad o neštandardnom správaní v OT sieti. Už v prvom mesiaci dokáže systém odhaliť niekoľko potenciálnych bezpečnostných incidentov a zraniteľností, ktoré by inak zostali nepovšimnuté.

Riešenie poskytuje hĺbkovú viditeľnosť a extrémne detekčné schopnosti v komplexných OT prostrediach. Cieľom je nepretržitá analýza sieťového prenosu a logov za účelom zisťovania anomálií počítačovej bezpečnosti, monitorovanie a zhromažďovanie údajov z ďalších zdrojov dát rozmiestnených naprieč celou priemyselnou sieťou, a to všetko v reálnom čase.

Implementácia riešenia do prostredia podniku

Implementácia riešenia pozostávala z troch samostatných fáz. V prvej etape sa vykoná detailné posúdenie kybernetickej bezpečnosti OT prostredia. Výsledkom auditu je identifikovať a priorizovať oblasti kybernetickej bezpečnosti podľa urgencie z pohľadu požiadaviek kybernetického zákona a prislúchajúcich vyhlášok ako i z pohľadu kybernetických rizík a hrozieb, ktoré by mohli ohroziť prevádzku informačných ako i výrobných procesov.

Druhá fáza spočíva v návrhu architektúry a riešenia bezpečnostného monitoringu pre OT prostredie, jeho implementácie a spustenia prevádzky pilotného riešenia na vybraných lokalitách. Po vyladení monitoringu a prevádzky je riešenie nasadené aj na ostatné nepokryté lokality, čím sa maximalizuje schopnosť zachytenia a detekcie ukrytej bezpečnostnej hrozby, ktorá by mohla podniku spôsobiť problémy v budúcnosti. V prípade výskytu kybernetickej bezpečnostnej hrozby je o tomto potenciálnom riziku bezpečnostný tím na strane podniku okamžite notifikovaný, vie presne určiť zasiahnuté zariadenia a, je pripravený čo najskôr vykonať nápravné opatrenia v celom prostredí.

Účel bezpečnostných opatrení

Claroty je navrhnutá tak, aby riešila špecifické výzvy a riziká pre OT siete, kombinujúc hlboké pochopenie domény ICS s útočným know-how kybernetickej bezpečnosti. Riešenie monitoruje sieť OT, pričom využíva jedinečnú kombináciu signatúr, účelových modelov správania OT a vlastných možností detekcie anomálií, aby okamžite odhalilo a poskytlo akcie na ľudské chyby, zlyhania siete, alebo škodlivé aktivity. Korelovaním informácií v celej sieti poskytuje riešenie organizáciám situačné povedomie, ktoré potrebujú, na identifikáciu hlavnej príčiny incidentov a zmien, aby bolo možné zmierniť kybernetické riziká.

Článok čítajte na platformofinvention.sk

klikni alebo oskenuj QR



Monika Vilimová
monika.vilimova@gamo.sk



Phishing bez rizika? Simulované útoky ako diagnostika odolnosti firmy

Kybernetická bezpečnosť je závislá od človeka. Hoci firmy čoraz viac investujú do technologických riešení, práve ľudský faktor zostáva jednou z najčastejších príčin úspešných kybernetických útokov.

Phishing, teda podvodný e-mail vydávajúci sa za dôveryhodnú komunikáciu, sa stále radí medzi najefektívnejšie nástroje útočníkov. Relatívne jednoducho im umožňuje získať prístupové údaje, citlivé informácie, alebo spustiť škodlivé procesy v sieti.

Phishingové kampane sú dnes mimoriadne presvedčivé. Už dávno v nich nejde o ‚dedičstvo po princovi'. Útočníci precízne napodobňujú vizuál aj jazyk reálnych firiem, čím výrazne zvyšujú šancu na úspech. Stačí jedno nepozorné kliknutie a dôsledky môžu byť fatálne.

Zisťovali sme pripravenosť firiem

Ešte pred spustením novej služby simulovaných phishingových kampaní sme uskutočnili prieskum medzi zákazníkmi. Zaujímalo nás akú majú s phishingom skúsenosť a aké formy ochrany by ocenili.

