platform of invention

Informačné technológie pre podnikanie s nápadom

online | pdf | print

Užitočné v správnych hlavách
magazín pre CTO, CFO, CEO

číslo 8
ročník štvrtý | 2/2024

Greenwashing pod tlakom nových regulácií v EÚ

Ako NIS 2 ovplyvní kybernetickú bezpečnosť

SIEM - má ešte zmysel?

Magazín o informačných technológiách

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

Čítajte 8. číslo

Venované dvom legislatívnym témam NIS 2 a ESG reporting.

PDF magazín

Online portál

Najnovšie číslo

Predchádzajúce

Predchádzajúce čísla vo formáte PDF

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 slovenský 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

Silná reťaz potrebuje pevné všetky články

V dnešnom digitálne prepojenom svete sme všetci súčasťou väčšieho celku. Rovnako ako sa každý článok dodávateľského reťazca podieľa na tvorbe hodnoty, podieľa sa aj na riziku. Túto skutočnosť som si uvedomila nespočetnekrát pri diskusiách s našimi klientmi z rôznych odvetví. Spoločným menovateľom týchto rozhovorov je vždy rovnaký problém – bezpečnostné hrozby, ktoré môžu ohroziť nielen jednotlivca, ale celý digitálny ekosystém.

Keď sa zamyslíme nad tým, aké dôsledky môže mať slabé miesto na jednom konci reťazca, uvedomíme si, aká krehká je táto komplexná sieť vzťahov. Skutočnosťou je, že mnohé malé a stredné podniky, tvoriace základnú infraštruktúru dodávateľských reťazcov, nemajú dostatočné prostriedky na zabezpečenie svojich systémov. Ich kybernetická odolnosť tak často zaostáva za potrebami. Ak veľká korporácia investuje do bezpečnosti, ale jej subdodávateľ nie, aké pevné sú potom reálne hranice jej ochrany?

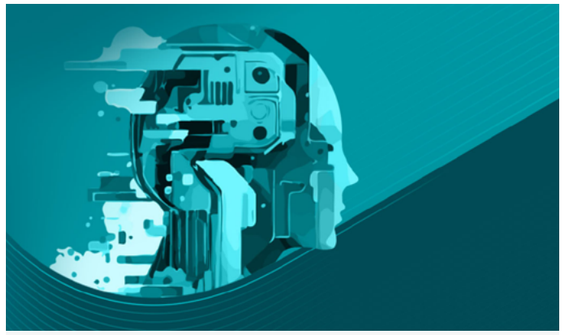
Riziká však nekončia len pri subdodávateľoch. IT spoločnosti spravujúce kľúčové systémy, logistickí poskytovatelia prepravujúci kritické komponenty, manažéri digitálnych platforiem – všetci sú potenciálnymi terčmi útokov. A čím viac sa svet digitalizuje, tým viac rastie význam týchto hrozieb.

Naša odpoveď na tento problém je jasná: zdieľaná zodpovednosť. Certifikácie, analýzy rizík, šifrovanie, segmentácia siete či plánovanie reakcií na incidenty nie sú už len odporúčaním, ale nutnou požiadavkou pre každého z partnerských strán.

V tejto súvislosti vítame transpozíciu smernice NIS 2, ktorá zdôrazňuje bezpečnostné povinnosti dodávateľov. Táto legislatíva nám, vám dáva právo vyžadovať, aby subdodávatelia dodržiavali rovnaké bezpečnostné štandardy. Ide o krok správnym smerom, pretože len tak dokážeme vytvoriť odolnú, no flexibilnú sieť, ktorá zvládne akékoľvek búrky digitálneho veku.

Každý, bez ohľadu na veľkosť firmy, nesie kúsok tejto zodpovednosti. Súčasný svet už nepotrebuje len silných jednotlivcov, potrebuje pevné reťazce. A tie začínajú pri každom z nás.

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



Umelá inteligencia v službách bezpečnostných správcov

Firmy čelia aktuálne mnohým kybernetickým hrozbám, ktoré ich môžu zasiahnuť z rôznych strán. Nie sú v tom však sami.
Správcovia IT bezpečnosti majú neľahkú úlohu reagovať na detekcie pochádzajúce z počítačov, mobilných zariadení či cloudu. Zvládať tieto výzvy im teraz umožní umelá inteligencia. **ESET AI Advisor** pomôže v reálnom čase operátorom identifikovať, analyzovať a zmierniť hrozby prostredníctvom interaktívneho dialógu. Plnenie bezpečnostných úloh sa tým zredukuje na niekoľko kliknutí. Chatbot umožňuje bezpečnostným analytikom s rôznymi úrovňami zručností rýchlo reagovať na kritické situácie a minimalizuje následky narušenia bezpečnosti, čo vedie k efektívnejšej správe incidentov. Nástroj ESET AI Advisor je aktuálne v ponuke ako súčasť XDR modulu ESET Inspect v rámci úrovne ochrany ESET PROTECT MDR Ultimate.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Igor Kmiť
PR Specialist Slovakia
ESET, spol. s r.o.

Apache Superset: Open-Source alternatíva k Power BI

Rastúce náklady na licencie tradičných Business intelligence nástrojov nútia firmy hľadať nové možnosti ako efektívne spravovať a vizualizovať svoje dáta.
Apache Superset ponúka funkcie porovnateľné s Power BI, pričom v niektorých aspektoch ho dokáže aj prevýšiť. Vďaka nulovým nákladom na licencie je ideálnym riešením pre firmy, ktoré chcú implementovať moderný Business intelligence nástroj bez dodatočných finančných bremien. Platforma podporuje tvorbu interaktívnych dashboardov, automatizovaných reportov a umožňuje ich zdieľanie bez obmedzení.
Prispôsobenie užívateľského rozhrania je ďalším výrazným plusom Supersetu. Na rozdiel od Power BI, kde sú úpravy často limitované výrobcom, tento systém umožňuje zásahy priamo do kódu. Firmy si tak môžu prispôsobiť vzhľad aplikácie, od loga hlavičky až po zobrazovacie pole, podľa svojich potrieb.
Čo všetko dokáže Superset urobiť za vás a ako je to s bezpečnosťou zdieľaných dát sa dočítate ďalej.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Roman Schmidt
Starší špecialista
GAMO a.s.

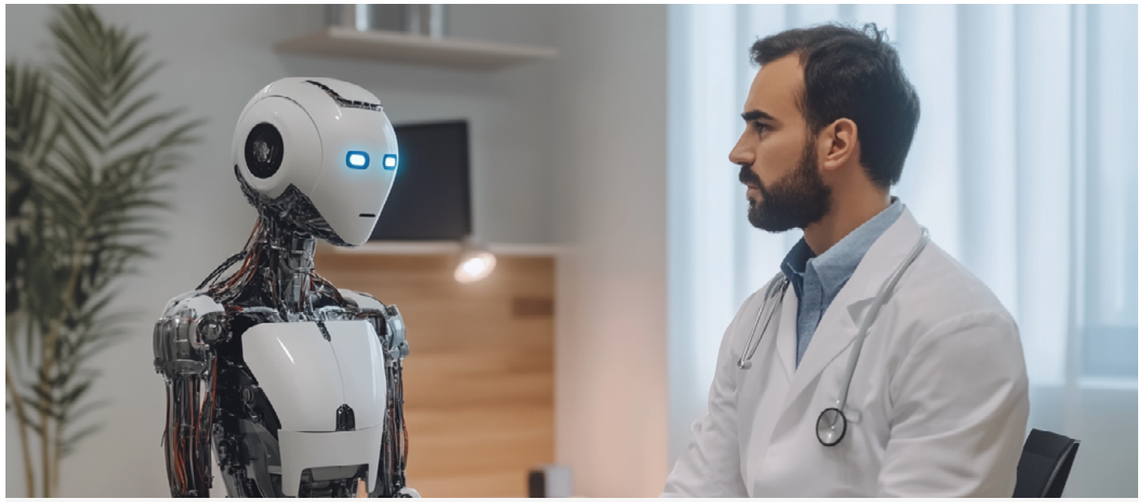
Zo slovníka kybernetickej bezpečnosti

V tejto oblasti existuje množstvo špecifických odborných termínov, vybrané z nich postupne vysvetľujeme. Zmenám, ktoré prináša transpozícia smernice NIS 2 do Zákona o kybernetickej bezpečnosti 69/2018 sa venujeme podrobne v samostatnom článku, preto dnes zo slovníka vyberáme tri slovíčka:

