

platform of invention

Informačné technológie pre podnikanie s nápadom



číslo 4

ročník druhý | 2/2022

Digitálne dvojča

Štíhle riadenie výroby a úspory v energiách

Ransomvér v akcii

Kritické roky: nedostatok pracovníkov v IT

Magazín o informačných technológiách

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



PDF magazín

Tlačený magazín

Online portál

Čítajte 1. číslo

Venované téme kybernetickej bezpečnosti.



PDF magazín

Tlačený magazín

Online portál

Čítajte 2. číslo

Venované téme cloud.



PDF magazín

Online portál

Čítajte 3. číslo

Objavte benefity IT made in Slovakia.



PDF magazín

Online portál

Aktuálne 4. číslo

Balíček IT opatrení ako recept na krízu.

platform of invention

Informačné technológie pre podnikanie s nápadom

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

Výzva pre všetkých CEO, CTO a CFO

Ponúkajte nám svoj príbeh využitia IT vo vašej firme a my vám bezplatne ponúkame exkluzívnu možnosť prehovoriť do publika slovenských firiem.

Chcete zistiť viac a zapojiť sa?

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

www.platformofinvention.sk/profil-magazinu/



Klikni alebo oskenuj QR

Čítajte nás online!

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

www.platformofinvention.sk



Klikni alebo oskenuj QR

Balíček IT opatrení ako recept na krízu

Energetická kríza má aj svoje pozitíva. Núti nás žiť úspornejšie, šetrnejšie k našej planéte, a myslieť na budúcnosť a bezpečnosť našich detí. Neplatí to a zefektívniť vyvinuté úsilie pre dosiahnutie cieľa. Premýšľať ako a kde ušetriť, čo optimalizovať a čo automatizovať. To isté platí pre biznis. A práve vďaka moderným IT technológiám môžeme dopady ekonomickej krízy zmierniť. Ako na to?

Zhromažďovanie a vizualizácia dát v reálnom čase s cieľom optimalizácie rôznych procesov môže byť kľúčová pre štithle riadenie výroby alebo odhaľovanie plytvania energiami. Ak má firma desiatky závodov, je pre ňu obrovským prínosom, keď monitoruje a prispôsobuje proces výroby, logistiky či skladu v reálnom čase z aplikácie na mobilnom zariadení. Identifikuje tak prípadné bezpečnostné riziká, ktoré môžu ohroziť chod prevádzky, a poskytuje možnosť okamžitého zásahu. Digitálne dvojča posúva aj túto oblasť do novej dimenzie.

Dôležitou súčasťou každého biznis kritického procesu je aj nastavenie adekvátnej bezpečnosti tohto procesu. Potvrdzuje sa, že nechať si poradiť s problémom, preveriť

systémy alebo infraštruktúru a zvýšiť ich pridanú hodnotu na maximum, sa oplatí. Cloud ako flexibilné a škálovateľné riešenie dokáže v tomto smere ponúknuť veľa príležitostí. Mnoho úspor pramení už z podstaty cloud computingu: platí sa len za aktuálne využívanú službu. Interné zdroje, ľudské aj finančné, nie sú miňané na prevádzku a servis, a možno ich sústrediť na nové rozvojové projekty. Čo povieť?

Nové lekcie z balíčka IT opatrení vám vďaka ochote partnerov a klientov komunikovať a zdieľať pozitívne aj negatívne skúsenosti z každodennej praxe prinášame na stránkach štvrtého vydania magazínu.

A nezabudnite, že akékoľvek opatrenia, ktoré vo firme zavediete, potrebujú svoj čas, reálne ich oceníte až z dlhodobého hľadiska, preto s nimi začnite už dnes.

Prajeme vám príjemné čítanie.



Kristián Alakša
Generálny riaditeľ
kristian.alaksa@gamo.sk



AVPP je odpoveďou na neproduktívnu administratívnu záťaž

Stretli ste sa so situáciou, keď za bránou fabriky zostal dodávateľ s tovarom, lebo nemal vstupné povolenie? Stáva sa a komplikuje to fungovanie oboch zainteresovaných strán.

Otázkou je: Ako si uľahčiť administratívnu záťaž? Ako eliminovať byrokraciu a zefektívniť pracovný čas? Odpoveď je jednoduchá: Automatizáciou, minimalizujúcou neproduktívnu administratívu a vzdelávanie, ktoré sa absolvujú digitálnou formou priamo z appky.

Jednoduchá aplikácia na vydávanie pracovných povolení – AVPP – zjednoduší pracovný život automatizovane, bez zásahu a dozoru zodpovedného pracovníka. Dodávateľia si v nej pozrú videoškolenie, absolvujú test, získajú výsledky, po úspešnom vyhodnotení podpíšu formulár pre vydanie povolenia priamo v appke, a získajú ho už pred samotnou návštevou podniku či iného subjektu tiež online. AVPP tak šetrí nielen papier, ale najmä čas všetkých doteraz zúčastnených strán.



Článok pokračuje na
platformofinvention.sk
klikni alebo oskenuj QR



Branislav Lupták
Softvérové riešenia
branislav.luptak@gamo.sk

Zero Trust: Autentizujte a autorizujte, každého, vždy a všade

Zero Trust nie je služba, produkt alebo technológia. Je to filozofia a metodológia tvorby, implementovania a správy kybernetickej bezpečnosti.

Tradičná bezpečnostná architektúra bola primárne založená na mohutnej ochrane perimetra prostredníctvom nástrojov ako firewally, systémy prevencie prienikov a podobne. Vzdialená a dynamická práca, využívanie cloudových úložísk, nástrojov a aplikácií, spolu s neustále sa zvyšujúcim počtom pripojených zariadení a rýchlo narastajúcou veľkosťou bezpečnostného perimetra, majú



ESET NetProtect: Ochrana pred digitálnymi hrozbami už na úrovni siete

Spoločnosť ESET predstavuje novinku, ktorá pomocou aktívneho DNS filtra ochráni všetky zariadenia pripojené v domácej pevnej sieti alebo v mobilnej sieti operátora. ESET NetProtect je riešenie integrované v sieti poskytovateľov telekomunikačných a internetových služieb. Operátori tak svojim zákazníkom môžu ponúknuť ochranu pred stránkami, ktoré šíria malvér, používajú sa na phishing, majú pochybnú povest' alebo ponúkajú potenciálne nechcený obsah. Filter čerpá z databázy hrozieb, ktorá je neustále aktualizovaná. Dokáže tak okamžite rozoznať škodlivé domény a zablokuje prístup ešte pred tým, ako stihnú napáchať škody. Výhodou je, že zákazníci si nemusia nič inštalovať, ochranu si aktivujú prostredníctvom jedného kliknutia. Na zákazníckom portáli svojho operátora si následne môžu nastavovať pravidlá pre blokovanie obsahu a pozeráť si bezpečnostné reporty.



Článok pokračuje na
platformofinvention.sk
klikni alebo oskenuj QR



Igor Chudáčik
Produktový manažér
GAMO a.s.



Článok čítajte na
platformofinvention.sk
klikni alebo oskenuj QR



Branislav Orlík
Produktový manažér
ESET, spol. s r.o.

Doba si žiada maximálne flexibilné riešenia

Prečo sú cloudové služby najvhodnejším IT riešením a dokonca jedným z možných opatrení k zdražovaniu energií? Je to benefitmi, ktoré cloud computing vnáša do pracovného prostredia firiem.

Je váš hardvér v nedohľadne? Virtuálny server v cloude je rýchlym spôsobom, ako si zabezpečiť IT infraštruktúru s podporou 24/7. Trend postupného presunu ERP systémov do cloud prostredia je z roka na rok zásadnejším riešením. Zvoľte si technologické prostredie a kombináciu IT služieb tak, aby ste fungovali s maximálnym efektom pre váš biznis.



Cloud si môžete vyskúšať prenajatím menšej inštancie na skúšobnú dobu predtým, ako sa k nemu zaviazete. Uchovávaním dát mimo firmy a on-premise prostredia minimalizujete bezpečnostné riziká. Navyše, poskytovatelia cloudu garantujú prevádzku, starajú sa o údržbu aj upgradu systémov. Nie je na čo čakať. Presvedčíme vás TOP 10 výhodami cloudu?



Článok čítajte na
platformofinvention.sk
klikni alebo oskenuj QR



Erik Kirschner
Cloud konzultant
GAMO a.s.



Článok čítajte na
platformofinvention.sk
klikni alebo oskenuj QR



Marcela Gottwaldová
Obchodný konzultant
GAMO a.s.

Novinka Veeam Backup for Salesforce eliminuje riziko straty dát a metadát

Spoločnosť Veeam® Software, líder v oblasti riešení zálohovania, obnovy a správy dát umožňujúcich ich modernú ochranu, predstavila novinku Veeam Backup for Salesforce. Tá eliminuje riziko straty dát a metadát Salesforce v dôsledkoch ľudskej chyby, problémov s integráciou, a ďalších bežných scenárov.

„Až 97 % respondentov si uvedomuje potrebu chrániť svoje najdôležitejšie aplikácie SaaS, ako sú napríklad Salesforce a Microsoft 365,“ vyplýva zo štúdie Veeam Salesforce Protection Trends Report 2022. Práve zálohovanie týchto aplikácií bolo v minulosti zo strany IT najviac prehliadané, čo viedlo k zraniteľnostiam, bezpečnostným rizikám, strate a poškodeniu dát.