Postreh etického hackera:

„Zo skúsenosti viem, že s použitím voľne dostupných nástrojov a minimálnou investíciou času a financií je možné kompromitovať firmu cez jej zamestnancov. Všetky zabezpečenia ako WAF, IDS, IPS či MFA tomu nijako nezabránia. Nakoniec aj v tejto dobe plnej umelej inteligencie a technického pokroku všetko stojí a padá na človeku."

Výsledky potvrdili, že ide o mimoriadne aktuálnu tému: 74 % respondentov uviedlo, že sa s phishingom stretávajú veľmi často alebo občas. Ako najužitočnejšie služby označili:

- 36 % detekciu podozrivých e-mailov a odkazov
- 34 % simulované phishingové kampane
- 30 % pravidelné školenia zamestnancov

Simulácia bez následkov, výsledky s dopadom

Simulované phishingové kampane predstavujú bezpečný spôsob ako v praxi otestovať pripravenosť zamestnancov na útoky, a to bez akéhokoľvek rizika pre infraštruktúru spoločnosti.

Podľa štatistík otvorí podvodný e-mail pred absolvovaním školenia v priemere 30 až 40 percent užívateľov. Pravidelné simulované kampane a dodržiavanie odporúčaní však môžu v priebehu jedného roka zvýšiť schopnosť zamestnancov rozpoznať phishingové e-maily až o 80 percent.

Cieľom simulácií nie je ‚nachytať' zamestnancov, ale získať objektívny obraz o zraniteľnosti firmy a identifikovať tímy s vyšším rizikom zlyhania.

Služba prebieha v niekoľkých kľúčových krokoch:

- Pripravíme realistické phishingové e-maily, ktoré vychádzajú zo skutočných útokov. Dôraz kladieme na dizajn, jazyk a behaviorálne prvky.
- Odošleme ich vybraným skupinám používateľov testovanej organizácie alebo spoločnosti, aby sme získali reprezentatívne dáta.
- Sledujeme mieru otvorenia, kliknutia, a ďalšie reakcie.
- Výsledky následne vizualizujeme a vyhodnocujeme spolu s konkrétnymi návrhmi na zlepšenie povedomia aj bezpečnostných procesov testovanej strany.

Opakovaním kampaní v pravidelných intervaloch dosahujeme dlhodobý efekt. Zamestnanci si vytvárajú návyk kriticky vyhodnocovať každý prijatý e-mail. Navyše, porovnávanie výsledkov v čase umožňuje firmám sledovať reálne zlepšenie a efektivitu prijatých opatrení.

Viac ako technológia, ide o správanie

Aj keď firmy nasadzujú moderné technológie ako firewally, EDR riešenia, segmentáciu či zálohovanie, konečný výsledok stále závisí od každodenného správania sa používateľov. Phishingové kampane totiž neútočia na technické zraniteľnosti, ale využívajú psychologické triky. Práve preto sú často úspešné. Dokážu oklamať aj technologicky dobre chránené organizácie.

Výhodou simulovaných phishingových útokov je ich vysoká výpovedná hodnota pre manažment aj IT oddelenie. Firma nezískava len všeobecný obraz o riziku, ale konkrétne dáta: ktoré tímy sú najzraniteľnejšie, ako rýchlo používatelia nahlásili podozrivý e-mail, kde zlyháva interná komunikácia.

Pretože v kybernetickej bezpečnosti platí jedno nepísané pravidlo: Najlepší útok je ten, ktorý sa nikdy nestane.

Článok čítajte na platformofinvention.sk

klikni alebo oskenuj QR



Diana Filadelfi
diana.filadelfi@gamo.sk



Kyberbezpečnosť: Ako si vybrať správnu úroveň ochrany

Myslíte si, že antivírus stačí? Realita je zložitejšia. To, čo mnohí považujú za dostatočnú ochranu, je dnes často len základ. Skutočná kybernetická bezpečnosť sa začína tam, kde bežné nástroje prestávajú stačiť. V ére prepracovaných útokov a sofistikovaných hrozieb si ochrana vyžaduje viac než len technológiu – potrebuje stratégiu, odborné znalosti a neustále zlepšovanie.

