platform of invention

Informačné technológie pre podnikanie s nápadom

online | pdf | print

Užitočné v správnych hlavách

magazín pre CTO, CFO, CEO

číslo 3
ročník druhý | 1/2022

Útok nie je iba číslo

Čo robiť na ochranu firemných dát?

Cloud Made in Slovakia!

Hybridná práca: fenomén doby

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.

Tlačený magazín
Online portál

Aktuálne 3. číslo
Objavte benefity IT made in Slovakia.

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

Ponuka dňa: SK kvalita 24/7

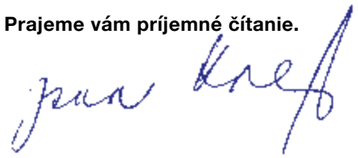
Všetci poznáme značku @SK. Ide o najznámejšie označenie kvality domácich slovenských výrobcov a pôvodu potravín. Áno, je to diametrálne odlišný sektor podnikania ako IT, ale existuje dôvod aby rovnaký princíp neplatil aj pre náš biznis? Aj my sme lokálny poskytovateľ cloudu a hrdo sa hlásime k Made in Slovakia.

Uznávame, že byť konkurentom gigantov ako Google, Amazon či Microsoft nikdy nebola a nebude jednoduchá cesta, no určite je správna. Pretože my VIEME. Pretože si ROZUMIEME. Pretože nám sa DOVOLÁTE. Ponúkame kvalitu, hovoríme po slovensky, a sme k dispozícii 24/7.

Poďme si to rozobrať na drobné. V čom môže byť slovenský cloud iný? Zahraničné spoločnosti sú rozhodne dobrými poskytovateľmi, sú väčší rozsahom a majú viac služieb v ponuke. Spoločné však máme toto: špičkové technológie, garantovanú spoľahlivosť, bezpečnostné certifikácie, pravidelné audity. Plus s nami nemusíte tápať v zložitých konfiguráciách, v aktualizáciách operačného systému, aplikačných vybaveniach či bezpečnostných nastaveniach. Zistíme čo prevádzkujete a spoločne navrhneme vhodné a dostupné riešenia. S okamžitou dostupnosťou podpory bez akejkoľvek jazykovej bariéry.

Aj manažér pre EMEA región z Lenovo Slovakia Branislav Kartik potvrdzuje s GAMO Cloud spokojnosť. Na stránkach 6 a 7 tretieho vydania magazínu Platform of Invention sa dozviete, prečo táto nadnárodná firma dôveruje nášmu SK produktu, a aj to, ako IT technológie uľahčujú firmám život a podporujú úspešné podnikanie.

Prajeme vám príjemné čítanie.



Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Jana Kohárová
Obchodná riaditeľka
jana.koharova@gamo.sk

Nemáte vlastných bezpečnostných špecialistov? Máte ESET

Pri digitálnom zabezpečení firiem je jednou z najväčších výziev pokrytie kompletného perimetra spoločnosti tak, aby sa nenašla ani malá medzierka, kadiaľ by útočníci prepašovali svoj škodlivý kód. Už tak komplikovanú úlohu výrazne sťažuje aj nedostatok odborníkov na kybernetickú bezpečnosť. Na Slovensku overiteľne chýba vyše 10-tisíc IT špecialistov. V prípade, že spoločnosti nemajú ľudí, ktorí by dokázali reagovať na jednotlivé hrozby a správne zaplátať bezpečnostné diery, prichádza na scénu ESET so svojím produktom ESET PROTECT MDR. S touto službou zákazníci získajú nielen špičkovú technológiu rozšírenej detekcie a reakcie (XDR), ale aj neustále dostupnú podporu od špecialistov spoločnosti ESET a ich bezkonkurenčné odborné znalosti, s ktorými majú firmy istotu maximálneho využitia všetkých bezpečnostných riešení.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Július Selecký
Senior Technical Pre-Sales Representative
ESET, spol. s r.o.

Až 89% organizácií má nedostatky v ochrane dát

Nárast objemu dát sa za ostatné dva roky viac než zdvojnásobil. V nemalej miere sa to deje vďaka rozširovaniu prác na diaľku alebo využívaniu cloudových služieb. Úmerne s masívnym nárastom sa logicky zvyšujú aj riziká spojené s dátovou ochranou. Až 89% organizácií priznalo v tejto oblasti nedostatky. Osemnásť percent organizácií vo svete dáta nezálohuje a tým ich vystavuje nechránené napospas kybernetickým zločincom. Závery najväčšej štúdie svojho druhu Veeam Data Protection Trends Report 2022 sú však povzbudivé. Organizácie

chcú ročne vynakladať na ochranu dát o 6 % viac ako na všeobecné investície do IT a už 67 % podnikov sa pri ochrane dát spolieha na cloudové riešenia.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Michal Štětina
Field Marketing Manager CEE
Veeam

Bezpečnosť naša každodenná. Pre malé a stredné firmy

V čase, keď riziko kybernetických útokov rastie zo dňa na deň, stojí veľa firiem pred otázkou Ako zabezpečiť naše dáta a ochrániť našich používateľov? A vôbec sa to netýka len veľkých, ale aj malých a stredných podnikov.
Odpoveď na ňu dnes priniesol Microsoft. Spoločnosť predstavila novú službu na poli bezpečnostných nástrojov práve pre firmy zo segmentu malých a stredných firiem. Microsoft Defender for Business je nástroj, ktorý pomáha chrániť koncové zariadenia používateľov. Vďaka automatizácií a prvkom umelej inteligencie dokážete nasadiť rýchlu ochranu pred hrozbami, zisťovať a reagovať na ne. Nastavenie používania tohto nástroja je jednoduché a intuitívne.

Hlavné kľúčové funkcie sú:

- Zjednodušená konfigurácia klienta - jednoduchá konfigurácia zariadenia, nastavenia politík zabezpečenia;
- Prehľad hrozieb a rizík - identifikácia hrozieb a rizík v reálnom čase;
- Ochrana ďalšej generácie - posilnenie a overenie si zabezpečenia vašej siete;
- EDR - detekcia útokov na základe správania.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Lukáš Okál
Product Marketing Manager
Microsoft

Za každým útokom je zraniteľnosť, o ktorej ste nevedeli

Viete čo majú spoločné sociálne inžinierstvo a zneužívanie zraniteľností? Sú to s vysokým náskokom dve najjednoduchšie a najpoužívanejšie taktiky útočníkov na prekonanie bezpečnostných opatrení. Sociálne inžinierstvo a využitie zraniteľností boli základom viac než 75% všetkých úspešných útokov v roku 2021. Chcete IT bezpečnosť firmy posunúť na vyššiu úroveň? Pravidelné vzdelávanie zamestnancov a vykonávanie testov zrani-

teľnosti sú dvoma najdôležitejšími krokmi pre kohokoľvek, kto to myslí s bezpečnosťou vážne. Za každým väčším kybernetickým útokom je zraniteľnosť, ktorá nebola odstránená - odhaľte ju skôr ako útočník. Po vykonaní scanu získate komplexný prehľad o slabých miestach všetkých vašich aktív, vrátane zraniteľnosti, chybných konfigurácií a ďalších potenciálnych bezpečnostných hrozieb ohrozujúcich vašu firmu.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Igor Chudáčik
Produktový manažér
GAMO a.s.