Salesforce je číslo jeden medzi riešeniami SaaS (softvér ako služba) pre riadenie vzťahov so zákazníkmi (CRM). Nové riešenie Veeam umožňuje firmám a organizáciám nasadiť záložné prostredia, a to v lokálnom prostredí aj v cloude, a poskytnúť im úplný prístup k údajom a metadátam Salesforce spoločne s kontrolou nad nimi. Veeam Backup for Salesforce je ako samostatný produkt k dispozícii a predáva sa v podobe ročného predplatného na 1 až 5 rokov.



Článok pokračuje na
platformofinvention.sk
klikni alebo oskenuj QR



Michal Štětina
Field Marketing Manager CEE
Veeam



Kontinuálny rozvoj Microsoft 365

Pomáhame zákazníkom neplývať peniazmi a využívať potenciál Microsoft 365 naplno. Nehľadáte aplikácie tretích strán, naučíme vás ako si vyskladať vlastné portfólio aplikácií a služieb. Vybrať presne také, aké potrebujete. Pracovníci často venujú mnoho času úlohám, čo sa dajú zautomatizovať. Krčkovite sa držia zabehnutého spôsobu práce, neuvedomujúc si, že drobné zmeny v ich doterajších návykoch môžu podstatne zefektívniť prácu. V mnohých prípadoch im stačí ukázať možnosti a dostaví sa efekt „heureka“.

Aj dlhodobí používatelia služby Microsoft 365 využívajú len obmedzený počet aplikácií z tých, ktoré majú k dispozícii v rámci licenčných plánov. Microsoft 365 je živým ekosystémom. Priebežne sa vyvíja, dopĺňa o nové funkcie. Nastaviť ho ako optimálny systém práce v našom ponímaní znamená mať ho čo najjednoduchší, intuitívny pre používateľov, a bezpečný zároveň. To si vyžaduje poznať existujúce možnosti, rozumne ich skĺbiť a uviesť do života.



Článok čítajte na
platformofinvention.sk
klikni alebo oskenuj QR



Marcela Gottwaldová
Obchodný konzultant
GAMO a.s.





Digitálne dvojča

Kým donedávna boli digitálne dvojčatá doménou predovšetkým plánovania a simulácií v priemysle, dnes sa ich záber začína dostávať aj do nových sfér.



Popri zobrazení dát v reálnom čase sa už jedná aj o výstavbu celých mestských blokov, skenovanie a monitoring existujúcich objektov a, samozrejme, aj o oblasť kybernetickej bezpečnosti.

Základom štithej výroby je demokratizácia prístupu k informáciám o výkone danej organizácie. V prípade výrobných závodov ide najmä o dáta k aktuálnej výrobe (OEE, dáta z MES, WMS, ERP systémov), logistike, skladových zásobách a dnes, veľmi aktuálne, aj o spotrebe rôznych typov médií. A to nielen elektrickej energie, hoci

tá je stále kľúčová. Digitálne dvojča umožňuje ponúknuť živé dáta v 3D priestore, ktoré dátam dávajú úplne nový kontext, tzv. "spatially oriented dataset".

Práve toto spojenie rôznych dátových zdrojov prináša úspory na miestach, kde ich len ťažko očakávať. Pri analýze sú logicky očakávaniami práve redukcie flotily, znižovanie stavu personálu v logistike a iné priamočiare úspory. Vidieť v reálnom čase okamžité využitie flotily v spojení s históriou slúži práve na to. Málokomu však napadne spojitost s úsporami vo vý-

robe. Ak stojí minúta mikroprestoja 1 000 Eur a takéto prestoje spolu tvoria 20 minút denne, ich odstránenie sa neprejaví síce na žiadnej úspore, ale na zvýšení kapacity "zadarmo". Napríklad plynulé zásobovanie výrobných liniek umožňuje zníženie rýchlosti vozíkov, čo má vplyv na zníženie stresu a bezpečnostných rizík a prináša benefit zase smerom k zamestnancom.

To bola logistika, čo však výroba? Nie každý závod má dáta o svojom behu pod jednou strechou v jednom systéme. Dáta sú spravidla distribuované v množstve systémov a jediným prepojením medzi nimi býva ručný prepis dát do MS Excel. Práve ten môže byť nahradený digitálnym dvojčatom, pretože nerozlišuje dátové zdroje či formáty a umožňuje takto diverzifikované dáta umiestniť do priestoru

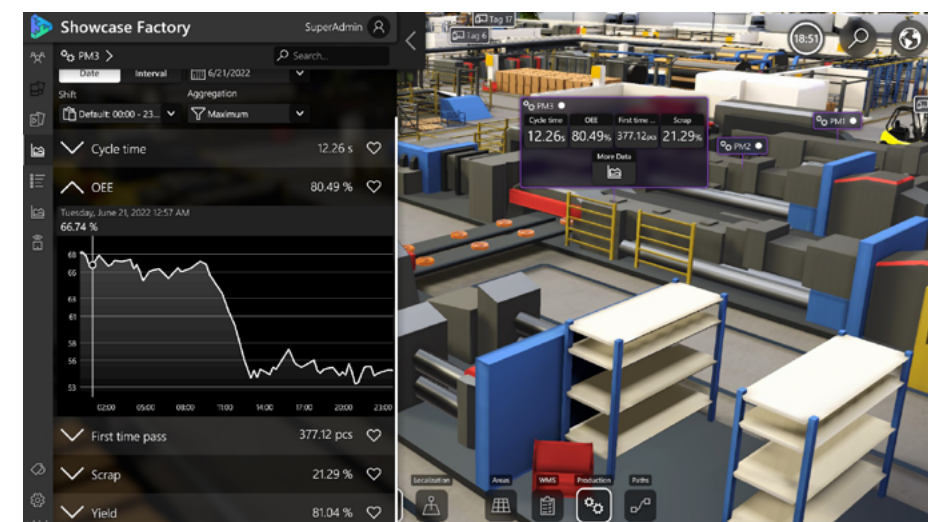


a času. Nerovnomerný beh výroby má priamy dopad nielen na spotrebu, ale aj opotrebenie strojov. Zariadenia sú spravidla dizajnované na určitý počet výrobných cyklov, avšak predpokladá sa rovnomerná výroba. Výrobca nepočíta s tým, že stroj bude cez deň vyrábať v "správnom takte", na začiatku nočnej smeny nepobeží vôbec, a na konci nočnej smeny pôjde na maximum. Okrem prekročovania 15-minútových maxim to má, samozrejme, na stroj negatívny dopad a predlžuje sa čas jeho návratnosti skrz neplánovaný a neželaný servis. Prostredníctvom digitálneho dvojčata je možné celú túto situáciu vizualizovať v konkrétnom 3D prostredí, pričom zodpovedný manažér môže veľmi rýchlo na vzniknutú situáciu reagovať.

V oblasti spotreby médií je zaujímavá kombinácia s environmentálnymi senzormi, kde je možné hľadať vzťah medzi napr. vonkajšou teplotou, vnútornou teplotou a úrovňou kúrenia. A to celé v spojení s otvorenými alebo zatvorenými bránami na vykládke a nakládke tovaru či materiálu. Predovšetkým v zimných mesiacoch zvyšujú otvorené brány spotrebu energií úplne zbytočným vetraním. Podobným plytvaním bývajú zapnuté stroje, ktoré nevyrábajú, ale spotrebu majú na úrovni 60% ako keby vyrábali. Príčina? Operátori stroj ráno zapli, pretože si mysleli, že budú vyrábať, ale v skutočnosti výroba začne až o 3 hodiny a tie 3 hodiny stroj bežal zbytočne.

Na to, aby bola prevádzka výroby zabezpečená, je potrebné dohliadať aj na bezpečnostné riziká. Vizualizácia napadnutí, anomálií sieťovej infraštruktúry a útokov je silnou stránkou bezpečnostných systémov, digitálne dvojča však posúva aj túto oblasť do novej dimenzie. Možnosť vidieť ako sa prípadný útok rozvíja, na ktoré zariadenie je útok vedený, aký je dátový prenos a podobne, to sú veci, ktoré v tejto oblasti nie sú vôbec bežné. Digitálne dvojča umožňuje rýchlejšie rozhodnutie na základe korelácie rôznych zdrojov dát, či sa skutočne jedná o kybernetický bezpečnostný incident, alebo o poruchu stroja zavinenú inou veľičinou. Napríklad len dohľadať, ktorý počítač je kde a na ktorom porte je napojený, je veľmi zdĺhavé, a presuny po závodoch tiež berú drahocenný čas.

Zviditeľniť dáta rôznymi úrovňami vedenia závodu a premeniť ich na relevantnú informáciu je teda kľúčom k štithej výrobe, ktorá tak môže reagovať na zmeny



pružnejšie a nespolieha sa iba na plán, čo sa v dnešnej dobe dodržiava stále ťažšie a ťažšie. Prostredníctvom digitálneho dvojčata môžete monitorovať akýkoľvek typ senzora IoT alebo IIoT, databázy a dátového toku, procesu alebo pracovného postupu. Majiteľ firmy alebo manažér si tak môže dopriať komfort robiť rozhodnutia aj z miesta na druhom konci sveta prostredníctvom vizualizácie, ktorou sleduje akýkoľvek

druhu technológie, jej efektívnosť, jej funkčnosť v reálnom čase. Stačí na to len jedno kliknutie na digitálne dvojča, napríklad jeho výrobné haly, v mobilnom zariadení.