Nezáleží na tom, či práve vyberáte antivírus pre koncové zariadenie alebo navrhujete architektúru robustnej bezpečnostnej infraštruktúry. Sme tu pre každého, kto to s ochranou dát myslí vážne. Naši experti pomáhajú meniť bezpečnosť na systematický a efektívny proces. Modelové príklady kybernetickej ochrany ukazujú, aký stupeň zabezpečenia môže firma dosiahnuť – od základných opatrení až po profesionálne systémy postavené na technológiách ako SIEM.

Level 1 - Základná úroveň ochrany

Najnižšia úroveň ochrany predstavuje minimálne opatrenia, ktoré sú pre každú firmu a zamestnanca nevyhnutné. Riešenia prvej úrovne si nevyžadujú aktívnu správu, no vyžadujú si profesionálnu IT implementáciu a nastavenie.

Modelový príklad 1: Malá účtovná spoločnosť

Zoberme si príklad malej účtovnej spoločnosti s 8 zamestnancami, ktorá sa zameriava na spracovanie účtovníctva a miezd pre živnostníkov a menšie firmy. Spoločnosť nevykonáva špeciálne IT operácie – jej hlavnými pracovnými nástrojmi sú cloudové účtovné systémy a e-mailová komunikácia. Firma nemá vlastné servery ani IT oddelenie, pričom technickú podporu zabezpečuje externý dodávateľ.

Bezpečnostné opatrenia tejto spoločnosti sú pomerne jednoduché, ale efektívne: Antivírus, Firewall, Zálohovanie, Aktualizácie, Školenie zamestnancov, Dvojfaktorová autentifikácia.

Level 2 – Pokročilá úroveň ochrany

Druhý level kybernetickej bezpečnosti stále zahŕňa už spomenuté základné bezpečnostné opatrenia, no zároveň umožňuje nasadiť pokročilejšie a komplexnejšie technické riešenia. Hlavným rozdielom je potreba aktívnej interakcie a správy bezpečnostných systémov. Bezpečnostné technológie tejto úrovne zahŕňajú vyššiu komplexnosť a nároky na odborné schopnosti, preto potrebujú nielen profesionálnu správu, ale aj neustály monitoring.

Tieto systémy si vyžadujú minimálne jedného bezpečnostného špecialistu na aktívne sledovanie a správu ochrany a technológií, ktoré môžu zahŕňať pokročilé nastavenia sieťovej infraštruktúry, pokročilú autentifikáciu alebo riadenie prístupu.

Modelový príklad 2: Pokročilé zabezpečenie siete

Spoločnosť, ktorá je súčasťou veľkého holdingu s firmami rôzneho zamerania, sa rozhodla pre čiastočný outsourcing IT služieb, pričom na zabezpečenie a správu sieťovej infraštruktúry vo všetkých piatich lokalitách na Slovensku si vybrala GAMO. Ostatné systémy, ako napríklad Microsoft 365, má na starosti iný dodávateľ.

Návrh bol zameraný na zvýšenie úrovne bezpečnosti siete a eliminovanie rizík. Na základe diagnostiky a komunikácie s klientom sme identifikovali niekoľko nedostatkov, vrátane pripojení neautorizovaných zariadení. Ako opatrenie sme navrhli implementovať 802.1X autentifikačný framework, ktorý obmedzuje pripojenie neautorizovaných zariadení do lokálnej siete.

Pre (ne)technikov: Tento bezpečnostný rámec funguje ako „recepčný“ so zoznamom schválených zariadení a používateľov, ktoré môžu „vstúpiť“. Každý prístup do siete je overený, čím sa zabráni pripojeniu neautorizovaných alebo nezabezpečených zariadení. Systém tiež umožňuje administrátorovi prístup do siete kontrolovať a riadiť, čím výrazne zvyšuje bezpečnosť firemných dát. Podobné bezpečnostné riešenie prináša firme niekoľko kľúčových benefitov:

- **Kontrola nad prístupom:** Len schválené zariadenia majú prístup k firemným dátam, čo znižuje riziko úniku dát.
- **Ochrana pred útokmi:** Zabraňuje pripojeniu neautorizovaných zariadení, čo znižuje pravdepodobnosť útokov.
- **Sledovanie prístupu:** Administrátor má prehľad o všetkých pripojených zariadeniach, čo zjednodušuje správu IT.