Bezpečnostný incident je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému alebo porušenia bezpečnostnej politiky či záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť.
Bezpečnostné opatrenia sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.
Stratégia kybernetickej bezpečnosti je plán alebo súbor opatrení, ktoré organizácia prijíma na ochranu svojich digitálnych aktív, systémov, sietí a dát pred rôznymi hrozbami a útokmi v kybernetickom priestore.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Jana Kohárová
Obchodný konzultant
GAMO a.s.



Čo je AI Akt? Naštudujte si možnosti a zodpovednosti nadväzujúcich poskytovateľov

Ak akákoľvek spoločnosť použije ChatGPT cez API na svojej platforme, označí ho svojou značkou alebo ochrannou známkou, podstatne zmení systém alebo jeho účel, môže byť považovaná za poskytovateľa vysokorizikového AI systému. Čo je AI Akt? Ide o legislatívny rámec ukladajúci povinnosti nadväzujúcim poskytovateľom využívajúcim alebo integrujúcim umelú inteligenciu vytvorenú inými subjektmi.

Medzi zákonné povinnosti druhých strán, teda nadväzujúcich poskytovateľov AI, patria napríklad zabezpečenie transparentnosti, ochrana údajov, a bezpečné použitie AI systémov. Platí, že aj keď nie sú vývojármi daného užívateľského typu AI, zodpovedajú za to, aby používané technológie spĺňali všetky zákonné požiadavky a neohrozovali používateľov.

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

Kvantové výpočty: R/Evolúcia, ktorá môže narušiť základy IT bezpečnosti

Kvantová výpočtová technika prináša revolučné možnosti, ale zároveň predstavuje hrozbu pre moderné šifrovacie metódy. Čo to znamená pre podnikové IT a kybernetickú bezpečnosť?

Kvantové technológie už nie sú iba teóriou z akademických kruhov. S narastajúcim počtom qubitov a zlepšením kvantovej korekcie chýb sa stávajú realitou pripravenou zasiahnuť do komerčnej sféry.

Kvantové počítače majú potenciál výrazne urýchliť riešenie zložitých problémov, ktoré boli pre klasické počítače prakticky nedosiahnuteľné. Technológie strojového učenia a umelej inteligencie môžu s kvantovými algoritmami dosiahnuť nové úrovne presnosti a efektivity. Prínosy sú jasné - od optimalizácie procesov a logistických systémov až po analýzu veľkých objemov dát. Kvantová budúcnosť však nie je len o možnostiach, s každou novou technológiou prichádzajú aj nové výzvy.

Aké sú riziká kvantovej technológie a čo robiť pre ich elimináciu sa dočítate na platformofinvention.sk

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Zuzana Holý Omelková
Obchodná riaditeľka
GAMO a.s.

Ako NIS 2 ovplyvní kybernetickú bezpečnosť:

Nové pravidlá, povinnosti a výzvy pre slovenské firmy

Kybernetická bezpečnosť sa stáva neoddeliteľnou súčasťou každodenného fungovania moderných spoločností. Smernica Európskej únie NIS 2 (Network and Information Security) je odpoveďou na rýchlo sa vyvíjajúce kybernetické hrozby, ktorých dôsledky presahujú hranice jednotlivých štátov aj sektorov.

Transpozícia smernice NIS 2 do slovenského právneho poriadku má za cieľ posilniť ochranu kritickej infraštruktúry, ekonomických subjektov a širokého spektra spoločností pred rastúcimi rizikami kybernetických útokov. Novelizovaná smernica reaguje na nové výzvy a riziká, ktoré priniesla doterajšia prax.

Pôvodný rámec bol často obmedzený len na najväčšie spoločnosti a kritické sektory, čo spôsobovalo slabé miesta v ochrane menších subjektov, ktoré sú čoraz častejším cieľom kybernetických útokov. Existenčné hrozby ako sú ransomware útoky, phishingové kampane alebo využitie zraniteľností v softvéri, nepoznajú rozdiely medzi malými a veľkými organizáciami. Útoky často mieria na menšie subjekty, nedisponujúce dostatočnými bezpečnostnými opatreniami, a tieto incidenty môžu spustiť reťazovú reakciu postihujúcu celé sektory.

Rozšírenie pôsobnosti: Kto bude ovplyvnený?

Jednou z najvýznamnejších zmien, ktoré smernica prináša, je rozšírenie okruhu subjektov, na ktoré sa vzťahujú nové pravidlá. Kým pôvodná legislatíva sa sústredila na tzv. poskytovateľov základných služieb (PZS) v oblastiach ako energetika, doprava, zdravotníctvo a bankovníctvo, NIS 2 výrazne rozširuje tento zoznam. Po novom sa do pôsobnosti zákona dostávajú organizácie v oblasti výroby, distribúcie potravín, odpadu, ale medzi plnohodnotných PZS sa zaradia aj poskytovatelia digitálnych služieb.

Okrem toho sú stanovené jasné kritériá pre veľkosť a význam organizácií. Subjekty, majúce viac ako 50 zamestnancov alebo ročný obrat presahujúci 10 miliónov eur, a predmet ich podnikania je určený v prílohe zákona, automaticky spadajú do jeho pôsobnosti. „Táto definícia však nie je univerzálna. Niektoré služby, ktoré sú z hľadiska bezpečnosti obzvlášť citlivé, ako napríklad poskytovanie DNS služieb alebo správca TLD, budú zahrnuté bez ohľadu na svoju veľkosť. Tento krok je nevyhnutný, keďže útok na tento typ služieb môže mať zásadný vplyv na tisíce zákazníkov vrátane veľkých korporácií," vysvetľuje dôvody Zuzana Holý Omelková, CCO zo spoločnosti GAMO (na snímke).

Rozšírenie pôsobnosti zároveň prináša nové výzvy pre podniky, ktoré doteraz nemuseli riešiť otázky kybernetickej bezpečnosti na takejto úrovni. Napríklad menší výrobcovia alebo distribútori potravín, podceňujúci možnosť výskytu kybernetických útokov a hlavne ich dopad, teraz musia byť pripravení chrániť svoje IT systémy, analyzovať potenciálne riziká či zvyšovať úroveň bezpečnostného povedomia u svojich zamestnancov.