Článok čítajte na platformofinvention.sk
Klikni alebo oskenuj QR



Zuzana Omelková
zuzana.omelkova@gamo.sk

Ransomvér v akcii

Každú minútu sa vo všetkých kútoch sveta potvrdzuje, že najzraniteľnejším bezpečnostným článkom v IT sfére je človek. Bezpečnostné riziká v online priestore sa dajú iba minimalizovať, nie odstrániť. S vyspelou technológiou pracujeme takmer všetci, preto stačí sekundová nepozornosť či kliknutie na podozrivý odkaz a problém je na svete. Svoje o tom vie výrobná spoločnosť Remeslo strojal, s.r.o., ktorú stál jeden takýto klik 130-tisíc Eur.

A to hovoríme o príbehu so šťastnejším finále. Všetky dáta sa podarilo vďaka duchapřítomnosti manažérov podniku a rýchlemu zásahu odborníkov tretích strán zachrániť pre ďalšie fungovanie. Ale vráťme sa do marca 2022 a udalosťiam krok za krokom.

Ransomvér v akcii

Spoločnosť Remeslo strojal, s.r.o., je súčasťou holdingu Remeslo a svoje strojárské produkty exportuje do 17 krajín sveta. Útok zaznamenala skoro ráno.

„Kolega mi oznámil, že nevie otvoriť súbor na sieťovom disku. Mal príponu .xlsx. kqgs,“ začína rozprávanie IT technik Richard Ševčík. To .kqgs nesedelo, tak ho odstránil. Súbor však nemal správny obsah a rovnaká prípona bola v každom adresári na sieťovom disku. „Už som začal tušiť, že niečo nie je v poriadku. Z ekonomického oddelenia prišlo hlásenie - Nemôžeme otvoriť databázu účtovníctva, a problémy začali nahlasovať ďalšie oddelenia. Neboli to ľahké chvíle. Sme zašifrovaní,“ oznámil zjavný fakt vedeniu holdingu a začal konať.

Okamžite zhodil všetky servery a switche vo firme, aby prerušil sieťovú komunikáciu cez internet so svetom. Oslovil firmu, čo sa starala o firewall, internet, e-mail. Tá na riešenie akútneho problému odporučila bratislavských špecialistov, ktorí mali

s podobnými situáciami skúsenosť. Bolo jasné, že ide o ransomvérový útok: v adresári bol pripojený súbor s pokynmi na odšifrovanie. Otázka, či zaplatiť útočníkovi bola zreteľne na stole.

„V týchto prípadoch máte vždy len dve možnosti. Zaplatiť útočníkovi výkupné a čakať, či skutočne pošle sľúbený odšifrovací kľúč, alebo sa spoľahnúť na obnovu dáta zo záloh. Zaplatili sme,“ priznáva Richard Ševčík. S tým, že suma, našťastie, nebola likvidačná, a útočník skutočne zaslal funkčný dešifrátor, ktorým dešifrovali potrebné údaje.

Riešenia po odšifrovaní

Spoločnosť následne zakúpila 5 počítačov, aby na nich IT pracovníci nanovo vystavali „čistú“ lokálnu sieť. Nahrali dáta zo záloh, čo neboli napadnuté. Údaje z obnovených odšifrovaných dát, vrátane ekonomických, prechádzali antivírovými programami: „Šlo naozaj o vysoko náročnú, pedantnú prácu.“

Šťastím bolo aj to, že útočník sa nedostal ďalej ako do sieťových adresárov, že zálohy boli v dobrom stave, aj že výrobný program Remeslo strojal, s.r.o., fungoval. Zároveň na všetky napadnuté počítače, zapli switche a skúmali aktivitu na sieti. Pre kolegov zriadili provizórne pracovisko, zasadačku s piatimi kusmi počítačov, na ktorých sa zatiaľ striedali účtovníci

a výrobní. Po zistení, že výrobný server nebol napadnutý, pripojili 3 počítače už aj na výrobný server.

„Vytvorili sme krízový tím, denne sa na pravidelných poradách stretávalo vedenie s výrobou a ekonómami, ktorí rozhodoval o ďalších krokoch: ako zabezpečiť komunikáciu cez e-mail, ako si plniť záväzky a dodať ekonomické údaje štátu, ako rýchlo požiadať o odklady DPH a podobne. Bolo toho dosť,“ potvrdzuje Richard Ševčík a je vďačný za absolútne nasadenie všetkých kolegov.

Smerom k budúcnosti

Richard Ševčík tiež priznáva, že o útočníkovi, našťastie viac nepočuli. „Prípad sme, samozrejme, nahlásili polícii a tá začala trestné stíhanie voči neznámemu páchateľovi. Zo skúseností iných napadnutých spoločností či jednotlivcov však neočakávame, že by sa nám „výpalné“ vrátilo. Ideme ďalej a obozretnnejšie.“

Po prvom náročnom týždni oslovila napadnutá spoločnosť zo Žiaru nad Hronom odborníkov z banskobystrickej firmy GAMO, a. s., ktorá riešila podobný prípad aj neďaleko, v Kremnici. Išlo o komplexné navrhnutie systému obnovy spoločnosti zasiahnutej ransomvérovým útokom aj s dodaním riešenia.

Spoločnosť Remeslo strojal, s.r.o., potrebovala zabezpečiť LAN infraštruktúru

s bezpečným pripojením do a z internetu, serverovú infraštruktúru a jednotné desktopové prostredie na prácu. Za prítomnosti ich vedenia a prizvaných hostí následne GAMO so svojím tímom vypracovali postupný plán obnovy. Alternatívu nasadenia riešenia či prejdú do cloudu, alebo vybudujú servery vo firme, nechali na rozhodnutí napadnutej spoločnosti.

„Absolvoval som množstvo telefonátov a mailovej komunikácie s dodávateľmi účtovných a mzdových programov, s dodávateľom výrobného programu a GAMO špecialistami, aby sme pre nás vybrali to najvhodnejšie a najbezpečnejšie riešenie,“ vysvetľuje rozhodnutie IT technika. „Výsledkom bolo zostať s dátami na on-premise infraštruktúre, teda na našich serveroch.“

Riešenia tretích strán

Spoločnosť Remeslo strojal, s.r.o., spätne hodnotí stav zabezpečenia pred útokom a dnes takto: „Mali sme nainštalovaný antivírový program na jednotlivých počítačoch, mali sme zabezpečený firewall aj zálohovanie. Sieť sme mali však len na Workgroupe, bez doménového servera, čo je na dnešnú dobu určite málo.“

Riešenie od GAMO a. s. bolo navrhnuté s tým, že spĺňalo najvyššie štandardy bezpečnosti pri práci s dátami a zaisťovalo ich ochranu. Richard Ševčík: „Návrhy boli korektné a na vysokej technickej a profesionálnej úrovni. Rozhodli sme sa

pre spoluprácu, pre bezpečné a finančne únosné riešenia.“

Rozmeňme si to rekapituláciou na drobné.

Aké boli dôvody pre obnovu infraštruktúry?

- Výmena a konsolidácia zastaraných hardvérových zariadení;
- Prechod na virtualizačnú platformu, ktorá zjednoduší prevádzku a umožní ďalej rozvíjať systémy v budúcnosti;
- Zariadenia s aktívnou podporou výrobcov – garantovaná záruka, t. j. v prípade poruchy zariadenia jeho výmena za nové zariadenie, bude realizovaná v krátkom čase;
- Zvýšenie celkovej bezpečnosti pri práci s dátami spoločnosti.

Úlohou špecialistov bolo vytvoriť hardvérové zázemie, ktoré umožní Remeslu dlhodobé a stabilné používanie informačného systému. Riešenie, ktoré môže firma v čase ďalej rozvíjať, bude jednoduché na správu, a zvýši odolnosť systémov.

Finále v praxi

GAMO postupne dodalo nové servery, počítače a notebooky, a začali sa na ne nahrávať čisté a skontrolované dáta. Medzitým boli na USB kľúče sťahované dáta zo starých počítačov a zasielané na kontrolu antivírusom do Banskej Bystrice, sídla GAMO, a. s. Napadnutá spoločnosť zakúpila novú doménu remeslostrojal.sk a na ňu sa vkladali dáta, aj s priamym

vkladením do aplikácií v cloudovom prostredí. Na Microsoft 365 sa ukladali zložky jednotlivých pracovníkov zo skontrolovaných USB kľúčov a postupne sa pripájalo do siete všetkých novozakúpených 62 počítačov. Zároveň sa pracovalo na rozdelení siete na jednotlivé segmenty a na nastavení nových pravidiel. Prebehli školenia pracovníkov a zaviedli sa striktné obmedzenia, politiky, ako aj pravidlá vhodného správania sa užívateľov na internete.