Rýchlosť. Škálovateľnosť. Automatizovaná prevádzka

Doprajte si funkčný ekosystém Kubernetes, ideálnu platformu pre hosťovanie aplikácií vo svete riadenom z cloudu. Nemusí vás trápiť nedostatok skúseností. Stačí si vybrať spoľahlivého partnera, ktorý vám cestou kontajnerizácie a Kubernetes umožní prevádzkovať moderné aplikácie. Tak nielen ľahko nasadíte nové aplikácie, ale upravíte už aj existujúce. Môžete sa plne sústrediť na vývoj, tvorbu a implementáciu softvéru s vedomím, že infraštruktúra beží vo výkonnom a bezpečnom cloud prostredí. Jej poskytovateľ sa postará nielen o funkčnosť platformy Kubernetes, ale zabezpečí aj jej pravidelné aktualizácie a údržbu.
Technicky zdatných špecialistov je na trhu málo a navyše sú drahí. V Kubernetes im vytvoríte podmienky, aby sa venovali vášmu biznisu reagujúc na požiadavky v čase a kvalite.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Martin Pisák
Vedúci divízie realizácie MSP
GAMO a.s.

Kybernetická bezpečnosť musí stáť na pevných základoch

EDR, CVE, SIEM, ATP, XDR... Snažíte sa zvýšiť IT bezpečnosť vašej firmy, ale strácate sa v záplave skratiek? Vstúpiť do oblasti kybernetickej bezpečnosti je veľkou výzvou a jej komplexnosť môže mnohých odrádzať. Čo je premyslený marketing a čo sú technológie zásadným spôsobom ovplyvňujúce úroveň vášho zabezpečenia?
Kybernetická bezpečnosť musí stáť na silných technologických základoch, na ktoré v tesnom závese nadväzujú služby riadenia a správy nasadených technologických riešení. Postupujete schémou bezpečnostnej pyramídy a systematicky si budujete kybernetickú odolnosť od základov až po expertné služby. Pri zostavovaní jednotlivých úrovní je braný ohľad na aspekty, ktoré sú z pohľadu firiem očakávané - dôležitosť a relevantnosť pri dosahovaní bezpečnosti, čo najlepší pomer cena/zvýšená bezpečnosť, ako aj komplexnosť riešenia a s ním spojená potreba pokročilej expertízy. Ako budovať a porozumieť bezpečnosti úroveň po úrovni?

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Igor Chudáčik
Produktový manažér
GAMO a.s.

Útok nie je iba číslo!

Prečo je zálohovanie v M365 nutnosť a čo robiť na ochranu firemných dát

To, že kybernetických útokov pribúda, je holý fakt. Čítame o nich na sieti, počujeme v rádiu, sledujeme ich v televízii. Neznamená to však, že idú mimo nás. Nik nie je pred útokom kybernetických zločincov chránený. V roku 2021 bol v Európe zaznamenaný nárast kyber útokov o 68% oproti 2020 (zdroj: Check Point research). Pred stratou firemných aj osobných dát pomôže len jediné – byť dobre pripravený.

Na úvod si predstavme číslo 777. To je podľa Check Point Cyber Attack trends priemerný počet kybernetických útokov za týždeň na organizácie v regióne EMEA zahŕňajúcich Európu, Stredný východ a Afriku. Tento región má zároveň nelichotivé prvenstvo v trende ich nárastu a priamo úmerne sa zvyšujú aj objemy uniknutých dát. V minulom roku šlo až o 260 terabytov, čo predstavuje viac ako 1,8 miliardy dokumentov, súborov a e-mailov (zdroj: Tenable's 2021 threat landscape retrospective).

Sofistikovaný útok? Nie. Len odhalenie zraniteľností

Za číslom 777 si nemusíme predstaviť sofistikovaných a najlepších hekerov sveta. Sú to stredne zruční, menej motivovaní jednotlivci, organizované skupiny, prípadne softvér, ktorý sa snaží veci zjednodušiť. Na útok nevynakladajú veľké úsilie, ale využívajú už existujúce zraniteľnosti. „Ide o slabé miesto informačného aktíva, doslovne o slabinu informačného systému," vysvetľuje Igor Chudáčik, produktový manažér IT spoločnosti GAMO. „Chápe sa ako problematické alebo ľahšie napadnuteľné miesto systému či prekonateľné miesto bezpečnostných opatrení, prípadne ako nevhodný spôsob implementácie systému alebo jeho ochrany." Pre ilustráciu: v porovnaní s rokom 2016 narástla zraniteľnosť až o 241%.

Alarmujúce je navyše to, že na väčšinu zraniteľností sa dá jednoducho nájsť exploit, spôsob na vniknutie do systému. Tie sú navyše verejné dostupné s celým kódom aj vysvetlivkami na stiahnutie, úpravu a spustenie. Platí pritom, že čím viac je zraniteľností, tým je väčšia pravdepodobnosť na vniknutie útočníka do systému.

Ransomvér ako služba

Ponúkajú ho na kybernetické útoky zamerané spoločnosti ďalším počítačovým zločincom, ktorí chcú spolupracovať na útokoch ransomvérom. Ten je pripravený na nasadenie spolu s príručkami ako ho vykonať. Jednoducho povedané, na dark nete sa dá kúpiť celý návod, ako ransomvér útok vykonať smerom ku konkrétnej spoločnosti. Obe strany sa následne dohodnú na sume, prípadne na podiele z výkupného, ktorú obeť zaplatí.

Prime Threat

Z útokov, ktoré obsahovali malvér, bolo až 38% ransomvérových. Viacerými medzinárodnými organizáciami bol vyhlásený ako najväčšia hrozba rokov 2020 a 2021.

Práve v dobe pandémie šlo o jeden z najviac používaných útokov a každý týždeň sa až 1200 organizácii stane obeťou atakov takéhoto typu.

Dobrou správou však je, že ak máme nasadený manažment zraniteľností, znamená to, že o nich vieme a napravíme ich. Tým môžeme výrazne znížiť riziko napadnutia.Organizácie využívajúce manažment zraniteľností založený na rizikách, zaznamenávajú o 80 % menej prípadov narušenia (zdroj: Forcepoint – Cybersecurity, compliance and protecting critical data, 2021).

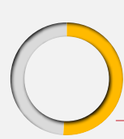
Testy zraniteľnosti sú bežne dostupnou službou, ktorú ponúkajú rôzne IT spoločnosti. Pre ochranu systémov je manažment zraniteľnosti absolútnou alfou a omegou v zabezpečení informačného systému.

V uplynulých 18 mesiacoch až 80% organizácií zaznamenalo data breach - prišlo o dáta. Pričom až 43% týchto firiem uviedlo 10 a viac takýchto prípadov! To znamená, že po prvom úniku nespravili žiadne kroky k lepšiemu zabezpečeniu svojich systémov.

DÁTA SÚ PRE FIRMU ŽIVOTNE DÔLEŽITÉ

Až 94% firiem po masívnom úniku dát zanikne

43% z nich už nikdy neotvorí prevádzku



51% z nich zanikne do 2 rokov

Zdroj: Univerzity of Texas.

Sme malá firma, nikoho nezaujímame

Staré známe a opakujúce sa ‚Nám sa to nemôže stať', rozhodne neplatí. Kybernetickí zločinci „nediskriminujú". Malé a stredné firmy sú pre nich dokonca zaujímavejšie ako veľké korporáty so sofistikovanými bezpečnostnými riešeniami. Veľký počet malých firiem s malým rozpočtom na kybernetickú bezpečnosť a nedostatkom kvalifikovaného personálu ich robí pre kyber útok naopak veľmi atraktívnymi.