Tento pokročilý systém zabezpečenia, ktorý umožňuje aktívne monitorovanie bezpečnostných hrozieb, si už vyžaduje minimálne jedného IT špecialistu na denné sledovanie a správu. Riešenie je dostupné aj pre menšie firmy, ktoré nechcú alebo nemôžu investovať do plne integrovaného bezpečnostného operačného centra (SOC).

Modelový príklad 3: Systémový integrátor

Zákazník nás kontaktoval so zadaním vybudovať pracovné prostredie pre novovzniknutú špedičnú spoločnosť, ktorá bude postupne zamestnávať od 3 do 6 ľudí. Ich požiadavkou bolo zabezpečiť nielen internetové pripojenie, ale aj bezpečnostnú bránu firewall, switch, AP pre pripojenie zamestnancov a server pre aplikácie. Okrem toho požadovali prísne reštrikcie prístupu pre rôznych zamestnancov.

Návrh riešenia zahŕňal:

- Virtuálne servery v GAMO cloud pre aplikácie a dáta.
- Licencie Windows a Eset pre ochranu serverov.
- Firewall Fortigate F40, switch Aruba HP, Access Point wifi.
- M365 pre produkty ako Outlook, Word, Excel.
- Bezpečnostný monitoring ako doplnkovú službu.

Na implementáciu tohto riešenia sme pripravili podrobný návrh, ktorý zahŕňal migráciu, správu serverov a technické špecifikácie. Vďaka tomu môže firma získať pokročilé zabezpečenie a flexibilitu, ktorú potrebuje na efektívnu prevádzku a riadenie prístupov k citlivým dátam a aplikáciám.

Level 3+ – Profesionálna enterprise bezpečnosť

Technológie a služby tretieho a štvrtého levelu predstavujú špičkové bezpečnostné state of the art riešenia na úrovni najmodernejších technologických možností. Sú určené najmä pre organizácie, ktoré majú vysoké nároky na bezpečnostnú úroveň a disponujú buď interným tímom odborníkov, alebo využívajú služby špecializovaných partnerov.

So stúpajúcou úrovňou bezpečnosti rastie nielen komplexnosť technológií, ale aj požiadavky na špecializáciu personálu. Implementácia, konfigurácia a najmä každodenný monitoring nástrojov ako EDR, XDR, SIEM a ďalších, si vyžaduje dedikovaných bezpečnostných špecialistov.

Modelový príklad 4: SIEM a služby SOC operátorov

Dlhoročný zákazník z výrobného segmentu, ktorému GAMO spravuje kompletnú IT infraštruktúru – od systémov, cez sieť až po aplikácie hostované v GAMO Cloud, prešiel v roku 2024 na novú úroveň bezpečnosti. Po konsolidácii celej IT infraštruktúry po kybernetickom útoku a v rámci prípravy na legislatívne požiadavky smernice NIS 2 sme mu navrhli nasadenie komplexnej služby.

Kľúčovou súčasťou riešenia je nasadenie systému SIEM (Security Information and Event Management) a služieb SOC (Security Operation Center). Nami dodané riešenie, využívajúce open-source platformu Wazuh, môže byť alternatívou ku komerčným a robustným riešeniam (ako napr. IBM QRadar) a zároveň poskytovať vysokú funkcionalitu.

SIEM od GAMO umožňuje:

- Zhromažďovanie a normalizáciu bezpečnostných údajov z celej infraštruktúry;
- Koreláciu udalostí a rozpoznávanie podozrivých aktivít;
- Automatizované upozornenia na bezpečnostné hrozby;
- Úplnú viditeľnosť do všetkých častí systému;
- Efektívnejšie reakcie na incidenty a zjednodušenie dodržiavania noriem a regulácií.

