platform of invention

Informačné technológie pre podnikanie s nápadom

Užitočné v správnych hlavách

magazín pre CTO, CFO, CEO

1 / 2021

do vlastných rúk pre
výkonný riaditeľ, finančný riaditeľ, riaditeľ IT

ročník prvý | náklad 8000 výtlačkov

Ako prežiť kyberútok

Poradí vám expert na kybernetickú bezpečnosť

Nebezpečný home office

Vlastné železo alebo prechod do cloudu?

+ Darček pre platform of invention čitateľov

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 5 000 slovenských firiem s obratom nad 6 mil. €.

Chcete zistiť viac a zapojiť sa?

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

www.platformofinvention.sk/profil-magazinu/

Čítajte nás online!

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

www.platformofinvention.sk

Pandémia sa dostala spolu s prerušením prevádzky a kybernetickými útokmi medzi najväčšie riziká podnikania na rok 2021. A je jedno v akej sfére podnikáte. Náročný čas, ktorý žijeme, nastavuje podnikateľom a firmám zrkadlo v pripravenosti ako čeliť nepríjemným situáciám a na čom stavať do budúcnosti.

Všetci musia podstúpiť určitú zmenu, prispôsobiť sa novej situácii, ktorá sa nateraz môže javiť ako vynútená okolnosťami, no nie je to tak. Zodpovedné spoločnosti pochopili, že ide o prirodzený vývoj trhu.

Digitalizácia a bezproblémový prístup k dátam aj bez fyzickej prítomnosti zamestnancov sa stali každodennou nevyhnutnosťou a pripomienkou, že riadenie rizík je jedinou možnou cestou, ako zvládať aj extrémne scenáre a prežiť ich. Či sú nimi epidémie, prírodné katastrofy alebo kybernetické útoky.

IT technológie, služby a riešenia majú jedinečnú šancu stať sa motorom inovácií a transformácie ekonomiky. Želanou zmenou, ktorá prospeje uplatneniu podnikateľských nápadov a naštartuje biznis aktivity v slovenských firmách.

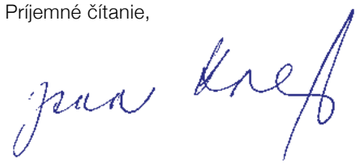
Otázkou doby teda je, ako IT správne nastaviť a rozumne využívať a s čím začať, aby bol efekt maximálny a všetko fungovalo.

Pilotné vydanie **Platform of Invention** sa venuje práve téme bezpečnosti z pohľadu zachovania biznis kontinuity. Zoči-voči pandémii a každodenným správam o útokoch hekerov je každý v tvrdeniach ‚Nám sa to nemôže stať' opatrný. Spoločnosti precitajú a podnikajú zásadné opatrenia voči bezpečnostným hrozbám tak, aby rizikové počínanie používateľov neohrozilo ich zisky, dôveru klientov či dobré meno.

Ambíciou magazínu je inšpirovať a podporovať tých, ktorí si chcú rozšíriť obzor v IT.

Platform of Invention je vydávaný s cieľom ukázať, ako IT technológie ul'ahčujú firmám život. Má ambíciu prinášať najnovšie a atraktívne informácie o biznis riešeniach, inováciách a trendoch v tejto sfére. Aj váš príbeh, spojený s IT-čkom, môže byť súčasťou jeho obsahu!

Príjemné čítanie,



Jana Kohárová
jana.koharova@gamo.sk

Pandémia prináša sofistikovanejšie útoky a nové výzvy v kybernetickej bezpečnosti

Antivírusové programy založené čisto na signatúrach známych hrozieb? Toto môžeme považovať za stredovek kyberbezpečnosti. Súčasný digitálny priestor si vyžaduje pokročilú ochranu cez exploitačné metódy a spúšťanie podozrivých súborov v izolovanom prostredí. Pre prístup do vnútra siete je nutné zvoliť zabezpečené pripojenie VPN. Ako štandard sa už používa viacfaktorové overovanie pri prihlásení. Stále však platí: prístup Zero Trust, overovanie a nutnosť prístupu prísnych zásad riadenia a správy identít.
Čo však starý známy ransomware, záloha dát či novinky ako umelá inteligencia či IoT (Internet of Things)? Zvyšujú síce produktivitu, no stále sú viac využívané pri útokoch na iné zariadenia v sieti. Pozrite sa na nové i staré výzvy v bezpečnosti firiem a domácností.

Článok pokračuje na platformofinvention.sk

Martin Pisák
Technický riaditeľ
GAMO a. s.

Ako digitalizovať firmu?

Využívanie moderných technológií dokáže ušetriť firme množstvo financií. Podľa štatistík slovenskej pobočky Konica Minolta napríklad len manuálne spracovanie faktúry stojí zhruba 50 centov. S elektronizáciou nákladov dokáže cena klesnúť o viac ako polovicu. Slovenské firmy si príležitosť v podobe nastupujúcej digitalizácie naplno uvedomujú. Počet firiem, ktoré nepôsobia v oblasti technológií a zároveň sa do digitalizácie pustili, sa za posledných päť rokov viac než zdvojnásobil. Zavádzať moderné technológie je však pre mnohých veľmi náročné. Akékoľvek šliapnutie vedľa môže stáť veľa financií. Ukážeme vám ako úspešne zaviesť digitalizáciu aj vo vašej firme tak, aby ste sa vyhli najčastejším chybám a zbytočne nepremrhali váš čas a peniaze.

Článok pokračuje na platformofinvention.sk

Milan Libuša
Solutions Consultant
Konica Minolta Slovakia

Dôležitosť zákazníckej skúsenosti pre dobrý predaj. Ako zlepšiť jej stratégiu?

Povedzme, že z vášho pohľadu fungujete zvnútra skvele. Ľudia oceňujú firemnú kultúru a vnímajú dobre nastavené vnútorné procesy. No predaj tomu nezodpovedá. Pozrime sa preto na situáciu cez zákaznícku skúsenosť.
Predstavte si zákazníka vo všetkých situáciách, kde sa môže stretnúť s vašou spoločnosťou. Ktoré to sú? Zvyčajne sa jedná o obchod, marketing a o zákaznícky servis, ale často komunikuje aj s oddelením financií. Má váš zákazník v každom bode rovnako dobrú skúsenosť s pozitívnym výsledkom? Získa konzistentnú a personalizovanú komunikáciu a pocit, že je jedinečný? Zákazník vás vníma počas celého procesu, od toho ako marketujete svoje produkty, až po moment, ako riešite starostlivosť a podporu v prípade problémov. Ako tému zákazníckej skúsenosti uchopiť profesionálne a maximalizovať benefity pre firmu?

Článok pokračuje na platformofinvention.sk

Miroslav Procházka
CX/EX Solutions Manager
Anodius, a.s.