„Zakúpili sme zariadenie, kde sa nahrali zálohy zo starých serverov. Išlo o veľké množstvo dát, ktoré sa niekoľko dní kontrolovali, a až potom sa uložili na zariadenie. Skoro 6 mesiacov sa čakalo na nové switche, z dôvodu nedostatku špecializovaných čipov na trhu. Asi až po 7 mesiacoch sme sa dostali do normálu a spustenia všetkých programov, doterajšie výdavky sa vyšplhali na 130-tisíc Eur,“ rekapituluje polročnú cestu IT technik.

Cestu, ktorú spustil jeden nešťastný klik na zašifrovaný súbor.

Dobré správy na záver

Situácia, spôsobená kyber útokom, prinútila Remeslo strojal, s.r.o., zabudnúť na postupnú digitálnu transformáciu a urobiť veľký skok. Z úrovne pred 10-tich rokov naplno vkročili do prostredia modernej digitálnej kancelárie a na všetkých úrovniach začali pracovať so systémami a aplikáciami Microsoft 365. Tie umožňujú dokonalú kolaboráciu, jednoduchú komunikáciu a, hlavne, poskytujú prvotriednu ochranu identít a zariadení. Vďaka technológii EDR dnes majú v tomto úspešnom výrobnom podniku podrobný prehľad o hrozbách v systéme, detegujú nezvyčajné správanie a narušenia zabezpečenia.



Článok čítajte na
platformofinvention.sk
klikni alebo oskenuj QR



Branislav Lupták
branislav.luptak@gmail.sk



Aké služby M365 využíva personálna agentúra?

Úspešná firma potrebuje ľudí oddaných práci, a zároveň IT služby, ktoré im ich každodennú prácu uľahčia. V nasledovnom článku priblížime príbeh spoločnosti Adecco Slovakia, jednej z TOP 3 personálnych agentúr na Slovensku, ktorá pôsobí na trhu od roku 2002. „Klientom poskytujeme komplexný servis, nábor zamestnancov, spracovanie miezd, konzultácie,“ hovorí riaditeľka Ivana Heretik Vačoková. „Máme širokú sieť pobočiek a pracujeme s rozsiahlou databázou vyše 50-tisíc kandidátov. Našou úlohou je na jednej strane pomôcť najsť uchádzačom o zamestnanie vhodnú prácu, na druhej strane pre spoločnosti vyhľadávať talenty, najsť správneho kandidáta pre špecifickú pozíciu klienta.“

Personálne agentúry musia byť maximálne flexibilné. Zabezpečiť presný a rýchly nábor vyžaduje pružné jednanie so všetkými zúčastnenými stranami. Preto Adecco Slovakia využíva moderné technológie Microsoft 365, umožňujúce rozvíjať kolaboráciu v pracovných tímoch a využívať najvyššie štandardy zabezpečenia dát. S IT špecialistom Adecco Slovakia MAREKOM ŠEFČÍKOM sme sa rozprávali o tom, s akým zámerom išli do implementácie M365, prečo kladú dôraz na nastavenie bezpečnostných politík, aj čo považujú za najväčší prínos danej služby.

V článku sa ešte dozviete:

- Prečo využívajú služby M365
- Ako sa adaptovali
- Kam sa chcú posunúť

Dôvody implementácie prostredia Microsoft 365 bývajú rôzne. V príbehu Adecco Slovakia to bolo osamostatnenie sa spoločnosti, patriacej medzi TOP 3 vo svojom odvetví, od zahraničnej matky. Ako s odstupom času implementáciu hodnotíte z pohľadu IT administrátora?

Nešlo o prechod na niečo nové, implementácia spočívala hlavne v migrácii. Infraštruktúra „matky“ bola postavená ako hybridné riešenie (kombinácia vlastnej on-premise infraštruktúry s cloudovou). Reálne, čo Adecco Slovakia potrebovalo, bolo dostať všetky dáta od materskej firmy do nového prostredia, k sebe. To bolo gro migrácie.

Osamostatnenie spoločnosti nieslo so sebou aj ukončenie poskytovania IT podpory a všetkého, čo s IT súvisí. Migráciu bolo potrebné zvládnuť v stanovenom období.

Migrácia bola potrebná práve preto, aby sme si zachovali históriu dát. Keďže pracujeme s množstvom klientov, kandidátov a ich dátami, nejednalo sa len o migráciu Office a Microsoft vecí. Išlo o zabezpečenie čo najplynulejšieho prechodu. A ten sa dá dosiahnuť tým,

že sa nejde do niečoho úplne nového. To znamená v krátkom čase zabezpečiť dostupnosť všetkých potrebných údajov, funkčnosť systémov a celkovú správu IT riadenia. S tým súviseli aj bezpečnostné nastavenia, keďže politiky nadnárodného korporátu sa líšia od toho, čo potrebuje stredne veľká alebo veľká firma z pohľadu nárokov na IT, aj aké požiadavky majú používatelia a čo potrebujú. Migrácia vo výsledku priniesla fungujúcu kooperáciu cloud služieb a vlastnej infraštruktúry.

Prirodzene sa však dotkla aj oblasti bezpečnosti. Tá bola, rovnako ako všetky IT služby, do určitej doby zabezpečovaná „materskou spoločnosťou“. V čase, keď riziko kybernetických útokov rastie zo dňa na deň, bolo rozhodujúce zodpovedať si otázku: Ako zabezpečiť firemné dáta a ochrániť zároveň aj samotných používateľov?

Spoločnosť Adecco už od samého začiatku kladla veľký dôraz na ochranu nielen svojho know-how, ale aj identít a koncových zariadení. Uvedeným požiadavkám plne vyhovovalo obstaranie licencií Microsoft Business Premium. Tento nástroj vnímam pozitívne nielen v práci, ale aj súkromne. Nastavenia pomáhajú chrániť koncové zariadenia používateľov. Identifikujú, čo sa deje na ktorom počítači, detekujú možný útok na základe správania sa. Nástroj ma ako admina upozorní na to, čo

potrebujeme. Veľmi rád využívam Group Policy (skupinové politiky), odporúčania na ochranu proti úniku informácií (DLP politiky - data loss prevention), vyneseniu dát, GDPR problémom, a hlavne obmedzia používateľa minimálne, stále môže fungovať v plnom rozsahu. Napríklad ho obmedzia tým, že nemôže používať USB kľúče, čo by mohlo byť nevhodné a z pohľadu bezpečnosti problémové. Nielen pre jeho PC, ale zároveň pre celú firmu.

Pre firmu je dôležité, že na platforme Microsoft 365 pristupujete k službám v jednotnom prostredí, vyhovujúcim bezpečnostným štandardom vrátane GDPR. To vám zrejme výrazne uľahčí prácu a zvýši bezpečnosť a dohľad nad dátami. Zaznamenali ste zásadné zmeny v spôsobe práce po migrácii - prechode od matky?

Niektorí kolegovia áno. Boli to tí, ktorí dovtedy používali Office 2016. Ale keď zistili, aké existujú v M365 kolaboračné funkcie, tak im to určite pomohlo v ich práci. Kameňom úrazu pri migrácii môže byť časová náročnosť, preto sa oplatí obrátiť na vhodného partnera, ktorý má dostatok skúseností s implementáciou M365, odporučí kombináciu služieb alebo vhodný licenčný balíček pre firmu.

Čiže OneDrive a čaro zdieľania.

Ide o veľmi užitočnú funkciu zdieľania, lebo človek si OneDrive otvorí aj na inom zariadení, overí sa svojím účtom, a vytiahne čo potrebuje. Je zaznamenávané zariadenie, aj čo sa udialo na OneDrive. Reálne to je skvelá vec aj na backup pracovných staníc, čo vnímam ako podstatu OneDrive. Uvedme to na príklade: ak človeku „umrie“ počítač, stane sa niečo nepredvídané, prihlási sa svojím Microsoft účtom na inom zariadení, a okamžite funguje ďalej. OneDrive dokáže držať súbory aj lokálne aj cloudovo. Autosafe je skvelá funkcia M365 a uvedomujú si to aj zamestnanci.

Excelovské súbory v on-premise úložisku majú svoje obmedzenia. Do reportu na on-premise sa používateľ nedostane, ak ho už má otvorený iný kolega. Musí čakať, kým dokument uzatvorí.

Áno, napríklad súbor dávno zatvorený užívateľom bol pre ostatných stále nedostupný. Stačilo, že niekto nezavrel otvorený Excel, a ostatní si ho vedeli otvoriť len na čítanie, alebo potrebovali, aby admin súbor „odblokoval“. Vykonané zmeny sa v takom prípade často neuložili alebo sa vytvárali kópie toho istého súboru. Preto som prišiel s návrhom zdieľania reportov

všetkým, komu sú určené. Vysvetlil som kolegom, aké to má výhody. Napríklad: Zazdieľame si dokument, keď ty v reporte niečo upraviš, ja to hneď vidím, ty vidíš, na ktorom poličku som reálne, aby sme needitovali to isté naraz. Vidiš tam históriu súborov, keď nám to niekto zmaže, vrátíme sa späť. Fungujeme naraz kľudne aj piati či pätnásti, ako je potrebné.

Je niečo, kam sa chcete posunúť? Uvažujete o SharePoint?