Zálohovanie v M365

Už teda veríte, že záloha dát je nesmierne dôležitá? Najpoužívanejším SaaS riešením na trhu je Microsoft 365. Od základov zmenil systém a firemnú produktivitu. Mnoho firiem je na ňom doslova závislých. Zdieľame kalendáre, súbory, mailboxy a spoločne pracujeme na projektoch kedykoľvek a kdekoľvek. ALE! Zdieľanie je snom každého hekera! Vzhľadom k tomu, aké sú pre nás súbory dôležité, je ich zabezpečenie a ochrana dát imperatívom pre zachovanie produktivity a kontinuity podnikania. V Microsofte 365 je o dáta dobre postarané. Jeho zodpovednosťou je udržať globálnu infraštruktúru, zabezpečiť dostupnosť služieb a dát a v neposlednom rade postarať sa o ne v datacentrách. Ak napríklad slovenská firma uchováva dáta v rámci Európskej únie, Microsoft uchováva dáta ešte v ďalšom inom datacentre s cieľom zabezpečiť vysokú ochranu a dostupnosť v prípade straty, ale aj prírodných katastrof.

Kde však môže nastať problém?

Vysvetlime si najskôr model zdieľanej zodpovednosti. Ak hovoríme o on-premise riešení, čo znamená, že sú dáta uložené vo vnútri firmy, zodpovednosť za všetko nesie práve a len firma. Od údajov, cez zariadenia, hardvér až po identity, ktoré k nim pristupujú. Ak hovoríme o riešení SaaS, zodpovednosť zčasti nesie firma a zčasti je už zodpovednosť aj na strane Microsoftu. Firma v tomto prípade zabezpečuje, aby mal systém správne nastavené údaje, kontá, a to, za akých podmienok pristupujú tieto kontá k aplikáciám.
Vykonať úspešný útok na Microsoft datacentrum, ktorého zabezpečenie predstavuje to najlepšie zo sveta kybernetickej bezpečnosti, je tak náročné a tak málo pravdepodobné, že to rovno môžeme aj vylúčiť. To znamená, že strata dát pri hekerskom útoku alebo akejkoľvek fyzickej poruche je málo pravdepodobná. Oveľa väčšou pravdepodobnosťou je, že o dáta firma príde pre najslabší článok technickej vyspelosti, ktorým je človek. Až 64% stratených dát bolo totiž spôsobených na základe ľudskej chyby, zlyhaním ľudského faktora (zdroj: Aberdeen Group Analyst Insight – SaaS Data Loss).
Ako sa to môže stať? Jednoducho. Stačí jeden klik na odkaz alebo súbor s malvérom, stačí získanie prihlasovacích údajov jediného zamestnanca na to, aby sa útočník dostal k firemným dátam. Podľa prieskumov sa to deje veľmi často. Až jeden z piatich zamestnancov napriek bezpečnostným školeniam klikne na phishing odkaz a až 67,5% ľudí zadá prihlasovacie údaje na phishing webe.

> Microsoft myslí na neúmyselné zmazanie dát a preto ponúka možnosti a nástroje na ich obnovu po dobu 30 až 93 dní. Vedeli ste však, že priemerný čas odhalenia útoku až 200 dní? Myslite na tento fakt pri vytváraní retenčnej politiky.

Hrozivé čísla ukazujú, že s rastúcim počtom útokov je čoraz viac na mieste uvažovať o vyššej ochrane dát vo firemnej politike. Informačný systém potrebuje naozaj dobrú ochranu, aby im vedel odolať. No zároveň firma potrebuje aj riešenia, ktoré minimalizujú následky ľudského zlyhania. S týmito výzvami môžu pomôcť 3 riešenia GAMO M365 BACKUP.
Ide o spravovanú službu poskytujúcu istotu, že kópia dát je zálohovaná v bezpečí pred akoukoľvek hrozbou, či už ide o neúmyselné zmazanie dát, externé kybernetické hrozby alebo interné hrozby pri personálnych zmenách. Služba zároveň poskytuje zabezpečenie retenčnej politiky nastavenej podľa legislatívnych požiadaviek alebo požiadaviek spoločnosti.

Služba M365 GAMO CLOUD BACKUP

Zabezpečuje bezpečné zálohovanie dát MS365 (Exchange, OneDrive, SharePoint, Teams) do cloudu. Využíva Veeam Software - lídra v zálohovacích riešeniach a slovenský GAMO CLOUD.

- Plné spravovanie poskytujúce istotu, že kópie dát sú zálohovaná v bezpečí pred akoukoľvek hrozbou;
- Uloženie dát výhradne na Slovensku;
- Vysoká dostupnosť;
- Vysoká bezpečnosť, spĺňajúca Európsku legislatívu, normy a nariadenia;
- Automatizovaný archivačný proces;
- Úplná kontrola – každý prístup a manipulácia s dátami je monitorovaná a logovaná;
- Jednoduché škálovanie – vhodné pre firmu akejkoľvek veľkosti a zamerania;
- Granularita - Možnosť obnovenia jednotlivých súborov, ako aj celých priečinkov;
- Nízke RTO (recovery time objective) – Minimalizovanie času na obnovu dát s cieľom zabezpečenia kontinuity podnikania;
- 3 – 2 – 1 – 1 -> uchovávanie kópie dát mimo organizácie a tradičného prostredia.

Je najvhodnejšia pre:

- Firmy s väčším počtom zamestnancov a malým objemom zálohovaných dát;
- Firmy so stabilnými nárokmi na objem zálohovaných dát;
- Firmy, ktoré chcú mať svoje údaje zálohované na Slovensku.

Služba M365 CLOUD BACKUP

Pomáha riešiť výzvy spojené s ochranou dát a poskytuje istotu, že dáta sú zálohované v bezpečí pred akoukoľvek hrozbou. Je postavená na svetových technológiách - IBM cloud a Veeam Software - lídra v zálohovacích riešeniach. Tie získali viacero ocenení, ako napríklad IBM - ‘Most Innovative Business Partner in Europe’ a Veeam ‘Best VCSP Partner’.

Výhody:

- 19 datacentier po celom svete, spĺňajúcich najvyššiu úroveň bezpečnosti s plnou certifikáciou ISO 27001, ISO 22301, ISAE3402 assurance, CSA a AIPCA SOC 2;
- Flexibilné nastavenie retenčnej politiky až na 10 rokov s neobmedzenou kapacitou pre zálohovanie za nezmenenú cenu;
- Platba len za počet užívateľov;
- Možnosť výberu regiónu pre uchovávanie dát.

Je najvhodnejšia pre:

- Firmy s potrebou zálohovania veľkého množstva dát;
- Rastúce firmy resp. firmy s dynamicky meniacimi sa potrebami;
- Firmy vyžadujúce predvídateľné náklady.

A čo ponúka GAMO M365 ON-PREMISE BACKUP?

V uplynulých 18 mesiacoch až 80% organizácií zaznamenalo data breach - prišlo o dáta. Pričom až 43% týchto firiem uviedlo 10 a viac takýchto prípadov! To znamená, že po prvom úniku nespravili žiadne kroky k lepšiemu zabezpečeniu svojich systémov.

Výhody:

- Dáta uložené v šifrovanej podobe v bezpečí spoločnosti;
- Automatizovaný archivačný proces;
- Rovnaká granularita - Možnosť obnovenia jednotlivých súborov, aj celých priečinkov;
- Platba za dáta, nie za užívateľa – flexibilne prispôsobíme zálohovaciu kapacitu Vašim potrebám;
- Lepšia cena – platíte len za dáta a nie za užívateľa. Pri cloudových službách platíte aj za dáta aj za užívateľa.

