platform of invention

Informačné technológie pre podnikanie s nápadom

online pdf print

Užitočné v správnych hlavách

magazín pre CTO, CFO, CEO

číslo 5
ročník tretí | 1/2023

Kybernetická odolnosť

Kľúčové je byť pripravený a rýchly

Darujte podnikaniu budúcnosť. Zálohujte

ChatGPT Kontroverzný pomocník

Magazín o informačných technológiách

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

nové číslo

Čítajte 5. číslo
Venované téme kybernetickej odolnosti a umelej inteligencii.

PDF magazín | Online portál

Čítajte 1. číslo
Venované téme kybernetickej bezpečnosti.

Online portál | PDF magazín

Čítajte 2. číslo
Venované téme cloud.

Online portál | PDF magazín

Čítajte 3. číslo
Objavte benefity IT made in Slovakia.

Online portál | PDF magazín

Čítajte 4. číslo
Balíček IT opatrení ako recept na krízu.

Online portál | PDF magazín

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

Záchranné koleso kybernetickej bezpečnosti

Keď sme s kolegami diskutovali aké témy z IT-čka by sme pripravili do 5. vydania, jednoznačne prevládali tie, čo sú spojené so zvyšovaním úrovne kybernetickej odolnosti. Áno, môžete si povedať, že sa dookola opakujeme. Ale je to dôležité! Ako je fascinujúce sledovať rýchlo sa meniace technologické trendy, hlavne masívny rozvoj v oblasti umelej inteligencie, tak nás v opačnom garde stále fascinuje naša nepoučiteľnosť, ktorú vo veľkom využívajú útočníci v kyber priestore.

Aj na Slovensku sa pravidelne stretávame s prípadmi útočných kampaní. Ľudia sú podvodníkmi klamaní a prichádzajú o svoje alebo firemné peniaze. Phishingové stránky sú na nerozpoznanie od reálnych, sú vytvárané čoraz sofistikovanejšie a ťažšie sa rozpoznávajú od tých originálnych.

Preto je dôležité, aby sme prinášali informácie, ktoré ukážu rôzne spôsoby ako sa v online svete chrániť, mať zabezpečené zariadenia aj dáta. Musíme byť pripravení na všetky možné scenáre, naučiť sa rozpoznávať podvodné e-maily a webstránky. Byť obozretní, keď klikáme na rôzne odkazy, a opatrní pri otváraní neznámych príloh. Nesmieme zabúdať na pravidelné aktualizácie zariadení – mobil, notebook. Určite neodporúčame používanie verejných wifi sietí, a o tom, že dvojfaktorová autentifikácia je ‚must have', už ani nedebatujme.

Vraciame sa aj k témam, ktoré odzneli na podujatí GAMO koncom marca 2023. Venujeme sa službám zálohovania v cloude, upozorňujeme na fakt, že výber bezpečnostného nástroja je ideálne prispôsobiť hlavne potrebám firmy. Ak k obsluhe EDR/XDR riešení nemáte odborne zdatných ‚bezpečákov', zverte sa do rúk špecialistov, ktorí preberú starostlivosť o bezpečnostný monitoring, detekciu a reakcie na incidenty v rámci poskytovanej služby.

Kybernetická odolnosť je o zodpovednom prístupe k ochrane nášho súkromia a dôverných informácií.
Príjemné čítanie.

Zuzana Omelková
Obchodná riaditeľka
zuzana.omelkova@gamo.sk

Kyberbezpečnosť má zelenú! Európska komisia otvorila ďalšie výzvy na jej podporu

Až do 6. júla sa môžete prihlásiť k európskemu grantu na kyberbezpečnostné projekty vo firmách, štátnej správe aj samospráve, na školách, univerzitách, vedeckých pracoviskách a organizáciách tretieho sektora. Výška grantu je zväčša 50 percent, pre malé a stredné podniky až 75 percent z celkového rozpočtu. Aktuálna výzva Európskej komisie bude posudzovať projekty na budovanie tréningových centier, stredísk bezpečnostných operácií, či projekty s inovatívnymi riešeniami. Ste medzi nimi? Choďte do toho! Úspešné projekty nepodliehajú kvótam a národným obmedzeniam, takže predstavujú rovnakú príležitosť pre všetkých. V jarnej, predchádzajúcej výzve, dala Európska komisia zelenú ôsmim kyberbezpečnostným projektom zo Slovenskej republiky, zameraným na inovatívne riešenia a na budovanie stredísk bezpečnostných operácií. Gratulujeme. Viac informácií nájdete na bit.ly/3OSEb5L

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Alexandra Húsková
Obchodná manažérka
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Služba Veeam Backup pre Microsoft 365 prináša efektívne zabezpečovanie údajov

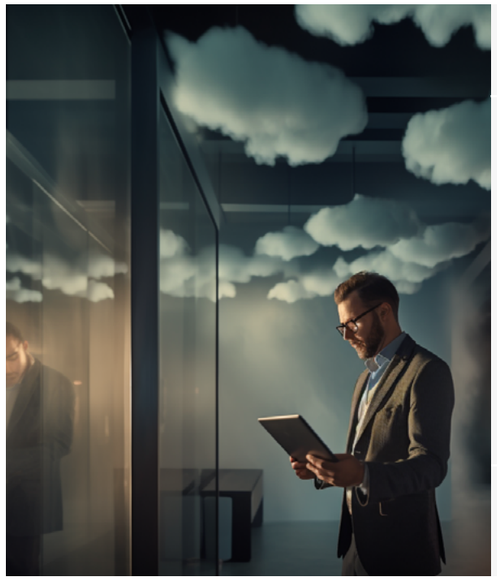
Správa Veeam Cloud Protection Trends Report 2023 ukázala, že až takmer 90 % zákazníkov služby Microsoft 365 využíva aj iné riešenia pre zálohovanie a obnovu dát, než len integrované možnosti. Potreba chrániť svoje prostredia SaaS a byť pripravený na potenciálne kybernetické útoky núti podniky riešiť otázky lepšieho zabezpečovania dát. Práve Veeam Backup prináša efektívne možnosti zálohovania a obnovy dát pre Microsoft 365. Chráni už viac ako 14 miliónov používateľov na celom svete. Nová verzia v7 uviedla niektoré inovácie a posilnila ochranu dát v Microsoft 365. Nový model poskytuje:

- nemenné zálohy,
- pokročilé monitorovanie a analýzu v celom prostredí zálohovacej infraštruktúry,
- vysokú kontrolu vďaka hlbšej integrácii s konzolou Veeam Service Provider Console.

Medzi hlavné prednosti v7 patria: úplný prehľad, ochrana pred útokmi ransomvéru a výpadkami, no zároveň i ochrana dát v prípade odchodu zamestnanca. Dôležitosť ochrany citlivých podnikových údajov, ako aj zabezpečenie rýchlej obnovy dát po útokoch, sú pre Veeam prioritou a poskytujú používateľom a IT správcom pokoj a istotu pri správe údajov v službe Microsoft 365.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Michal Štětina
Field Marketing Manager CEE
Veeam



Cloudové aplikácie sú čoraz populárnejšie, nezabúdajte na ich ochranu

Veľké množstvo používateľov služby sa v očiach útočníkov vždy premieňa na vidinu veľkého zisku. Inak tomu nie je ani v prípade cloudových platforiem na spoluprácu ako Microsoft Teams, ktorých popularita raketovo vzrástla počas pandémie. Integrované zabezpečenie týchto služieb však nedokáže úplne eliminovať možné bezpečnostné problémy. ESET preto prišiel s riešením **ESET Cloud Office Security**, vyvinutým špeciálne na ochranu cloudových aplikácií. Riešenie, ktorého súčasťou je aj účinný cloudový sandbox, firmy ochráni pred malvérom, phishingom, ale aj pred pokročilými hrozbami pochádzajúcimi z týchto platforiem. Každý súbor, nahraný do úložiska OneDrive, zdieľaný cez SharePoint alebo prenesený cez Teams, je skontrolovaný pomocou výkonného detekčného systému, ktorý využíva rovnakú technológiu ako produkty ESET pre koncové zariadenia.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Miroslav Ardon
Channel Sales Manager Slovakia
ESET, spol. s r.o.

Efektívna správa dát a centralizácia systémov je to, čo chceme. Prečo a ako na to

Čo majú spoločné dátový analytik, manažér controllingu a CFO? Zjednodušene: Ich prianím je pracovať s kvalitnými, konzistentnými a aktuálnymi dátami, aj vyhnúť sa duplicitám a chybovosti v záznamoch, ktoré spracovávajú alebo vyhodnocujú. Existuje viacero spôsobov ako pristupovať k centralizácii systémov a správe dát, voľba závisí od konkrétnej situácie a požiadaviek organizácie. Jednotný agendový systém môže byť jednou z možností, ktorá prinesie nový pohľad na existujúce dáta, poskytne kvalitný prehľad o výkonnosti organizácie a podporí biznis rozhodovanie v reálnom čase.
Inštitúcie prevádzkujúce množstvo informačných systémov, registrov, a vedúce rôzne agendy či vytvárajúce nespočetne veľa excelových prehľadov s položkami v desiatkach tisíc záznamov, rozhodne ocenia zavedenie Master Data Managementu. Systém pre centrálnu správu dát (MDM) je jednoznačnou voľbou aj pre pozície troch pracovníkov v úvode.

O čo presne ide? MDM je základným prvkom pre centrálne riadenie a distribúciu kľúčových číselníkových dát a zároveň dôležitou súčasťou jednotného agendového systému JAS. Čo všetko MDM zabezpečuje, umožňuje, a ako funguje, čítajte v našej online verzii.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Martin Vosko
Produktový manažér
GAMO a.s.