Upozornenia a odporúčania vyplývajúce z NIS 2

Časový harmonogram:	Analýza rizík:	Povinnosti MKB:
• Účinnosť zákona od 1.1.2025. • Ak organizácia spadá pod sektory definované v prílohe 1 alebo 2 novely, musí do 60 dní požiadať o zápis do registra PZS, ktorý vedie NBÚ. • Na zosúladenie s požiadavkami zákona sú dôležité určenie manažéra kybernetickej bezpečnosti (MKB), vypracovanie analýzy rizík a aplikáciu bezpečnostných opatrení podľa §20 ods. 2. novely má ďalších 12 mesiacov.	• Mal by ju vykonávať skúsený manažér rizík alebo MKB. • Organizácia by sa pri jej vypracovaní mala riadiť uznávanými metodikami ako ISO 27005:2022, ISO/IEC 31000, NIST SP 800-39. • Vlastné metodiky MIRRI SR a NBÚ SR sú dostupné na ich webových stránkach.	• Nezávislý od IT oddelenia a spĺňa znalostné štandardy pre výkon role. • Do 72 hodín od identifikácie nahlasuje bezpečnostné incidenty. • Podáva komplexnú správu o každom incidente do jedného mesiaca. • Najneskôr do 24 hodín od zistenia (bez zbytočného odkladu) nahlasuje významné kybernetické hrozby či udalosti odvrátené v poslednej chvíli.

Analýza rizík: základ efektívnej ochrany

Jednou z kľúčových požiadaviek novej legislatívy je zavedenie systematickej analýzy rizík. Ide o proaktívny prístup k identifikácii a manažmentu rizík, presahujúci tradičné modely ochrany. Analýza rizík už nie je len o ochrane konkrétnych systémov alebo údajov. Organizácie musia posudzovať celé svoje prevádzkové prostredie, vrátane interakcií s externými dodávateľmi, používaného softvéru a fyzickej infraštruktúry.

„Napríklad spoločnosť poskytujúca logistické služby musí zvážiť riziká spojené nielen s vlastným IT systémom, ale aj s integráciou so systémami svojich partnerov. Zraniteľnosť na jednej strane dodávateľského reťazca môže predstavovať bezpečnostné riziko pre celý systém," potvrdzuje Zuzana Holý Omelková.

Pre efektívnu analýzu rizík je potrebné pravidelne aktualizovať bezpečnostné politiky, testovať systémy na odolnosť voči útokom, a spolupracovať so špecializovanými konzultantmi alebo bezpečnostnými tímami.

Implementácia bezpečnostných opatrení

Výsledky analýzy rizík sú základom pre implementáciu technických, organizačných a personálnych opatrení, ktoré sa musia prispôsobiť konkrétnym potrebám organizácie. „Na technickej úrovni ide napríklad o nasadenie firewallov, šifrovanie komunikácie, monitorovanie prevádzky a pravidelné aktualizácie softvéru. Na organizačnej úrovni je kľúčová edukácia zamestnancov, zavádzanie bezpečnostných politík a vypracovanie plánov reakcie na incidenty," približuje podrobnosti obchodná riaditeľka a odborníčka na kyberbezpečnosť zo spoločnosti GAMO.

Niektoré organizácie musia ísť ešte ďalej a zaviesť špecializované opatrenia. Napríklad podniky, ktoré uchovávajú citlivé údaje ako sú napríklad zdravotné záznamy, musia zabezpečiť nielen prístupové práva ale aj auditovateľnosť správy týchto údajov. Cloudoví poskytovatelia sú viazaní ku garancii vysokej dostupnosti svojich služieb a zároveň bezpečnosť infraštruktúry pred útokmi zo strany hackerov.

Manažér kybernetickej bezpečnosti: kľúčová úloha

Pozícia je nevyhnutná na koordináciu všetkých opatrení v oblasti bezpečnosti. Manažér musí byť kvalifikovaný a nezávislý od iných oddelení, aby mohol efektívne dohliadať na bezpečnostné procesy. „Pre mnohé menšie organizácie to predstavuje výzvu, keďže nemajú interné kapacity na obsadenie takejto pozície," upozorňuje Zuzana Holý Omelková a ponúka alternatívu, ktorou môže byť outsourcing služby externým poskytovateľom: „Toto riešenie je často dokonca finančne efektívnejšie."

Povinnosť hlásenia incidentov a prevencia

Smernica NIS 2 kladie veľký dôraz na prevenciu a včasnú reakciu. Organizácie sú viazané hlásiť nielen incidenty, ktoré už spôsobili škody, ale aj potenciálne hrozby a odvrátené útoky. Tento proaktívny prístup dokáže na národnej úrovni vytvárať širší prehľad o aktuálnych rizikách a zdieľať dôležité informácie medzi subjektmi. Hlásenie musí byť vykonané do 72 hodín od zistenia incidentu, pričom pri významných hrozbách je lehota len 24 hodín.

Ekonomické a reputačné výzvy

Implementácia NIS 2 si vyžiada značné investície, čo môže byť náročné najmä pre menšie podniky. Tieto náklady zahŕňajú nákup technológií, školenie zamestnancov, audit bezpečnostných opatrení a prípadné pokuty za nesplnenie požiadaviek. Na druhej strane, z dlhodobého hľadiska sú tieto investície výrazne nižšie ako škody spôsobené kybernetickými útokmi.

Okrem finančných aspektov je dôležitá aj reputácia. „Spoločnosti, ktoré preukážu vysokú úroveň ochrany svojich systémov a údajov získavajú dôveru zákazníkov a obchodných partnerov. Naopak, nedostatočná bezpečnosť môže viesť k strate dôvery a poklesu konkurencieschopnosti," upozorňuje Zuzana Holý Omelková zo spoločnosti GAMO.

Zavedenie smernice NIS 2 na Slovensku predstavuje prelomový moment pre oblasť kybernetickej bezpečnosti. Je to výzva, ale aj príležitosť na modernizáciu, zvýšenie odolnosti a zlepšenie spolupráce medzi súkromným a verejným sektorom.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR


Martin Ondrušek
martin.ondrusek@gamo.sk

SIEM – má ešte zmysel? Ako ďalej?

Systém SIEM (Security Information and Event Management) je s nami už viac ako 30 rokov. Za túto dobu sa technologické prostredie kybernetickej bezpečnosti dramaticky zmenilo a treba hľadať odpovede na nové výzvy.

Povedať, že SIEM je ‘mŕtvy‘ je tvrdením, ktoré v komunite kybernetickej bezpečnosti vyvoláva intenzívne diskusie. Je pravdou, že v posledných rokoch sa objavujú nové prístupy a nástroje, ako sú XDR (Extended Detection and Response), ktoré sa často porovnávajú so SIEM a niekedy sú považované za jeho náhradu. SIEM však stále zohráva nezastupiteľnú úlohu v mnohých organizáciách, najmä v tých, ktoré sa zaoberajú komplexnými a citlivými dátami, kde je nevyhnutná robustná detekcia a analýza bezpečnostných incidentov.

Čo je SIEM

SIEM je systém navrhnutý na zbieranie, ukladanie a analýzu bezpečnostných udalostí a informácií. Jeho úlohou je zhromažďovať logy a ďalšie dáta zo všetkých systémov, aplikácií a zariadení v infraštruktúre organizácie, a tieto dáta následne spracovávať na účely detekcie, vyhodnocovania a reagovania na bezpečnostné hrozby.

Na začiatku bol SIEM najmä nástrojom na audit a zabezpečenie súladu s predpismi ako sú GDPR alebo ISO/IEC 27001. No jeho schopnosti sa postupne vyvinuli a dnes je neoddeliteľnou súčasťou komplexnej kybernetickej obrany organizácií.