Nevýhody:

- Nižšia škálovateľnosť;
- Starostlivosť o hardvér a možnosť HW problémov.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR


Igor Chudáčik
igor.chudacik@gamo.sk

Cloud Made in Slovakia

Maximálna dostupnosť, flexibilita, veľký výpočtový výkon. To sú požiadavky na vyhovujúce cloudové služby. Nadnárodná firma Lenovo si pre ne vybrala providera zo Slovenska. Z toho cloudového prostredia poskytujú interné IT systémy pre EMEA región.

Lenovo Slovakia je oficiálnym zastúpením korporácie na Slovensku, poskytuje interné IT systémy a služby pre región EMEA (Európa, Stredný východ, Afrika), využíva servery v GAMO Cloud. S manažérom pre tento segment Branislavom Kartikom sme viedli rozhovor.

Aký je váš pohľad na súčasný vývoj a smerovanie technológií?

Tiež si myslím, že cloudové riešenia majú budúcnosť. Je to prirodzený prístup ako k programovaniu, tak aj k používaniu aplikácií. Naďalej sa však bude rozvíjať aj umelá inteligencia, IoT, inteligentné aplikácie, analytika, virtuálna realita alebo biometrické funkcie, ktoré potrebujú centrálne úložiská a musia byť spravované.

Akú infraštruktúru preferujete? Tradičnú, cloudovú, hybridnú?

Každému to, čo aktuálne potrebuje. Prakticky však vychádza, že cloudové riešenia majú väčší význam. Najmä pre spoločnosti, ktorých nie je biznisom IT alebo iba v malej miere. V takomto prípade by sa nemali snažiť spravovať si infraštruktúru sami, je to totiž drahšie ako si myslia. Často totiž nesledujú takzvané, neviditeľné náklady‘, čo je napríklad suma za elektrinu, za chladenie serverovne. A samozrejme, ide o ďalšie náklady najmä na ľudské zdroje.
Pre spoločnosti, ktoré robia IT, majú tradičná infraštruktúra a vlastné laboratórium zmysel. Aj my v Lenove skúšame nové veci na vlastnom hardvéri, ale väčšinu služieb sa snažíme umiestňovať do cloudových úložísk. Je to pre nás výhodnejšie.

Kde vidíte tie výhody?

V zjednodušení správy systémov. Používateľ sa nemusí zaoberať samotnou infraštruktúrou, službu si zaplatí. Poviem to na jednoduchom príklade: vlastné auto verzus taxík. Keď nemám auto, nepotrebujem sa oň starať, platiť poistenia, opravy, ani aktuálne čoraz drahšie pohonné hmoty. Ak sa potrebujem niekam odviesť, zavolám si taxík, teda len samotnú službu. Je to síce nepraktické pri ceste na dovolenku, ale pre mnohé presuny to riešením je. Čiže ďalším pozitívom sú ušetrené peniaze. Dokonca aj v horizonte 3, 4, 5 rokov cloudového riešenia, nielen dočasne. Inokedy sú prípady, keď napríklad aktuálne potrebujeme úložisko, ale investovať úvodných 5 000 Eur do hardvéru, bez vedomia či bude dostačujúce alebo zbytočne veľké, sú riskantne investované peniaze.

Za značku Lenovo spravujete interné IT systémy a služby pre celý EMEA región. Čo všetko to zahŕňa?

Je to správa IT prevádzky v oblasti od Dublinu cez Moskvu, Dubaj po Johannesburg, všade tam, kde je Lenovo prítomné. Približne v každej európskej krajine je jedno zastúpenie. Väčšinou ide o predaj, logistiku a správu služieb. Správa IT sietí je riadená z Číny. Môj tím má na starosti kontakt s koncovým používateľom v rámci Lenova.

Branislav Kartik
Senior IT Manager,
EMEA IT On-site Support
Lenovo Slovakia

Lenovo má know-how historicky získané vďaka investíciám do veľkých laboratórií pre rozvoj hardvéru a technológií. Má divíziu riešení pre kompletnú infraštruktúru, vnímame ho ako globálneho hardvérového giganta. Čo vás teda priviedlo ku cloudu?

My sme začali riešiť cloudové riešenia už v roku 2011. V tom čase existovalo viacero drobných takzvaných ‚pochodových‘ serverov. Ľudia z rôznych oddelení, napríklad z reportingu, mali dodatočné aplikačné či databázové servery. Tie sa vyskytovali rôzne - na chodbe, na stoloch v kanceláriách, v lepšom prípade v nejakej serverovni, bez poriadnej centrálnej správy a kontroly zabezpečenia. Jedného dňa sa stalo, že takýto server kvôli kritickému množstvu prachu, ktoré stihol nasať, prestal fungovať. Vtedy sme nemali cloud rozvinutý ani v regiónoch a jednoducho sme museli začať s externým partnerom.

Prečo ste sa rozhodli dôverovať slovenskému poskytovateľovi cloud služieb namiesto veľkého globálneho hráča? Čo boli hlavné dôvody a výhody?

Viac ako lokálpatriotizmus poteší človeka pracovať s lokálnym partnerom. Jednou z požiadaviek bola fyzická blízkosť kvôli latencii siete. Veľkosť providera u nás nehrala úlohu, skôr to bola bezpečnosť a kvalita služby. Nás ani nezaujíma presná frekvencia procesora, pamäte, ale potrebujeme vedieť ako sa to správa a čo to robí. A hlavne, keď je problém, ako partnerská strana reaguje, to je úplne kľúčové. Ďalšou výhodou sú možnosti konzultácie a konzultačných služieb. Totiž držať si vlastného experta na IT siete je drahé. Radšej ho zaplatíme na niekoľko hodín do mesiaca k ostatným službám a v tejto súvislosti sme mali s GAMO vždy dobrú skúsenosť. Vždy sme zaznamenali rýchlu reakciu aj riešenie. A hoci všetci vo firme hovoríme po anglicky, výhodu vidím aj v komunikácii v materinskom slovenskom jazyku.

Niektoré firmy majú obavy z migrácie. Je to relevantný strašiak v procese?

Hovorí sa, že vždy treba mať plán, aby človek vedel, ako ísť aj mimo neho. (Smiech.) Najskôr bolo potrebné urobiť sieťový VPN tunel do vnútra spoločnosti, čo je vždy bezpečnostná výzva. Pri jeho bezpečnosti je to opačne ako s ľudskými právami. Povolené je iba to, čo je explicitne povolené, všetko ostatné je zakázané. Následne sme si vybrali najmenej komplikované služby, kde sme si vedeli predstaviť chvíľkový výpadok. My sme do prechodu šli s tým, že celé aplikčné riešenia, ktoré pôjdu naimplementovať nanovo, sa vyrobia nanovo. Nebudeme migrovať staré veci so starým operačným systémom. Tých scenárov teda môže byť viac, ale musí existovať aj plán, ako sa vrátiť z polcesty, ak migrácia nedopadne podľa očakávaní.

Keby ste mali radiť iným IT manažérom a top manažmentu firiem, aké by boli vaše odporúčania pre prechod do cloudu?

Cloud systém je to nádherný nástroj na obchodný prístup Try and Buy. Kúpený hardvér za 5000 Eur nemôžete o dva mesiace vrátiť. S cloudom sa dá začať s niečím menším, nenáročným, neriskovať pri tom stratu biznis kontinuity, premrhaných investícií a tak skúsiť, či to funguje. Ak to nefunguje, tak to jednoducho nechať tak. Chybou by skôr bolo nevyskúšať to. A vyskúšanie nestojí veľa. Niekedy aj nič. S dobrým partnerom sa vždy dá dohodnúť na skúšobnej prevádzke, teste. Investovať efektívne je nevyhnutnosťou v biznise a cloud vychádza ako finančná výhoda. Ale aj ako nevyhnutnosť i technologicky správny smer.