Je Vendor Lock – In vo verejnom obstarávaní vždy protiprávny? Určite nie

Stav Vendor Lock – In (ďalej len VLI) zjednodušene popisuje stav exkluzivity existujúceho dodávateľa tovarov alebo služieb, ktorý spôsobuje závislosť verejného obstarávateľa pri zabezpečovaní jeho potrieb od existujúceho dodávateľa. Môže vzniknúť umelým spôsobom, ale môže byť aj výsledkom objektívnych skutočností.
Stav VLI je v súčasnosti vnímaný najmä zo strany štátnych orgánov negatívne, s a priori predpokladom, že vznikol umelým spôsobom. S takýmto záverom, že stav VLI je vždy protiprávny, však nie je možné súhlasiť. Umelo vyvolaný stav VLI je dôsledkom nevhodného postupu samotného verejného obstarávateľa, keď bolo buď účelovo alebo aj nedbanlivostne vykonané verejné obstarávanie nesprávnym spôsobom. Stav VLI následne verejného obstarávateľa limituje do budúcnosti.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

JUDr. Milan Žoldoš
Advokát
BCH Advokáti Chlipala

Čas a pripravenosť hýbu dnešným svetom

Kybernetická bezpečnosť predstavuje aktuálne dôležitú výzvu aj pre malé a stredné podniky. Kybernetické útoky exponenciálne rastú v dôsledku vojnového konfliktu a v čase kovidovej pandémie sa kybernetická kriminalita zvýšila až o 600 percent!

Pred desiatimi až pätnástimi rokmi mali firmy vlastné IT infraštruktúry vo fyzicky zabezpečených serverovniach, siete boli chránené firewallmi a antivírusovými programami, smartfóny ani cloud sme nepoznali. Dnes je všetko diametrálne odlišné od bývalého spôsobu života, nový sa vyvíja veľmi rýchlo, napríklad smartfóny i cloudové služby sú neodmysliteľnou súčasťou nášho života a pracovného prostredia, a pandémia zmenila podmienky aj tak, že sa v mnohých prípadoch súkromné zariadenia využívajú na prácu vrátane cloudových služieb Microsoft 365, e-mailových či SharePoint služieb. Otázkou teda je, nakoľko sú tieto zariadenia a služby dostatočne bezpečné a zabezpečené, aby boli údaje firmy chránené?

Nelichotivý pohľad cez čísla

Prejdime si pár čísiel a faktov koho sa kybernetické útoky týkajú najviac a prečo sú alarmujúce:

- V posledných rokoch bol, podľa štatistík spoločnosti Microsoft, zaznamenaný takmer 30-percentný nárast úspešných phishingových útokov na firmy, bez ohľadu na to, či prevádzkujú on-premises alebo cloudové prostredie.
- Aj 93 % zdravotníckych organizácií malo v nedávnej minulosti skúsenosti s rôznymi typmi útokov.
- 25 % ransomvérových útokov bolo zameraných na priemyselný sektor.
- Až 43 % útokov je definitívne sústredených na malé podniky, ktoré predstavujú väčšinu slovenského trhu.

Áno, takmer polovica kybernetických útokov sa sústreďuje práve na malé a stredné podniky, pričom až 51 % týchto firiem nealokuje takmer žiadne finančné prostriedky na kybernetickú bezpečnosť a ochranu.

Prečo je to alarmujúce

Ilustrujme to na zdanlivo (!) triviálnom príklade. Každá firma denne využíva e-mailovú komunikáciu. A aj keby sa mohlo zdať, že e-maily, ktoré firma dostáva, uškodiť nemôžu, až 94 % škodlivého softvéru sa šíri práve prostredníctvom nich. Pre útočníkov je to jeden z najjednoduchších spôsobov ako sa dostať do firemnej siete. Zaujímajú ich najmä e-mailové servery, ktoré sú prenajímané od hostingových spoločností, pretože sú zjavne miestom najmenšieho odporu. A poďme ďalej: útočníci sa naučili prenášať škodlivý obsah aj v súboroch, ktoré sú historicky povolené. Office dokumenty ako Word, Excel, PowerPoint či PDF tvoria dnes v e-mailoch až polovicu škodlivých príloh.
Fakt, že 95 % úspešných útokov je výsledkom ľudského zlyhania, je na stole.
Kybernetické útoky sú reálnou hrozbou, preto by mala byť kybernetická bezpečnosť prioritou každej firmy bez ohľadu na jej veľkosť. Elementárne kroky predstavujú investovanie do moderných bezpečnostných riešení a vzdelávania zamestnancov.

Ako sa brániť útokom? Spôsoby GAMO pomoci

Predstavíme vám dva vhodné bezpečnostné nástroje, ktoré sa dajú na ochranu zariadení a sietí pred kybernetickými hrozbami efektívne využívať: Microsoft 365 Defender a ESET Protect. Reprezentujú zabezpečenie pred vírusmi, malvérom, ransomvérom a ďalšími škodlivými softvérmi.

Oba tieto nástroje sú si v niečom podobné, no líšia sa usporiadaním, farebnosťou alebo grafickými prvkami. Ponúkajú rovnocenné základné funkcie ako je skenovanie systému, detekcia škodlivého softvéru a ochrana pred ransomvérom.
Microsoft Defender prináša navyše aj rozšírené funkcie, napríklad ochranu prehliadania s využitím technológie SmartScreen, ochranu e-mailového klienta či integrovaný firewall.
ESET Protect zase disponuje pokročilými možnosťami konfigurácie a správy, ktoré by mohli byť vhodnejšie pre firmy s vlastnými IT oddeleniami a komplexnými bezpečnostnými požiadavkami.
Poďme sa pozrieť na každý z týchto nástrojov samostatne.

Microsoft 365 Defender

Komplexný balík služieb pre pokročilú kybernetickú ochranu a detekciu hrozieb organizácií, s názvom Microsoft 365 Defender, je určený pre cloudové služby ako napríklad Exchange Online, SharePoint, Teams a podobne. Poskytuje najmä efektívne a výkonné monitorovanie a správu bezpečnosti. Prehľadný a intuitívny dashboard zobrazuje dôležité detailné informácie v podobe grafov a diagramov pomáhajúcich sledovať všetky bezpečnostné aspekty, zhromažďuje a analyzuje logy, identifikuje hrozby a prezentuje ich v časovo usporiadaných prehľadoch. Umožňuje včasne reagovať na vzniknuté incidenty a chrániť systémy firmy.
Microsoft 365 Defender následne sleduje nielen servery a pracovné stanice, ale aj sieťové prvky a IoT zariadenia. Jeho schopnosti teda presahujú firemné siete. Dokáže monitorovať a chrániť zariadenia kdekoľvek na internete, vrátane súkromných zariadení a systémov, rovnako aj Linux.
Integrovaná platforma zároveň poskytuje informácie o vzniknutých incidentoch či bezpečnostných hrozbách a sleduje ich závažnosť. Okrem toho dokáže sledovať aj vnútorné aktivity ako je konfigurácia služieb a potenciálne riziká spojené so „sivým“ IT. Poskytuje i dôležité odporúčania ako incidenty riešiť alebo ako zabrániť ich vzniku.
Treba však pripomenúť, že len samotné zakúpenie platformy nepostačí. Správna implementácia a pravidelné monitorovanie, ako aj vzdelávanie zamestnancov, tvoria dôležitú súčasť kybernetickej bezpečnosti podniku.
S robustným nástrojom, akým Microsoft 365 Defender rozhodne je, bude bezpečnosť podniku v spoľahlivých rukách, čo iste ocenia nielen veľké spoločnosti, ale aj malé firmy.

Microsoft 365 Defender a vzdelávanie

Zamestnanci by mali byť v oblastiach kybernetickej bezpečnosti dostatočne vzdelávaní a informovaní. Ako píšeme vyššie: až 95 % úspešných útokov spôsobuje podľa štatistík spoločnosti Microsoft ľudský faktor. Tu môže Microsoft 365 Defender ponúknuť tréningy na zvýšenie povedomia a schopností zamestnancov v oblasti kybernetickej bezpečnosti. Bezpečnostné tréningy sa zameriavajú na simuláciu rôznych phishingových útokov, aby ich zamestnanci pochopili a rozpoznali. Cieľom je naučiť premýšľať a reagovať ešte pred otvorením podozrivých odkazov a príloh. Alarmujúce totiž je, že zamestnanci otvárajú podozrivé prílohy už za 10 sekúnd od doručenia e-mailu. Integrita a bezpečnosť firmy sú vtedy v nezabezpečenom priestore v jednom z najvyšších stupňov ohrozenia.

ESET Protect

Veľmi úspešnú alternatívu k Microsoft Defenderu predstavuje balík služieb ESET Protect. Dalo by sa povedať, že riešenie poskytuje 95 % toho, čo bežný malý a stredný podnik na Slovensku potrebujú. V niektorých prípadoch môže byť ESET aj lacnejším variantom v porovnaní s Microsoftom a jeho implementácia a nasadenie sú rýchlejšie.
Kým Microsoft Defender je integrovaný do operačného systému Windows, ESET Protect reprezentuje samostatný bezpečnostný produkt, hodí sa teda aj pre užívateľov Linuxu alebo Lotus Notes IBM. Poskytuje ochranu e-mailového servera i služby Microsoft 365. ESET disponuje menším rozsahom správy zariadení než Defender, ktorému v tomto smere naozaj nemôže veľmi konkurovať, avšak pri malých podnikoch na Slovensku iste postačí. Nastaviť základné obmedzenia typu blokovania USB zariadenia, Bluetooth na mobiloch, alebo obrazovky aplikácie Teams, budú pre daný účel bezpečnosti v mnohých prípadoch postačovať.

Čokoľvek si vyberiete, vždy len správne urobíte

Pri výbere medzi týmito dvoma nástrojmi kybernetickej ochrany by mala každá firma zvážiť svoje potreby a požiadavky. Zaváži iste najmä porovnanie funkcií, integrácie s existujúcimi systémami, používateľské rozhranie, podpora i cena. Pre veľkú prevádzku s potrebou komplexných možností správy a konfigurácie by mohol byť ESET Protect tou správnou voľbou. Ak firma preferuje integrované riešenie, súčasť operačného systému s rozšírenými funkciami, zvolí zase Microsoft Defender.

Je však tiež nutné poznamenať, že bezpečnostný softvér sa neustále vyvíja, aktualizuje a vylepšuje. Vhodné je tiež zvážiť aj ďalšie bezpečnostné opatrenia ako je firewall, zálohovanie údajov alebo výber správnej politiky zabezpečenia.
Netreba zabúdať, že každá zodpovedná firma by mala mať okrem antivírusu nasadené aj XDR alebo EDR riešenia, čím zabezpečí bezpečnostný monitoring svojej infraštruktúry a zariadení. Aj na to poslúži jeden zo spomínaných dvoch bezpečnostných nástrojov. Vašu sieť a zariadenia síce nemusia určité útoky obísť, no zabezpečia dostatok času na zareagovanie. Bezpečnostné nástroje slúžia totiž upozorňujú na hrozbu už do niekoľkých minút, čím získa každá bezpečnostne zodpovedná spoločnosť čas na zastavenie potenciálneho útoku.