IT bezpečnosť sa presúva do oblakov

V dôsledku pandémie vymenili zamestnanci firemné kancelárie za home office. V praxi to znamená rozšírenie firemnej siete do stoviek rôznych domácností po celej krajine. Aby sa organizácie dokázali v týchto podmienkach ochrániť pred neustále sa vyvíjajúcimi kybernetickými hrozbami, musia vedieť čo presne sa deje na všetkých koncových zariadeniach. Spoločnosť ESET ponúka dokonalý prehľad s novým produktovým balíkom ESET PROTECT. Cloudové nasadenie umožňuje spravovať koncové zariadenia z jedného miesta jednoducho a rýchlo prostredníctvom cloudovej konzoly. Výhodou vzdialenej správy, ktorá začala byť trendom ešte pred pandémiou, je tiež cenová dostupnosť. Pri cloudovom zabezpečení odpadajú náklady na údržbu serverov, ktoré sú bežné pri lokálnych riešeniach v priestoroch firmy. Platforma je navyše škálovateľná tak, aby vyhovela potrebám firiem každej veľkosti.

Článok pokračuje na platformofinvention.sk

Martin Čirik
Channel Sales Manager Slovakia
ESET, spol. s r.o.

Komplexným riešením pre maximálnu bezpečnosť zdieľaných dát je Safe Private Drive

Ide o IT riešenie pre bezpečné ukladanie a zdieľanie citlivých obchodných aj súkromných dát a súborov. Cloudové úložisko, pri ktorom nie je potrebné dáta posielať elektronickou poštou či už šifrované, zipované plus chránené heslom, je bezpečne k dispozícii konkrétnym adresátom. Dáta, ktoré sú privátne umiestnené výhradne na Slovensku, je možné zdieľať s neobmedzeným počtom užívateľov z akéhokoľvek miesta a ľubovoľného zariadenia. Sú spoľahlivo zálohované - každých 24 hodín s retenciou 7 dní. Prehliadať a spravovať súbory je možné prostredníctvom webového rozhrania, verzionovanie dokumentov umožňuje návrat v čase. K službe Safe Private Drive je možné pristúpiť cez https://NázovVašejFirmy.safeprivatedrive.sk alebo cez využitie synchronizačného nástroja udržiavajúceho obsah medzi PC/NB a úložiskom alebo prístupom k súborom umiestneným cez WebDAV.

Článok pokračuje na platformofinvention.sk

Dušan Štrbík
IT manažér
DITEC Commerce s.r.o.

Výhody manažéra kybernetickej bezpečnosti, jeho nevyhnutnosť a pozícia vo firme

Kybernetická bezpečnosť nie je len nový marketingový nástroj či byrokratický nezmysel Európskej únie. Kybernetická bezpečnosť, to sú predovšetkým opatrenia smerujúce k zaisteniu bezpečnosti vašich informačných aktív. Tak, ako poznáme CISO z komerčnej sféry, je dôležitá aj úloha MKB – manažéra kybernetickej bezpečnosti. Pričom nejde len o legislatívnu povinnosť. Predovšetkým ide o príležitosť zodpovednej spoločnosti mať k dispozícii skutočného odborníka, riadiaceho kybernetickú bezpečnosť firmy tým správnym spôsobom.
Že takého človeka nepoznáte? Nejde o žiadnu prekážku - zákon pripúšťa manažéra kybernetickej bezpečnosti outsourcovať. Zverte teda kybernetickú bezpečnosť odborníkovi, ktorým je MKB. Nielen preto, že musíte, ale aj preto, lebo je to správna cesta k plneniu požiadaviek legislatívy pre danú oblasť.

Článok pokračuje na platformofinvention.sk

Miroslav Chlipala
Advokát/Partner
Bukovinský & Chlipala, s.r.o.

Nebezpečný home office

Ponúkame riešenia, čo ochránia vaše dáta a firmu od katastrofy

Už je to rok, čo sme preniesli náš osobný a pracovný život do online sveta. Komunikujeme cez platformy, sťahujeme aplikácie pre dištančné vzdelávanie, nakupujeme cez eshopy, a v neposlednom rade pracujeme na home office. A práve práca z domu dnes predstavuje obrovské kybernetické nebezpečenstvo a riziko katastrofy pre firmu. Ide o nevedomé vytváranie komfortného prostredia pre hekerov. Čo s tým?

Po rozpačitých začiatkoch, keď zamestnávatelia pristúpili k nevyhnutnosti práce z domu, firmy zvažujú preferovať túto formu naďalej. Je to v poriadku, ak splnia základné technické podmienky. Tými sú hardvérové vybavenie, bezpečné pripojenie k firemným systémom či logistika pre identifikáciu softvérových i hardvérových problémov a ich riešenia. Plus treba brať do úvahy osobnosti ľudí, ich individuálne možnosti a domáce zázemie. To všetko by mala firma zabezpečiť, skontrolovať a vylepšovať, aby jej bezpečný home office fungoval.

Najrizikovejšia zložka: človek

Ako rastie počet kritickej IT infraštruktúry, zložitosť systémov, narastá aj zraniteľnosť technológií. K tomu neúmerne rýchlo rastie kvalita a početnosť cielených útokov. Často netreba skúseného hekera, aby prístupové údaje skončili v zlých rukách. Drvivá väčšina moderných útokov je totiž zameraná na najslabší článok – na človeka, a ľudia majú tendenciu prehliadať a podceňovať záležitosti bezpečnosti, kým je všetko v poriadku. Pričom aj tu platí, že prevencia je vždy lacnejšia ako odstraňovanie následkov, v týchto prípadoch v podobe odstavenej výroby, vymazanej databázy či dôverných dokumentov voľne lietajúcich internetom.

Zdravé zabezpečenie = zdravá firma

Otázkou teda je, ako ste na kybernetické hrozby pripravili firmu vy. Dokážete predchádzať rizikám spojeným s krádežou citlivých dát, zneužitia prístupu do cloudu či používania nezabezpečeného zariadenia?

Pre zabezpečenie alebo zvýšenie bezpečnosti firemného IT prostredia existujú legislatívne opatrenia. Riadiť sa môžete napríklad normou ISO/IEC 27002 Best Practices v oblasti informačnej bezpečnosti. Zahŕňa opatrenia a návod na riešenie problémov ako ochrana citlivých údajov, riadenie aktív, riadenie prístupov a prístupových práv, bezpečnosť prevádzky, bezpečnosť komunikácie, prenosu dát, zvládanie bezpečnostných incidentov a iné.

Na základe edukácie si následne vyberiete pre vašu firmu najvhodnejšie technologické riešenie aj rozsah služieb.