SOC operátori GAMO monitorujú systém nepretržite, vyhodnocujú incidenty v reálnom čase a zabezpečujú:

- Zber a analýzu podozrivých udalostí z rôznych systémov;
- Identifikáciu pôvodu, miesta a dôvodu incidentu;
- Pravidelný reporting a návrhy nápravných opatrení;
- Kontrolu zavedenia odporúčaných zmien.

Výsledkom je centralizovaný, vysoko profesionálny bezpečnostný dohľad nad celou IT infraštruktúrou spoločnosti, ktorý spĺňa moderné požiadavky aj náročnejších regulačných rámcov.

Článok čítajte na platformofinvention.sk
Klikni alebo oskenuj QR


Jana Kohárová
jana.koharova@gamo.sk





Staňte sa partnerom GAMO. Rozšírte podnikanie o klientmi overený cloud zo Slovenska

Hľadáte nový impulz pre svoje IT podnikanie? Rastúci dopyt po digitálnych riešeniach so sebou prináša potrebu moderných, bezpečných a lokálnych cloudových služieb. Partnerský program spoločnosti GAMO otvára cestu k novým obchodným príležitostiam v IT segmente. Ponúka overené cloudové riešenia, ktoré využívajú popredné slovenské aj medzinárodné firmy.

Cieľom je technologický náskok, odborná podpora a výhodné podmienky spolupráce. Nástup cloudových technológií zásadne ovplyvnil očakávania firemných zákazníkov. Či už ide o rozvíjajúce sa IT štúdio alebo etablovaného poskytovateľa digitálnych služieb. Tí dnes požadujú škálovateľnosť, optimalizáciu nákladov, a, predovšetkým, maximálnu bezpečnosť firemných dát. Program spoločnosti GAMO umožňuje partnerom rozšíriť svoje portfólio o robustné cloudové riešenia, kybernetickú bezpečnosť a IT služby s certifikáciou špičkovej úrovne.

Výhody GAMO Cloud

Digitalizácia, cloud-hosting firemných systémov, zálohovanie dát aj zabezpečenie infraštruktúry – všetky tieto oblasti predstavujú príležitosť ako osloviť novú klientelu a posilniť svoju pozíciu na trhu. Služby GAMO dnes využívajú firmy ako Lenovo, ELBA, Oftal, Sashe.sk, Biometric či IDS BBSK, pričom ich dlhodobá dôvera potvrdzuje kvalitu poskytovaných riešení. Medzi hlavné dôvody, prečo si partnerské firmy volia GAMO Cloud, patria:

Technológie a bezpečnosť: Virtualizácia na platformách VMware a Proxmox, najmodernejšie dátové centrum DATACUBE spĺňajúce kritériá TIA-942 Tier III a bezpečnostné štandardy ISO 27001 či ISO 27018.
Ochrana dát je prvoradá: Klientske dáta sú zálohované minimálne raz denne (v prípade potreby aj v hodinových intervaloch) s možnosťou obnovy po výpadku alebo incidente.
Flexibilita a škálovateľnosť: Bez obmedzenia na počet používateľov či objem prenesených dát sa konfigurácia serverov vždy prispôsobuje aktuálnym potrebám klienta.
Podpora a školenia: Prístup ku školeným IT špecialistom, zákaznícke centrum dostupné 24/7 a odborné školenia v slovenskom aj anglickom jazyku.

Partnerské ceny a férové podmienky: Výhodnejšie cenové nastavenie pre partnerov, individuálne zaškolenie, aj zrozumiteľné zmluvné podmienky.

Ako partnerská spolupráca funguje?

GAMO ponúka partnerom dve formy spolupráce, ktoré zohľadňujú rôzne obchodné modely aj úroveň technického zázemia. V prípade, že má partner k dispozícii vlastné obchodné alebo technické oddelenie, môže služby GAMO nakupovať a ďalej poskytovať svojim zákazníkom vo vlastnom mene.

Tento model je ideálny pre firmy, ktoré chcú zachovať plnú kontrolu nad vzťahom so zákazníkom a vystupovať ako primárny dodávateľ.

Alternatívou je sprostredkovateľský model, pri ktorom partner odporučí konkrétnu službu klientovi, no samotná zmluva aj servisná starostlivosť už prebiehajú priamo medzi klientom a GAMO.