Spoločnosť GAMO poskytuje nielen implementáciu bezpečnostných nástrojov spoločností, no preberá aj starostlivosť o bezpečnostný monitoring, detekciu a reakcie na incidenty v rámci poskytovanej SLA služby – všetko garantovane a na kľúč, s odbornými znalosťami a skúsenosťami.
Zabezpečujeme, aby boli spoločnosti z našej klientely pripravení a dokázali adekvátne zareagovať aj odolávať potenciálnym kybernetickým útokom.
Čas a pripravenosť, to sú dnes nielen v kyber priestore jednoducho kľúčové heslá hýbajúce svetom.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR


Tomáš Tuba
tomas.tuba@gamo.sk

Sme TUBAPACK, a.s. Sme zodpovední ku klientovi, našej histórii aj zamestnancom

Národný bezpečnostný úrad Slovenskej republiky firmy s mesačnou pravidelnosťou varuje: Zvýšte kybernetickú bezpečnosť! Cieľom viac ako 70 percent zo všetkých kybernetických útokov sú malé a stredné podniky. Presne tie, čo väčšinovo najpoctivejšie plnia požiadavky zákazníkov. V čom spočíva ich zraniteľnosť a čo s tým?

V prvom rade: zraniteľnosť akejkoľvek spoločnosti spočíva v podcenení ich významu pre kybernetických zločincov.
V druhom rade: tu sa naozaj oplatí zainvestovať do účinnej ochrany a spoľahnúť sa na špecialistov.
Výsledkom je: investícia = zisk. Ochránim sa, som chránený, a v prípade likvidačného útoku ochránim svoju dlhoročnú prácu aj zamestnancov.
Takto zodpovedne a podnikateľsky ukážkovo sa správa aj TUBAPACK, a.s., najväčší výrobca hliníkových a laminátových túb v regióne Strednej Európy, poskytujúci produkty a služby zákazníkom kozmetického, chemického, potravinárskeho a farmaceutického priemyslu. Gratulujeme!
Predstavitelia spoločnosti si uvedomujú význam a dôležitosť postupného zvyšovania IT bezpečnosti, jej preventívnych opatrení, a z pohľadu kybernetickej odolnosti vopred ošetrujú zraniteľnosti. O ich správnych rozhodnutiach sme sa zhovárali s Petrom Trubenom, IT Administrátorom v spoločnosti TUBAPACK, a.s.

Zodpovednosť a zraniteľnosť sa javia ako opozitá, vo Vašom prípade ale idú ruka v ruke. Ako cesta ku kybernetickej zodpovednosti vašej firmy eliminujúcej zraniteľnosť začala?

Analýzou a testami zraniteľnosti. Čiže dôkladným overením stavu našej kybernetickej odolnosti. Krok po kroku? Úvodná analýza zmapovala stav a testy zraniteľnosti identifikovali niekoľko zraniteľností. Po získaní výsledkov z analýzy sme si prešli jednotlivé body, vysvetlili nedostatky a bezpečnostné riziká, a skonzultovali odporúčania na nápravu súčasného stavu. Súbežne sme spustili proof of concept bezpečnostného monitoringu na technológii Security Onion. Výsledky z monitoringu, zo zbierania logov a ich vyhodnotenie doplnili výstupy analýzy a testov zraniteľnosti.

> Bezpečnostný monitoring by mal byť súčasťou riadenia kybernetickej a informačnej bezpečnosti v každej organizácií, bez ohľadu na jej veľkosť a legislatívne povinnosti. Pri absencii takéhoto systému má organizácia nulovú alebo významne zníženú tzv. visibilitu, čiže prehľad nad bezpečnosťou vlastnej infraštruktúry.

Dostali sme tak sumárny výstup k stavu bezpečnostnej odolnosti našej infraštruktúry a na jeho základe mohli postupne odstraňovať a sanovať miesta prieniku možných útokov: vymenili sme firewall, upgradovali ESET licencie, a pristúpili sme aj k nevyhnutným nastaveniam a segmentácii siete.
Už prvými prijatými opatreniami sme zvýšili úroveň bezpečnosti našej spoločnosti o niekoľko desiatok percent. Zlepšenie štandardov pre biznis kontinuitu a zamedzenie narušenia dôvernosti, integrity a dostupnosti údajov, je výsledkom.

Prvou fázou skúmania bezpečnosti infraštruktúry je monitoring. Aké to je pre úspešnú firmu poznať prvé výsledky?

Dobré, vieme kam ísť. S konzultantom na bezpečnosť z GAMO sme viedli od prvej chvíle rozhovory o možnom spôsobe pokrytia ďalšej úrovne bezpečnosti. A výsledkom bola ponuka nasadenia Proof of Concept bezpečnostného riešenia Security Onion, ktorú sme uvítali.
Analýza – centralizovaný zber dát a monitoring, prebiehala v reálnej prevádzke a na vopred dohodnutej časti infraštruktúry. Mesačné nasadenie nástroja bezpečnostného monitoringu nám umožnilo získať prehľad o celkovom dátovom toku, o počte logov a zdrojoch dát, ktorým je naša podniková sieť vystavená. Pilotná fáza poslúžila na odhalenie špecifík nášho prostredia aj niekoľkých prípadov potenciálne nebezpečnej aktivity v rámci našej siete. Mohli sme sa ‚na vlastné oči' presvedčiť o funkčnosti bezpečnostného monitoringu a získali sme parametre pre rozhodnutie a správny výber produkčného hardvérového riešenia do budúcnosti. To dnes môžeme škálovať podľa reálnych výsledkov práve z PoC.

PoC je niekedy zbytočným strašiakom, neobávali ste sa napríklad výpadku infraštruktúry?

Určite nie. Stačilo, že sme poskytli základnú súčinnosť poskytovateľovi pri inštalácii fyzického servera do racku v serverovni a pri pripojení do siete a vybraných segmentov. Potom prebehlo nastavanie monitorovacieho rozhrania na serveri a vybraných sieťových prvkov, a tiež nastavenie logovania na externý sever. Poskytovateľ nás ubezpečil, že celý proces nepredstavuje žiadne zvýšené riziko pre našu infraštruktúru, že ani v prípade úplného výpadku systému nemôže dôjsť k ohrozeniu bezpečnosti prevádzky infraštruktúry alebo informačných systémov, a tak aj bolo.
A k tomu strašiaku: boli sme ubezpečení, že v prípade výpadku by sme stratili len dočasne visibilitu prostredia, čiže by išlo o návrat do stavu pred spustením systému. Nebolo nad čím váhať.

Security Onion je vlastne taká sonda dovnútra spoločnosti, čo ste zistili z jej pilotného nasadenia?

Report sumarizoval zistenia o stave siete a zraniteľných aktívach, predstavujúcich potenciálnu cestu k útoku alebo problémov so sieťou. Dostali sme napríklad upozornenie na klienta v lokálnej sieti, ktorý používa nevhodné stránky pre dospelých - pričom, isteže, mohlo sa jednať aj o malvér, ktorý odosiela takéto DNS dotazy – a odporučenie vďaka Security Onion bolo: Rýchlo skontrolujte zariadenia a zablokujte aktivitu. Tak sme aj urobili.

Súčasťou balíka štartovacích bezpečnostných služieb sú práve aj testy zraniteľnosti. Ocenili ste ten benefit?

Samozrejme. Jeho úlohou je vyhľadať počítačové a sieťové systémy a zariadenia s existujúcimi technickými zraniteľnosťami a dopadom na stabilitu a bezpečnosť informačných systémov a dát. Prvý test zraniteľnosti u nás bol vykonaný s cieľom identifikovať riziká a detekovať slabé miesta. Následne po aplikovaní nápravných opatrení bude vykonaný aj kontrolný test, ten nás ešte čaká. A z vykonaných testov zraniteľnosti vyplynulo, že veľké množstvo zistených zraniteľností je možné odstrániť úplne jednoducho - pravidelným aktualizovaním systémov.

Ochrana pred kybernetickými hrozbami je kľúčová pre každú organizáciu. Podľa štatistík, ktoré uvádza Microsoft, je až 95% úspešných útokov spôsobených ľudským faktorom. Stretli ste sa s týmto tvrdením?

Áno. A rýchlo sme pochopili, že nasadenie bezpečnostného riešenia bude neúčinné a nesplní svoj účel, ak naši zamestnanci nebudú o tejto problematike informovaní.

> **V priemere 1 hodina a 42 minút stačia na to, aby sa útočník po ‚hacknutí' jedného zo zariadení spoločnosti dostal do zvyšku firemnej siete. Zaujímavosťou pritom je, že používateľ či celá napadnutá firma ani netušia, že majú v systéme narušiteľa. Výnimkou vôbec nie je to, že útočník sa v systéme len tajne ‚prechádza' a oficiálne nič nespraví. A po celé nasledujúce týždne či mesiace si napadnutá spoločnosť vôbec nemusí všimnúť, že je hacknutá.**
>
> Zdroj: štúdia Microsoft Digital Defense Report 2023

Preto sme sa zamerali na zvýšenie povedomia zamestnancov v oblasti kybernetickej bezpečnosti školeniami s prihliadnutím na rôzne pracovné pozície.

Splnili školenia účel a celofiremnú zodpovednosť?