Základným cieľom SIEM je identifikovať potenciálne bezpečnostné incidenty, ktoré môžu ohroziť organizáciu ako sú úniky údajov, neautorizované prístupy, ransomvérové útoky alebo iné nebezpečné aktivity. Dosahuje to analýzou veľkého množstva dát, ktoré sa generujú v rámci organizácie a ich následnou koreláciou, aby sa odhalili vzorce a anomálie, naznačujúce útoky.

Výhody SIEM

- **Žiadny zo známych systémov nedokáže zabezpečiť tak veľkú mieru viditeľnosť do infraštruktúry.**
- **Porovnáva údaje naprieč rôznymi nástrojmi a tým zvyšuje efektivitu odhaľovania útokov.**
- **Vytvára jedno miesto na reportovanie hrozieb, či už pre potreby auditu alebo kvôli požiadavkám na súlad.**

SIEM dnes a jeho porovnávanie s novšími nástrojmi

V čase keď sa bezpečnostná technológia neustále vyvíja si mnohí kladú otázku či je SIEM stále relevantný. Nové prístupy, prezentované ako plnohodnotná alternatíva, však nemusia vždy pokryť všetky potreby organizácií v oblasti kybernetickej bezpečnosti.

Napríklad XDR je skôr nástrojom zameraným na detekciu a reakciu na bezpečnostné incidenty v reálnom čase. Zameriava sa na konkrétne hrozby, ako sú neautorizované prístupy alebo pokusy o infiltráciu, a často sa spolieha na blokovanie komunikácie vykazujúcej podozrivé správanie. Táto metodika má však svoje limity, najmä pokiaľ ide o detekciu nových, neznámych hrozieb alebo komplexných útokov, ktoré si vyžadujú analýzu historických dát a identifikáciu vzorcov správania.

V praxi sme sa stretli s prípadmi, kedy organizácie nasadzovali XDR v kombinácii so SIEM, čím získali najlepšie z oboch svetov - pokročilú detekciu a rýchlu reakciu na konkrétne hrozby s prehľadom o bezpečnostnom dianí v celej infraštruktúre. SIEM, analyzujúci metadáta z rôznych zdrojov, poskytuje hlbšiu a širšiu analýzu, ktorú XDR nedokáže ponúknuť.

Normálnosť a detekcia anomálií

V oblasti bezpečnosti je jedným z kľúčových výziev identifikácia toho čo je normálne správanie sa a čo už nie. Tieto vzorce sa zvyčajne definujú na základe histórie a kontextu prevádzky konkrétnej organizácie. Z hľadiska SIEM nie je cieľom iba detekovať konkrétne, známe hrozby, ale identifikovať vzorce anomálií, ktoré môžu signalizovať útoky. Práve táto schopnosť zistiť neznáme, zložité hrozby, robí SIEM nezastupiteľným.

Na identifikáciu spomínaných anomálií môžeme využiť prístup založený na viacerých detekčných pravidlách. Napríklad, ak sa v krátkom časovom období objaví viacero podozrivých aktivít, je to signál, že sa môže diať niečo znepokojivé a SIEM by mal spustiť alarm. Tento prístup sa osvedčil v praxi, najmä pri prevencii útokov typu „zero-day“, ktoré sú ťažko rozpoznateľné tradičnými bezpečnostnými nástrojmi.

Prínosy SIEM v praxi

V reálnom svete vidíme ako implementácia SIEM riešení zlepšuje kybernetickú bezpečnosť a ochranu podnikania. Môžeme to ilustrovať na príklade malého výrobcu automobilových súčiastok, ktorý čelil ransomvérovému útoku. Pred implementáciou SIEM sa útok zjavil až po tom ako spôsobil výrazné škody – výpadok výroby, finančné straty a poškodenie reputácie. Po nasadení SIEM však firma dokázala rýchlo zareagovať na podobný útok v priebehu niekoľkých minút, a tak sa im podarilo zamedziť ďalším stratám.

Okrem toho sa SIEM ukázal ako neoceniteľný nástroj pri odhaľovaní vnútorných hrozieb, čím bol pokus o neautorizovaný prístup k citlivým dátam. V jednom prípade systém identifikoval nezvyčajný prístupový vzor k patentovaným dizajnom firmy, čo mohlo viesť k úniku duševného vlastníctva. SIEM túto hrozbu včas identifikoval a ochránil tým cenné údaje, plus zabezpečil, že firma neprišla o svoju konkurenčnú výhodu.

SIEM a jeho nezastupiteľná rola v zabezpečení regulačných požiadaviek

Mnohé výrobné odvetvia sú povinné dodržiavať prísne bezpečnostné normy ako napríklad ISO/IEC 27001. Implementácia SIEM v týchto organizáciách zjednodušuje proces spĺňania týchto noriem. Systém poskytuje nepretržité monitorovanie bezpečnostných incidentov a umožňuje o nich rýchle podávanie správ, čo je kľúčové pre udržanie súladu s regulačnými požiadavkami.

Okrem toho, vďaka konsolidácii bezpečnostných dát zo všetkých systémov do jedného miesta a ich následnej analýze, organizácie dokážu rýchlejšie a efektívnejšie reagovať na incidenty, čo nie je možné dosiahnuť s rozptýlenými bezpečnostnými nástrojmi. To prináša nielen časové, ale aj finančné úspory.

SIEM je stále nevyhnutný

Napriek tomu, že sa bezpečnostné nástroje vyvíjajú a objavujú sa nové prístupy, SIEM stále zohráva kľúčovú rolu v moderných bezpečnostných infraštruktúrach. Jeho schopnosť korelovať údaje zo všetkých systémov, detegovať anomálie a vyhľadávať komplexné vzorce správania je nenahraditeľná. Preto je implementácia systému, aj keď časovo a finančne náročná, jednou z najlepších investícií do kybernetickej bezpečnosti, ktorú môže organizácia urobiť.

SIEM je nástroj, poskytujúci hlboký prehľad o bezpečnostnom dianí v organizácii a umožňuje efektívnu detekciu nových hrozieb. V kombinácii s inými možnosťami, ako je XDR alebo IDS, ponúka organizáciám vyvážený a efektívny spôsob ochrany pred rôznymi typmi kybernetických útokov.

Ak sa teda rozhodujete ako presvedčiť svojho CEO o dôležitosti SIEM, zamerajte sa na jeho schopnosť zmierňovať riziká, stabilizovať prevádzku a chrániť konkurenčné výhody spoločnosti. SIEM nie je len nástroj na ochranu, ale aj strategická nevyhnutnosť pre budúcnosť kybernetickej bezpečnosti v podniku.

Článok čítajte na platformofinvention.sk

klikni alebo oskenuj QR

Peter Bednár
peter.bednar@gamo.sk

Jednoduchšia verejná doprava vďaka cloudu

Nadväznosť spojov a jeden cestovný lístok na vlak aj autobus – banskobystrická župa úspešne integruje verejnú dopravu v regióne a zásadne ju zmodernizovala. Kľúčovou súčasťou tohto úsilia sa stalo na mieru ušité cloudové riešenie, ktoré bolo pre celý projekt nevyhnutné.

Na začiatku modernizácie banskobystrický kraj založil akciovú spoločnosť Organizátor IDS BBSK. Dostala úlohu pripraviť integráciu rôznych druhov dopravy - od regionálnej (prímestskej) autobusovej až po železničnú. Cieľom bolo zlepšiť efektivitu a komfort cestujúcich. „Chceli sme dosiahnuť, aby verejná doprava bola pre cestujúcich pohodlná, rýchla aj dostupná," vysvetľuje Ing. Radoslav Vavruš, predseda predstavenstva spoločnosti IDS BBSK.

