platform of invention

Užitočné v správnych hlavách

magazín pre CTO, CFO, CEO

2 / 2021

Informačné technológie pre podnikanie s nápadom

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

ročník prvý | náklad 7 300 výtlačkov

Éra cloudu, nekonečné možnosti

Rozhovor s expertom na cloudové riešenia

Je potrebné sa obávať migrácie?

Rekonštrukcia kyberútoku na výrobnú firmu

+ 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 3 500 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

Výkonný, bezpečný, spoľahlivý. S unikátnou kombináciou technológií a dostupnosti služieb. Komfortný, cenovo výhodný a škálovateľný. To všetko je cloud. Nielen módny trend čo príde a odíde, ale realita a celosvetový technologický fenomén, výrazne meniaci spôsob nášho pracovného aj súkromného života. Vďaka nemu sa dnes môžeme sústrediť na to najdôležitejšie: na dosahovanie obchodných cieľov a úspechov.

Cloud a jeho riešenia poskytujú okrem moderného prostredia pre firemnú infraštruktúru flexibilitu, zrýchľujú procesy a umožňujú vyvíjať sa s potrebami spoločností. Efektivita na realizáciu projektov je v cloudovom prostredí znásobená príchodom, rozvojom a aplikáciou nových technológií a služieb. Niet pochýb o tom, že sa doň presúvajú firemné systémy.

Pričom je nezanedbateľným faktorom bezpečnosť. Prístupnosť technológií a systémov firmy aj pre prácu z domu je neodolateľným benefitom smerujúcim k vyššej digitalizácii pracovného prostredia. V čase pandémie a každodenných kybernetických útokov na podnikateľské subjekty sa navyše osvedčil cloud ako nenapadnuteľná istota.

Cloudová stratégia je aktuálne nutnosťou IT plánovania každej organizácie, ktorá chce zlepšiť spoľahlivosť systémov a zabezpečiť si automatizovanú prevádzku. V tvrdých konkurenčných podmienkach obstoja tí, čo sú pripravení.

Rozvoj digitalizácie spoločnosti, efektivity jej procesov, a v neposlednom rade znižovanie každoročných nákladov – napríklad na životnosť „železa“ v podobe dnes už prežitých serverovní pod stolom - je súčasťou moderne zmýšľajúceho manažéra.

Viac sa dočítate na stránkach nášho magazínu.

Ambíciou **Platform of Invention** je inšpirovať a podporovať všetkých, čo si chcú rozšíriť obzor v informačných technológiách. Otvorme spoločne komunikáciu a nachádzajme riešenia, ktoré pomáhajú rozvíjať naše podnikanie.

Príjemné čítanie,

Martin Pisák
Technický riaditeľ
martin.pisak@gamo.sk

Sofistikované hrozby si vyžadujú pokročilú EDR ochranu

Kybernetické hrozby sa vyvíjajú dynamickým tempom a hekeri sa snažia naplniť svoje vrecká čoraz vyspelejšími taktikami. Počas pandémie sa prechodom na home office riziká znásobili. Na tie najsofistikovanejšie útoky je pritom iba základná úroveň IT zabezpečenia firmy prikrátka. Pokročilé pretrvávajúce hrozby, nové typy ransomvérov či bezsúborové útoky dokáže odvrátiť iba komplexnejšia, viacvrstvová ochrana vo forme nástroja na detekciu a reakciu na útoky na koncové zariadenia (EDR). Spoločnosť ESET ho má vo svojom arzenáli vo forme riešenia ESET Enterprise Inspector, ktoré nepretržite v reálnom čase monitoruje siete a koncové zariadenia. To umožňuje detailnú analýzu podozrivého správania už v počiatočnom štádiu útoku. EDR nástroj zároveň analyzuje incidenty, ktoré by mohli byť súčasťou väčšieho útoku a izoluje zariadenia, ktoré môžu byť infikované.