Po dokončení migrácie som zo svojej pozície IT špecialistu začal presadzovať zdieľanie aj na ostatné tímy. Naším cieľom je vybudovať silný celofiremný SharePoint, s tým, že ho chceme využívať naplno, od schvaľovania cez power automate, všetko, čo si dokáže človek predstaviť. Jednou z užitočných funkcií sú SharePoint Listy. Obsahujú reporty, zoznamy, je to veľká výzva. Pôjde o prepojenie komplexnej agendy s dopadom na viac systémov.

Mobilita prácu admina vždy uľahčuje.

Isteže. Ako komunikačný kanál využívame Teams, používame ho hlavne ako Instant Messenger. Skupinu si môže vytvoriť každý, kto ju potrebuje. Nemáme aplikované žiadne obmedzenia. Máme možnosť pracovať vo webovom prehliadači a funguje to. Flexibilita Office je posunutá omnoho vyššie. Doplnené služby, ktoré sme získali v balíčkoch M365, nám veľmi pomáhajú. Mne osobne napríklad v situáciách, keď sa na mňa obráti niekto s otázkou cez Teams, či sa viem pozrieť do tabuľky na niečo, čo tam nefunguje. Ja si ju okamžite otvorím v telefóne, tak, ako by som to urobil na počítači, a problém vyriešim aj cez mobil.

Ako administrátor veľmi oceňujem a využívam aj Admin Center pre telefón, aplikáciu, kde dostávam push notifikácie o určitom probléme, a hneď viem reagovať.

M365 používa takmer celý svet – je to mainstream. Všetci sa následne prispôbujeme funkcionalite, ktorú aktuálne nastaví či ponúknu.

Keď niekoho prijímame do zamestnania, počítame s tým, že uchádzač ovláda základy, videl Word, Excel. Čo má Microsoft výborné, to sú fóra, skvelá vec, čo sa týka používania produktov MS. Otvorím si Google a hľadám Microsoft fórum, Microsoft dokumentácie, idem rad za radom, a pozerám si možné riešenia respektíve príčiny. Dostanem sa k tomu, čo potrebujem, alebo identifikujem

odporúčenie, ktoré sa najviac hodí na daný problém. Microsoft je vysoko „user friendly“ vec. Automaticky sa ako používateľ prihlásite do nástrojov a aplikácií, ktoré máte využívať: OneDrive, Teams, Outlook a ďalšie. Admin robí prvotný setup, úvodné nastavenia, používatelia dostávajú počítače, ktoré majú už predinštalovaný softvér, sú skontrolované, a majú obsah, čo tam má byť. A rovno pracuje. Je intuitívne navádzaný pre používanie tých funkcionalít, ktoré sú v aplikáciách k dispozícii. Nepokazí veci, ak niečo nevie, má podporu. Dokáže sa v základoch orientovať a učiť sa za pochodu. Zbiera skúsenosti a má k dispozícii dokumentáciu. Aj keď nemá znalosť EN, nájde odpovede aj v SK návodoch.

Z vyjadrení IT špecialistu zo spoločnosti Adecco Slovakia, či už v pozícii admina alebo používateľa, vyplýva, že je s Microsoft 365 spokojný. A to aj s benefitmi čo poskytujú nástroje a aplikácie, aj s podporou dokumentácie či funkciami pre používateľov. Samozrejme, ide o široký ekosystém, existujú v ňom rôzne rozšírenia, nadväzujú na data collection, Power BI, a ďalšie veci. Tým, že je to mainstream, admin má omnoho menej starostí s používateľmi.

Orientovať sa v širokom spektre služieb nemusí byť jednoduché aj vzhľadom na fakt, že Microsoft 365 je živý, stále sa rozvíjajúci ekosystém, u ktorého treba poznať možnosti a vnímať novinky. Kľúčovým je však poznať potreby zamestnancov, navrhnúť a naučiť ich používať prácu zjednodušujúce aplikácie, a tým chrániť celú firmu.



Článok čítajte na
platformofinvention.sk
Klikni alebo oskenuj QR



Marcela Gottwaldová
marcela.gottwaldova@gamo.sk

Novela ZoKB alebo aké zmeny prinesie nová smernica NIS 2

Ku koncu roka 2022 je bilancia taká, že zákon o kybernetickej bezpečnosti („ZoKB“) sme na Slovensku novelizovali celkovo sedemkrát. A predvídať vieme aj ďalšiu, relatívne rozsiahlu novelu. Novelu vyvolanú novou Smernicou NIS 2, ktorá by mala vo finálnom znení uzrieť svetlo sveta ešte tento rok.

Smernica NIS 2 nielenže nahradí svoju predchodkyňu z roku 2016, ale významným spôsobom rozšíri okruh povinných osôb, ktoré dnes na Slovensku poznáme pod pojmom prevádzkovateľ základnej služby. Povinné osoby sa po novom budú rozlišovať na dve základné skupiny, a to kľúčové a dôležité subjekty.

Významnejšie je ale rozšírenie oblastí regulácie, kedy oproti súčasnej právnej úprave ZoKB pribudnú nasledovné odvetvia (sektory) a pododvetvia (podsektory):

- Odpadová voda;
- Vesmír;
- Kuriérske služby;
- Odpadové hospodárstvo;
- Výroba, spracovanie a distribúcia potravín;
- Vodík;
- Diaľkové vykurovanie a chladenie;
- Výroba (zdravotnícke pomôcky, počítačové výrobky, elektrické zariadenia, stroje, motorové vozidlá, ostatné dopravné prostriedky a iné.

Zmeny zaznamenávajú aj niektoré už existujúce odvetvia a pododvetvia, kde

napríklad v odvetví „Digitálna infraštruktúra“ pribudnú poskytovatelia služieb dátového centra.

Zmena nastáva aj u poskytovateľov digitálnych služieb, kedy sa upúšťa od poskytovateľov služieb cloud computingu. Z nich sa po novom stávajú kľúčové subjekty. Poskytovatelia digitálnych služieb však naďalej zostanú „traja“, nakoľko k súčasným poskytovateľom služieb online trhoviska a internetového vyhľadávacieho prirubujú poskytovatelia platforiem služieb sociálnej siete.

Je očakávané, že na Slovensku by vďaka tomuto rozšíreniu mohlo odhadom pribudnúť niekoľko stoviek až tisíc nových subjektov. Výsledný rozsah je ťažké predvídať, keďže bude determinovaný nastavením identifikačných kritérií (prahových hodnôt), ktoré si bude Slovenská republika určovať v rámci existujúcej Vyhlášky č. 164/2018 Z. z. a ktoré určia, aký subjekt nám do pôsobnosti ZoKB padne a aký nie. Za všetko napokon hovorí porovnanie národných úprav kybernetickej bezpečnosti u nás a v Českej republike. Po transpozícii rovnakého predpisu (Smernice NIS z roku 2016) máme na Slovensku cca 3000 povinných osôb, zatiaľ čo v Českej republike desaťnásobne menej.

Nakoľko transpozícia Smernice NIS 2 sa vysoko pravdepodobne udeje aj (najmä) prostredníctvom ZoKB, vybrané subjekty vykonávajúce činnosti vo vyššie

uvedených odvetviach budú tiež povinné plniť požiadavky ZoKB.

Rozšírenie pôsobnosti ZoKB na nové sektory a podsektory je teda zrejmé. Smernica NIS 2 však oproti svojej predchodkyňi prichádza aj s novými požiadavkami, ktoré by sa mali odraziť v národných právnych úpravách členských štátov.

V tejto súvislosti je podstatná otázka, s akými konkrétnymi požiadavkami Smernica NIS 2 vstupuje do platnosti a v akom rozsahu a akým spôsobom sa odrazí vo vnútroštátnom práve. Smernica NIS 2 rovnako ako jej predchodkyňa prichádza len so všeobecným minimálnym bezpečnostným rámcom, ak chceme „must have“ požiadavkami, ktoré sa majú zrkadliť v národných právnych úpravách.

Sú to nasledovné požiadavky:

- Analýza rizík a bezpečnostné politiky informačného systému;
- Riešenie incidentov (predchádzanie incidentom, ich odhaľovanie a reakcia na ne);
- Kontinuita činností a krízové riadenie;
- Bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho dodávateľmi alebo poskytovateľmi služieb, ako sú napr. poskytovatelia služieb ukladania a spracúvania dát alebo riadených bezpečnostných služieb;
- Bezpečnosť pri nadobúdaní, vývoji

- a údržbe sietí a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach;
- Politiky a postupy (testovanie a audit) na posúdenie účinnosti opatrení na riadenie kyberneticko bezpečnostných rizík;
- Používanie kryptografie a šifrovania.

Z tohto pohľadu môžeme náš slovenský ZoKB hodnotiť ako nadčasový, nakoľko všetky vyššie uvedené požiadavky už máme zahrnuté v dnešnom znení ZoKB. Samozrejme nie je vylúčené, že v rámci transpozície dôjde k ďalším úpravám či rozšíreniam existujúcej právnej úpravy, tieto sa však ťažko predvídať. Napokon, ani súčasné znenie ZoKB nebolo v celosti vynútené požiadavkami pôvodnej Smernice NIS, kde Slovenská republika išla znením ZoKB na rámec európskych požiadaviek. Preto jedinou istotou dnes je, že so zamýšľanou zmenou ZoKB sa budeme vedieť oboznámiť v rámci legislatívneho procesu, v ktorom plánujeme našu aktívnu účasť.