Partnerovi je následne vyplácaná provízia na základe vopred zmluvne dohodnutých podmienok.

Oba modely sú navrhnuté tak, aby partnerom priniesli flexibilitu, minimálnu administratívnu záťaž a nové zdroje príjmu, bez ohľadu na veľkosť alebo štruktúru ich organizácie.

Partnerstvo sa začína jednoduchým kontaktovaním nášho tímu. Po prejavení záujmu sa vám ozve kolega z obchodného oddelenia, ktorý vám podrobne predstaví možnosti spolupráce, vysvetlí detaily partnerského modelu, a pomôže s výberom vhodných služieb z portfólia – od cloudových riešení a kybernetickej bezpečnosti až po softvérové nástroje ako je napríklad informačný systém IS JAS.

Nasleduje zaškolenie a príprava na štart predaja. Všetky dôležité kroky – technické, obchodné aj procesné, vám priblížia naši odborníci. Získate prehľad o konfigurácii služieb, o spôsoboch fakturácie a možnostiach podpory, vrátane monitoringu a zákazníckeho centra.

Cieľom je zabezpečiť, aby ste mohli začať predávať bez zbytočných bariér a so všetkými potrebnými nástrojmi.

Po podpise partnerskej zmluvy si zvolíte formu predaja, ktorá najlepšie vyhovuje vášmu obchodnému modelu. V prípade priameho predaja si služby objednávate a spravujete vo vzťahu ku klientovi sami. Ak sa rozhodnete pre sprostredkovateľský model, stačí, ak privediete zákazníka – a o zvyšok, vrátane technickej realizácie a zákazníckej podpory, sa postará náš tím.

Voľba pre slovenské cloud riešenie

GAMO Cloud je postavený na najmodernejších technológiách a prevádzkovaný priamo na Slovensku, v jednom z najbezpečnejších dátových centier strednej Európy. Služby sú zároveň poskytované v plnom súlade so zákonom o kybernetickej bezpečnosti. Spĺňajú všetky požiadavky na ochranu osobných údajov podľa platných noriem vrátane certifikácií ISO 27001 a ISO 27018. Lokálny tím odborníkov je navyše partnerom neustále k dispozícii – zabezpečuje technickú asistenciu aj pre náročné projekty a poskytuje komplexnú podporu v slovenčine aj angličtine.

Výhodou domáceho cloudového riešenia je aj schopnosť rýchlo reagovať na technické, legislatívne či biznis požiadavky slovenského prostredia – či už ide o zmeny v zákonoch alebo o špecifické požiadavky domácich firiem.

A treba dodať, že bežné cloudové hosťovanie je len začiatkom. Svoju ponuku môžete ďalej rozšíriť napríklad o tieto služby:

Zálohovanie a obnovu dát v cloude
Automatické zálohovanie v denných alebo hodinových intervaloch, obnova dát po výpadku a možnosť individuálneho nastavenia podľa špecifík konkrétneho klienta.

Firemné cloudové úložiská a virtuálne privátne servery
Privátna inštalácia servera bez obmedzenia počtu používateľov, veľkosti dát či ich prenosnosti. Ideálne riešenie pre firemné prostredie so zvýšenými nárokmi na kontrolu a dostupnosť.

Monitoring a bezpečnostné služby
Nepretržité sledovanie infraštruktúry, rýchla reakcia na incidenty, a odborný bezpečnostný dohľad v súlade s najprísnejšími normami kybernetickej bezpečnosti.

Škálovateľnosť pre vývojárov a enterprise riešenia
Poskytovanie optimálnych podmienok pre vývoj, testovanie aj produkčnú prevádzku firemných aplikácií.

Zapojením sa do siete partnerov spoločnosti GAMO získate možnosť ponúkať moderné cloudové služby firmám, ktoré hľadajú istotu výkonu, bezpečnosti a kvality. Partnerský program je navrhnutý tak, aby prinášal obchodnú flexibilitu, technickú istotu, a možnosť rozšírenia služieb v súlade s aktuálnymi trendmi digitalizácie.