Balíček Microsoft 365

Najbežnejšími riešeniami pre bezpečnosť sú balíčky Microsoft 365. Obsahujú pokročilé bezpečnostné funkcie, ktoré fungujú spoľahlivo a za každých okolností bez nutnosti byť vždy na rovnakom mieste či v jednom meste. Stačí oddeliť pracovný svet od domáceho a bezpečnostnou politikou mať správu všetkých zariadení aj dát pod kontrolou. Až 99,9 percentám útokov na identitu zabráni viacfaktorová autentifikácia.

Riešenie GAMO Drive

Pre všetkých, ktorí nie sú fanúšikom vyššie uvedeného a radi uprednostnia úložisko v bezpečnom cloude s garanciou spoľahlivej ochrany je tu GAMO Drive. Služba plne spĺňa nároky na bezpečnú modernú kanceláriu. Cloudové úložisko pre citlivé údaje sa postará o ukladanie, archiváciu, zdieľanie a synchronizáciu dokumentov.

Prístup k informáciám v GAMO Drive majú iba oprávnení používatelia, nemá na ne dosah ani samotný poskytovateľ služby. Bezpečnosť dát a informácií stráži viacúrovňová ochrana šifrovania a univerzálny prístup umožňuje dostať sa k dokumentom z akéhokoľvek zariadenia. Každý zákazník si navyše definuje vlastné preferencie a pravidlá práce s dokumentami ako upravovanie, sťahovanie, nahrávanie či čítanie.

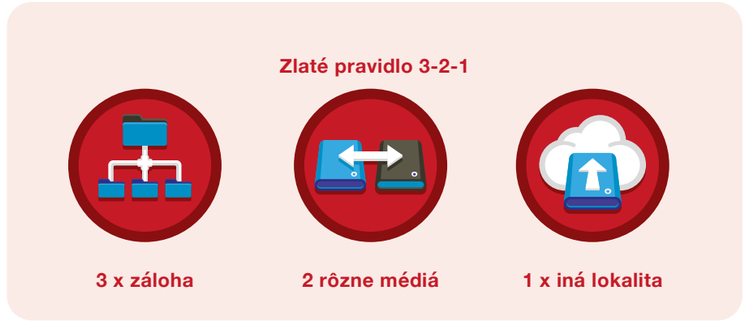
Na plnohodnotnú prácu či rýchle zásahy do dokumentov v rámci online kancelárie je možné využívať službu OnlyOffice.

> Bezpečnosť a jednoduchosť výmeny a zdieľania dokumentov so zákazníkmi presvedčila pre GAMO Drive účtovnú a daňovo-poradenskú spoločnosť LOGRO, ktorá ocenila aj ďalší dôležitý faktor v podobe customizácie riešenia. *„Prispôsobenie vizuálu prostredia pôsobí tak, že náš klient má pocit vstúpenia do spoločnosti LOGRO,“* hovorí jeho konateľka Ailin Hanková. *„Riešenie pôsobí na klientov profesionálne a je jednoduché na obsluhu pre všetkých. Výhodou je flexibilita, možnosť využívania služby aj v mobilných telefónoch,“* dodáva.

Bezpečne aj s 300 ľuďmi online

Z hľadiska bezpečnosti je veľmi dôležitý aj výber online komunikácie. Efektívnych nástrojov je hneď niekoľko, všeobecne známe sú platformy globálnych značiek ako Microsoft, Cisco či Google. Ak však hovoríme aj o psychologickom nastavení v rámci pocitu bezpečnosti, technicky aj funkčnosťou sa globálnym plne vyrovnajú aj riešenia zo Slovenska. Či už ide o online pracovnú poradu alebo o zabezpečenie videokonferencie pre 300 účastníkov. To všetko zabezpečuje napríklad GAMO Meet.

Ide o videokonferenčný systém, ktorý má všetky predpoklady, aby online komunikácia prebiehala pre organizátorov aj účastníkov komfortne a zároveň bez bezpečnostných rizík. Jeho webové riešenie si nevyžaduje inštaláciu a je k dispozícii po prihlásení sa cez webový portál meet.gamo.sk. Umožňuje organizovať online konferencie pre veľký počet účastníkov, interaktívne zdieľať obsah prezentácií, hlasovať alebo riadenou formou zapájať účastníkov do diskusie s maximálnou bezpečnosťou cloudového riešenia.



Zlaté pravidlo 3-2-1

Ak hovoríme v úvode, že človek je najrizikovejším faktorom, v závere treba prízvukovať, že aj najrozumnejším, ak sa rozhodne pre prevenciu. Doplnkovou k vyššie uvedenému a úplne najjednoduchšou pre predídenie scenáru zlyhania je využívanie pravidla 3-2-1. Jednoducho trojvrstvové fyzické zálohovanie. Zálohovanie pomôže pri omylom vymazanom e-maile i dokumente, pri samovoľne poškodených aj hekerom zakryptovaných dátach či vírusom zničených citlivých údajoch.

Koncovka s ESETom

Ak preferujete zosúladený systém IT bezpečnostných riešení poskytujúci ucelený prehľad, zvážte výber nástroja na detekciu a reakciu útokov ku koncovým zariadeniam.

Napríklad od firmy ESET. Nástroj Endpoint Detection & Response zhromažďuje údaje o udalostiach v pripojených koncových zariadeniach v reálnom čase a automaticky kontroluje, či údaje zodpovedajú kritériám podozrivej aktivity. Umožňuje tiež identifikovať nezvyčajné správanie a útoky, vyhodnocovať riziká, riešiť incidenty a nežiaduce aktivity v sieti. Nevynímajúc to, že ide o riešenie slovenskej spoločnosti, rešpektované na celom svete.