Článok pokračuje na platformofinvention.sk

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

Arrow Cloud Backup vás zbaví starostí so zálohovaním

Arrow Cloud Backup pre Microsoft 365 je zálohovacie riešenie formou služby, ktorá vás zbaví starostí so zálohovaním dát. Ako zistiť, či sú vaše dáta v rámci služby Microsoft 365 chránené?
Vo firmách je rozšírená mylná predstava, že produkty Microsoft 365 sú zálohované. Mnohí zákazníci si však neuvedomujú, že hoci spoločnosť Microsoft chráni prevádzkyschopnosť infraštruktúry, za ochranu samotných dát sú zodpovední práve oni. Vaše dáta budú s ACB chránené a zálohované: až na 10 rokov, s neobmedze-

nou kapacitou úložiska, za minimálne mesačné poplatky bez záväzkov a bez počiatočnej investície.
Arrow Cloud Backup zálohuje dáta v nasledujúcich aplikáciách: Outlook e-maily, kalendár, kontakty, MS Teams, SharePoint, OneDrive for Business.

Článok pokračuje na platformofinvention.sk

Martin Pisák
Technický riaditeľ
GAMO a.s.

Staré, nové, najnovšie. Vyvraciame všetky mýty o cloude!

Cloud si získava čoraz väčšiu pozornosť aj na Slovensku. Pre firmy je ideálnym riešením ako sa prioritne sústrediť na rozvoj a budovanie svojho biznisu, nie mať starosť o vlastné servery a IT. Napriek tomu sa mu niektoré stredné a menšie firmy bránia. V mnohým prípadoch podliehajú fámam, ktoré zavádzanie cloudu sprevádzajú na celom svete. Opakujúce sa otázky sú: Je to pre mňa rentabilné? Budem musieť školiť a platiť nových ITčkárov? Nie sú dáta bezpečnejšie doma na vlastných serveroch? Čo keď bude poskytovateľ sledovať a predávať moje obchodné tajomstvá?
Pozrime sa pozornejšie na MÝTUS 1.: Malá firma vraj nevyužije cloudové služby a je to pre ňu nerentabilné. Faktom však je, že cloud dávno nevyužívajú len veľké korporácie. V čoraz väčšej miere je výhodný vo využití či finančnej dostupnosti aj pre menšie a stredné podniky s desiatkami zamestnancov. Vďaka škálovateľnosti si každý z nich nastaví a zaplatí parametre, ktoré aktuálne potrebuje, a oživí systém. Ten cloudový je jednoduchý, dynamický a bezpečný. Ďalších 7 mýtov a faktov o cloude nájdete v pokračovaní článku na platformofinvention.sk.

Článok pokračuje na platformofinvention.sk

Jana Kohárová
Obchodná riaditeľka
GAMO a.s.

Výber správneho SD-WAN-u prináša poskytovateľom služieb cenné príležitosti

Spoľahlivé Secure SD-WAN riešenie je nevyhnutné pre urýchlenie sprístupnenia geograficky rozptýlených pobočiek k využívaniu základných podnikových aplikácií a služieb. Všetky potrebujú konektivitu, bezpečnosť a možnosť zjednotenej správy, aby poskytovali čo možno najlepšiu používateľskú skúsenosť. Dôležitá je tiež možnosť zaobchádzať s každou pobočkou ako so samostatnou entitou vždy, keď to situácia vyžaduje.

Príliš veľa SD-WAN riešení má však isté obmedzenia čo sa týka rozsahu možností a doplnkových služieb, ktoré poskytujú. Nesprávne riešenie SD-WAN môže navyše zvýšiť zložitosť infraštruktúry či náklady na samotné nasadenie aj následnú réžiu.

Článok pokračuje na platformofinvention.sk

Veracomp Slovakia s. r. o.
www.veracomp.sk

Služba S3. Počuli ste o nej?