Mali sme ich vo viacerých cykloch. Vzdelávanie pre bežných užívateľov IT z radu zamestnancov bolo zamerané na osvojenie si pojmov a základných pravidiel kybernetickej bezpečnosti a postupov na predchádzanie vzniku incidentov. V ich prípade sme sa sústredili hlavne na oblasť bezpečnostných rizík, spojených s ochranou firemného know-how a citlivých údajov, a zároveň na prezentáciu reálnych príkladov z oblasti kybernetickej kriminality. Naším cieľom bolo, aby si pracovníci osvojili pravidlá bezpečného správania sa v kybernetickom priestore, dokázali rozpoznať prvky phishingových kampaní, dodržiavali zásady ochrany identity (heslá, MFA, e-mail, sociálne siete a podobne). Vzdelávanie pre tímlídrov a IT špecialistov bolo rozšírené už aj o implementáciu bezpečnostných opatrení, o monitoring, vyhodnocovanie a riadenie bezpečnostných incidentov.
Ocenili sme prístup, keď poskytovateľ školenia priblížil problematiku a aplikoval riziká kybernetickej bezpečnosti na súkromný život zamestnancov. Webové stránky aj sociálne siete sú totiž plné nebezpečného obsahu. Kliknutie na zdanlivo výhodnú ponuku môže spustiť škodlivý softvér, ktorý sa následne šíri ďalej aj na príbuzné zariadenia. Je to naozaj tak - ľudia sú podvodníkmi klamaní a prichádzajú o svoje peniaze. V e-mailovej schránke si na pravidelnej báze nachádzajú podvodné správy o predvolaniach na súd alebo políciu, falošné informácie o doručení zásielok, o neočakávaných finančných ziskoch alebo naliehavých žiadostiach o podporu. Preto školenie splnilo účel dvojnásobne – v zodpovednosti vo firemnom správaní sa v IT priestore, ale aj súkromne pre našich zamestnancov. Navyše, ak poukážete na útočné kampane a vystríhate ich pred škodlivým obsahom, ktorý by ich mohol pripraviť o vlastné peniaze, súkromie aj identitu, dokážu byť potom ostražitejší a dodržiavať pravidlá aj vo firemnom prostredí.

Počúvať zodpovedného manažéra o nastaveniach spoločnosti je obohacujúce nielen pre zamestnanca. Aké sú vaše ďalšie plány k rozvoju?

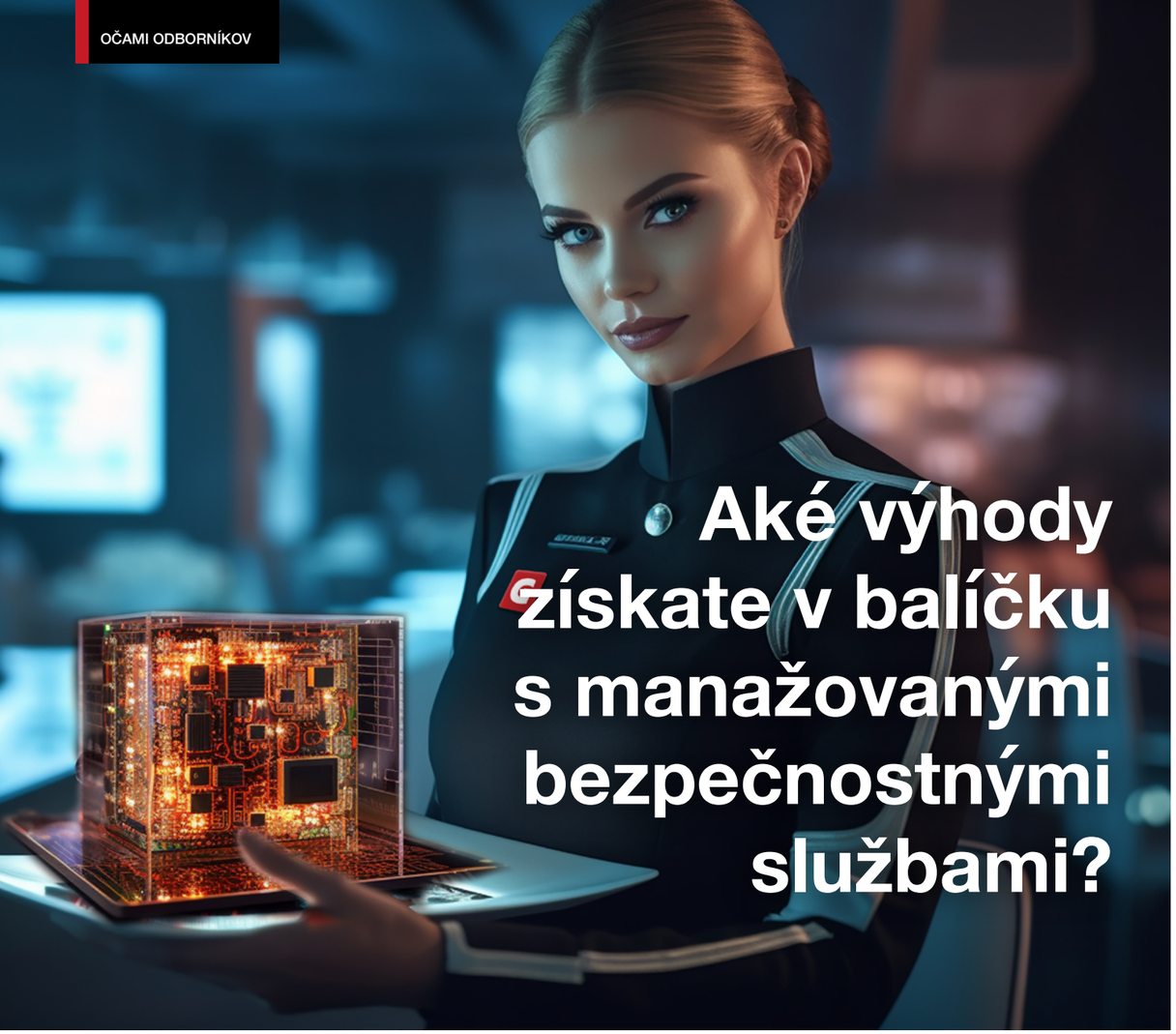
Spoločnosť TUBAPACK, a.s., investuje do rozvoja IT infraštruktúry dlhodobo podľa potrieb spoločnosti.

Denne naše pracovné e-mailové schránky zaplaví množstvo informácií. Útočné phishingové kampane nejdú mimo nás, nevynímajú hranice Slovenska, napadajú aj naše firmy a e-mailové účty. Dokonca: práve na Slovensku si útočiace skupiny často trénujú svoje taktiky, učia sa a zdokonaľujú. Preto je dôležité, aby sme boli informovaní, a vedeli, ako sa v online svete chrániť. Základom je byť pripravený na všetky možné scenáre a vedeli ako sa brániť proti rôznym druhom útokov. Úplným základom je napríklad naučiť sa rozpoznávať podvodné e-maily a webstránky, zabezpečiť prístupové kontá a súbory, a byť opatrný pri otváraní neznámych príloh.

V blízkej dobe chceme naďalej držať krok s narastajúcimi nárokmi: či už legislatívy ohľadom kybernetickej bezpečnosti, alebo s vývojom v IT technológiách pre efektívnejšie spracovanie výroby. Máme preto rozpracovaných niekoľko riešení. Samozrejmosťou je modernizácia výpočtovej techniky, ktorá sa v posledných rokoch stáva akosi rýchlejšie zastaralou (rýchlosť vývoja v oblasti IT sa stupňuje a dáva nám tým nové možnosti, ktoré môžeme uplatniť pri výrobe hliníkových, či laminátových túb). Dokončili sme cieľ zvirtualizovať dosluhujúce servery a zlepšiť zálohovanie dát. Veď dáta spoločnosti sú tou najcennejšou komoditou.
Do budúcna uvažujeme využiť niektoré z cloudových riešení pre uchovávanie firemných dát mimo spoločnosti ako aj možnosť komunikovať s našimi zákazníkmi pomocou vlastných bezpečnostných úložísk s výmenou dát a grafických predlôh. Momentálne musíme pre nedostačujúce priestorové kapacity rozšíriť spoločnosť o ďalšie výrobné priestory, do ktorých je nutné zapracovať IT infraštruktúru (zabezpečiť automatizáciu vstupov, monitorovanie kamerovým systémom, prepojenie na existujúce sieťové a bezdrôtové prvky). Minulý rok sme spustili do prevádzky linku na výrobu hliníkových túb s poradovým číslom 10 a momentálne pracujeme na dokončení a spojazdnení linky s číslom 11. Zámerom je pokryť dopyt po hliníkových tubách na trhu a rozšíriť našu ponuku výroby o nové priemery a veľkosti túb. V neposlednom rade sa snažíme o automatizáciu výroby. Dokončujeme automatizáciu balenia túb a nepretržite implementujeme do výroby nové prvky (tablety, PDA čítačky na QR kód, prenosné tlačiarne s bluetooth pripojením, kamerové systémy na kontrolu kvality túb priamo na výrobných linkách) vedúce k zefektívneniu výroby.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Branislav Lupták
branislav.luptak@gamo.sk



Aké výhody získate v balíčku s manažovanými bezpečnostnými službami?

Manažované služby sa vzťahujú na outsourcing každodennej správy IT infraštruktúry alebo vybranej časti z nej. Špecializovaní partneri ponúkajú týmto spôsobom celý rad služieb vrátane správy sietí a serverov, kybernetickej bezpečnosti, zálohovania a obnovy dát, cloud computingu aj IT podpory.
Mnohé firmy majú obmedzené IT zdroje a odborné znalosti, preto môže byť pre nich správa IT infraštruktúry zložitá. Ide o časovo a finančne náročnú úlohu, odvádzajúcu pozornosť a zdroje od hlavných obchodných činností. Tak načo ju riešiť?

Obstaraním manažovaných služieb firmy prekonávajú práve tieto výzvy a získavajú prístup k odborným znalostiam v oblasti IT, ktoré by inak boli pre nich nedostupné. Poskytovatelia manažovaných služieb ponúkajú outsourcing IT služieb zákazníkom za mesačný poplatok eliminujúci investovanie do drahej IT infraštruktúry a personálu. Týmto spôsobom môžu spoločnosti ušetriť náklady, zvýšiť produktivitu a získať prístup k odborným znalostiam v oblasti IT.
Pomenujme si výhody, ktoré firmám manažované služby prinášajú, a dôvody, ktoré ich k nasadeniu priviedli.