Najúčinnejšia a najlacnejšia je prevencia

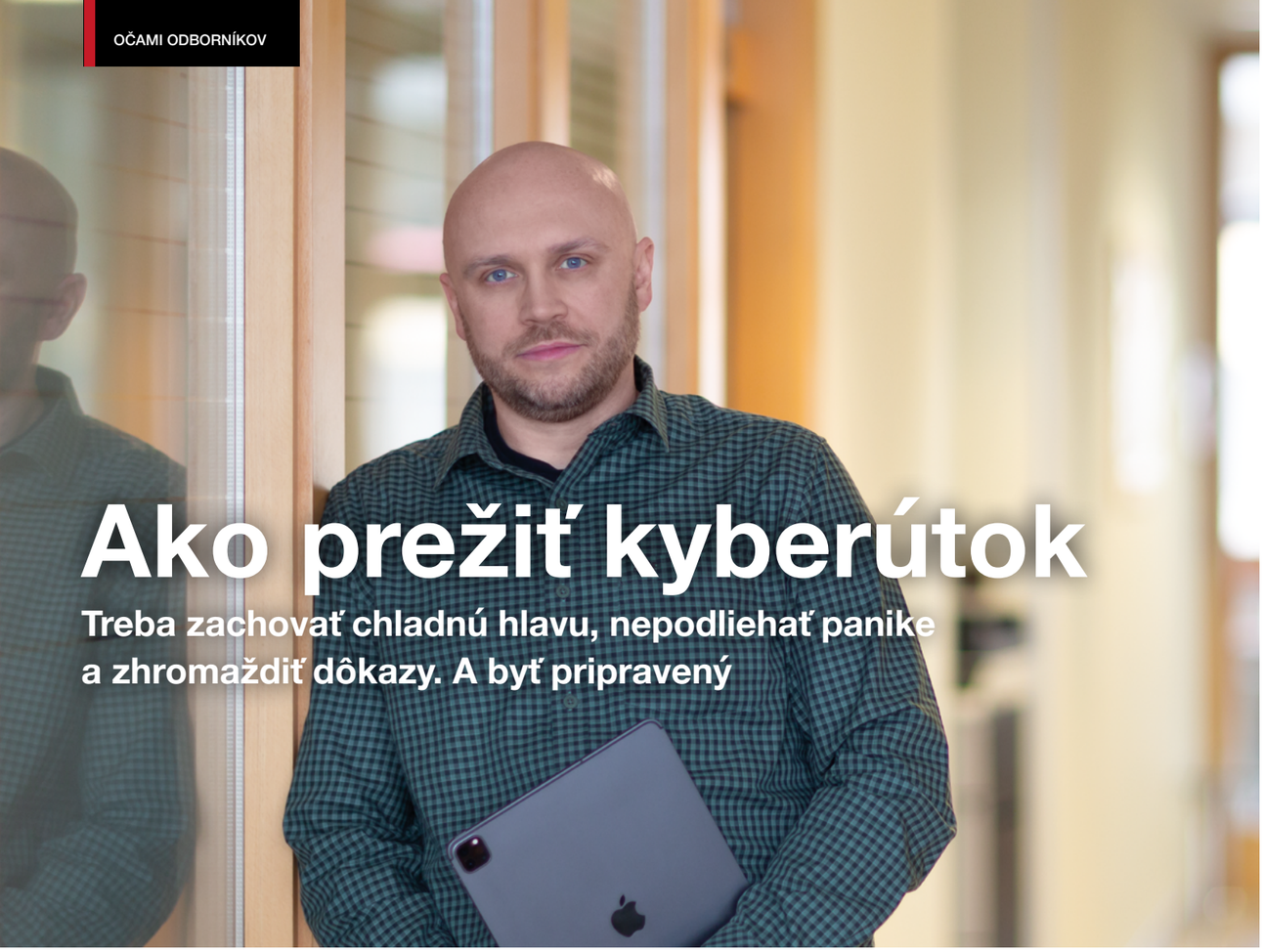
Univerzálny spôsob ako spraviť prácu z domu absolútne bezpečnú a odolnú ku kyber hrozbám neexistuje. Preto je dôležité položiť si jednoduchú otázku a úprimne odpovedať: Má firma interné zdroje a know-how, aby kľúčové veci riešila vlastnými kapacitami? Disponuje požadovanou úrovňou zabezpečenia pre reálne hrozby, relevantné pre daný typ biznisu a veľkosť firmy? Požiadavky na bezpečnosť rastú rýchlejšie ako ich reálna adaptácia vo firmách, preto je čas zvážiť všetky za a proti firemných schopností.

Najjednoduchším krokom pre začiatok budovania bezpečného home office je konzultácia s firmami, ktoré bezpečnostnými špecialistami disponujú. Vôbec nie je totiž nutné mať kyber špecialistu in-house, ale prizvať ho na spoluprácu poradensky, tak ako pri právnych či investičných aktivitách.

Vhodná kombinácia služieb pomôže - nielen pri home office - prekonať všetky technické úskalia. Experti vytvoria spoľahlivé prostredie, ktoré firma potrebuje. Navrhnú riešenie, ktoré chráni pred útokmi a identifikuje podozrivé interné incidenty. Vo výsledku to firme v prípade útoku ušetrí nemalé financie a nepoškodí reputáciu. A tu už hovoríme o miliónoch a potupe, ktoré zažili svetové giganty ako Amazon, Maersk, Garmin, Rosneft či americko-kanadská farmaceutická firma Merck, ktorá kvôli zničeným dátam z výskumu zaznamenala stratu 870 miliónov dolárov.

Žijeme v dobe spoločenskej zodpovednosti a popri nej je nevyhnutnosť budovať aj firemnú. Aj tu platí, že včera bolo neskoro.


Jana Kohárová
jana.koharova@gamo.sk



Ako prežiť kyberútok

Treba zachovať chladnú hlavu, nepodliehať panike a zhromaždiť dôkazy. A byť pripravený

Ľubomír Kopáček, expert na kyberbezpečnosť | GAMO a.s.

Zabezpečiť kontinuitu svojho podnikania bez vkladu do kyberbezpečnosti je v dnešnom online svete nemožné. Napriek tomu ju firmy radia na chvost investičných priorít. Len málo manažérov si uvedomuje, že reputačné a finančné následky po útokoch môžu naprávať roky. Viac sa dozviete v rozhovore s expertom na kybernetickú bezpečnosť Ľubomírom Kopáčkom.

Ako pristupujú slovenské firmy k otázke kyberbezpečnosti?

Väčšina sa touto témou zaoberá, až keď je neskoro. Najčastejšie ak už organizácia čelila útoku, ak je predmetom zákonnej regulácie a ak má materskú firmu v zahraničí alebo potrebuje naplniť požiadavku na kyberbezpečnosť od svojich obchodných partnerov. Treba povedať, že výrazne lepšia situácia je práve v spoločnostiach so zahraničnou účasťou, kde sa kyberbezpečnosť berie vážne. Predovšetkým to platí vo firmách pochádzajúcich z Nemecka a Francúzska.

Podobná situácia je aj v štátnych inštitúciách?

Tie sa v drvivej väčšine iba snažia formálne naplniť požiadavky zákona o kybernetickej bezpečnosti. Od jeho účinnosti žijú v omyle, že po audite je pre nich téma uzatvorená. Neuvedomujú si, že audit sa bude pravidelne opakovať a teda, že kybernetická bezpečnosť musí byť systematicky riadená.

Aký je motív útočníkov pri cielení na firmy a organizácie?

Neexistuje jednotný motív, ale najbežnejšie motívy sú peniaze a poškodenie organizácie.

Dá sa konkretizovať, koľkým útokom čelia slovenské firmy a štátne inštitúcie v ročnom priemere?