Dnes je nevyhnutnosť cloud, nedávno sme mali spomínané chodbové servery, kam sa posunieme a ako rýchlo sa to bude diať?

Napriek tomu, že sa hovorí ako všetko ide rýchlo a ako sa všetko rýchlo mení, nejaví sa to až tak. Nedávno som si pozrel stratégiu z pred 10 - 12 rokov, a hovorilo sa v nej o podobných veciach ako dnes. A stále sme do toho cieľa neprišli. Moja úvaha znie, že zmeny sa až tak rýchlo nedejú. Postupne sa však posúvame ďalej a ľudia budú nachádzať lepšie a výhodnejšie riešenia. A efektívnejší budú vytláčať tých, ktorí sa neprispôsobili nevyhnutným zmenám súčasnosti.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Jana Kohárová
jana.koharova@gamo.sk

Hybridná práca: Fenomén tejto doby

Sedem z desiatich zamestnancov si na home office ako ideálny spôsob práce nezvyklo. Podľa prieskumov preferujú kombináciu práce z domu a kancelárie. Ako nastaviť fungovanie firmy tak, aby bola zachovaná vysoká produktivita a optimálna spokojnosť ľudí?

Uplynulé obdobie nás prinútilo hľadať formy práce, ktoré nás na jednej strane izolovali a chránili naše zdravie, na strane druhej umožňovali firmám, inštitúciám aj jednotlivcom fungovať.
Fungovať znamenalo: udržať firmu, rozvíjať obchody, zabezpečiť vzdelávanie, nebyť úplne izolovaný.
Home offce sa osvedčil ako efektívny model, a to nielen plnohodnotnou náhradou kancelárskeho prostredia. Ďalšími benefitmi práce z domu sa ukázali byť:

- Úspora prevádzkových nákladov
- Úspora času a cestovných nákladov
- Väčšia sloboda v rozvrhovaní pracovného času
- Efektívnejší ľudia a zvýšená produktivita práce

Výsledkom však nebol spokojný zamestnanec. Rôzne prieskumy (Profesia, IT-čkári, Microsoft) poukazujú na spoločný fakt, že väčšina Slovákov, sedem z desiatich, napriek počiatočnému nadšeniu trvalo z domu pracovať nechce.
Fyzické prostredie kancelárie naďalej zostane dôležitým miestom, kde sa môžu kolegovia stretávať, spolupracovať na spoločných úlohách a projektoch.
Na manažéroch zostalo nájsť obojstranne výhodné riešenie. A ukazuje sa, že odpoveďou by mohol byť model hybridnej formy práce.
Hybridná práca predstavuje zásadnú výzvu vytvoriť zamestnancom aj zákazníkom optimálny priestor, poskytnúť nástroje a technológie na efektívnu, spoľahlivú a bezpečnú spoluprácu. Firmy by mali mať na zreteli fakt, že najdôležitejší sú spokojní a angažovaní zamestnanci. Vytvoriť pracovné prostredie, ktoré je dynamické, plynulé a umožňuje ľuďom pracovať odkiaľkoľvek, ale tiež kedykoľvek.
Kde a ako začať? Piliermi stratégie sú definované pravidlá, vďaka ktorým budú môcť ľudia pracovať flexibilne. Rovnako je nutné vytvoriť si novú predstavu o fyzickom priestore a investovať do technológií, ktoré dokážu ľudí spájať aj umožňujú hladkú, bezproblémovú spoluprácu. Popritom v každej chvíli nezabúdať na ochranu firemného know-how, firemného prostredia ako takého, a odolať útokom alebo minimalizovať ich riziko.

Pravidlá režimu hybridnej práce

Ak chcete ľuďom poskytnúť možnosti mimoriadnej flexibility, musíte najskôr odpovedať na tieto otázky:

Kto bude môcť pracovať na diaľku? Ako sa pripojí k firemným systémom?

Ľuďom pracujúcim na diaľku je potrebné umožniť bezpečný prístup k firemným systémom a k dokumentom. Riešením je spravila využitie VPN, RDP alebo šifrované prihlásenie sa do webového prostredia.

Je vzdialené pripojenie dostatočne bezpečné?

Byť podozrievavým a nedôverčivým je v tomto prípade namieste. Technológia RDP je častým terčom kybernetických útokov. Vyskytli sa viaceré prípady narušenia bezpečnosti, hlavne keď sa útočníkom podarilo nájsť spôsob ako zneužiť zle nakonfigurované nastavenia alebo slabé heslá, a tak získať prístup do firemných sietí.

Ako viem, že prihlásená osoba v systéme je môj zamestnanec?

Tak, že využijem formu Overenia identity. Takýto vstup do firemného prostredia by už mal byť nevyhnutným - bazálnym preventívnym / bezpečnostným úkonom. Aby sa frekvencia overovania nestala obťažujúcou a obmedzujúcou, tam, kde je to vhodné, možno aplikovať scenáre tzv. podmieneného overovania. Zjednodušene, pôvodné overenie identity sa aktivuje automaticky pri zaznamenaní podozrivých, nelogických alebo neštandardných aktivít.

Kto bude musieť chodiť do kancelárie, na ako dlho a kde budú ľudia vykonávať svoju prácu?

Striedavý režim práce zo sebou nesie redukciu „pracovných stolov a stoličiek“. Niektoré spoločnosti ich dokonca eliminovali úplne a fungujú plnohodnotne. Umožňujú im to vhodne vybrané nástroje a technológie. Bežné pracovné aktivity ako sú stretnutia s kolegami, pracovné porady, obchodné konzultácie, sme sa naučili vybavovať online. Experimentovanie s rôznymi „free“ riešeniami sa môže ukázať ako najdrahšia a najťažšia cesta.

Ako si teda správne vybrať službu, aplikáciu resp. nástroj spĺňajúci kombinovaný spôsob práce?

RIEŠENIE
Konzultácia so špecialistami je určite bezpečná skratka. Návrh sa „šije“ na mieru, zohľadňuje potreby a zvyklosti, a vníma situáciu z nadhľadu a vo výsledku je optimálne riešenie a spokojné všetky zainteresované strany.

Vytváranie „nového“ fyzického priestoru

Určením pravidiel režimu hybridnej práce sa prirodzene štartuje fáza ich aplikovania t. j. vytváranie „nového“ fyzického priestoru. Hybridný režim vyžaduje prepájať fyzický svet - kancelárske priestory, s digitálnym a napĺňa potreby jednotlivcov aj jednotlivých tímov a špecifických rolí.
Čo však zostáva v oboch formách práce spoločné sú používané pracovné nástroje – počítač, notebook, tablet, smartfón, tlačiareň. Čiže zariadenia, prostredníctvom ktorých sa zamestnanec pripája k firemným systémom. Tieto obsahujú rôzne firemné údaje vrátane citlivých alebo dôverných. No, povedzme si otvorene, nie vždy využívame pracovné zariadenia iba na prácu. Koľkokrát si dieťa potrebuje splniť školskú povinnosť, zahrať sa alebo si potrebujete LEN niečo narýchlo objednať. Zariadenia, ktoré firma nemá pod kontrolou, sú slabým miestom organizácie, bez ohľadu na miesto práce.