Najzásadnejšou zmenou, ktorú Smernica NIS 2 z pohľadu súčasného znenia ZoKB prináša, teda nie sú nové povinnosti, ale počet nových subjektov, ktoré budú povinné plniť už existujúce a výhľadovo ďalšie povinnosti v zmysle ZoKB.

Ak by som mal predsa len predvídať, kde a ako sa ZoKB bude (mal by) meniť, bolo by to nasledovné:

- Doplnenie novej povinnosti popri kybernetických bezpečnostných incidentoch hlásiť aj závažné kybernetické hrozby;
- Doplnenie lehôt v rámci riešenia kybernetických bezpečnostných incidentov (do 24 hodín od zistenia incidentu poskytnúť prvotné oznámenie



Štefan Pilár
Bukovinsky & Chlipala

- a najneskôr jeden mesiac po uskutočnení prvotného oznámenia predložiť konečnú správu o riešení incidentu);
- Možnosť dohody s príslušnými orgánmi (napr. jednotkou CSIRT) na predĺžení lehôt podľa bodu vyššie;
- Poskytnutie odpovede k prvotnému oznámeniu o incidente vrátane počiatočnej spätnej väzby k incidentu zo strany prijímateľa oznámenia;
- Získanie usmernenia k vykonávaniu možných zmierňujúcich opatrení k hlásenému incidentu (na žiadosť oznamovateľa);
- Zvýšenie pokút až do 10 000 000 EUR alebo najviac 2 % celkového svetového ročného obratu.

V kontexte vyššie uvedených možných vstupov do ZoKB stojí za povšimnutie nižšie uvedené.

Prvým je síce nenápadné, ale veľmi dôležité rozšírenie notifikačných povinností aj o kybernetické hrozby. ZoKB totiž v súčasnom znení pod hrozbou sankcie vyžaduje len to, aby prevádzkovatelia hlásili „až“ tie závažné kybernetické bezpečnostné incidenty, ktorých atribúty (klasifikáciu) stanovuje osobitná vyhláška. Právnym výkladom by sa dalo dospieť k nezmyselnému, no právne súladnému záveru, podľa ktorého prevádzkovateľ „čaká a môže čakať“ na to, kým incident dosiahne aspoň prvý stupeň závažnosti a až následne ho nahlási príslušnému orgánu. Hoci dobrovoľnosť hlásenia tým nie je dotknutá. Tým, že po novom budú povinné osoby musieť hlásiť aj závažné kybernetické hrozby (klasifikácia podľa všetkého pribudne neskôr), odstráni sa tento možno výkladovo udržateľný, ale z praktického, logického a v neposlednom rade bezpečnostného pohľadu nešťastný „vyčkávací“ výklad procesu hlásenia incidentov.

Druhou je časť riešenia incidentov, kedy na strane štátu (najmä jednotkám CSIRT) pribúda explicitná požiadavka na poskytovanie odpovedí, spätných väzieb či usmernení k hláseným incidentom. Z praxe vieme, že v minulosti nastávali aj také situácie, kedy prevádzkovatelia základných služieb k svojim hláseniam nedostali žiadnu spätnú väzbu, súčinnosť alebo pomoc. Niekedy nezískali ani potvrdenie o prijatí oznámenia. Nie je to ani tak kritika, ale skôr obraz skutočného stavu kapacít štátu, od ktorých nemožno rozumne očakávať, aby sa individuálne venovali každému nahlásenému incidentu.

Nové povinnosti na strane štátu nepochybne prispievajú ku rýchlejšim či kvalifikovanejším reakciám na incidenty, ktoré by popri povinných osobách riešili aj na to určené expertné zložky štátu. Avšak bez navýšenia kapacít, ako aj dostatočného ohodnotenia aspoň sa približujúceho trhového priemeru, to nepôjde. Spoliehanie sa na úprimnú motiváciu expertov pomôcť štátu a tvoriť hodnoty vo verejnom záujme nás totiž dostalo tam, kde sme dnes. Dopady Smernice NIS 2 by tak bolo možné popísať nasledovne: Rozšírenie povinných osôb, potvrdenie smerovania súčasného ZoKB, čo sa požiadaviek týka, a v neposlednom rade zmena slovenského pohľadu na pôsobnosť jednotiek CSIRT pri riešení kybernetických bezpečnostných incidentov.

Pokiaľ ide o poslednú možnosť, želaným dopadom Smernice NIS 2 by mohli byť postupy, vďaka ktorým sa od analýz a zamýšľania posunieme k riešeniu dlhodobého problému, ktorý na Slovensku máme. Tým je budovanie a udržanie expertných kapacít na strane štátu. Konkrétne jednotiek CSIRT s dostatočným personálnym a materiálnym technickým zabezpečením. Napokon, zo správy o kybernetickej bezpečnosti v Slovenskej republike v roku 2021 jednoznačne vyplýva, že celkový počet detegovaných a hlásených incidentov presahuje číslo 600 000, čiže práce v tejto oblasti je viac ako dosť. Vývoj u nás pozorne sledujeme a svoje skúsenosti radi odovzdáme ďalej, či už v rámci legislatívneho procesu alebo inak.



Článok čítajte na
platformofinvention.sk
klikni alebo oskenuj QR



Štefan Pilár
spilar@bch.sk

Kritické roky

Digitálny svet stále trápí nedostatok pracovníkov v IT

Na Slovensku sa otvorene hovorí o kríze ľudských zdrojov. A netýka sa to len zdravotníckeho a učiteľského sektora, ale výrazne aj sektora informatiky a digitálnych zručností. Až 54 percent absolventov vysokých škôl nepracuje po ich ukončení vo vyštudovanom odbore. Až 68 percent absolventov odborných stredných škôl nepokračuje v zvolenom štúdiu. Firmy dlhodobo vnímajú, že nájsť kvalifikovaných pracovníkov je ťažká úloha. Dôvodmi sú podľa odborníkov zle nastavené školské osnovy a zrušenie povinnej praxe.

Je to tak? Podme si bez hodnotiacich úsudkov utriediť čísla, fakty a názory. Ivan Dolnák z FEIT Žilinskej univerzity v Žiline hovorí: „Vzťah slovenského školstva a jeho prepojenia na prax je poznačený sebaklamom. Sebaklamom na strane školstva aj na strane firemného sektora. Školstvo si mylne myslí, že pripravuje absolventov pre prax, a firemný sektor si myslí, že školstvo dokáže vychovať dokonalého absolventa pripraveného riešiť akúkoľvek pracovnú úlohu. Realita je však taká, že bežný absolvent dosahuje maximálne úroveň svojho učiteľa a len málokto ju dokáže prekročiť.“

Čísla z praxe

V Ročenke trhu práce 2021 je IT sféra vyhodnotená ako odvetvie s najnižším priemerným počtom reakcií na pracovnú ponuku, rovnajúcu sa číslu 5. Napríklad IT spoločnosť GAMO robila za ostatný rok 26 výberových konaní na 16 pracovných pozícií. Využívala na to okrem štandardných kanálov ako Profesia.sk, LinkedIn a webové kariérne stránky služby recruiterov a renomovaných personálnych agentúr. Na jednu pracovnú pozíciu sa pri tom hlásilo v priemere len 19 uchádzačov zo všetkých zdrojov a 3 pozície sú stále neobsadené. Nakoniec sa ukázalo, že najväčšiu úspešnosť má odporúčanie kolegu (až

v 55% prípadoch), následne boli úspešné agentúry (30%) a nakoniec portál Profesia.sk (15 %).

Čísla z ITAS

Zhruba 12 500 IT pracovníkov chýbalo v praxi už v roku 2015 a číslo sa neustále zvyšuje v negatívnom smere. Za jeden z najväčších dôvodov je stále považovaný školský – na Slovensku máme podľa ITAS len päť fakúlt, ktoré možno považovať za IT, tri „hard“ a dve „soft“ IT, a potom niekoľko fakúlt alebo odborov hospodárskej informatiky, kvalifikovaných v IT odbore ako „soft“.

A práve rôzna kvalita výučby informatiky na školách ovplyvňuje digitálne kompetencie študentov, vyplýva z výsledkov IT Fitness Test 2022, do ktorého sa zapojilo až 100-tisíc respondentov z krajín V4. Odborníci z ITAS na ich základe hovoria, že na školách je potrebné viac sa venovať rozvoju kritického myslenia, vyhodnocovaniu informácií a posudzovaniu ich kvality, dôveryhodnosti a pravdivosti.

Viceprezident ITAS Mário Lelovský rozumie tomu, že poddimenzovanosť začína u učiteľov. Osobne sa snaží priviesť vycestovaných Slovákov späť na Slovensko, aby vyučovali na tunajších školách. „Asi 40, 50 sa ich vrátilo, no problémami sú, samozrejme plat a všeobecné prostredie.

Keď firmy v priemere platia programátorom 2500 Eur, skúsený informatik nepôjde vyučovať na školu za 1000 Eur,“ priznal pre StartitUp. Dôležité je presadiť, aby vyučujúci na školách mali vyšší plat ako zamestnanci firiem.