Nedá. Zasiahnuté subjekty sa k útokom neradi priznávajú, vnímajú to ako reputačné riziko a obávajú sa poškodenia dobrého mena. Štátne inštitúcie a organizácie, ktoré sú regulované zákonom o kyberbezpečnosti, majú zákonnú povinnosť hlásiť závažné incidenty autorite, v tomto prípade Národnému bezpečnostnému úradu. Takáto informácia je však predmetom utajenia a teda sa o nej okrem dotknutej inštitúcie a NBÚ nik nedozvie.

Existujú aj subjekty, ktoré kyberútokom nečelia?

Ak si to nejaká spoločnosť myslí, je to utópia a jednoznačný dôkaz, že majú nulovú viditeľnosť. V skutočnosti o žiadnych incidentoch nevedia preto, lebo nie sú schopné ich identifikovať. Incidentom čelí každá jedna firma alebo štátna inštitúcia bez výnimky.

Z toho vyznieva, že slovenské subjekty venujú kyberbezpečnosti nedostatočnú pozornosť. Hoci je v dnešnom online svete nevyhnutná pre zabezpečenie ich biznis kontinuity.

Prevažne ju považujú za zbytočnú investíciu. Nedochádza im, že môžu prísť o cenné dáta, citlivé informácie, ohrozený môže byť výrobný proces, a v hre je aj strata dôveryhodnosti pred klientami či dodávateľmi, ktorú si budovali roky. Schopní manažéri dobre vedia, aké ťažké je firmu budovať a určite si dokážu predstaviť, že ešte ťažšie by bolo napraviť si reputáciu po takomto incidente. Mnoho firiem používa dokonca stratégiu, kedy si spočítajú škody pri najhoršom možnom scenári, toto číslo si porovnajú s výškou investícií do kyberbezpečnosti, a rozhodnú, že potenciálne škody sú jednorazovo akceptovateľné.

To môže z čisto ekonomického pohľadu dávať zmysel.

Áno, ale má to chybičky krásy. Ten najhorší možný scenár sa môže zopakovať, a nie raz. Bude sa opakovať dovtedy, kým organizácia nezačne kyberbezpečnosť aktívne riadiť tak, aby mohla útokom predchádzať. Tu už ekonomický pohľad až taký zmysel nedáva. Incidenty môžu byť pre firmy aj likvidačné.

Čo je potrebné zmeniť, aby dokázali moderní manažéri incidentom predísť?

Ideálne by bolo, ak by mali organizácie úprimnú snahu a záujem riešiť kyberbezpečnosť bez toho, aby im to niekto prikazoval. Toto sa však nedeje. Potrebná je zmena myslenia a edukácia manažérov, pretože žiadneho manažéra len tak neosvieti a nepovie: Poďme minúť 5 percent zo zisku na kyberbezpečnosť. Potrebuje vedieť o hrozbách aj možnostiach ochrany, aby vedenie nemuselo aktivovať plán obnovy po katastrofe (Disaster Recovery – DR), ktorým sa potom činnosť organizácie dostáva do normálneho stavu. V skratke je potrebné dostať sa z reaktívneho prístupu na proaktívny.

Hovorili ste o pláne obnovy po katastrofe, ten je nevyhnutnou súčasťou plánu na udržanie biznis kontinuity (Business Continuity Plan – BCP). Čo to ale znamená v súvislosti s kyberbezpečnosťou?

Je potrebné mať pripravené a najmä pravidelne testované rôzne scenáre, ktoré majú vplyv na chod a prežitie organizácie v súvislosti s rôznymi ‚katastrofami'. Aktuálnym príkladom je povinná práca z domu. Tak, ako bol home office štátom nariadený, sa dá hovoriť o katastrofe z pohľadu biznisu. Ak má organizácia plán na zvládnutie napríklad totálneho a dlhodobého výpadku dodávky elektrickej energie, tak tento istý plán môže aktivovať aj pri povinnej práci z domu. Je to totiž presne to isté. Keď príde organizácia o napájanie elektrickou energiou na dlhší čas, tiež môže väčšinu zamestnancov iba poslať domov. Ak chce tento výpadok organizácia prežiť, musí mať pripravený a otestovaný scenár ako prácu organizovať na diaľku. Dobrou správou je, že v oblasti kyberbezpečnosti netreba nič vymýšľať na kolene, keďže existujú normy a medzinárodné štandardy, ktoré nám pri tvorbe BCP krok za krokom dokážu poradiť ako takéto plány zostavovať.

Čo je teda potrebné riešiť v rámci plánu biznis kontinuity?

Na detailnú odpoveď by nám nestačilo ani niekoľko desiatok strán. Stručné zhrnutie: je nevyhnutné mať plány pripravené tak, aby sa neriadená kyberbezpečnosť nestala prostriedkom, ktorý bude zosilňovať dopady katastrofy. Konkrétnym príkladom je, že spoločnosti by sa mali vyvarovať tomu, aby v prípade nútenej práce z domu pracovali zamestnanci na svojich domácich počítačoch. Dôvod je jednoduchý. Organizácia nemá tieto počítače pod kontrolou a mohli by sa stať prostriedkom pre kybernetický útok na ňu.

Líšia sa plány a úroveň zabezpečenia proti kyberútokom podľa veľkosti, druhu či zamerania firiem?

Samozrejme. Zabezpečenie potrebujú mať vytvorené na mieru podľa toho, či ide o finančnú inštitúciu, online podnikanie alebo sú orientovaní na priemysel a výrobu. Líšia sa nielen podľa sektora, ale úroveň zabezpečenia je rôzna v každej jednotlivej spoločnosti. Mala by byť primeraná účelu a ekonomickým možnostiam organizácie. Toto sa dá jednoznačne nastaviť. Umením je nájsť primeranosť výšky investícií k potenciálnym škodám. U všetkých však platí, že najcennejšie sú dáta a v tom prípade je nepodstatné, o aký sektor ide.

Ako by teda mala vyzerať príprava na kybernetický útok?

Na útok musíme vedieť hlavne reagovať a ideálne mu predchádzať. Dá sa dostať do súladu s niečím, čo je vyskúšané a keď sa toho budeme držať, tak s veľkou pravdepodobnosťou budeme vedieť na útok reagovať. Hovorím napríklad o norme ISO 27001, alebo o vyhláške 362/2018, prípadne iné vhodné štandardy.

Je nakoniec možné útok zastaviť?

Len vtedy, keď máme schopnosť ho identifikovať a disponujeme ľuďmi a prostriedkami na jeho zastavenie alebo aspoň zmiernenie dopadov. V praxi by som manažérom poradil, aby si v takejto situácii zachovali chladnú hlavu, nepodliehali panike a zhromaždili čo najviac dôkazov. Ak si nevedia poradiť sami, mali by požiadať o riadenie celej udalosti špecializovanú firmu. Rozhodne nie je namieste riešiť to svojpomocne.

Zuzana Omelková
zuzana.omelkova@gamo.sk

Kyberútoky neobišli ani Česko a Slovensko

Podceniť bezpečnosť sa neopláca. Prečítajte si, kto všetko už čelil bezpečnostnému incidentu a čo všetko sa dá stratiť.