RIEŠENIE
Neotvárajte dvere výpalníkom, venujte sa ochrane zariadení. Dobre nastavená ochrana zariadení dokáže pokryť hneď niekoľko oblastí:

- Šifrovaním naplníte o. i. aj požiadavku GDPR;
- Detekciou hrozieb – predídete fatálnym dôsledkom útoku;
- V prípade odcudzenia zariadenia ho dokážete okamžite „odstaviť“ napr. vypnutím a vymazať jeho obsah;
- Zariadenia môžete monitorovať a aktualizovať a dokonca aj lokalizovať;
- Bezpečnostné politiky dokážete uplatniť - aplikovať z jedeného miesta na všetky typy zariadení (Windows, Android, iOS, Mac);
- Môžete chrániť a spravovať firemné aplikácie;
- Prijať model BYOD – a chrániť a spravovať firemný „priestor“ v súkromných zariadeniach a ušetríte náklady za zariadenia;
- Vykonávať forenzné činnosti po útoku;
- Využiť vlastnosti umelej inteligencie pri detekcii hrozieb.

Investovanie do technológií

Moderné technológie sa vyvíjajú obrovským tempom. Efektívne riešenia sa chrlia z každej strany, ovplyvňujú zamestnancov, zákazníkov aj dodávateľov. Ak už ste model hybridnej práce prijali za svoj štandard alebo sa naň pripravujete, kritériá na technologickú podporu sú v kľúčových bodoch rovnaké. Bezpečnosť, dostupnosť a flexibilita podporujúca mobilitu zamestnancov. Ponuka trhu nezaostáva, v niektorých prípadoch je dokonca o niekoľko krokov vopred.
Integrácia cloudových riešení a mobilných aplikácií, ktoré umožňujú spoluprácu medzi zamestnancami pracujúcimi na diaľku, je kľúčová pre zabezpečenie konzistentného zapojenia ľudí do práce na diaľku.
Sústrediť sa v tomto smere na bezpečnosť je nevyhnutné. Firmy, a najmä ich zamestnanci, častokrát zlyhávajú pri ochrane svojich dát a rýchlo sa stávajú obeťami hekerských útokov. Nielen hybridná práca si vyžaduje kvalitné zabezpečenie, ktoré včas upozorní na hroziace riziko. Kvalifikovaní IT odborníci špecializujúci sa na kybernetickú bezpečnosť sú nákladní a ťažko sa hľadajú. Firmy musia nájsť spôsoby ako optimalizovať svoju IT podporu pre zamestnancov pracujúcich na diaľku, aby sa mohli sústrediť na riešenie bežných biznis problémov. Ako ktorú technológiu správne integrovať do podnikových systémov a existujúcich procesov tak, aby všetko spolu fungovalo. Mať pre tento účel špecializovaného partnera, ktorý má vlastné cloudové riešenia a dokáže poskytnúť kvalifikovanú podporu aj v problematike bezpečnosti, môže byť neuveriteľne užitočné. Nemajte obavy využiť výhody externých služieb správy IT alebo konzultácií v prípade zmien v IT infraštruktúre, ktoré prichádzajú s novými riešeniami podporujúcimi hybridnú prácu. Jednoznačne sa to vyplatí.

Článok čítajte na platformofinvention.sk
klikní alebo oskenuj QR

Marcela Gottwaldová
marcela.gottwaldova@gamo.sk

Legislatíva kybernetickej bezpečnosti pomáha, nie naopak

Nedostatok odborníkov, málo osvety aj slabá pripravenosť odolávať kybernetickým incidentom. To je iba časť výziev, ktoré sú súčasťou v oblasti kybernetickej bezpečnosti. O budúcnosti legislatívy na Slovensku a európskej úrovni celkovo sme sa rozprávali so Štefanom Pilárom, právnikom advokátskej kancelárie Bukovinský & Chlipala.

Aké sú teda legislatívne výzvy v oblasti KB na rok 2022?

Legislatíva má svoju príjemnú stránku, a to predvídateľnosť. Kým konkrétny predpis nadobudne účinnosť, adresáti majú dostatok času na oboznámenie sa s jeho obsahom v podobe návrhu. Vybrané subjekty môžu návrh predpisu pripomienkovať. Pokiaľ hovoríme o európskej legislatíve, tam je toho času podstatne viac. Niektoré predpisy totiž vznikajú roky. Mnohé predpisy poskytujú povinným osobám prechodné obdobie, počas ktorého majú priestor na implementáciu a splnenie povinností.

Nanešťastie, táto predvídateľnosť ostáva často nevyužitá. So zákonom o kybernetickej bezpečnosti na Slovensku žijeme vyše štyri roky a jeho prechodné obdobia už dávno uplynuli. Aj napriek tomu máme na Slovensku subjekty, ktoré na požiadavky tohto zákona nereflektujú vôbec alebo len veľmi málo. Česť výnimkám. Dokonca si dovolím tvrdiť, že počet takýchto subjektov prevláda, mnohí audítori kybernetickej bezpečnosti by vedeli rozprávať. Svedčia o tom aj záverečné správy z auditov.

Výziev je teda veľké množstvo. Nedostatok odborníkov, prakticky neexistencia vzdelávania, málo osvety, nedostatočná pripravenosť odolávať kybernetickým bezpečnostným incidentom či nedostatočné chápanie účelu a podstaty legislatívy vyžadujúcej ochranu informácií. Tento stav tu máme roky a pred nami sú rozhodne ďalšie spolu s nepoznanými výzvami.

Nemá teda význam pozerať sa dopredu?

Určite má, napokon takto by to malo štandardne fungovať. Poznanie prichádzajúcej legislatívy a jej nových požiadaviek je nutnosťou. Ale uzavrieť to, že pozerať sa máme len na horizont a vyčkávať na ďalšiu reguláciu, by nebolo veľmi správne. Na Slovensku totiž máme veľký dlh ešte voči už roky platnej legislatíve, napr. už spomínanému zákonu o kybernetickej bezpečnosti.

Aký dlh máte na mysli?

Závisí to od uhla pohľadu, resp. kde začať. Začnime tým, že pojem kybernetická bezpečnosť je ešte stále pojmom abstraktným. Najhoršie je, že aj pre tých, ktorí by sa ňou zo zákona mali zaoberať. Mnohí tento pojem a jeho obsah vnímajú ako ďalší byrokratický výmysel Európskej únie, záťaž pre biznis, alebo ako niečo, čo vôbec nie je potrebné. Veď kto by už útočil práve na neho? No a keď sa dostaneme na druhú stranu spektra, iní tento pojem a jeho obsah vnímajú ako vynikajúcu marketingovú a obchodnú príležitosť. Pozor, ich výstupy často nemajú potrebnú kvalitu.

Prečo je tomu tak?

Dôvodov je viacero a problematika nedostatočného plnenia požiadaviek zákona o kybernetickej bezpečnosti nie je čiernobiela. Tvrdiť, že za všetko môžu adresáti týchto povinností, by bolo nesprávne a nefér. Je potrebné uvedomiť si, že problematika kybernetickej bezpečnosti je náročná. Nielen na Slovensku, ale v celom svete chýbajú kvalifikovaní odborníci. Nemôžeme sa čudovať takémuto výsledku, ak chýba dostatočná informovanosť a osveta alebo ak je vysvetľovanie podstaty novej legislatívy s jej jednoznačnou pridanou hodnotou slabé.

Aké je podľa Vás riešenie tohto stavu?