Kľúčová úloha cloudových služieb

Pre dosiahnutie týchto cieľov bolo potrebné vybudovať robustnú IT infraštruktúru. Spoločnosť GAMO, dodávateľ cloudových služieb, navrhla riešenie postavené na technológii VMware, ktoré zákazníkovi umožňuje plne spravovať svoje virtuálne dátové centrum. „Táto flexibilita a škálovateľnosť infraštruktúry boli pre nás rozhodujúcim faktorom," objasňuje Peter Maček, Vedúci útvaru prevádzky IDS a IT/ICT dôvody, prečo sa rozhodli pre prechod do cloudu.

Nové riešenie umožňuje župnej firme efektívne spravovať zdroje, systém je totiž možné prispôsobiť podľa aktuálnych potrieb. Ak je potrebné zvýšiť výpočtové zdroje, cloudová infraštruktúra umožňuje ich rýchle rozšírenie bez potreby nových investícií do fyzického hardvéru. „Máme tak možnosť spravovať všetky hardvérové zdroje vrátane vytvárania a úpravy virtuálnych strojov, sietí a ďalších prvkov," hovorí o pozitívach Peter Maček z IDS BBSK. Cloudové riešenie navyše beží na vysoko bezpečných a spoľahlivých serveroch v dátovom centre Data Cube v Bratislave, pričom záložná lokalita sa nachádza v Banskej Bystrici. „To nám zaisťuje dostupnosť 24 hodín denne sedem dní v týždni a vysokú úroveň zálohovania dát."

Prechod do cloudu šetrí župnej firme aj náklady. Služby sú udržiavané spoločnosťou GAMO, ktorá zabezpečuje aktualizácie a servis systémov, IDS BBSK tak nemíňa peniaze na správu hardvéru. „To nám umožňuje plne sa sústrediť na poskytovanie a skvalitňovanie služieb cestujúcim," pomenováva výhody Peter Maček. Nemenej dôležitá je aj bezpečnosť a ochrana dát. Údaje získané z externých zdrojov a v prvej fáze integrácie z autobusov sú spracovávané, overované a bezpečne uchovávané pre prípadné budúce potreby. Zálohovanie a obnova dát sú riešené automaticky, čo minimalizuje riziko straty údajov.

Výhody pre cestujúcich

Obyvatelia a návštevníci banskobystrického kraja využívajúci verejnú dopravu majú teraz vďaka cloudovému riešeniu prehľad o cestovných lístkoch a môžu si jednoduchšie plánovať trasy. „Zavedenie predplatných lístkov s neobmedzenými jazdami v určitej zóne, push-up notifikácie o konci platnosti lístka a možnosť manažovania cestovného cez rodinný účet zvyšujú komfort, šetria čas a peniaze," konkretizuje pozitíva pre cestujúcich Maček z IDS BBSK.

Cloudové riešenie umožnilo aj zavedenie inovatívnych platobných metód za cestovné. Zahŕňa to online nákupné možnosti cez e-shop, vrátane platieb cez debetné, kreditné, alebo IDS karty.

Vďaka integrácii do cloudu môže IDS BBSK spravovať celý systém z jedného centrálneho miesta a v reálnom čase reagovať na potreby cestujúcich a zmeny v prevádzke. Podľa Petra Mačeka virtuálne servery umožňujú zber a spracovanie údajov z viacerých zariadení a ich systémov umiestnených v dopravných prostriedkoch. „Tieto údaje nám výrazne napomôžu pri optimalizáciách trás, zlepšovania časových harmonogramov, a do budúcna poskytovania aktuálnych informácií cestujúcim."

Inšpirácia pre ďalšie regióny

Úspešná integrácia cloudových služieb od spoločnosti GAMO na príklade IDS BBSK ukazuje ako môže takéto riešenie prispieť k zlepšeniu verejnej dopravy. Je nielen praktickým riešením, ale aj inšpiratívnym príkladom pre ďalšie regióny a podniky, ktoré sa usilujú modernizovať svoje služby pre verejnosť.

„Preukázali sme, že správnym výberom technológií sú možné inovatívne zlepšenia v oblasti služieb, komfortu a efektivity verejnej dopravy. Zároveň sa budúci záujemcovia o podobné riešenie môžu spoľahnúť, že im poskytne rýchlu adaptáciu na meniace sa potreby aj v budúcnosti," oceňuje projekt Ing. Radoslav Vavruš, predseda predstavenstva IDS BBSK. Podľa neho jednoznačne dokazuje, že sa vďaka moderným technológiám podarilo vytvoriť efektívny a používateľsky príjemný systém, napomáhajúci k zvyšovaniu komfortu cestujúcich, ale tiež optimalizujúci prevádzku celého dopravného systému.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Branislav Lupták
branislav.luptak@gamo.sk

Power Automate, digitálna transformácia šetrí peniaze a čas

V dnešnom rýchlo sa meniacom podnikateľskom prostredí je efektivita kľúčom k úspechu. Firmy čelia rastúcim nárokom na flexibilitu, rýchlosť a kvalitu – a práve tu prichádza na scénu Power Automate od Microsoftu.

Chceli by ste vo vašej firme zaviesť poriadok do posudzovania a schvaľovania rôznych dokladov, objednávok alebo zmlúv? Potrebujete na to elektronický systém, ktorý odbúra behanie s dokumentom od dverí k dverám, z oddelenia na oddelenie. Minulosťou sa stane čakanie, kto z kolegov a kedy doklad posúdi, alebo kedy sa šéf vráti z pracovnej cesty, aby mohol dokument podpísať.

Nový nástroj, ktorý firmám umožňuje automatizovať každodenné procesy, je možno už teraz súčasťou vašej používanej licencie v aplikácii Microsoft 365. Šetrí tým čas, znižuje chyby a zvyšuje produktivitu zamestnancov. Power Automate v podstate transformuje spôsob akým firmy pracujú a pomáha dosiahnuť viac s menším úsilím. V nasledujúcich riadkoch vám predstavíme čo všetko dokáže.

Automatizácia šetrí čas a zvyšuje efektivitu

Väčšina zamestnancov trávi až 20 percent svojho pracovného času opakovanými, rutinnými úlohami. Prostredníctvom novej platformy môžu tieto procesy automatizovať a vytvoriť si priestor na dôležitejšie, kreatívnejšie a hodnotnejšie zadania.

“Power Automate je navrhnutý tak, aby umožnil firmám bez zbytočných komplikácií automatizovať každodenné operácie, ako sú napríklad spracovanie žiadostí a faktúr, ich schvaľovanie či plánovanie. Tento nástroj umožňuje vytvárať tzv. automatizované toky, ktoré sa spúšťajú na základe určitých podmienok alebo udalostí. Sú nimi napríklad prijatie e-mailu, zmena súboru či dokončenie formuláru,” vysvetľuje fungovanie systému Martin Hála, Business Unit Manager | Software & Cloud zo spoločnosti TD SYNNEX.

Systém sa okrem toho ľahko integruje s množstvom ďalších aplikácií, čo znamená, že firmy môžu okamžite začať zjednodušovať svoje procesy a dosahovať efektivitu bez zbytočných nákladov na jeho impelmentáciu.