Čítajte na platformofinvention.sk

Ako firme udržať rešpekt a bezpečie?

Matej Géci, generálny riaditeľ | Liptovská vodárenská spoločnosť a.s.

Je už každodennou realitou, že sa spoločnosti, prevádzkujúce IT a priemyselné systémy, stretávajú so sofistikovanými útočníkmi v ťažkom boji o kybernetickú bezpečnosť. Tieto incidenty majú veľký potenciál znižovať dôveryhodnosť, spôsobovať obrovské škody a ničiť reputáciu roky budovaných firiem. Výhodu majú tí, ktorí si riziká uvedomia včas a do protiopatrení investujú.

Krok pred hekermi sú aj spoločnosti regulované v oblasti kyberbezpečnosti zákonom. Medzi ne patrí Liptovská vodárenská spoločnosť, a.s., ktorá pod taktovkou externého manažéra kybernetickej bezpečnosti dosiahla v danom sektore nadpriemernú úroveň.

Vitajte v online svete

Už vieme, že podnikateľská sféra je atraktívny cieľ pre útočníkov, o to viac v oblasti základných služieb ako sú dodávka pitnej vody a energií. Aj Liptovská vodárenská spoločnosť si uvedomuje, že sa bez riadenia kyberbezpečnosti v dnešnej dobe nezaobíde. Navyše, v roku 2020 celý svet ovplyvnila pandémia COVID-19, kedy sa informačné a komunikačné technológie v ešte väčšej miere stali súčasťou každodenného života.

„Viac sa používala elektronická komunikácia, pracovné stretnutia sa z reálneho prostredia preniesli do online sveta. Potreba elektronickej komunikácie priniesla zvýšené riziko bezpečnostných incidentov. Preto Liptovská vodárenská spoločnosť, a.s., kladie veľký dôraz nielen na zvyšovanie úrovne svojich informačných systémov, ale i na zabezpečenie kybernetickej bezpečnosti," vysvetľuje Juraj Ivan, vedúci oddelenia informačných technológií vo firme.

Liptovská vodárenská spoločnosť nikdy nepatrila medzi podniky, ktoré by si neuvedomovali kybernetické hrozby. Preto prijali zaradenie prostredníctvom Národného bezpečnostného úradu pod zákon 69/2018 Z. z. o kybernetickej bezpečnosti ako prirodzenú súčasť rozvoja. „Vo svete sme zaregistrovali kybernetické útoky na vodárenské spoločnosti, ktoré predstavovali priamu hrozbu pre zabezpečenie výroby a dodávky pitnej vody. Tak ako aj v iných odvetviach stále viac využívame inteligentné riadiace prvky, ktoré sa môžu stať cieľom kybernetických útokov. Úspešne realizovaný útok môže mať za následok zmenu kvality vody alebo môže spôsobiť výpadok dodávky pitnej vody," uvedomuje si Matej Géci, generálny riaditeľ Liptovskej vodárenskej spoločnosti, a.s.

Externí experti

Spoločnosť v každej fáze implementácie systému riadenia kyberbezpečnosti spolupracovala s externými expertami. Dôvodom je, že pre efektívne zavedenie tohto systému je nevyhnutné mať odborné znalosti a najmä skúsenosti s jeho zavádzaním. Len odborníci so vzdelaním a skúsenosťami v oblasti riadenia informačnej bezpečnosti podľa normy ISO 27000 dokážu úspešne implementovať systém. Pretože je takých odborníkov na Slovensku nedostatok a sú pomerne nákladní, je na každej spoločnosti, či takého odborníka zamestná natrvalo alebo s ním spolupracuje iným spôsobom.

Veľké zmeny

V období apríl až jún 2020 boli vo firme realizované významné zmeny v oblasti kybernetickej bezpečnosti, kedy vznikla kompletná bezpečnostná dokumentácia vrátane politík a smerníc, bola uzatvorená zmluva na služby externého bezpečnostného manažéra a bol vytvorený interný tím kybernetickej bezpečnosti. Tento tím od začiatku pracoval v režime pravidelných operatívnych porád s prestavenými úlohami a zodpovednosťou za jednotlivé úlohy. V úvode bolo potrebné dôkladné poznanie procesov v spoločnosti. V praxi to znamenalo hodiny štúdia relevantných smerníc aj hodiny rozhovorov o zavedených postupoch.

> ***„Kybernetická bezpečnosť nám priniesla obrazne povedané pokojný spánok v oblasti prevádzky informačnej infraštruktúry a samotnej technológie výroby pitnej vody. Našim zákazníkom zasa istotu, že voda z kohútikov verejného vodovodu bude zdravotne nezávadná."***
>
> Matej Géci,
> generálny riaditeľ Liptovskej vodárenskej spoločnosti

„Naša spoločnosť stavila na externú spoluprácu, pretože nedisponuje kvalifikovaným zamestnancom s dostatočnou praxou na pozíciu manažéra kybernetickej bezpečnosti. Pristúpili sme k výberovému konaniu na poskytnutie služby manažéra, ktorý v závislosti od legislatívnych požiadaviek usmerňuje činnosť pracovníka spoločnosti, určeného pre informačnú bezpečnosť, zabezpečuje dosiahnutie súladu pre našu spoločnosť s príslušnými zákonmi o kybernetickej bezpečnosti, poskytuje poradenstvo a konzultácie týkajúce sa zákona a príslušných vyhlášok," odôvodňuje rozhodnutie generálny riaditeľ Matej Géci.

O spoločnosti

Liptovská vodárenská spoločnosť, a.s., Liptovský Mikuláš, vznikla 7.9.2006 ako nástupnícka organizácia zanikajúcej spoločnosti Severoslovenská vodárenská spoločnosť, a.s., Žilina, keď bola rozdelená na základe regionálneho princípu.

Prioritou Liptovskej vodárenskej spoločnosti je poskytovať obyvateľom liptovského regiónu spoľahlivé služby spojené s dodávkou kvalitnej pitnej vody a odvádzaním a čistením odpadových vôd svojim odberateľom na úrovni požadovanej slovenskou a európskou legislatívou.

Unikátne know-how

Za výraznými zmenami je spoločnosť GAMO, ktorá v rámci služieb zákazníkovi zrealizovala aj analýzu infraštruktúry využitím riešenia od izraelskej spoločnosti Claroty.