Hlasy z Technickej univerzity v Košiciach

Vedúci Laboratória počítačových sietí na KPI FEI TUKE Miroslav Michalko hovorí, že si nedovolí zovšeobecňovať, či je celé vzdelávanie zlé alebo dobré. „Veľmi záleží na konkrétnych vysokých školách, aj od úrovni katedier a pedagógov, ktorí na nich pôsobia,“ vysvetľuje. Oblasť IT je veľmi rýchlo vyvíjajúcim sa segmentom trhu a je trochu naivné očakávať od vysokých škôl, aby všetky trendy hneď zavádzali do výučby. „Cieľom škôl je naučiť študentov hlbšie základy problematiky, pomôcť im pochopiť súvislosti, vedieť sa rozhodovať na základe správnych vyhodnotení a porozumení vstupov. Až prax ich zacieli presnejšie, zaškolí ich na konkrétne riešenia či požiadavky ich budúcich zákazníkov.“

Výškoliť študentov tak, aby ich zamestnávatelia vedeli hneď využiť, je preto skôr idealizované očakávanie ako dosiahnuteľná realita ktorejkoľvek školy. Hoci aj tu už vidíme zmeny k progresu vznikom nových študijných programov. Napríklad Fakulta

elektrotechniky a informatiky TUKE zriadila študijný program Kyberbezpečnosť, viaceré predmety majú obsahovú náplň kompatibilnú s požiadavkami priemyselných certifikácií, čo je známkou ich aktuálnosti voči trendom a potrebám firiem. „To však neznamená, že priestor na skvalitňovanie tu už nie je, naopak. No s takými požiadavkami ide v ruka v ruka aj požiadavka na posilnenie ľudských a technických zdrojov, a tam je prvá slabina súčasného systému,“ hovorí Miroslav Michalko. A popisuje slová odborníkov z ITAS: „Stredné školy akútne bojujú s akútnym nedostatkom IT špecialistov – pedagógov. V každom regióne si lokálni zamestnávatelia vedia týchto odborníkov preplatiť. Na školách zostávajú častokrát len nadšenci, ktorí sú motivovaní poslaním, prácou učiteľa.“ Tí musia mať navyše svätú trpezlivosť a potvrdzujú, že dnešní študenti už nie sú ako kedysi, ich vnímanie je roztrieštenejšie a záujem mizne. Za veľký problém doby považuje demotiváciu študentov aj Ondrej Kainz z FEI TUKE: „Motivovať ich je náročné, najmä po období, keď bolo vzdelávanie presunuté do online roviny. Väčšine stačí splniť minimálne podmienky pre absolvovanie predmetu či kurzu, čím sa znižuje kvalita a vedomosti zostanú na priemernej úrovni. Podobný jav bol, samozrejme, aj v minulosti, avšak v súčasnosti je percento takých študentov enormne vysoké.“

Východiská

Hlasy, ozývajúce sa po reforme systému zaznievajú zo všetkých strán roky. S tým,

že nemožno čakať, že nejako bude, a angažovať sa musí každý. Základné školy spolupracujú so strednými školami, spoločne sa pridávajú firmy a vysoké školy, duálne vzdelávanie bolo pred koronou úspešným projektom a treba v ňom pokračovať. Prepojenie školy s praxou je tým, čo môže zachrániť aj ten nezaujem či apatiu zo strany študentov. Reálne zadania vo firmách s využitím technológií, ktoré sú predmetom ich štúdia, prinášajú reálne pozitívne výsledky. „Prepojenie akademického prostredia s firemným skrz rôzne spoločné projektové aktivity, záverečné práce, zdieľané pracoviská, privádza študentov nielen k moderným technológiám – ku ktorým sa štandardne nemusia vedieť dostať – ale aj umožňuje lepšie porozumieť vnútro firemným procesom, komunikácii so zákazníkom či až riadeniu projektov,“ potvrdzuje Peter Fecilák z Katedry počítačov a informatiky FEI TUKE. „To, čo nevedia dať školy, častokrát vedia nahradiť zamestnávatelia,“ súhlasí vedúci laboratória počítačových sietí Miroslav Michalko. „Dúálne vzdelávanie je overený model, ktorý pomáha vychovávať nielen zručnejších, ale aj motivovanejších študentov. Mnohým študentom to už na strednej škole pomôže rozhodnúť sa čomu sa budú v živote venovať. A získať motivovaných študentov je výhra pre každého pedagóga.“ Výrazným prínosom na desiatkach technických stredných škôl je v tomto procese implementácia Programu sieťových akadémií Cisco, ktorej obsah je v súlade s priemyselnými certifikáciami a požiadavkami zamestnávateľov, plus generuje kvalitných a odborne zdatných učiteľov.

„Na technických vysokých školách je už bežné, že významné percento študentov počas štúdia pracuje. Môžeme polemizovať o výhodách, či nevýhodách tejto reality – ale každopádne končiaci študenti sú oveľa lepšie pripravení pre prax ako kedysi. Celkovo je možné v danej oblasti spolupráce medzi školami a praxou konštatovať výrazne pozitívny posun. Firmy už častokrát nehľadajú na vysoké školy len ako na zdroj zamestnancov, ale hľadajú formy spolupráce na spoločných projektoch – aj prostredníctvom schém vedeckých parkov, ako je Univerzitný vedecký park TECHNICOM, alebo inovačných HUB-ov ako napríklad EDIH CASSOVIMUM,“ uzatvára Miroslav Michalko.

S GAMO v praxi

Takúto spoluprácu nadviazala v bansko-bystrickom kraji napríklad IT spoločnosť GAMO. Základná škola Jozefa Gregora Tajovského v Banskej Bystrici patrí medzi pár veľmi kvalitných škôl, ktoré priebežne inovujú vzdelávacie metodiky i technické vybavenie a spolupracujú so strednými, vysokými školami aj firmami. GAMO tam v rámci spoločného Memoranda o spolupráci zabezpečuje kyberbezpečnosť, vzdeláva zamestnancov v nových technológiách, robí osvetu a podporné programy pre rodičov, a podieľa sa aj na materiálnom zabezpečení.

Zároveň memorandum podporuje špirálu vzdelávania medzi základnou školou, odbornou strednou, technickými typmi vysokých škôl a vo finále s konkrétnou spoločnosťou. „Áno, je to tak, štartujeme spoločný projekt so zapojením viac škôl – od základnej až po vysokú,“ potvrdzuje výkonný riaditeľ GAMO, a. s., Rudolf Latiak. V bansko-bystrickom kraji ide o Prvé súkromné gymnázium špecializujúce sa na virtuálnu grafiku a kyberbezpečnosť, Strednú odbornú školu, ktorá okrem štandardného IT zamerania a kyberbezpečnosti otvára aj odbor IoT, a aj FEI na Žilinskej univerzite. „Cieľom je, aby deti už počas štúdia na základnej škole mali možnosť získať okrem všeobecného aj technické vzdelanie, aby dostali šancu na podchytenia ich talentu.“



Článok čítajte na
platformofinvention.sk
klikni alebo oskenuj QR



Iveta Hlaváčová
iveta.hlavacova@gamo.sk

Vzdelávaniu v IT bezpečnosti svieti kontrolka

Podľa prieskumu Slovak Business Agency a NBÚ medzi strednými a malými podnikmi sa v SR zaoberá kybernetickou bezpečnosťou len tretina menších a polovica stredne veľkých firiem, pričom odborníci v tejto sfére chýbajú v tisícoch. Čo s tým a kde treba začať? Zástupcov technických vysokých škôl sme oslovili s otázkou: Ako by mala vyzeráť budúcnosť vzdelávania IT a kybernetickej bezpečnosti? Budeme svedkami úspešného príbehu alebo premrhaných rokov?



Miroslav Michalko
vedúci LPS KPI FEI TUKE

Pozitívnu aktivitu prináša Digitálna koalícia a projekt IT Akadémia – tím, že na školách začala školiť digitálnych koordinátorov. Dôležité je aj posilniť spoluprácu IT firiem a škôl, keď prídu odborníci z praxe na pár hodín týždenne učiť IT na školy. Aj keď tomu čiastočne bráni legislatíva, verím, že je to riešiteľné. V rámci diskusií s riaditeľmi stredných

odborných škôl som zachytil aj myšlienku tzv. zdieľaných IT učiteľov – to znamená, že jeden učiteľ by vyučoval kybernetickú bezpečnosť na viacerých stredných školách. Aspoň na prechodné obdobie, kým si školy posilnia vlastné personálne kapacity, to môže byť riešenie. No tieto rozhodnutia patria do rúk kompetentným v rámci vedenia nášho školstva. Keď sa chce, tak sa určite cesta nájde.



Ivan Dolnák
FEIT UNIZA

Informatické odbory sa ženú za implementáciou vzdelávania v oblasti kybernetickej bezpečnosti, a pritom ignorujú fakt ako sa svet počítačov vyvíjal. Dôvod? Lebo slová „kybernetická bezpečnosť“ dobre znejú v ponuke študijných odborov. Aj v budúcnosti je najskôr potrebné naučiť študentov ako boli zamýšľané

funkčnosti počítačových technológií, a až následne aké zraniteľnosti obsahujú a ako sa proti ich zneužitiu brániť. Nie je možné učiť „len stále čosi nové“ bez základov. Najväčšou výzvou je však nepremrhať príležitosť a dostupný čas. O 5 rokov môže byť z témy kybernetickej bezpečnosti úspešný príbeh, podložený skupinou úspešných absolventov ďalej rozvíjajúcich túto oblasť. Alternatívny príbeh môže byť 5 premrhaných rokov a zopár sklamaných ľudí. Súčasne je výzvou zabezpečiť dlhodobé priebežné financovanie a prílev nových ľudí, aby dosiahnuté výsledky postupne nezanikli. Kybernetickú bezpečnosť našťastie nejdeme tvoriť od základu, ale vlastne „iba implementovať“.