Hlavné výhody Power Automate

Pre firmy je tento nástroj výhodný nielen z hľadiska úspory času, ale aj z pohľadu zvýšenej produktivity a kvality práce. Automatizáciou rutinných úloh sa zamestnanci môžu viac sústrediť na strategické aktivity, prinášajúce vyššiu pridanú hodnotu. Okrem toho sa znižuje riziko ľudských chýb, čo vedie k vyššej presnosti a spoľahlivosti výsledkov.

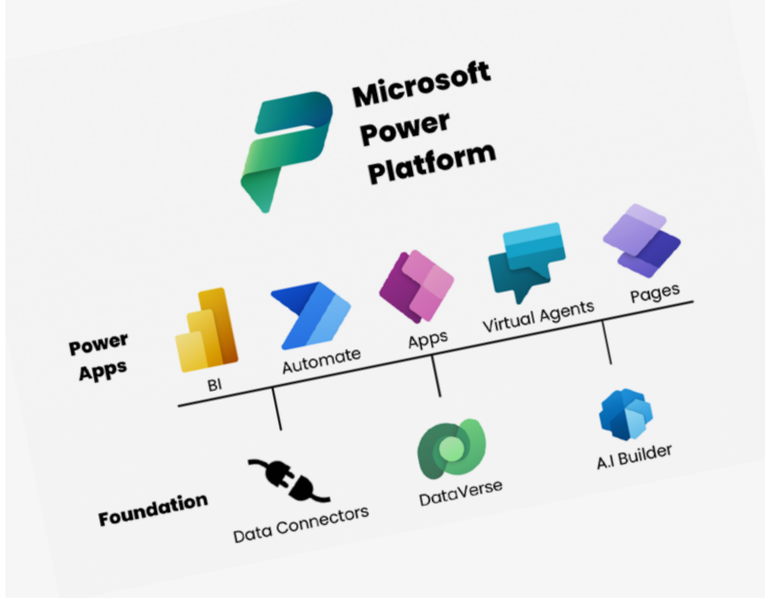
Ďalšou výhodou je lepšie využitie kapacít zamestnancov, ktorí môžu investovať viac času do tvorivých úloh, čo prispieva k celkovému zlepšeniu pracovnej atmosféry. Firmy tiež zaznamenávajú výrazné pozitíva v oblasti transparentnosti procesov a v správe projektov, pretože automatizované riešenia poskytujú presné a aktuálne informácie.

Ako pomáha v reálnom svete

Schvaľovanie žiadostí je jedným z procesov, ktoré Power Automate zjednodušuje. Namiesto manuálneho prechádzania e-mailov alebo formulárov tento nástroj v spolupráci s modulom Approvals automaticky odošle žiadosť o schválenie správnej osobe a zabezpečí, že všetko prebehne v reálnom čase. Systém teda minimalizuje oneskorenia a chyby, čím šetrí čas a zvyšuje efektivitu.

Iným príkladom je rezervácia miestností. Vo firmách s viacerými tímami môže ich ručné zapisovanie vyvolať chaos. Platforma synchronizuje kalendáre zamestnancov s dostupnosťou pracovných priestorov, čím eliminuje problémy ako napríklad dvojité rezervácie. Tento jednoduchý krok dokáže ušetriť až 5 hodín času mesačne, ktorý pracovníci trávili plánovaním a organizáciou.

Priemyselným podnikom nový nástroj ponúka riešenie pre monitorovanie strojov a predchádzanie výpadkom. Pomocou senzorov sa monitorujú kľúčové hodnoty, ako sú teplota alebo tlak, a v prípade prekročenia stanovených limitov sa okamžite spustí upozornenie pre údržbárov, čím sa minimalizujú náklady na opravy a neplánované výpadky. Eliminuje tým až 50 percent potenciálnych výpadkov.



Power Automate tiež výrazne zjednodušuje spracovanie faktúr. Ich automatické triedenie a integrácia do ERP systémov urýchľuje finančné procesy a minimalizuje administratívne chyby. Firmy všetkých veľkostí môžu ušetriť čas a znížiť náklady na administratívu v tejto oblasti až o 60 percent.

Nový nástroj dokáže pravidelne vytvárať aj rôzne reporty pre manažment. Ich ručné zostavovanie si obvykle vyžaduje veľa času a pozornosti. Systém dokáže s údajmi pracovať samostatne, automaticky generovať reporty a posielať ich členom tímu alebo vedeniu, čím zabezpečuje, že všetci majú včas aktuálne informácie. Znižuje to chybovosť, ktorú zvyčajne sprevádza ručné spracovanie dát, a automatizácia šetrí približne osem hodín času mesačne na zamestnanca.

Flexibilita vyhovuje každému

Power Automate je dostupný ako súčasť rôznych balíkov Microsoft 365 (Business Basic, Standard, Premium) a tiež ako samostatná služba. Základné funkcie sú k dispozícii aj v nižších licenčných edíciách, ale pre pokročilejšie potreby si klient môže zvoliť prémiové licencie, ponúkajúce robustnejšie možnosti automatizácie.

“K dispozícii sú licencie pre jednotlivcov, ktorí potrebujú vytvárať a spravovať automatizácie, ako aj licencie pre procesy, ktoré umožňujú firmám automatizovať konkrétne obchodné úlohy bez ohľadu na počet používateľov. To znamená, že Power Automate sa prispôsobí potrebám vašej firmy, či už ide o malé podniky alebo veľké korporácie,” objasňuje detaily Martin Hála.

Ako začať s novou platformou

Používanie nástroja na automatizáciu je veľmi jednoduché. Ponúka množstvo prednastavených šablón, ktoré zákazníkovi umožnia rýchlo spustiť prvé činnosti, ako napríklad zasielanie notifikácií alebo schvaľovanie požiadaviek. Power Automate je tiež možné integrovať s Microsoft Teams, SharePoint a ďalšími aplikáciami, čím získa flexibilitu potrebnú na efektívne riadenie procesov.

“Na úvod je lepšie využívať jednoduchšie úlohy ako sú automatické odpovede na e-maily alebo plánovanie schôdzok, a postupne sa môžete posúvať k zložitejším riešeniam,” odporúča Martin Hála z TD SYNNEX. Platforma je navrhnutá tak, aby bola prístupná aj používateľom bez technických znalostí, čo znamená, že každý tím v organizácii môže profitovať z jej výhod.

Power Automate predstavuje viac než len nástroj na automatizáciu. Je to systém, ktorý môže byť pre firmy rozhodujúcim kľúčom v ich digitálnej transformácii. Zamestnanci sa môžu zamerať na úlohy, ktoré skutočne prinášajú hodnotu, a to znamená v konečnom dôsledku posilnenie konkurencieschopnosti každej spoločnosti, ktorá ho začne naplno využívať.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Roman Slobodník
Business Development Manager | Microsoft Business Applications
TD SYNNEX Czech s.r.o.
roman.slobodnik@tdsynnex.com

Greenwashing pod tlakom nových regulácií v EÚ

Nové regulačné pravidlá prinášajú výzvy a aj príležitosti na zlepšenie dôvery spotrebiteľov. Európska únia schválila prelomovú smernicu, zakazujúcu zavádzajúce ekologické tvrdenia. Firmy budú mať povinnosť podložiť „zelenú“ komunikáciu presnými dátami a nezávislým overením. Hovorili sme o tom s Danielom Rabinom, spoluzakladateľom ESG KLUBU.

Skúsme na úvod vysvetliť čo je to takzvaný „greenwashing,“ ako by sme ho mohli preložiť do slovenčiny a ako súvisí s témou ESG?