„Máme s ňou veľmi dobré skúsenosti a aj unikátne know-how pri nasadení v hybridnom IT/OT prostredí. Takáto technická analýza býva obvykle argumentom, ktorý takpovediac zlomí pohľad klientov na potrebu riešenia kybernetickej bezpečnosti. Ak si klienti do technickej analýzy mysleli, že prostredie nemali v ideálnom stave, po takejto analýze väčšinou hovoríme o katastrofe. Vo svete kyberbezpečnosti sa občas dejú aj nečakané veci, a tak sa stalo, že v Liptovskej vodárenskej spoločnosti sme katastrofu nevideli. Videli sme, že máme stále rezervy, ale nenašli sme žiadne fatálne zlyhania," analyzuje manažér kyberbezpečnosti Ľubomír Kopáček.

Liptovská vodárenská spoločnosť má pred sebou stále množstvo úloh a niekoľko zásadných technických zmien. Po ich realizácii sa stane ukážkovou firmou vo svojom segmente a bez výhrad zvládne externý audit kybernetickej bezpečnosti, ktorý ju čaká v tomto roku.

„Možno konštatovať, že úroveň kybernetickej bezpečnosti v spoločnosti je na pomery bežných štandardov v danom sektore už na nadpriemernej úrovni. Musím ale zdôrazniť, že nič z toho, čo sme spomínali, by sa nedalo realizovať, keby firma ako taká nebola od začiatku nastavená posúvať sa v tejto oblasti vpred s úprimným záujmom," dodáva expert pre kybernetickú bezpečnosť Ľubomír Kopáček.

Prostredníctvom verejného vodovodu zásobujeme okres Liptovský Mikuláš

94%
68-tisíc obyvateľov

519 km
Dĺžka vodovodnej siete

14 934
vodovodných prípojok

Prostredníctvom verejnej kanalizácie odkanalizujeme skoro 57-tisíc obyvateľov okresu.

80%
57-tisíc obyvateľov

327 km
Dĺžka kanalizačnej siete

Branislav Lupták
branislav.luptak@gamo.sk

Vodáreň terčom útoku

Neznámy heker sa nabúral do riadiaceho systému vodárne na Floride a zmenil dávkovacie hodnoty hydroxidu sodného (NaOH). Ten sa používa na úpravu pitnej vody a mení jej pH tak, aby spĺňala požadované kvalitatívne parametre. Zdá sa vám to ako sľubný začiatok akčného filmu? Je to ale realita. Podľa bezpečnostného konzultanta a audítora kritickej infraštruktúry Martina Fábryho sa tento prípad z februára 2021 môže zopakovať aj na Slovensku. A to v prípade, ak si manažéri nedajú pozor na kvalitné riadenie kyberbezpečnosti.

Útočník presne vedel, kam zacieliť. Zmenil hodnotu dávky NaOH približne stonásobne, čím zvýšil množstvo chemikálie pridávanej do vody na nebezpečnú úroveň. Prevádzkový monitorovací systém vodárne však okamžite detekoval nadmerné množstvo anorganickej látky. Vďaka rýchlemu zásahu operátora sa dávkovanie dostalo do normálu. Ak by však monitorovací systém pre pH vody správne nezareagoval, prípadne by ho útočník napadol a vyradil z prevádzky, mohlo to mať závažný dosah na zdravie ľudí.

Riadiace systémy v moderných úpravniach vody používajú prístrojové vybavenie, ktoré nepretržite monitoruje parametre kvality vody, napríklad pH alebo chlór. Výstrahy pri prekročení prijateľných limitov poskytujú v reálnom čase. Kritické parametre sa zvyčajne monitorujú na viacerých miestach, nielen počas procesu úpravy, ale aj v prenosových a distribučných systémoch.

„Na Slovensku sa dokonca zvýšená hladina chemikálií vo vode odhaľuje aj pomocou pstruha dúhového, ktorý je na ňu mimoriadne citlivý. Je to akási neheknuteľná analógová poistka. Napriek mnohým bezpečnostným prvkom však vždy existuje riziko vyradenia kritických priemyselných procesov sofistikovaným útokom," vysvetľuje bezpečnostný konzultant Martin Fábry.

Situácia počas pandémie je ešte o čosi zložitejšia. Spoločnosti musia vykonávať údržbu riadiacich systémov vzdialene cez internet. Takéto spojenia však často mávajú nízku úroveň zabezpečenia. Aktuálne sa v internete nachádza stotisíc riadiacich systémov, ktoré by nemali byť viditeľné, pretože sú zraniteľné a môžu byť ľahkým terčom. Ich viditeľnosť znásobuje pravdepodobnosť útoku. „Je to výsledok nevedomosti prípadne ľahostajnosti. Vodárenské spoločnosti bývajú často finančne podvyživené a trpia slabou kybernetickou obranou. Preto sa klasifikujú ako jeden z najväčších rizikových sektorov kritickej infraštruktúry," hovorí Fábry.

Podľa neho sú na Slovensku poddimenzované IT tímy a kybernetických expertov, ktorí by boli schopní postaviť robustný program na ochranu kritickej infraštruktúry, je veľmi málo. Tvrdí, že podobné útoky môžu zasiahnuť aj ďalšie kritické sektory ako sú rafinérie, petrochémia či energetika. Ich dosah na spoločnosť môže byť citeľný, ba až nebezpečný.

„Preto je nevyhnutné brať kybernetickú bezpečnosť s plnou vážnosťou a implementovať hĺbkovú kybernetickú obranu. Je to záležitosť národnej bezpečnosti," varuje audítor kritickej infraštruktúry.

Zuzana Omelková
zuzana.omelkova@gamo.sk

Vlastné železo alebo prechod do cloudu?

Martin Pisák
martin.pisak@gamo.sk

V troch slovenských spoločnostiach sme sa pýtali na ich názor: preferenciu cloudového riešenia či vlastnej infraštruktúry.

V dnešnej dobe to nie je ani tak otázka buď / alebo, ale skôr spôsob vzájomného dopĺňania sa technológií. Žiadaná je efektívne fungujúca kooperácia cloud služieb a vlastnej infraštruktúry. Výhody vlastného on-premise hardvéru pre beh aplikácií a ukladanie údajov sú všeobecne známe: rýchla odozva, vyššia úroveň bezpečnosti, nižšie náklady na úložisko pri väčších objemoch dát. Cloud významne uľahčuje spoluprácu medzi kolegami v ére home office, umožňuje pružnejšie reagovať na potreby biznisu. Prakticky okamžite poskytne požadovaný výkon alebo priestor na ukladanie dát a odpadá réžia spojená so správou vlastného hardvéru. Je zabezpečená väčšia stabilita a kontinuita pri aktualizáciách. Rozhodnutie, ktorú technológiu použiť, tak závisí hlavne od požiadaviek kladených na projekt. V prípade spoločností ako Hydro Extrusion, ktoré sú súčasťou medzinárodných korporácií, však do výsledného riešenia vstupujú centrálne IT tímy s vlastnými požiadavkami a architektonickými rozhodnutiami. Vlastný hardvér a lokálne virtualizované prostredie, manažované v úzkej spolupráci s IT špecialistami z regiónu, nám umožňuje pružne otestovať, vyvinúť, kompletne nakonfigurovať a nasadiť riešenie bez zložitej korporátnej byrokracie.