Simple Storage Service alebo aj S3 je cloudová služba poskytujúca jednoduché riešenie pre ukladanie dát. Ide o objektové úložisko, kde pod pojmom objekt rozumieme dáta rôzneho typu ako obrazový materiál, textové súbory, webové stránky, mobilné aplikácie, podnikové aplikácie či zariadenia internetu vecí IoT.
Tieto položky sa aj so svojimi metadátami v S3 ukladajú do pomyselných zásuviek a možno ich nakonfigurovať tak, aby podporovali konkrétne potreby použitia.
Služba Simple Storage Service je vhodná pre firmy všetkých veľkostí a odvetví bez rozdielu. Poskytuje priestor pre bezpečné ukladanie dát s možnosťou automatického zálohovania, špičkový výkon, škálovateľnosť, dostupnosť a odolnosť. Jednou z jej výhod je aj ponechanie viacerých verzií objektu v jednej zásuvke, čo umožňuje obnovovanie omylom odstránených alebo prepísaných objektov.

Článok pokračuje na platformofinvention.sk

Martin Pisák
Technický riaditeľ
GAMO a.s.

Desktop ako služba. DaaS

DaaS je služba cloud computingu, v rámci ktorej poskytovateľ dodáva koncovým používateľom formu virtuálnych pracovných staníc prostredníctvom internetového prístupu s licenciou pre každého používateľa.
Služba odbremení administrátorov od rutinných činností a ušetrený čas môžu venovať rozvoju IT. Výpočtové zdroje klient prispôsobí svojim potrebám, pričom je nová pracovná stanica pripravená radovo v minútach. Je možné sa na ňu prihlásiť na ľubovoľnom zariadení vo svojej kancelárii, doma či na cestách. Všetky dáta sú bezpečne uložené v cloude a na Slovensku.
Používateľ sa navyše nemusí obávať, že svoje údaje stratí, pretože vzdialené dátové centrum ukladá dáta s vysokou úrovňou redundancie. Pokiaľ je napríklad zariadenie odcudzené alebo dôjde k strate, používateľ sa k pracovnej ploche dostane aj z mobilu, notebooku či tabletu.

Článok pokračuje na platformofinvention.sk

Martin Pisák
Technický riaditeľ
GAMO a.s.

Únik dát môže firmu pripraviť o financie či know-how

Hekerom i vírusom odolá kvalitný cloud

Pandémia nám ukázala, že nie sme v bezpečí nielen vo vonkajšom svete, ale ani v online. Firmy sa začali zodpovednejšie správať v oblasti ochrany dát voči kybernetickým útočníkom. Nástrahy v podobe straty reputácie či peňazí naštartovali procesy smerujúce k modernizácii technologických vybavení. Čoraz väčšie percento stredných aj malých spoločností ako nevyhnutnosť vyhodnocuje prechod z tradičnej serverovne do cloudu.

Erik Kirschner, cloud konzultant
GAMO a.s.

Bezpečnosť pritom nie je jedinou výhodou uloženia firemných dát do cloudových úložísk. Cloud konzultant spoločnosti GAMO **Erik Kirschner** na počkanie vymenuje ďalších päť. V neposlednom rade firmy ušetria.

Je slogan, že z cloudu pršia peniaze pravdivý?

Aj keď sa to firmám spočiatku nezdá, v konečnom dôsledku vždy ušetria peniaze. Už len z dôvodu, že v cloude sú dáta dostupnejšie, vždy zálohované, dokážete k nim pristupovať vždy rýchlo a bezpečne, čo je výrazný rozdiel oproti prevádzkovaniu aplikácií u seba, teda na vlastných serveroch. Nehovoriac o tom, že v prípade cloudu ide o modernejšiu infraštruktúru než je „železo doma pod stolom“.

Pozrime sa bližšie na výhody cloudu. V čom sú hlavné benefity?