Nezáleží na tom, či sa špecializujete na predaj IT riešení, správu infraštruktúry, alebo pôsobíte ako systémový integrátor. Partnerský program GAMO vám umožní vytvárať nové obchodné príležitosti, diverzifikovať portfólio a poskytovať služby na úrovni svetových štandardov.

Viac informácií o možnostiach partnerstva vám radi poskytneme.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR



Adam Majoroš
adam.majoros@gamo.sk



Chcete digitálnu zdravotnícku platformu z domu? Hilbi

Ako to funguje? Zadáte zdravotné komplikácie a špičkoví lekári vo svete sa nimi budú zaoberať.

Medzinárodná zdravotnícka platforma Hilbi vznikla ako inovácia na Slovensku, dnes má dva expertné tímy a funguje v nemocniciach a klinikách v Európe aj Ázii. Aktuálne vstupuje na český trh a pripravuje pilotné projekty vo Veľkej Británii a New Yorku.

Hilbi digitalizuje kľúčové procesy medzi pacientom a lekárom, umožňuje správu zdravotných údajov, komunikáciu a poskytovanie služieb cez jednotné rozhranie, a vďaka vlastnej AI technológii, digitálnemu dvojčaťu lekára, sprístupňuje diagnózy, vysvetľuje výsledky, a podporuje pacienta 24/7.

Digitalizované zdravotné záznamy sú bezpečne uložené na jednom mieste, čo pacientovi umožňuje riadiť svoju liečbu efektívne, často aj bez osobnej návštevy ordinácie. Okrem prijímania lekárskych správ a zrozumiteľnej interpretácie výsledkov vyšetrení umožňuje aplikácia aj objednanie nadštandardných služieb či konzultácií kdekoľvek na svete.

Lekárom a zdravotnému personálu šetrí Hilbi čas a zefektívňuje prácu, pacientov sprevádza počas liečby alebo prevencie. Zároveň otvára prístup ku zdravotnej starostlivosti aj za hranicami.

A na čom je architektúra platformy Hilbi postavená? Na princípe patient-centric s bezproblémovou integráciou do existujúcich nemocničných EHR/CRM systémov.

Znižuje administratívnu záťaž a zvyšuje efektivitu a kapacitu ambulancií až o 20 percent, zvyšuje príjmy zdravotných zariadení až o 35 percent. Umožňuje tiež legálne mikroplatby za nadštandardné služby, čím prispieva k vyššej udržateľnosti systému. Je to služba aktuálnej budúcnosti.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR



Iveta Hlaváčová
iveta.hlavacova@gamo.sk

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.

PONÚKAME ŠTARTOVACIE SLUŽBY KYBERNETICKEJ BEZPEČNOSTI

Konzultácia so špecialistom

Podeľte sa s nami o vaše výzvy, problémy, prekážky a potreby v oblasti kybernetickej bezpečnosti. Zoznámte sa s naším portfóliom a spoznajte ako náš multidisciplinárny tím neustále pracuje na adresovaní dnešných aj budúcich výziev s cieľom zabezpečiť maximálnu mieru ochrany a bezpečnosti zákazníkov. Objavte naše riešenia a zistite ako vieme naplniť vaše výzvy a ochrániť vás pred nástrahami digitálneho sveta.

Popis služby
Cena služby
Predbežný záujem

Usmernenie po telefóne

Stále ste sa nerozhodli? Zdá sa vám problematika kybernetickej bezpečnosti náročná? Poradíme vám a nasmerujeme k optimálnemu postupu pre špecifickú situáciu vašej firmy. Dohodnite si s nami krátky bezplatný telefonát.

Popis služby
Cena služby
Predbežný záujem

Školenie zamestnancov

Znížte mieru ohrozenia jednoduchým školením zamestnancov pristupujúcich k informačnému systému. Práve ľudský faktor stojí za veľkou časťou prieniku kybernetických útokov do vašich systémov.

Popis služby
Cena služby
Predbežný záujem

GAMO
INFORMAČNÉ TECHNOLÓGIE

Spoznajte odpoveď na neproduktívnu administratívnu záťaž

Chcem zistiť viac



GAMO
INFORMAČNÉ TECHNOLÓGIE