Aj riešení je viacero a názory na ich efektívnosť sa rôznia. Niekoho budovanie povedomia a osveta nezaujíma, skôr uprednostňuje represiu. A treba povedať, že tá v prípade zákona o kybernetickej bezpečnosti nie je zanedbateľná. Iní uprednostňujú zvyšovanie povedomia a osvetu pred pokutami. Možno netradične, ale ja ako právnik sa prikláňam práve k potrebe budovania povedomia. Pokuta je totižto len donucujúcim, možno zároveň „motivačným faktorom“, ktorý však reprezentuje skôr negatívnu emóciu a donútenie namiesto presvedčenia z prínosu. Zvyšovanie povedomia, to je cesta k pochopeniu podstaty a smerovania k racionálnemu presvedčeniu, že niečo potrebujem alebo chcem. Nie preto, lebo musím, ale preto, lebo je to dôležité. Kybernetická bezpečnosť je najmä o ľuďoch. Ľudia, v tomto kontexte zamestnanci, sú tou najväčšou a často opomínanou hodnotou. A tí istí ľudia aj značne vplývajú na bezpečnosť. Pod hrozbou sankcií konajúci manažment toho veľa nezmôže, kým zamestnanci nebudú rozumieť rizikám a nebudú chápať, aké hodnoty chránia. A platí to aj naopak. Kybernetická bezpečnosť bez podpory vedenia organizácií nemá šancu na úspech.

Tak to nie sú najlepšie vyhliadky.

Nechcel som byť zase úplne negatívny. (Smiech.) A treba povedať, že v tejto oblasti sa už vykonalo veľa práce, pričom

Štefan Pilár
Bukovinsky & Chlipala

nie všade je možné výsledky očakávať ihneď a všade. Typickým príkladom je toľko zmieňované vzdelávanie, ktoré je určite behom na dlhú trať. Podstatné je konečne sa na štart tejto trate postaviť.

Keď súčasnú situáciu porovnáme s rokom 2018, sme vo všeobecnosti omnoho ďalej. Každoročne sa uskutoční množstvo konferencií, seminárov, školení, kde zaznamenávame zvýšený záujem a účasť. Kybernetická bezpečnosť dostáva stále viac priestoru aj v médiách. Zlepšeniu situácie veľmi napomáhajú aj vykonané audity, na základe ktorých sú povinné osoby bezprostredne konfrontované s reálnym stavom. No a v neposlednom rade tému kybernetickej bezpečnosti posúva aj súčasná zlá bezpečnostná situácia.

Takže registrujeme aj pozitívne správy. A čo teda legislatíva a rok 2022?

Pokiaľ ide o súčasnú legislatívu a staré hriechy, dôležité bude správne odstránenie nedostatkov identifikovaných auditmi. Napokon, z dostupných informácií vieme, že percentá súladov sú prevažne nízke. Takže do ďalšieho auditu, v ideálnom prípade v rámci nasledujúcich dvoch rokov, budú mať tieto subjekty veľmi veľa práce. Zostáva veriť, že tejto práce sa chopia zodpovedne a so správnymi ľuďmi.

A prichádzajúca legislatíva? Čiastočne sa vieme ako na novú legislatívu pozerať aj na Cybersecurity Act. Na úrovni Európskej únie sa totiž pracuje na viacerých certifikačných schémach pre produkty, procesy či služby pre oblasť kybernetickej bezpečnosti. Spomeňme už skoro hotovú schému pre cloud – EUCS, pripravované schémy pre 5G, HW, SW

a služby. Tieto schémy budú následne prebrané do vnútroštátnych podmienok, kde budú certifikáciu vykonávať na to akreditované subjekty (v SR akreditované SNAS-om). Certifikácia by mohla pomôcť nielen lepšej orientácii v rámci veľkého množstva aj nekvalitných produktov či služieb dnes dostupných na trhu, ale aj zrýchleniu procesu verejného obstarávania, pokiaľ ide o vyhodnocovanie splnenia podmienok účasti na strane uchádzačov.

Ďalej je to pripravovaná Smernica NIS 2, teda legislatíva nadväzujúca na prvú smernicu, ktorej môžeme ďakovať za slovenský zákon o kybernetickej bezpečnosti. Pri správnej transpozícii novej smernice do nášho právneho poriadku (zrejme v podobe novelizácie zákona o kybernetickej bezpečnosti) môžeme očakávať rozšírenie sektorov a podsektorov, povinných osôb či bezpečnostných požiadaviek.

No a za zmienku určite stojí aj pripravovaný Cyber Resilience Act, ktorý by mal nadväzovať ako aj na úpravu zavedenú Smernicou NIS, tak aj na Cyber Security Act. Tento predpis zavedie spoločné pravidlá kybernetickej bezpečnosti (odolnosti) pre digitálne produkty a súvisiace služby umiestňované na trh v EÚ.

Môžeme očakávať legislatívnu aktivitu aj na Slovensku?

Na úrovni Slovenskej republiky môžeme v roku 2022 očakávať vydanie vyhlášky stanovujúcej znalostné štandardy pre určité bezpečnostné roly (napr. manažér kybernetickej bezpečnosti) a možno aj novelizáciu vyhlášky č. 362/2018 Z. z., ktorá reflektuje na znenie zákona o kybernetickej bezpečnosti spred 1. 8. 2021 vo vzťahu k oblastiam, pre ktoré sa prijímajú bezpečnostné opatrenia.

Dalo by sa povedať, že na Slovensko sa najmä z EÚ valí relatívne rozsiahla legislatíva pre oblasť kybernetickej bezpečnosti. Na pozore by sa mali mať subjekty, ktoré pod dnešný zákon o kybernetickej bezpečnosti nespadajú, ale počíta sa s nimi v rámci novej Smernice NIS 2. V zmysle súčasného znenia návrhu vieme povedať, že ide najmä o sektory energetiky (vodík), odpadového hospodárstva, výroby (napr. motorové vozidlá), potravinárskeho priemyslu či vesmíru. Ďalej je potrebné pripraviť sa na to, že aj keď zamýšľaná certifikácia produktov, procesov či služieb pre oblasť kybernetickej bezpečnosti by nemala byť povinná, nie je vylúčené, že certifikácia bude predstavovať podmienku účasti v rámci určitých typov verejných obstarávaní (Cyber Security Act to vyslovene pripúšťa).

Čaká nás teda veľa práce, a to nielen vo vzťahu k existujúcim, ale aj budúcim požiadavkám pre oblasť kybernetickej bezpečnosti. S kybernetickou bezpečnosťou je nutné počítať, intenzívne sa jej venovať a začať ju vnímať ako ucelený systém pravidiel, procesov a opatrení chrániaci organizáciám to najcennejšie, čo majú. Ich aktíva, bez ktorých nevedia fungovať tak ako oni, tak ani spoločnosť alebo štát. A my ostatní budeme naďalej trpezlivo vysvetľovať, pomáhať a hľadať ďalších nadšencov pre túto zaujímavú a dôležitú tému.

Článok čítajte na platformofinvention.sk

klikni alebo oskenuj QR

Zuzana Omelková
zuzana.omelkova@gamo.sk

Čo prinášajú firmám podnikateľské misie v zahraničí?

Zuzana Omelková
zuzana.omelkova@gamo.sk

Článok pokračuje na platformofinvention.sk

klikni alebo oskenuj QR

Potenciálne príležitosti a networking. Agentúra SARIO pomáha firmám bez rozdielu objavovať nové trhy a obchody. Získavanie know-how biznis efektívne rozvíja. Je teda možné vďaka misiám úspech akcelerovať? Ako ich hodnotia slovenskí partneri?

Michal Ukropec
CEO
twinzo j.s.a.