Greenwashing by sme mohli preložiť ako „zelené klamstvo“ alebo „zavádzajúca environmentálna komunikácia“. A že ide o závažný problém potvrdzujú aj dáta Európskej komisie - až 53% environmentálnych tvrdení firiem v EÚ je vágnych, zavádzajúcich alebo nepodložených, a 40% je úplne nedoložených.

Z marketingového hľadiska je síce pochopiteľná snaha firiem odlíšiť sa používaním pojmov ako „zelený“, „udržateľný“ či „ekologický“. Problém je, že tieto pojmy nemajú jasné definície. Navyše, keď táto komunikácia nie je podložená reálnymi dátami a merateľnými výsledkami, môže ísť o greenwashing.

Práve ESG prináša firmám povinnosť systematicky vykazovať svoju udržateľnosť, čo vytvára základ pre transparentnú komunikáciu založenú na dátach. Tým sa významne eliminuje priestor pre greenwashing.

Európsky parlament tento rok schválil smernicu o environmentálnych tvrdeniach (Green Claims Directive – GCD). Túto reguláciu experti označujú ako prelomový predpis pokiaľ ide o boj s greenwashingom v EÚ. Čo je jej obsahom a na čo sa majú firmy pripraviť?

Konečne sa dostávame do fázy, kedy už nebude stačiť len tvrdiť, že sme „zelení“ - všetko bude musieť byť podložené presnými a treťou stranou overenými dátami. Kľúčovým nástrojom bude takzvaná analýza životného cyklu produktu Life Cycle Assessment, ktorá je v podstate komplexným hodnotením sledujúcim celú „cestu“ produktu. Od získavania surovín cez výrobu, distribúciu, používanie, až po jeho likvidáciu. V praxi to znamená, že ak chce firma tvrdiť, že jej produkt je environmentálne šetrný, musí to dokázať na základe merateľných údajov z celého tohto cyklu.

Všetky informácie o environmentálnych aspektoch produktu budú musieť byť ľahko dostupné spotrebiteľom - napríklad cez QR kódy na obaloch. A, čo je dôležité, všetky “zelené” tvrdenia musia byť overiteľné nezávislou treťou stranou.

Prináša GCD smernica aj nejaké príležitosti pre firmy?

Smernica konečne vytvorí férové prostredie pre firmy, ktoré to s udržateľnosťou myslia vážne. Predovšetkým sa zvýši dôvera spotrebiteľov - keď uvidia environmentálne tvrdenie, budú vedieť, že je podložené reálnymi dátami. Navyše, firmy, ktoré sa prispôsobia novým pravidlám, môžu získať lepší prístup k zelenému financovaniu či väčšiu dôveru investorov.

Z pohľadu firmy však môže ísť o ďalší tlak na náklady nie?

Je to tak. Som toho názoru, že väčšie firmy tento tlak ľahko ustoja. Z prostriedkov, ktoré už teraz investujú do nie vždy zmysluplného marketingu pôjde o relatívne zanedbateľný náklad. V prípade menších a stredných firiem to môže byť problém.

Hrozia firmám podľa novej smernice aj nejaké konkrétne sankcie?

GCD zavádza komplexný sankčný mechanizmus, najvýraznejšia je pokuta až do výšky 4% ročného obratu firmy.

Sankčný mechanizmus však presahuje rámec finančných postihov. Zahŕňa možnosť konfiškácie príjmov z produktov, pri ktorých došlo k zavádzajúcej komunikácii, ako aj dočasné vylúčenie z procesov verejného obstarávania na obdobie až 12 mesiacov.

A, čo považujem za ešte dôležitejšie, to je riziko poškodenia reputácie. Firmy, ktoré porušia pravidlá, budú zverejnené na takzvanom sankčnom zozname.

Tvrdíte, že v rámci prevencie greenwashingu musia firmy dôsledne rozlišovať medzi komunikáciou ESG aktivít a tradičných CSR aktivít, prečo je to tak?

Mnoho firiem si myslí, že keď robia CSR aktivity automaticky sú „ESG compliant“. Ale nie je to tak. Uvediem jednoduchý príklad: ak logistická firma podporí výsadbu stromov na Deň Zeme, je to určite dôležitá CSR aktivita. Ale ak chce hovoriť o ESG, musí systematicky postupovať podľa analýzy dvojitej významnosti. Pre jednu firmu to môže byť systematické znižovanie vlastnej uhlíkovej stopy, pre inú opatrenia na úsporu vody, pre typický “korporát” to môže byť transparentné odmeňovanie zamestnancov.

Ak si vo firme zameníte CSR projekty s udržateľnosťou v zmysle ESG, riskujete, že vaša komunikácia bude označená za greenwashing. A to aj v prípade, že to nebolo vaším úmyslom.

Ako sa majú firmy vyhnúť greenwashingu v komunikácii? Kde robia vo všeobecnosti najväčšie chyby?

V našej praxi sa stretávame s tým, že firmy často začínajú od konca - chcú komunikovať skôr, než majú reálne →

výsledky. My v ESG KLUBE preto vždy zdôrazňujeme jednoduchý postup: najprv zbierajte dáta o vašej činnosti, na základe nich si vytvoríte komunikačnú stratégiu, a až potom komunikujte.

Najčastejšie vidím chyby v používaní vágnych tvrdení typu „eco-friendly“, “carbon neutral” alebo „zelený produkt“. Druhá častá chyba je, že firmy vyzdvihnú jeden pozitívny aspekt produktu, ale zamlčia jeho celkový dopad na životné prostredie. Alebo si vytvoria vlastné „eko certifikáty“, ktoré v skutočnosti nič neznamenajú.

Ako máme my – spotrebitelia alebo budúci investori či klienti firmy – odhaliť pri niečom konkrétnom, že zo strany firmy ide len o zavádzanie, „natieranie na zeleno“?

V súčasnosti je to pomerne náročné. Ale situácia sa bude zlepšovať - Európska únia zavádza digitálne pasy produktov umožňujúcich jednoducho overiť environmentálne tvrdenia. A spomínané sankčné zoznamy tiež pomôžu identifikovať firmy, ktoré sa dopustili greenwashingu.

Zatiaľ odporúčam sledovať niekoľko varovných signálov. Prvý je používanie príliš “okatých” vágnych tvrdení bez konkrétnych čísel a faktov. Rovnako podozrivé je, keď firma zdôrazňuje jeden malý aspekt, napríklad recyklovaný obal, ale o celkovom dopade svojej činnosti mlčí.

Všímajte si aj certifikácie. Skutočne zodpovedné firmy majú na obaloch medzinárodne uznávané “labely”, nie vlastnoručne vytvorené „zelené pečiatky“. Dôveryhodné firmy tiež zvyčajne komunikujú transparentne aj o oblastiach, kde ešte nie sú dokonalé, a majú jasný plán na zlepšenie.

Kvalifikované zahraničné štúdie ukazujú, že spotrebitelia – hlavne generácie Mileniálov a GenZ – kladú dôraz na environmentálne a etické aspekty nákupných rozhodnutí. Tým môžu zvýšiť celkový dopyt po zodpovednej kategórii firiem a produktov. Ako sme na tom na Slovensku?

Tu máme zaujímavý paradox, ktorý nám ukázal nedávny prieskum Ipsos. Na jednej strane až 82% Slovákov si myslí, že spoločenská zodpovednosť by mala byť súčasťou DNA každej firmy. Dokonca 86% očakáva od firiem investície do udržateľných technológií.