Po prvé je infraštruktúra poskytovateľa cloudových služieb robustnejšia a má vyššiu dostupnosť. Klientovi odpadá starosť o serverovňu, diskové polia, servery. Druhou výhodou je škálovateľnosť. Ak firma potrebuje na krátky alebo obmedzený čas veľký diskový objem, napríklad 6 TB kvôli zmenám ako účtovná uzávierka, tak si cloudový server zväčší cez webové rozhranie. To isté platí aj pre CPU, RAM a iné technické parametre virtuálnych serverov. Keď proces prebehne a firma už nepotrebuje také veľké úložisko, diskový objem v cloude vráti na pôvodný a takto šetrí financie. To je tretie plus. Poviem to na príklade: Keď má firma dáta na serveroch a chce napríklad dokúpiť RAM (operačnú pamäť), musí IT oddelenie žiadať manažment o peniaze na nákup, a manažment musí následne zaplatiť aj firmu, ktorá RAM-ku vloží do servera. To sú dve investície navyše, pričom v cloude na to stačí jeden klik alebo telefonát. Štvrtým pozitívnym faktorom cloudu je dynamika. Za piatu výhodu, ktorá súvisí aj s financiami, môžeme považovať flexibilitu – presun z investičných (CAPEX) do prevádzkových (OPEX) nákladov. Ak má firma cloudové úložisko postavené na prevádzkových nákladoch, nemusí robiť žiadnu investíciu do infraštruktúry, ale priamo v cloude si obstará to, čo práve potrebuje.
Ďalšou výhodou je nepretržitá podpora, konzultácie technických špecialistov v materinskom jazyku.
A, samozrejme, neposlednou výhodou cloudu je bezpečnosť. Poskytovateľ cloudových služieb má garantovať bezpečnosť na vysokej úrovni, keďže služby poskytuje širokému spektru zákazníkov.

V súčasnosti, keď zamestnanci mnohých firiem prešli na home office, by mal byť kvalitný cloud nevyhnutnosťou? Je to tak?

Nevyhnutnosťou nie, ale určite by firmám cloud pomohol. Každý, kto pracuje z domu, sa musí dostať k firemným aplikáciám. Väčšina firiem však nemá infraštruktúru postavenú tak, aby k aplikáciám umožňovala bezpečný prístup. Prechodom do cloudu získavajú dve služby v jednom. Pre bezpečný prístup k firemným aplikáciám nemusia kupovať nový hardvér, nemusia vymieňať firewall a rôzne bezpečnostné zariadenia, ale môžu využiť cloud, kde to všetko dostanú automaticky. V cloude sú teda garantované aj bezpečnosť aj lacnejšie hardvérové zdroje.

Ak by sme posúdili škody vzniknuté firme po hekerskom útoku sprevádzanom únikom dát v porovnaní s vynaložením financií na kvalitný cloud a jeho bezpečnostné garancie, čo by sme zistili?

Tu vyhráva jednoznačne ten, kto má dáta v cloude. Stačí si spočítať, o koľko peňazí firma príde, keď prestane vyrábať alebo jednoducho nefunguje.
Poznám príbeh, keď sa musela firma vysporiadať so situáciou po kyberútoku. Na masívny útok, ktorý zasiahol ich systémy aj zálohy neboli pripravení, a napriek tomu, že udržali chod výroby, prichádzali o státisíce EUR. Východiskom bolo zvoliť prostredie, v ktorom postavíte informačný systém rýchlo a bezpečne opäť na nohy. Zmigrovali do cloudu. Hardvérovú serverovú infraštruktúru síce stále majú aj u seba, ale používajú ju už len ako záložnú. Do cloudu presunuli všetky produkčné aplikácie. Pomohli sme im zmeniť aj architektúru niektorých aplikácií spolu s ich nastaveniami tak, aby už nebolo možné dáta zvonku zašifrovať. To, čo je zálohované v cloude, je úplne oddelené od infraštruktúry zákazníka a v prípade opätovného útoku naň pre útočníkov nedostupné. Cloud je presne na toto stavaný, v prípade ďalšieho útoku vieme dáta veľmi rýchlo obnoviť.
Predmetná firma má centrálu asi 200 kilometrov od svojich virtuálnych serverov v cloude, a nie je s tým žiaden problém. Dokonca to pre bezpečnosť vítajú.