TOP 5 benefitov prečo zaviesť manažované služby

Šetrenie nákladov

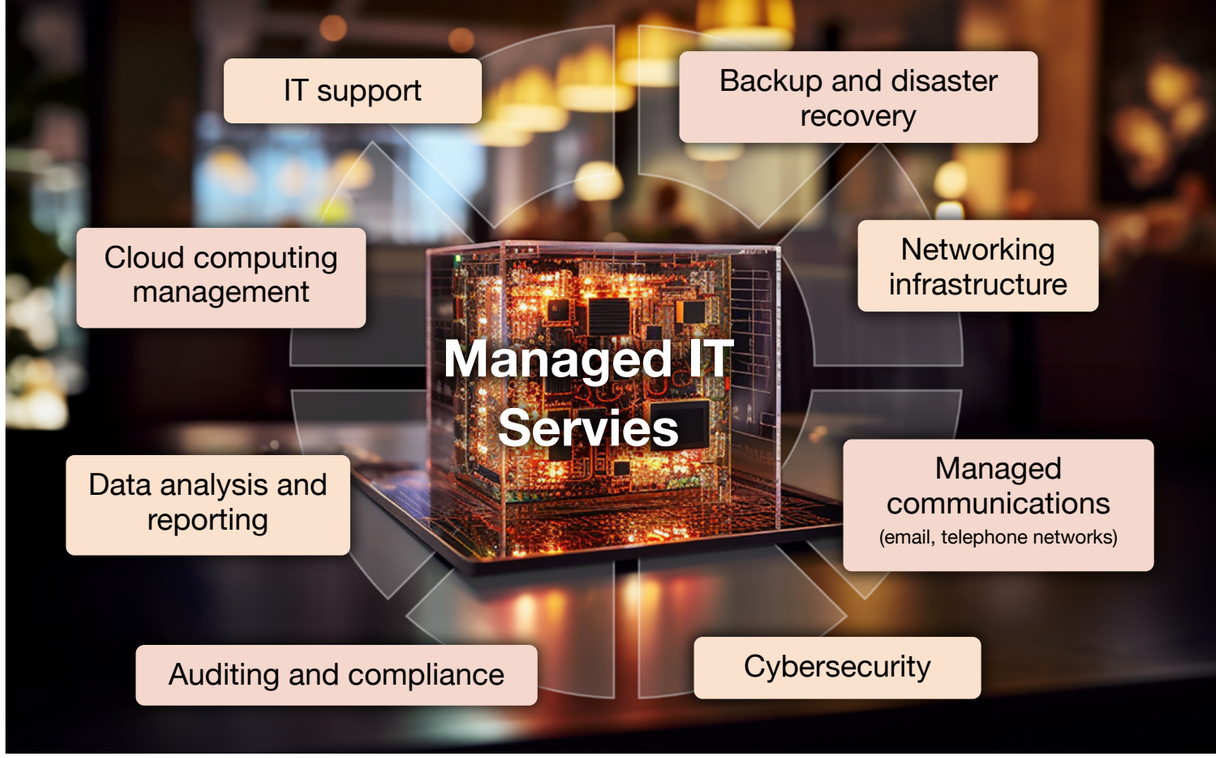
Poskytovatelia manažovaných služieb ponúkajú malým a stredným podnikom nákladovo efektívne riešenia. Namiesto investícií do drahej IT infraštruktúry a personálu môžu podniky platiť fixný poplatok za IT služby, ktoré zahŕňajú údržbu, aktualizácie a podporu. Poskytovatelia manažovaných služieb majú odborné znalosti a nástroje na optimalizáciu IT infraštruktúry, čo znižuje prestoje a maximalizuje produktivitu.

Škálovateľnosť

Manažované služby možno rozširovať alebo znižovať podľa toho, ako sa menia obchodné potreby. S rastom biznisu alebo počtu zamestnancov môžu pridávať ďalšie služby alebo používateľov bez toho, aby museli investovať do nového hardvéru alebo softvéru. Škálovateľnosť umožňuje malým a stredným podnikom prispôsobiť sa meniacim sa podmienkam na trhu bez vzniku dodatočných nákladov na IT.

Zvýšená bezpečnosť

Hrozby kybernetickej bezpečnosti sú pre všetky firmy bez rozdielu veľkým problémom. Poskytovatelia manažovaných služieb ponúkajú riešenia kybernetickej bezpečnosti, ktoré zahŕňajú detekciu hrozieb, prevenciu a reakciu. Zároveň majú odborné znalosti a nástroje na zabezpečenie IT infraštruktúry malých a stredných podnikov, čím znižujú riziko kybernetických útokov a únikov údajov.



Zlepšenie produktivity

Poskytovatelia manažovaných služieb môžu pomôcť malým a stredným podnikom zvýšiť produktivitu tým, že zabezpečia optimalizáciu a bezproblémový chod IT infraštruktúry. Poskytujú proaktívnu údržbu, aktualizácie a podporu, čím skracujú prestoje a zabezpečujú, že systémy zostávajú v prevádzke (business continuity).

Prístup k IT expertom

Odporúčame: Uchráňte sa pred stresovými situáciami a s dôverou sa oprite o certifikovaného IT partnera. Prenechajte mu riešenie a výkon zložitých technických IT úloh. Poskytovatelia manažovaných služieb majú odborné znalosti a nástroje na efektívnu správu IT infraštruktúry a služieb. Malé a stredné podniky môžu využiť tieto odborné znalosti a získať prístup k IT odborníkom, ktorí im pomôžu optimalizovať a rozvíjať ich vlastnú IT infraštruktúru aj služby.

Bola dôvodom pandémia?

Mnohé malé a stredné podniky začali využívať manažované služby ako reakciu na logistické riešenia priebehu pandémie Covid-19. Nevyhnutne potrebovali prijať bezpečnostné opatrenia, ktoré umožňovali vzdialenú správu ich IT prostriedkov. V prípade väčších firiem, ktoré majú zložitejšie IT potreby, to mohlo byť aj kvôli nedostatku vlastných IT kapacít.
V neistom a napätom ekonomickom prostredí podniky často čelia výzve realizovať okamžité úspory nákladov na IT. Manažéri, konatelia musia určiť ako pristupovať k znižovaniu nákladov spôsobom, ktorý neohrozí kybernetickú odolnosť, napr. pred ransomvér útokmi zasahujúcimi firmy bez ohľadu na veľkosť. Väčšina firiem má problém odraziť kybernetické útoky práve kvôli malému počtu v tejto problematike kvalifikovaných pracovníkov.
Výsledky rôznych prieskumov naznačujú, že poskytovatelia manažovaných služieb môžu výrazne uľahčiť život práve menším firmám. A to nielen poskytovaním IT podpory pre vzdialenú prácu zamestnancov či zabezpečením vzdialenej správy z cloudu. Malé a stredné podniky sa pri správe IT riešení čoraz viac spoliehajú na poskytovateľov manažovaných služieb práve v oblasti bezpečnostných služieb a kybernetickej odolnosti.

Nekupujte iba licencie

Okrem služieb poskytovaných certifikovanými IT špecialistami „bezpečákmi“, ktorí majú bohaté skúsenosti s implementáciou, nastavením a bezpečnostným monitoringom, vám v GAMO spolu s manažovanou službou v jednom balíku poskytneme aj ESET licencie. Nemusíte ich kupovať samostatne a viazať si prostriedky. V rámci mesačného poplatku uhradíte potom iba faktúru za službu podľa reálnej spotreby a využitia licencií. Vždy máte prispôsobený počet aj druh používaných licencií podľa aktuálnej požiadavky.
Zakúpte si manažovanú službu s požadovaným počtom licencií a my navyše:

- Zabezpečíme technologickú komplexnosť poskytovateľa manažovaných služieb, ktorý poskytuje sieťové služby, infraštruktúru, bezpečnostnú odolnosť, disponuje cloud prostredím a IT podporou 24x7.
- Rozptýlime vaše obavy o bezpečnosť.
- Poskytneme flexibilitu súvisiacu s financiami, presunom IT nákladov - z investičných (CAPEX) do prevádzkových (OPEX) nákladov.

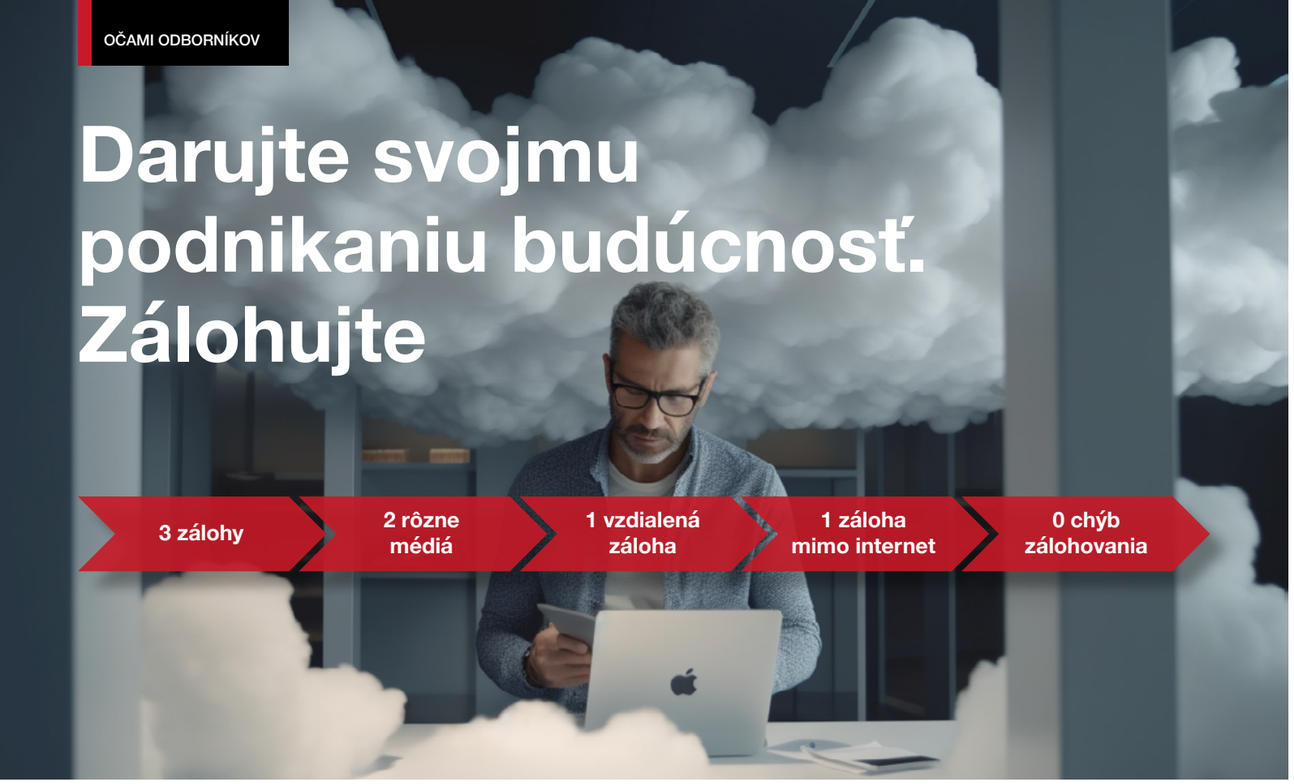
Platťte len za to, čo skutočne používate

Žiadne paušálne poplatky či dlhodobá viazanosť. Získate flexibilitu pri pridávaní alebo odstraňovaní licenčných jednotiek a prechod na vyššiu úroveň bez výrazného zvýšenia nákladov.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Gabriela Repatá
gabriela.repata@gamo.sk

Darujte svojmu podnikaniu budúcnosť. Zálohujte



Zálohovaním dát dneška a minulosti investujete do budúcnosti.