Peter Fecilák
KPI FEI TUKE

Mala by byť prepojená s jasne definovanými potrebami praxe, sledujúca aktuálne štandardy a garantovaná odborníkmi v danej oblasti. Vzdelávanie musí ísť ruka v ruke s hlbokým poznaním aktuálnych technológií, poznaním ich slabín, a následne so spôsobom ochrany pred jednotlivými zraniteľnosťami. Dôležitá je aj udržateľnosť odborníkov

v akademickom prostredí a dostupnosť hardvérového či softvérového vybavenia vzdelávacím inštitúciám.



Ondrej Kainz
KPI FEI TUKE

Podstatné je zabezpečiť kvalitných lektorov, ktorí majú nielen teoretické vedomosti z danej oblasti, ale aj praktické zručnosti z praxe. Zabezpečiť kvalitný vzdelávací proces postavený na aktuálnych trendoch a potrebách trhu.



Iveta Hlaváčová
iveta.hlavacova@gamo.sk



Článok čítajte na
platformofinvention.sk
Klikni alebo oskenuj QR

Sme uznávanými profesionálmi v segmente

Kde a ako to môžeme poslať do sveta?

Ostatné roky sú obrovskou skúškou pre podnikateľské subjekty v celej Európe. Nielen pre veľké korporáty, ale aj pre malé a stredné podniky. Niektoré firmy s 5 až 100 zamestnancami museli podstúpiť rozsiahle opatrenia alebo dočasne zastaviť činnosť. Podľa Slovak Business Agency bol pritom v roku 2020 ich podiel na celkovej zamestnanosti v SR 74,2 percenta. Prežili najmä tie, čo menili stratégiu a hľadali nové cesty pre biznis.

Ako však získať v sťažených podmienkach nových klientov? Ako rozšíriť svoj priestor doma aj mimo Slovenska? Kto v tomto malom a stredným podnikom pomôže? Aj o tom sme sa zhovárali s Kristiánom Alakšom, generálnym riaditeľom spoločnosti GAMO a.s.

Ako sa štát stará o veľký segment zamestnanosti na Slovensku? Kto najaktívnejšie vytvára networkingu a podpory malým a stredným podnikom? Kto im pomáha ukázať cestu a možnosti? Je na to u nás účinná špecializovaná forma pomoci?

Áno, je. Presvedčili sme sa o tom v ostatných rokoch aj my v GAMO. Takýmito subjektami sú najmä SARIO, Ministerstvo hospodárstva SR, ale aj EXIM banka a Ministerstvo zahraničných vecí a európskych záležitostí, ktoré robí exportné fóra. Na aktivitách SARIO vidno, že chcú pomáhať. Nikdy by som si nepomyslel, že štátna inštitúcia môže až v takej miere reálne pomáhať podnikateľom v tom, aby sa presadili na zahraničnom trhu.

Ako presne SARIO pomáha?

SARIO podporuje malé a stredné podniky pri prezentácii v zahraničí na rôznych podnikateľských misiách, výstavách a veľtrhoch. Vytvára priestor pre komunikáciu s potenciálnymi zahraničnými partnermi, poskytuje cenné kontakty, a zároveň pôsobí ako štátny garant dôveryhodnosti našich firiem. Poskytuje aj jazykovú podporu, ak je potrebná. Veľkým benefitom je networking počas

podnikateľských misií, ktorý prirodzene vzniká medzi slovenskými firmami. Synergické efekty zo stretávania sa podnikateľov sú dokonca častokrát väčšie než očakávania získania zahraničného biznisu. Povedal by som, že tieto firmy sú rovnako nastavené, myslia vo veľkom, chcú ísť za hranice. Neberieme sa ako konkurencia, naopak, aj navzájom rozvíjame spoluprácu alebo si aspoň posúvame cenné rady.

Ako sa možno prihlásiť do výziev týchto inštitúcií, otvoriť si cestu zo Slovenska do zahraničia?

SARIO ponúka napríklad pomoc formou Národného projektu, ktorý je financovaný z fondov Európskej únie. Určený je pre malé a stredné podniky so sídlom mimo bratislavského kraja. Na každú podnikateľskú misiu existuje jednoduchý registračný formulár a forma pomoci následne závisí od typu misie. Buď idú podnikatelia spolu so SARIO na konferenciu, na veľtrh, ako návštevníci, alebo idú ako spoloční vystavovatelia slovenského stánku vo vizuále Good Idea Slovakia. V tomto prípade majú vybrané firmy možnosť prezentovať svoje produkty a služby na veľkých medzinárodných fórach a takmer bezplatne.

Je prihlasovanie sa na tieto misie komplikované?

Každá jedna aktivita má svoj registračný formulár, v ktorom záujemca vyplní údaje o firme a o tom, čo by chcela prezentovať. Či ide o novú službu, nový výrobok, a podobne. Keďže Národný projekt je

určený pre malé a stredné podniky, musíte sa, samozrejme, kvalifikovať ako malý a stredný podnik. Následne príde spätná väzba o tom, či vás vybrali. Keď sa ale s niekým o týchto aktivitách bavíme, buď ich nepozná alebo tomu nedôveruje.

Prečo? Ide o slabé povedomie o SARIO ako o značke? Alebo je to finančne náročné?

Práveže naopak, náklady, ktoré si hradí firma, sú väčšinou oveľa nižšie ako náklady hradené SARIO. Firma hradí osobné náklady ako letenky a diéty, pri veľtrhoch to môže byť aj ubytovanie. Napríklad počas veľtrhu hradí SARIO celú výstavnú plochu, prenájom, dizajn, remeselné práce za postavenie celého stánku, poznateľnosť značky, propagačné materiály, catering a ďalšie položky.

Máte už aj praktickú skúsenosť v podobe spolupráce?

Áno, máme. Tak ako som spomínal, dôležitý je aj networking medzi slovenskými podnikateľmi. Podarilo sa nám v spolupráci s ďalšími partnermi poskladať spoločný produkt, ktorý je na túto dobu veľmi aktuálny. Dobrá príležitosť, ale aj dobrá škola medzinárodného obchodu bola hneď po prvej podnikateľskej misii v Dubaji. Šlo o nový produkt patriaci pod kybernetickú bezpečnosť. Obchodné príležitosti z iných misií sú momentálne v ďalšej fáze rokovaní.

Čo je najväčšou devízou spolupráce so SARIO?

Určite možnosť spolupráce s agentúrou z daného teritória, ktorá dohodne a zabezpečí obchodné rokovania na mieru. Je to ďalší náklad hradený zo strany SARIO. Pred podnikateľskou misiou prebehnú medzi nami a agentúrou online stretnutia, kde si určíme čo ponúkame, aké produkty a služby, čo očakávame, či hľadáme potenciálnych zákazníkov, obchodných partnerov, alebo máme záujem o zastúpenie v teritóriu. Agentúra následne predloží našu ponuku druhej strane.

Musím povedať, že stretnutia sú veľmi relevantné, dokonca často sa tu dohodnú stretnutia s predstaviteľmi vlády, veľkých národných a nadnárodných spoločností. Ďalšou výhodou je možnosť zoznámiť sa a priamo komunikovať s predstaviteľmi zastupiteľských úradov Slovenskej republiky, či už s veľvyslancami alebo ekonomickými diplomatmi. Devízou je aj už spomínaná spolupráca na projektoch s ďalšími slovenskými firmami, ktoré na týchto medzinárodných eventoch spoznávame.



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
Kybernetická bezpečnosť
zuzana.omelkova@gamo.sk



Branislav Lupták
Softvérové riešenia
branislav.luptak@gamo.sk



Martin Pisák
Technické riešenia, Cloud
martin.pisak@gamo.sk



Jana Kohárová
Obchod
jana.koharova@gamo.sk



Iveta Hlaváčová
Marketing
iveta.hlavacova@gamo.sk

Máte inšpiratívnu skúsenosť v oblasti informačných technológií pre podnikanie?
Oslovte našu redakciu a podelte sa o ňu v našom magazíne.

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

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

PONÚKAME ŠTARTOVACIE SLUŽBY KYBERNETICKEJ BEZPEČNOSTI



Konzultácia so špecialistom

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

Popis služby

Cena služby

Predbežný záujem



Usmernenie po telefóne

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

Popis služby

Cena služby

Predbežný záujem



Školenie zamestnancov

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

Popis služby

Cena služby

Predbežný záujem

GAMO
INFORMAČNÉ TECHNOLOGIE

Cloud ponúka výkon vždy, keď ho potrebujete.

Chcem zistiť viac



ZMENIL SOM
INVESTIČNÉ NÁKLADY
NA PREVÁDZKOVÉ

AKTIVUJEM,
ZAPLATÍM A VYUŽÍVAM
GAMO CLOUD!