Ale keď sa pozrieme na realitu nákupného správania sa, vidíme zaujímavý trend. Kým v roku 2021 bolo 70% Slovákov ochotných priplatiť si za environmentálne šetrný produkt, dnes je to len 53%. To je pomerne výrazný pokles, ktorý súvisí najmä so súčasnou ekonomickou situáciou a infláciou.

Ak platí, že Slováci „idú najmä po cene“, aká je šanca, že sa ich postoj časom zmení a čo sa pre to musí stať?

Ja som v tomto optimista. Vidím, že zmena postojov už prebieha, len je pomalšia, než by sme si želali. Kľúčové bude vzdelávanie. Keď ľudia lepšie pochopia súvislosti medzi svojimi nákupnými rozhodnutiami a stavom životného prostredia, tak budú ochotnejší investovať do udržateľných produktov.

Veľa závisí aj od firiem. Musia prísť s inovatívnymi riešeniami, ktoré spoja udržateľnosť s ekonomickou výhodnosťou. Už dnes vidíme príklady, kde zodpovedný prístup vedie k úsporám - či už ide o energeticky efektívne spotrebiče alebo obnoviteľné zdroje energie.

Dôležitú rolu zohrá aj nastupujúca generácia. Vzhľadom na ich silné environmentálne presvedčenie a preferenciu udržateľných produktov to vytvára bezprecedentnú príležitosť pre firmy, ktoré sa skutočne venujú ESG, nie greenwashingu.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Zuzana Peciarová
zuzana.peciarova@gamo.sk

Kybernetická bezpečnosť a ESG sú už dnes neoddeliteľnou súčasťou

V súčasnosti, keď sa digitálna transformácia stáva hlavným pilierom podnikateľských stratégií, rastie dôležitosť ESG (Environmental Social and Governance) prístupov. Zvláštnu pozornosť si zasluhuje práve pilier „G“ – riadenie, ktorý zahrnuje interné procesy, kontrolné mechanizmy a riadenie rizík.

Ako podčiarkuje Kristián Alakša, CEO spoločnosti GAMO, práve tento aspekt tvorí základ integrity a zodpovednosti každej modernej firmy: „Riadenie v ESG je o zabezpečení efektívneho, etického a súladného rozhodovania. Aj keď je často v tieni environmentálnych a sociálnych otázok, jeho význam je v digitálnej ére zásadný – najmä vzhľadom na kybernetické riziká, ktoré predstavujú jednu z najväčších výziev.“

Kybernetická bezpečnosť sa prirodzene stáva kľúčovým prvkom „G“ v ESG. Firmy, ktoré do svojho riadenia implementujú robustné bezpečnostné stratégie, nielenže chránia svoje digitálne aktíva, ale zároveň zvyšujú dôveru zainteresovaných strán a plnia legislatívne požiadavky. Takýto prístup zabezpečuje súlad s nariadeniami ako sú GDPR alebo Zákon o kybernetickej bezpečnosti 2024, ktoré chránia údaje, produkty a služby. Posilňuje aj ochranu dát a reputáciu tým, že minimalizuje dopady únikov dát a narušení prevádzky. Firmy, ktoré majú zavedené systémy na riešenie kybernetických incidentov, zároveň preukazujú svoju schopnosť reagovať na nepredvídané udalosti a zvyšujú odolnosť svojho podnikania. „Implementácia kybernetickej bezpečnosti v rámci ESG priamo súvisí s vyspelosťou riadiacich procesov. Transparentné vykazovanie týchto ukazovateľov nielenže zvyšuje dôveru investorov a zákazníkov, ale ponúka aj jasný obraz o schopnosti firmy chrániť svoje digitálne aktíva,“ zdôrazňuje Kristián Alakša.

Jedným z kľúčových krokov k zahrnutiu kybernetickej bezpečnosti do ESG reportovania je transparentné vykazovanie ukazovateľov a prijatých opatrení. Podľa skúseností spoločnosti GAMO môžu firmy v ESG správach zverejňovať metodológie na identifikáciu a zmiernenie kybernetických rizík, programy školení pre zamestnancov zamerané na zvládanie digitálnych hrozieb, alebo implementáciu moderných technológií na ochranu pred vyvíjajúcimi sa hrozbami. Takto koncipované ESG správy sa stávajú nielen nástrojom na prezentáciu zodpovedného podnikania, ale aj významným indikátorom vyspelosti firmy.

Aj keď sú náklady na zavedenie kyberbezpečnostných opatrení nemalé, firmy, ktoré túto oblasť implementujú, získavajú konkurenčnú výhodu. „Zahrnutie kybernetickej bezpečnosti do riadenia je investíciou do dôvery, kontinuity a udržateľnosti. Spoločnosti, ktoré tento aspekt podcenia, riskujú nielen regulačné postihy, ale aj oslabenie reputácie,“ vysvetľuje riziká CEO spoločnosti GAMO Alakša.

V dobe, keď sa digitálne hrozby stávajú neoddeliteľnou súčasťou podnikania ESG bez dôrazu na governance a kybernetickú bezpečnosť stráca svoj plný potenciál. Firmy vydávajúce sa na cestu proaktívnej ochrany svojich digitálnych aktív a transparentného reportovania nielenže splnia legislatívne požiadavky, ale získajú aj dlhodobú dôveru investorov, zákazníkov a zamestnancov. Cesta k budúcej konkurencieschopnosti preto vedie cez bezpečnosť, dôveru a odolnosť.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Zuzana Peciarová
zuzana.peciarova@gamo.sk

Mladí hekeri reprezentovali Slovensko na najväčšej súťaži pre kybertalenty

Na októbrovom európskom finále súťaže pre mladé ‚hekerské' talenty The European Cybersecurity Challenge v Turíne sa zúčastnil po tretíkrát aj slovenský reprezentačný tím.

Národný Team Slovakia 2024 tvorilo desať členov – jedno dievča a deväť chlapcov vo veku od 15 do 22 rokov, vybraných z 15 účastníkov národnej súťaže CybeGame.

Mladé talenty sa na finále pripravovali niekoľko mesiacov na tréningových bootcampoch, medzinárodnom vo Viedni a šiestich víkendových v kaštieli v Brunovciach. Absolvovali tam prednášky a workshopy na témy OSINT, WEB, Forenzia, Krypto, Radio, a zúčastnili sa online CTF súťaží. Zvyšný čas venovali príprave v online forme.

Národnú prípravu a organizáciu vrátane súťaží zabezpečujú Alexandra Húsková a Tomáš Hettych z Kompetenčného a certifikačného centra kybernetickej bezpečnosti. Technickú prípravu tímu vedú Lukáš Balážik a Adam Gajdošík.

Prestížna súťaž The European Cybersecurity Challenge spája talentovaných mladých ľudí a organizuje ju Agentúra EÚ pre kybernetickú bezpečnosť ENISA. Tímy riešia úlohy z rôznych oblastí: webová a sieťová bezpečnosť, mobilná bezpečnosť, krypto hádanky, reverzné inžinierstvo či digitálna forenzia. V desiatom ročníku finále v talianskom Turíne bolo prítomných až 400 ‚hekerov' zo 40 krajín.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Iveta Hlaváčová
iveta.hlavacova@gamo.sk

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

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

Marcela Gottwaldová
Obchod
marcela.gottwaldova@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.

Spoznajte odpoveď na neproduktívnu administratívnu záťaž

Chcem zistiť viac

GAMO
INFORMAČNÉ TECHNOLÓGIE