Backup ako služba alebo Objektové úložisko? Účinným spôsobom ochrany dát pred ransomvérom je ich pravidelné zálohovanie.

Zlyhanie hardvéru, kybernetický útok, nesprávny konfiguračný zásah či zlyhanie ľudského faktora. To všetko môže zapríčiniť výpadok funkčnosti IT systémov a tým stratu produktivity, tržieb, či trvalé poškodenie reputácie.
S rastúcim počtom útokov je čoraz viac na mieste uvažovať o vyššej ochrane dát vo firemnej politike, a to najmä spôsobom ich rýchlej obnovy. Aj v prípade, že nepodceňujete význam kybernetických hrozieb a pracujete na odstránení zraniteľností a na zvyšovaní úrovne zabezpečenia, potrebujete riešenia, ktoré minimalizujú následky ľudského zlyhania. S týmito výzvami vám môžu pomôcť služby zálohovania do cloudu. Stačí si vybrať riešenie, typ služby v závislosti od potrieb firmy, ale aj požiadaviek na zálohovanie, retenciu a prístup k dátam.
Hľadáte účinný spôsob ochrany dát pred ransomvérom? Pravidelne zálohujte! Zálohovaním do cloudu získate istotu, že vaša kópia dát je v bezpečí pred akoukoľvek hrozbou, či už ide o neúmyselné zmazanie dát, externé kybernetické hrozby, alebo interné hrozby po personálnych zmenách.
Základným odporúčaním, ktorého funkciou je zabezpečiť ochranu dát pred stratou alebo poškodením, je princíp 3-2-1-1-0. Vysvetľovať ho väčšine z vás nemusíme, ak sa potrebujete predsa len trochu zorientovať, pozrite na titulný obrázok.

Tento princíp je najlepším pravidlom na ochranu pred ransomvérom, čo pomáha minimalizovať riziko straty údajov a zabezpečuje, že zálohovacie kópie sú spoľahlivé a použiteľné pri obnove dát.
Práve vzdialená záloha môže byť v jednej alebo viacerých cloudových službách.

Akú cloudovú službu zvoliť na zálohovanie?

Pre správnu voľbu zálohovacej služby je dôležité si povedať:
- čo chceme zálohovať,
- o akom objeme dát hovoríme,
- ako často sa majú dáta zálohovať,
- ako rýchlo potrebujeme opäť k dátam pristupovať.

Zároveň je dobré rozdeliť si dáta na tie, ktoré sa už nemenia, ako napr. dokumenty zo starších projektov, fotky, obrázky a dokumentácie, ktoré zálohujeme z dôvodu ich archivácie. A zálohy, ktoré obsahujú dáta, ku ktorým potrebujeme neustále pristupovať alebo pravidelne ich editovať.
Väčšinou sú to dáta, s ktorými aktívne pracujete v rámci každodenného biznisu. Potom si už jednoducho zvolíte službu, ktorá najlepšie sedí vašim požiadavkám:

- **Služba backup as a service** je zameraná primárne na zálohovanie a obnovenie dát. Je to outsourcovaná služba, ktorá zabezpečuje, že dáta sú pravidelne zálohované a uložené na bezpečných serveroch poskytovateľa služby, a zároveň sú rýchlo opäť dostupné v prípade potreby.
- **Object Storage, Objektové úložisko** je určené pre trvalé ukladanie a správu dát. Poskytuje dlhodobé úložisko pre veľké objemy dát a umožňuje prístup k nim prostredníctvom identifikátorov objektov.

Aký je medzi týmito službami rozdiel?

Tu je niekoľko hlavných rozdielov:

Prístup k dátam
Služba backup as a service často pracuje na báze zálohovania a obnovy súborov alebo blokových úrovní. Zálohy sú vytvárané pravidelne (napríklad každý deň inkrementálny backup a raz za niekoľko dní plná verzia) a môžu byť použité na obnovenie dát v prípade straty alebo poškodenia. Oproti tomu Objektové úložisko poskytuje prístup k dátam na úrovni objektov. Každý objekt má jedinečný identifikátor, ktorý sa používa na vyhľadávanie a manipuláciu s dátami. Je navrhnuté na ukladanie a správu veľkých objemov dát s možnosťou rôznych typov dát ako sú obrazy, zvukové súbory, videá a dokumenty.

Škálovateľnosť a úložný priestor
Služba backup as a service zvyčajne poskytuje obmedzený úložný priestor pre zálohy a často sa vyžaduje, aby sa dodržiavali určité limity. Kapacita úložiska je zvyčajne závislá od dohodnutého plánu služby. Objektové úložisko, naopak, je škálovateľné a poskytuje neobmedzený úložný priestor pre dáta. Môžete pridávať ďalšie objekty a zvyšovať kapacitu podľa potreby.

Správa a zabezpečenie dát
Služba backup as a service zabezpečuje pravidelné zálohovanie a obnovu dát podľa dohodnutých politík zálohovania. Používatelia nahrávajú svoje dáta na servery poskytovateľa, ktorý je zodpovedný za zálohovanie a správu týchto dát. BaaS poskytuje príjemné užívateľské rozhranie a zjednodušuje proces zálohovania a obnovy.
Object Storage: Objektové úložisko je typ úložiska, ktoré sa zameriava na ukladanie veľkého množstva dát vo forme objektov. Objekty majú unikátny identifikátor a môžu obsahovať rôzne typy dát ako súbory, obrázky, videá atď. Objektové úložisko poskytuje škálovateľnosť a umožňuje efektívne ukladať a spravovať veľké objemy dát.
Poskytovatelia BaaS zabezpečujú redundantné kópie dát, aby sa minimalizovala pravdepodobnosť straty dát v prípade havárie. Používatelia majú často prístup k rôznym zálohovacím bodom, z ktorých môžu svoje dáta obnoviť.
Objektové úložisko tiež poskytuje určitú úroveň zabezpečenia dát. Dáta v objektovom úložisku sú často duplikované na rôznych fyzických umiestneniach, aby sa minimalizovala strata dát v prípade výpadku. Prístup k dátam je zabezpečený prostredníctvom autentifikácie a autorizácie.

Retenčná politika a obnova dát
Služba backup as a service poskytuje možnosť nastaviť retenčnú politiku podľa potrieb klienta, ktorá určuje, ako dlho sú zálohy uchovávané. To umožňuje obnovu dát z rôznych časových okamihov v minulosti podľa potreby. Objektové úložisko sa zameriava na trvalé uchovávanie dát bez obmedzení časových rámcov. Dáta sú uložené dlhodobo a môžu byť sprístupnené v akejkoľvek časti ich životného cyklu.

Prístupnosť a rýchlosť obnovy
Služba backup as a service sa zameriava na rýchlu a spoľahlivú obnovu dát v prípade ich straty alebo poškodenia. Poskytovatelia služby často zabezpečujú rôzne mechanizmy pre obnovu, vrátane možnosti obnovy na rôznych miestach a v rôznych rýchlostiach. Táto služba je vyhľadávaná predovšetkým v prípadoch nevyhnutnosti rýchleho prístupu k „živým“ dátam, ktoré sú dôležité pre fungovanie biznisu klienta.
Objektové úložisko je určené pre prístup k dátam na dlhodobú archiváciu a sprístupňovanie veľkého množstva dát. Rýchlosť obnovy môže byť nižšia v porovnaní so službou backup as a service, pretože je navrhnuté pre ukladanie a trvalú dostupnosť dát.
V digitálnej ére sa množstvo dát, ktoré organizácie zhromažďujú a spravujú, neustále zvyšuje. A preto v GAMO Cloud ponúkame pre našich klientov obe služby:

Služba BaaS umožňuje zálohovanie aplikácií z virtualizovaných systémov vo vašej infraštruktúre alebo u nás v cloude. Sami si určíte, ktoré kritické dáta chcete chrániť a čas, kedy má byť cloud záloha aktívna. Cez web portál pre zálohovanie máte v rámci tejto služby pod kontrolou všetky úlohy, politiku zálohovania, stav a výsledok jednotlivých úloh spolu s pravidelným reportingom. Zálohovať môžete manuálne alebo naplánovať automatické pravidelné zálohy. Dáta máme výhradne umiestnené na Slovensku a neopúšťajú krajinu. Zálohovanie používa End-to-End kryptovanie s využitím SSL, bez potreby nastavenia VPN. Dáta sú zakryptované ešte pred opustením vášho sieťového perimetra. Na BaaS si navyše môžete nastaviť vlastnú bezpečnostnú politiku. Na každú zálohu aj na každý server separátne retencie a šifrovania. Ceny za túto službu sú rovnaké ako má Amazon alebo Azure, rozdiel je v tom, že oni ešte účtujú objem prenesených dát, GAMO Cloud nie.

S3 Object Storage je cloudová služba, resp. spoľahlivé rozhranie pre bezpečné ukladanie obrovských objemov dát. Objektové úložisko je škálovateľné na neobmedzené množstvo dát, nemusíte sa obmedzovať v množstve, ktoré potrebujete ukladať a spravovať. Bez ohľadu na to, či ide o rozrastajúce sa transakčné dáta, rozsiahle multimediálne súbory alebo dáta zo senzorov Internetu vecí, objektové úložisko dokáže všetky efektívne zvládnuť. Zatiaľ službu poskytujeme len vo forme API. Ide o typ storage, ktorý primárne slúži na zálohovanie a archiváciu, bezpečné uchovávanie si dát. Viete si ho namapovať ako vzdialený disk do servera, ale nemôžete z neho spúšťať zálohované aplikácie, slúži vyslovene na odkladanie súborov.