Inovatívne riešenia prinášajú výzvy nielen technologické, ale aj obchodné. Východná Európa má, napriek rastu miezd, stále pozíciu lacnej pracovnej sily a implementácia najnovších technológií nemusí dávať z pohľadu očakávaných úspor zmysel. V krajinách, ktoré sú rastovo nastavené, je však po inováciách veľký hlad a východoeurópske krajiny vedia získať konkurenčnú výhodu. Tou je určite cena, ale na rovnakej úrovni aj ochota k ďalšiemu rastu a v neposlednom rade aj ochota riskovať, ktorá je vyššia ako pri západoeurópskych krajinách. Obchodné misie tak dávajú firmám priestor ísť do nového teritória s podporou, dopredu dohodnutými stretnutiami a potrebným zázemím. Vždy je totiž jednoduchšie ísť do sveta s tým, že máme poruke ľudí, ktorí sa v regióne vyznajú a vedia pomôcť radou, či kontaktom. A pokiaľ má firma dosť trpezlivosti a produkt, ktorý v danom regióne dáva zmysel, nie je dôvod na ostych, pretože mnohé slovenské firmy skutočne majú čo ponúknuť.

Heliodor Macko
IT manažér
SEAK, s.r.o.

SEAK vyvíja a vyrába systémy pre smart osvetlenie a nabíjanie elektromobilov. Ceny energií sa zvyšujú globálne, spolu s nimi aj dopyt po riešeniach šetriacich energiu - a tak je správny čas rozširovať aktivity na ďalších trhoch. So SARIO sme sa zúčastnili už niekoľkých podnikateľských misií a dobré výsledky máme hlavne z účastí na veľtrhoch. Je oveľa efektívnejšie, ak sme súčasťou spoločného stánku Good idea Slovakia, ako keby sme zabezpečovali vlastný stánok, a tiež to pôsobí lepším dojmom (a prvý dojem môžeme urobiť len raz).

Väčšinou sa podarí nájsť aspoň jedného partnera, s ktorým pokračuje nielen komunikácia, ale aj neskoršia spolupráca. Podstatné je nezabudnúť na následné follow-ups.

Odporučil by som si preto pred pracovnou cestou spraviť vlastný prieskum trhu a dohodnúť si vlastné stretnutia, nespoliehať sa na B2B stretnutia ktoré dohodne lokálna agentúra. Tým sa šance na úspešné nadviazanie obchodných vzťahov výrazne zvyšuje.

Juraj Tomlain
Obchodný riaditeľ
T-Industry, s.r.o.

T-Industry, s.r.o., je spoločnosť s 20-ročnou históriou, ale to nijako nemení fakt, že musí neustále hľadať a analyzovať nové obchodné príležitosti doma aj v zahraničí. Jednou z efektívnych možností pri vstupe na nové teritórium je aj účasť na podnikateľskej misii organizovaných agentúrou SARIO. V rôznych krajinách, a najmä v krajinách mimo EÚ, platia iné formálne či neformálne pravidlá, na ktoré slovenskí podnikatelia nemusia byť pripravení či zvyknutí. SARIO odbremení podnikateľa od dôslednej analýzy všetkých potrebných základných znalostí o danom teritóriu a organizovaný networking prináša istú skratku na trh danej krajiny. Organizovanie bilaterálnych stretnutí resp. návštev s vopred definovaným zákazníckym profilom šetrí veľa času a nákladov na hľadanie optimálneho partnera v tom danom podnikateľskom sektore. Rovnako dostávame už istú predklasifikáciu potenciálnych miestnych partnerov, čo zase šetrí energiu a pomáha to v prvých fázach budovania obchodných kontaktov a partnerstiev.

Priekopnícka základná škola v Banskej Bystrici

Kyber útokov pribúda, no špecialistov na bezpečnosť je ako šafranu. Na tento fakt upozorňujú všetky zodpovedné firmy a inštitúcie uvedomujúce si likvidačné dôsledky. Dlhodobý dopyt po odborníkoch pociťujú sektory IT, elektrotechniky aj energetiky. Čo s tým? Ako podporiť inovatívnu ekonomiku?

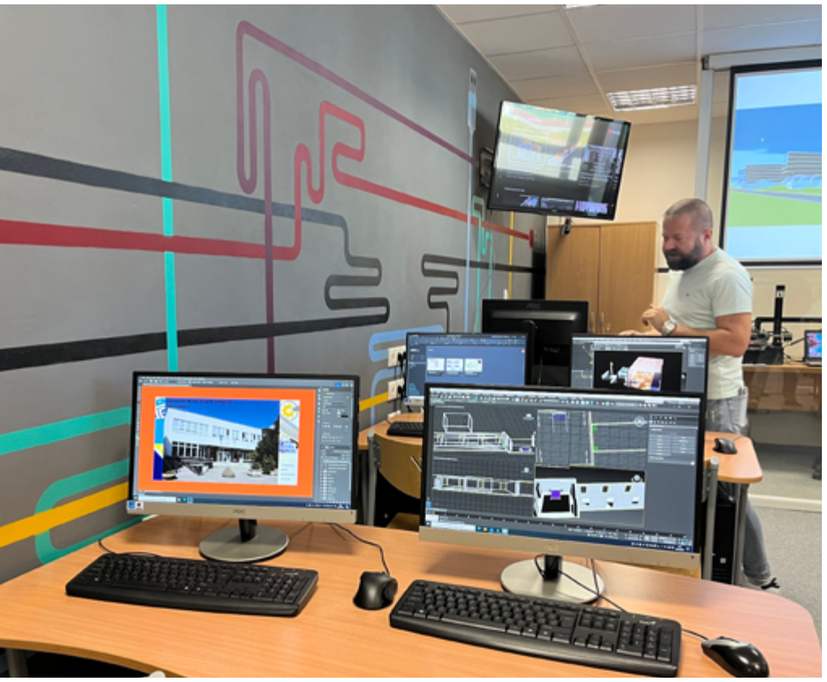
Na to pozná odpoveď manažment a učiteľský tím Základnej školy Jozefa Gregora Tajovského v Banskej Bystrici. Sú priekopníkmi v riešení s ambíciou pripravovať žiakov na dobu, v ktorej budú žiť zakrátko.

Vybudovali moderné centrum vzdelávania CeTech, unikátny komplex technických učební. Do vzdelávacích plánov zahrnuli hodiny techniky pre zdokonaľovanie technických a praktických zručností pri práci so systémami, 3D tlačiarňami, CNC stavebnicami či rôznymi grafickými programami. Vedú deti ku spoznávaniu trendov techniky a rozširovania si digitálnych zručností na jednoduchých praktických zadaniach. Rozvinuli osnovy pre oblasť techniky a robotiky. A v neposlednom rade podchytujú potenciál najšikovnejších s následnými odporúčaniami pokračovania na stredných technických školách. Na úrovni vzdelávacieho systému ZŠ–SŠ–VŠ zastrešujú nesmierne dôležitú spoluprácu škôl s praxou a potencionálnymi zamestnávateľmi a otvárajú svojim študentom dvere do profesií žiadaných na trhu.

To je Základná škola Jozefa Gregora Tajovského v Banskej Bystrici a jej tím hodný nasledovania. Čo si priať viac? Odpoveď je jasná: aby bolo takto ambicióznych učiteľských zanietencov, nastavených na cestu inovácií a hľadania potenciálu pre prax, oveľa viac.

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 podeľte 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

Cloud ponúka výkon vždy, keď ho potrebujete.

Chcem zistiť viac

GAMO
INFORMAČNÉ TECHNOLÓGIE