Marek Ondík
Country supervisor IT
Hydro Extrusion Slovakia a.s.

Úlohou nášho startupu je predaj licencií aplikácií a riešení súvisiacich s elektronizáciou spoločností, ktoré vyvíja naša materská firma. Pri jeho vzniku v roku 2017 bolo nutné riešiť infraštruktúru pre internetový portál, ktorý zabezpečí pohodlný nákup produktov a starostlivosť o všetkých klientov. V infraštruktúre materskej spoločnosti bolo komplikované a časovo náročné realizovať to in-house. Pri hľadaní riešenia ako rýchlo zabezpečiť HW pre prevádzku 24 x 7 spolu so zálohovaním systému a dát e-shopu sme preto prišli k záveru, že jediná cesta je využiť cloudové služby.

Pri výbere cloudového providera sme sa zamerali na vysokú bezpečnosť a dostupnosť poskytnutej služby. Uprednostnili sme prevádzkovateľa, ktorý má svoje riešenie umiestnené len na území Slovenska. Pre začiatok sme si vybrali službu IaaS s primeranými počiatočnými parametrami virtuálneho servera. E-shop - produkčný systém, nastavili pre naše potreby dodávateľsky a podľa našich predstáv. Celé riešenie bolo v krátkej dobe postavené a pripravené na predaj našich produktov. Počas 4-ročného používania nevznikol žiadny výpadok a nemali sme žiadne problémy s infraštruktúrou a dostupnosťou e-shopu v internete. Jednoducho: ide o rýchle a bezpečné riešenie za prijateľnú cenu.

Dušan Štrbík
IT manažér
DITEC Commerce s.r.o.

PLH Advanced Engineering SK je etablovaná spoločnosť poskytujúca pokročilé inžinierske služby širokému okruhu zákazníkov s cieľom ponúknuť im konkurenčnú výhodu pri vývoji produktov. Prioritou je najvyššia úroveň výskumných a vývojových prác pre maximálne optimalizované a inovované produkty našich zákazníkov. Jednou z odborných činností, pomáhajúcich dosahovať naše ciele, sú výpočtové simulácie využívajúce metódu konečných prvkov (FEM). Aplikácie, schopné vykonávať tieto simulácie, sa vyznačujú vysokými nárokmi na zariadenia, kde sú nainštalované a spúšťané.

Hardvérová náročnosť daných softvérových riešení býva obvykle veľmi vysoká a vzhľadom na premenlivú komplexnosť inžinierskych úloh aj rôznorodá. Nie je preto vždy rentabilné investovať do vybavenia pokrývajúceho všetky výkonové požiadavky spomínaných aplikácií. Cloudové riešenia nám pomáhajú vykonávať pokročilé a hardwarovo náročné simulácie, a to najmä vďaka dostupnej flexibilite a škálovateľnosti využívanej cloudovej platformy, kde sme schopní riešiť aj tie najkomplexnejšie simulácie. To všetko pri maximálnej efektivite vynaložených prostriedkov.

Tomáš Špánik
Riaditeľ
PLH Advanced Engineering SK s.r.o.

Kam na výlet? Slovenská aplikácia Rozhliadni sa vás zavedie na krásne miesta

Ideálnou odmenou za zdolaný kopec je zvyčajne krásny výhľad. Ten vám na Slovensku poskytnú doslova desiatky turistických rozhľadní a vyhliadkových veží. Ako ich však nájsť, ako sa k ním dostať a čo od nich vlastne čakať?

Všetky odpovede o vašej najbližšej ceste za výhľadom vám poskytne slovenská aplikácia Rozhliadni sa.

Aplikácia pre Android aj iOS obsahuje všetky informácie o turistických rozhľadniach a vyhliadkových vežiach na Slovensku aj v pohraničí, ku ktorým sa majú v budúcnosti dostať aj rozhľadne v susedných krajinách. Aplikácii stačí povoliť prístup k vašej aktuálnej polohe a na domovskej obrazovke už uvidíte najbližšie rozhľadne vo vašom okolí. Tie ostatné vám aplikácia ukáže na mape.

Rozhľadne môžete vyhľadávať aj podľa názvu mesta, obce alebo okresu. Ak vašu obľúbenú rozhľadňu či vyhliadkovú vežu v aplikácii nenájdete, stačí klepnúť na tlačidlo „+“ a vyplnením webového formulára na chýbajúcu rozhľadňu upozorniť vývojárov aplikácie. Jedna vec je rozhľadňu nájsť, tá druhá sa k nej dostať. Každá rozhľadňa a vyhliadková veža v aplikácii by mala obsahovať stručné informácie o tom, ako sa k nej dostať, konkrétnejšie detaily trasy a základné informácie o samotnej rozhľadni. Vďaka týmto popisom rýchlo zistíte, či je vhodné na rozhľadňu vyraziť aj s deťmi a či sa k nej prípadne náhodou nedostanete aj pomocou MHD.

Aplikácia Rozhliadni sa je dostupná bezplatne a tak sa z nej stáva adept na ideálneho parťáka pre plánovanie výletov na najbližšie týždne a mesiace. Počas nich však nezabúdajte na aktuálne platné protipandemické opatrenia a tak si v aplikácii vyberajte skôr menej navštevované rozhľadne, prípadne si priestor na výlet vyhraďte mimo víkendovej špičky, kedy zvyknú byť na tých najznámejších rozhľadniach väčšie davy ľudí.

Stanislav Vinc
Techbox
Dennik N

Stiahnuť na App Store

GET IT ON Google Play

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

ESET.SK/FIRMY

PROTECT

BIZNIS RIEŠENIA NOVEJ GENERÁCIE

Spravujte IT bezpečnosť vašej firmy odkiaľkoľvek prostredníctvom cloudovej konzoly ESET PROTECT. Nové balíky bezpečnostných riešení prinášajú progresívnu ochranu pre firmy všetkých veľkostí.

NOVÉ BALÍKY FIREMNÝCH BEZPEČNOSTNÝCH RIEŠENÍ

ESET PROTECT Advanced

Viacvrstvové zabezpečenie koncových zariadení s ochranou pred ransomvérom a zero-day hrozbami, doplnené o riešenie na šifrovanie celých diskov.

ESET PROTECT Complete

Rozširuje balík bezpečnostných riešení Advanced o ochranu firemných cloudových aplikácií a e-mailovej komunikácie.

ESET PROTECT Enterprise

Komplexný bezpečnostný balík pre veľké firmy s proaktívnou ochranou pred neznámymi hrozbami a s riešením na detekciu a nápravu bezpečnostných hrozieb (EDR).