To, čo určite poteší každého, je omnoho nižšia cena, a nie na úkor kvality služby. Objektové úložisko ponúka výrazné výhody v oblasti nákladov. Svojou schopnosťou škálovať sa znižujú náklady spojené s investíciami do drahých fyzických úložísk a správou zložitých infraštruktúr. Objektové úložisko tiež optimalizuje správu dát a znižuje administratívne náklady, čím uvoľňuje zdroje pre ďalšie kľúčové iniciatívy. My v GAMO neúčtujeme objem prenesených dát.
Objektové úložisko je navrhnuté s dôrazom na bezpečnosť a odolnosť voči chybám.

Zhrnutie

Služba backup as a service a objektové úložisko majú odlišné prístupy k zálohovaniu a správe firemných dát. Je dôležité vybrať si správne riešenie v závislosti od potrieb organizácie ako aj požiadaviek na zálohovanie, retenciu a prístup k dátam. Zabezpečenie dát je dôležitým aspektom oboch prístupov. BaaS poskytuje zálohovanie a redundantné kópie dát na minimalizáciu straty dát v prípade havárie. Objektové úložisko zabezpečuje dáta prostredníctvom duplikácie a autentifikácie/autorizácie prístupu.

Potrebujete poradiť?

Sme tu pre každého, kto si uvedomuje dôležitosť zálohovania. Či už sa rozhodnete pre zálohovanie a obnovu dát ako službu, alebo vás presvedčí škálovateľné úložisko pre ukladanie veľkých objemov dát vo forme objektov, spolu navrhneme optimálne riešenie s najlepším pomerom účel/cena/bezpečnosť.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR


Jana Kohárová
jana.koharova@gamo.sk

Power BI efektívne režíruje dátový svet malých aj veľkých podnikov

Nestrácajte už čas zdĺhavými exportami dát, nastavovaním formátov alebo hľadaním chýb v nekonečných výkazoch a reportoch. Miesto toho jednoducho popíšte svoju požiadavku a čo presne očakávate od interpretácie dát.

O cloudovej technológii od Microsoftu s názvom Power BI (Power Business Intelligence) ste už možno počuli. Efektívne nástroje na spracovanie a analýzu obrovského množstva dát sú v dnešnom digitálnom veku pre riadenie firmy dôležité. Power BI je jedným z najpopulárnejších nástrojov na trhu, ktorý to umožňuje. Ponúka používateľom spôsob ako premieňať zozbierané dáta na zmysluplné a navzájom poprepájané informácie. Poďme sa preto pozrieť na to, aké výhody služba Power BI prináša firmám i jednotlivcom.
V prvom rade tento praktický cloudový nástroj umožňuje firemné dáta jednoduchým spôsobom analyzovať a vizualizovať. Poskytuje tak prehľad o celej organizácii. Široké možnosti prispôsobenia, vytváranie analýz v reálnom čase, aj integrované prvky zabezpečenia a správy dát robia z Power BI prínos pre všetky firmy, ktoré chcú zrýchliť a zlepšiť svoje rozhodovacie procesy.
V praxi zbiera podnik dáta z rôznych systémov v rámci prevádzky, ekonomiky, obchodu a podobne. Vyhodnocovať sa tak musí množstvo rôznorodých údajov, aby mal manažment prehľad o tom, čo sa vlastne v podniku deje. Pomocou Power BI dokáže firma prepájať stovky rôznych zdrojov dát, zjednodušovať ich spracovanie, a následne dáta analyzovať. Služba vytvára samostatné analýzy, prehľady, reporty i štatistiky.

Ktoré základné otázky vie Power BI zodpovedať:

- Ako sa darí našim maloobchodným prevádzkam;
- Aká je hodnota našich zásob;
- Ktoré produkty sa najviac predávajú a kde;
- Ktorá lokalita najviac prosperuje;
- Ktorá reklamná kampaň nám prináša konverzie, v ktorých kanáloch;
- Ako sa darí jednotlivým obchodným zástupcom pri predaji;
- Ako sa darí jednotlivým zákazkám.

Firmy sa s Power BI môžu pripojiť k rôznym systémom a zdrojom dát a navzájom ich skombinovať, vrátane tých, čo súvisia s prevádzkou, financiami či ľudskými zdrojmi.
Služba Power BI poľahky zintegrujete aj s ďalšími nástrojmi od Microsoftu ako sú Excel a SharePoint. Možno ju používať i v spojení s inými dátovými službami. Celkovo tak ide o flexibilný a výkonný nástroj analýzy a vizualizácie údajov, ktorý môže firmám pomôcť prijímať rozhodnutia na podkladoch z kvalitnejších a prepojenejších informácií.

Výhody Power BI

Jednou z výhod platformy je možnosť analýzy dát v reálnom čase, keď sa reporty následne dajú zdieľať a zverejňovať online. Rôzne pracovné tímy tak môžu v reálnom čase spolupracovať a zdieľať len relevantné informácie.
Ďalšou výhodou sú integrované bezpečnostné funkcie. Zdieľaním reportov online obchádza platforma otváranie príloh v e-mailoch, kde hrozia napríklad strety s vírusmi. Práva pre otváranie a čítanie reportov sú nastaviteľné a pracovník dostane prístup, povolený len do úrovne zodpovedajúcej jeho pracovnej pozícii. Zabudovaná správa a nastavenia práv používateľov je určite bezpečným a škálovateľným riešením pre organizácie všetkých veľkostí.
Po tretie: reporty sa dajú prezentovať a sledovať aj pomocou mobilných zariadení alebo tabletov. Budete tak neustále informovaní o dôležitých biznis parametroch firmy. Prostredníctvom Power BI dokážu používatelia vytvárať vlastné informačné panely s údajmi a zdieľať ich s ostatnými. K ovládacím panelom sa jednoducho dostanú na webe, mobile, alebo ich vložia do iných aplikácií.
A čo je dôležité: výkonné možnosti analýz, ktoré Power BI umožňuje, sprostredkujú a vytvoria aj veľmi zložité výpočty a štatistické vyhodnotenia.
Na zostavách údajov sa dá vzájomne spolupracovať a zdieľať ich v rámci firmy ďalej.

Najpodstatnejšie trendy pre business intelligence (BI)

Automatizácia a predikcia: Tento globálne narastajúci trend umožňuje používateľom BI generovať reporty a vizualizácie automaticky, bez nutnosti manuálneho vstupu. Môžu tak vytvárať vlastné reporty a informačné panely bez potreby zásahu IT alebo dátových analytikov. Power BI je obľúbená najmä vďaka prívetivému používateľskému rozhraniu a funkcii drag-and-drop.
Interaktívne vizualizácie: Dôležitý trend umožňujúci používateľom priamo v reporte meniť parametre a sledovať zmenu výsledku.
Cloudové technológie: Prístup k dátam prakticky odkiaľkoľvek a z rôznych zariadení, ľahká a rýchla implementácia či jednoduchšie škálovaná infraštruktúra sú dôvodom rastúceho trendu cloudu pre BI. Power BI predstavuje cloudové riešenie integrovateľné s inými cloudovými službami. Je obľúbenou voľbou firiem so stratégiou cloud-first.
Bezpečnosť a správa dát: Dáta majú jednoducho cenu zlata. Power BI preto pridala funkcie týkajúce sa bezpečnosti a správy dát, v súlade s predpismi GDPR a CCPA.
Mobilné aplikácie: Trendom rozhodne je aj vytváranie mobilných aplikácií pre BI reportovanie a vizualizáciu, prístupných kdekoľvek cez mobilné zariadenie.
AI a strojové učenie: Nový trend AI nemôže v oblasti BI chýbať. Do Power BI boli preto pridané funkcie AI ako sú dotazy v prirodzenom jazyku a automatizované náhľady. Umožňujú rýchlejšie identifikovať vzory a trendy v údajoch.
Dátové príbehy: Ďalší trend v BI odbore, ktorý umožňuje ľahšie chápať a interpretovať dáta. Vytváranie presvedčivých vizualizácií, ktoré sú lepšie schopné komunikovať poznatky a sprístupniť dáta širšiemu publiku.
Integrácia s inými systémami: Trendom sú aj integrácie s inými systémami ako CRM, ERP a podobne.

I keď sa tieto trendy menia a vyvíjajú

podľa potrieb používateľov, BI reporty a vizualizácie dát prinášajú jednoznačne efektívne spravovanie podnikových informácií a zdrojov. Preto by mali byť v prvom rade jednoduché a zrozumiteľné pre každého používateľa.

Scenáre využitia Power BI v reálnom svete

1. Analýza predaja a marketingu: Marketingový tím dokáže prostredníctvom Power BI sledovať napríklad návštevnosť webových stránok, zapojenie do sociálnych médií, alebo zistiť, ktoré kampane vedú k najväčším konverziám. Power BI možno teda použiť na analýzu marketingových a predajných údajov.
2. Finančné výkazníctvo: Finančný tím môže Power BI využiť na vytváranie finančných prehľadov, ktoré sledujú príjmy, výdavky, či ziskovosť. Informačný panel by tak mohol ukazovať napríklad trendy peňažných tokov alebo neuhradené faktúry.
3. Analýza prevádzky a dodávateľského reťazca: Výrobná spoločnosť by mohla pomocou Power Bi sledovať výrobné plány, efektívnosť výroby, úroveň zásob, ap.
4. Analýza ľudských zdrojov: Tím ľudských zdrojov zase môže Power BI využiť na analýzu údajov o ľudských zdrojoch ako angažovanosť zamestnancov alebo údaje o odmeňovaní.
5. Analýza v oblasti zdravotníctva: Power BI možno použiť napríklad aj na analýzu údajov o zdravotnej starostlivosti ako sú výsledky pacientov, miera opätovného prijatia aj využívania zdravotnej starostlivosti.

Power BI je osvedčeným riešením pre firmy všetkých veľkostí. Organizácia môže prejsť od excelových tabuliek a posielania príloh k online reportom na webe.

Prečo si Power BI vybrať?

Okrem už spomínaných vlastností a funkcií platformy vám naši skúsení procesní analytici radi pomôžu s analýzou požiadaviek a procesov. Databázoví a BI špecialisti zase uľahčia výber vhodného nástroja, implementáciu, zber dát, nastavenie reportov a grafov, ako aj priebežnú starostlivosť a úpravy. Power BI sa tak môže stať skvelým prínosom pre zrýchlenie a zlepšenie rozhodovacích procesov aj vo vašej spoločnosti.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Branislav Lupták
branislav.luptak@gamo.sk

ChatGPT: Umelá inteligencia ako nový pracovný nástroj

V novembri minulého roku predstavila spoločnosť OpenAI nový nástroj umelej inteligencie s názvom ChatGPT. Rozsiahly chatbot dokáže generovať množstvo odpovedí založených na približne 8 miliónoch dokumentov a 10 miliárd slov na internete.

Niet divu, že sa ChatGPT po svojom uvedení stal okamžite hitom a téma umelej inteligencie dnes často zaznieva v médiách. Funguje totiž vo forme dialógu v rámci chatu, pričom poskytuje relevantné odpovede podobajúce sa tým „ľudským“. Je postavený na najnovšom jazykovom modeli GPT (Generative Pre-trained Transformer) a i keď má obmedzenia, dokáže vygenerovať prirodzené odpovede na enormné množstvo otázok, stačí mu len správne zadať úlohu. Môže byť teda nápomocný v rôznych ohľadoch.

Momentálne je aplikácia prístupná každému, kto sa zaregistruje prostredníctvom e-mailu, a existuje niekoľko jej verzií. Líšia sa veľkosťou a množstvom trénovaných dát, pričom dostupná je aj výkonnejšia platená verzia. Používanie GPT technológie v NLP sa neustále rozširuje a v súčasnosti ide o jeden z najvýkonnejších modelov na generovanie textu. ChatGPT môže byť aplikovaný na rôznorodé zadania i pre online marketing. Pomocou technológie je možné vytvárať personalizovaný a relevantný obsah alebo automatizovať rutinné úlohy. Nové technológie sú v dnešnom digitálnom svete neustále rastúcim trendom, preto aj ChatGPT ponúka nové možnosti. Úlohy ako sú generovanie nových textov, odpovedanie na otázky či vedenie konverzácie s užívateľom GPT zvláda výborne. ChatGPT dokáže operovať v mnohých jazykoch, vrátane slovenčiny, a funguje na základe spracovávania informácií cez strojové učenie a algoritmy spracovania jazykov. Veľmi zjednodušene by sa dalo povedať, že ide o jazykový model fungujúci na základe pravdepodobnosti. Uhádne totiž, aké slovo by malo vo vete nasledovať a neustále sa učí (deep learning).

Na čo všetko sa dá ChatGPT využiť v praxi?

1. Vytváranie obsahu: Nástroj dokáže pripraviť napríklad osnovu článku, nadpisy, pútavé titulky, textový obsah, či už ide o článok, alebo popis, dokáže nájsť najčastejšie frekventované otázky (FAQ) a podobne.

2. Analýza kľúčových slov: Je treba povedať, že v prípade ChatGPT nie je veľmi priestor na prácu s veľkými datasetmi. Dá sa však použiť pri analýze kľúčových slov, ako je napríklad základná kategorizácia alebo priradenie nákupného úmyslu ku konkrétnemu kľúčovému slovu.

3. Sociálne siete: ChatGPT dokáže vytvárať a formulovať príspevky na sociálne siete, pričom je v zadaní úlohy možné definovať presný počet znakov, ktoré by mal príspevok obsahovať, jeho charakter či podobnosť s vami vytvoreným textom. Zdá sa teda, že generatívna umelá inteligencia vytvorí texty na pohľad na nerozoznanie od tých, ktoré sú napísané človekom. Výstupy z ChatGPT je však potrebné starostlivo kontrolovať, keďže informácie nie sú vždy 100-percentné. Dĺžka výstupu je obmedzená a nie sú k dispozícii nové dáta, takže aktuálne trendy zatiaľ chatbot nepozná.

Avšak, nový chatbot sa dá definitívne využiť pre základy online marketingu, tvorby textov či popisov. Tam, kde by človek mohol tráviť hodiny štúdiom a hľadaním materiálov k téme, dokáže tento AI nástroj zjavne ušetriť množstvo času.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Iveta Hlaváčová
iveta.hlavacova@gamo.sk

ChatGPT je skvelý pomocník, ale zlý pán

V IT brandži nie je snáď nikto, kto by si nevyskúšal konverzáciu s ChatGPT. Téma umelej inteligencie rezonuje v médiách, a preto sme sa niekoľkých klientov opýtali na ich názor.

Ako vnímate postupnú integráciu umelej inteligencie do pracovného života? Vidíte v nej príležitosť (vo vašej oblasti pôsobenia, v inom sektore) alebo máte skôr obavy?

Róbert Obertík
Banskobystrický pivovar, a.s.

Pre mňa bolo stretnutie s umelou inteligenciou vzrušujúce a poučné. Vidím v nej obrovský potenciál. AI odpovedala na rôzne otázky z problematiky pivovarníctva, IT, komunikačných zručností, zákonníka práce. Zadal som jej nakresliť obrázok, resp. vygenerovať fotku. To, čo som pred 30-timi rokmi videl iba v science fiction filmoch, sa stalo skutočnosťou. AI je skutočne vynikajúci pomocník. Obávam sa však, čo všetko dokáže v prípade, ak by sa stala našim pánom. Už len predstava, že vie ovplyvňovať myslenie, resp. smerovanie myslenia obrovského počtu ľudí, je desivá. Dnes aj jednoduché a prehliadnuteľné dezinformácie a konšpiračné teórie dokážu zmanipulovať obrovské davy ľudí, ktorí nie sú ochotní prijímať argumenty druhej strany. Už len fakt, že AI bez váhania odpovedá na akúkoľvek otázku z akéhokoľvek vedného odboru, dokáže programovať, generovať obrázky, filmy, články, diplomové práce, jej dáva neuveriteľnú silu manipulácie. Stačí malá zmena v odpovediach a razom sú názory miliónov ľudí vedené požadovaným smerom. Zneužitie AI je veľmi jednoduché už aj v tomto štádiu. Obávam sa toho. Napriek tomu si nemyslím, že sú správne návrhy na zákaz jej použitia resp. ďalšieho vývoja. Pokiaľ ju vieme zmysluplne využiť, urobme to a využime ju naplno. Som presvedčený, že nás AI vie posunúť vpred.

Martin Hauptvogel
MediaJet Group a.s.

Postupná integrácia umelej inteligencie do pracovného života je nevyhnutnosť. V rámci činnosti mediálnej divízie našej agentúry vidím prínos AI pre spresnenie a urýchlenie procesov v plánovaní a vyhodnocovaní reklamných kampaní. V produkčnej divízii sa ponúka využitie AI vo výskume a vývoji AVD formátov, v našej športovej talkshow, v cestovateľskej reality show alebo v docu-reality s trénovacím programom zvierat. Keď portál BuzzFeed oznámil využívanie AI na generovanie obsahu, hodnota akcií firmy sa okamžite zdvojnásobila (aspoň dočasne). Redakcia už začala pomocou AI vyrábať kvízy – ľudia odpovedia na niekoľko otázok a robot nazvaný Buzzy im ponúkne personalizovanú odpoveď, neskôr začala pridávať články s cestovateľskými odporúčaniami generované AI. No podľa reakcií čitateľov boli dosť zlé. A tu niekde sa podľa mňa skrýva slabá stránka AI. Zodpovednosť za výstupy, pri ktorých je potrebný úsudok alebo vytvorenie očakávanej emócie, bude, verím, ešte dlho a nezastupiteľne na človeku, ktorý zabezpečuje pre AI dostatočne ‚čisté‘ a kvalitné dáta.

Jozef Slovák
Verisoft Slovakia, a.s.

ChatGPT vnímame, ako užitočný a výkonný nástroj pre každodennú prácu. Často sme prekvapení, akú obsahovo kvalitnú odpoveď dokáže vygenerovať. Otázka však musí byť formulovaná relatívne presne. Dokonca aj môj 10-ročný syn využíva ChatGPT prakticky denne. Keďže sa jedná o neurónovú sieť, ktorá sa neustále učí, tak problém môže z môjho pohľadu nastať vtedy, ak ChatGPT začneme učiť zlým veciam a budeme ohýbať jeho ‚názor‘. Preto je nevyhnutný neustály dohľad a kontrola nad obsahom.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Iveta Hlaváčová
iveta.hlavacova@gamo.sk

Umenie vytvárané z bežných fotografií mobilom

Rozpoznávanie a tvorba obrazu pomocou umelej inteligencie sú kľúčovou esenciou slovenského startupu Dog Moments Art.

Riešenie umožňuje premeniť bežnú fotografiu domáceho miláčika vytvorenú mobilom na výtvarné dielo.

Na stránke dogmoments.art môžete využiť optimalizované algoritmy AI, ktoré premenia fotografiu vášho psíka na obraz v štýle veľkých majstrov (Vincent van Gogh, Henri Matisse, Pablo Picasso), prípadne iných zaujímavých výtvarných štýlov.

Riešenie ponúka aj fyzické vytlačenie obrazu na plech. Rám obrazu je doplnený o 3D štruktúru imitujúcu povrch dreva.

Proces tvorby zvládnete za pár minút. Výsledok určite zaujme nielen milovníkov psíkov a umenia.

Vďaka magnetickým samolepkám sa jednoducho upevní na stenu.

V spojení s pekným balením si Dog Moments Art nachádza obľubu v komunite majiteľov psov a ich blízkych ako netradičný a jedinečný dar.

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

Branislav Lupták
Obchod
branislav.luptak@gamo.sk

Gabriela Repatá
Technické riešenia
gabriela.repata@gamo.sk

Tomáš Tuba
Technické riešenia
tomas.tuba@gamo.sk

Jana Kohárová
Obchod
jana.koharova@gamo.sk

Martin Vosko
Softvérové riešenia
martin.vosko@gamo.sk

Iveta Hlaváčová
Marketing
iveta.hlavacova@gamo.sk

Vydavateľ
GAMO a. s.
www.gamo.sk

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

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

Štylistická úprava a spracovanie textov
TIME.is COMMUNICATION
www.time-is.eu

Spoznajte odpoveď na neproduktívnu administratívnu záťaž

Chcem zistiť viac

GAMO
INFORMAČNÉ TECHNOLÓGIE