Sú známe prípady, keď firmy stratili svoje dáta napriek tomu, že mali zálohy? Je cloud 100-percentne bezpečný?

Nič nemôžeme považovať za 100% bezpečné. Ale len z dôvodu, že jedným z medzičlánkov je človek, ľudský faktor je vždy najväčším rizikom.
Sekretárka napríklad otvorí mail, ktorý automaticky stiahne ransomvér a zakryptuje dáta v celej firme. Ak má zákazník servery v cloude bezpečne zálohované, obnova je rýchla, ale firma môže stáť pol dňa, kým preinštaluje PC/Notebooks. Určite je to však neporovnateľne rýchlejšie a menej finančne bolestivé ako hľadanie riešení na záchranu dát a funkčnosť firmy, čo má úložiská „v železe“.

Sú medzi existujúcimi cloudmi rozdiely? Zadefinujme typy cloudov a komu sú určené.

Pre menšie a stredné firmy je vhodnejší public cloud, pretože predstavuje nízky náklad a okamžite dostupný výpočtový výkon.
Privátny cloud je vhodný pre väčšie firmy na špeciálne aplikácie, ktoré musia z nejakých licenčných dôvodov byť na dedikovanom hardvéri.
Ako optimálne riešenie pre všetkých by som odporúčal hybridný cloud. Tu môže byť časť prevádzky v public cloude a časť v privátnej infraštruktúre, alebo môže mať firma jeden z cloudov ako pracovný a druhý záložný.
Všetko však záleží aj od povahy aplikácií, pretože každá firma používa niečo iné. Jedna môže mať aplikácie špecifické z hľadiska ich výrobného procesu, iná ich používa prevádzkované priamo v cloude. Všetko je to „case by case“ a veľmi individuálne. Predstavme si prevádzku obchodu s pobočkami po celom Slovensku. Je pre nich jednoduchšie a rozumnejšie napojiť sa na centrálne aplikácie - napríklad do pokladne či skladov - v cloude, ako keby ich mali u „seba“ na serveroch. Internetové pripojenie k aplikáciám by totiž bolo aj pomalšie, aj drahšie.

Nie je však prechod do cloudu zložitý? To je asi otázka, s ktorou sa stretávate najčastejšie.

Spolu s tou, koľko by to stálo (úsmev). Tu sa snažíme klientom vždy vysvetliť, že cena súvisí so škálovateľnosťou cloudového prostredia. Čo sa týka prechodu do cloudu, migrácia je jednoduchý proces, ak máte dostatočný čas na prípravu a kvalifikovaného partnera.

Ako prebieha migrácia do cloudu?

Dvoma pomerne jednoduchými, no odlišnými spôsobmi.
Prvý spôsob: Celý server firmy so všetkými dátami sa presunie do cloudu a tam sa spustí ako virtuálny. Čiže z fyzického sveta prejde spoločnosť do virtuálneho. Všetok „bordel“, staré softvéry, neupratané databázy, staré dáta, sa takisto prenesú do cloudu. V tomto prípade bude však aktualizácia dát a systémov vždy náročnejšia.
Druhý spôsob: Odzálohujú sa len produkčné, aplikačné dáta, ktoré firma naozaj potrebuje. V cloude sa nainštaluje nový, aktuálny virtuálny server, nainštalujú sa nové verzie operačných systémov, nové verzie aplikácií, a naimportujú sa len čisté a užitočné dáta. Výsledkom je konečné fungovanie na vynovenom softvéri.
U nás v GAMO je migrácia do cloudu grátis. Ja osobne odporúčam spôsob, keď sa nepresúva celý server, ale ide o inštaláciu dát načisto. Všetko sa neskôr oveľa jednoduchšie a rýchlejšie updatuje aj udržuje.

V čom je slovenský cloud výnimočný oproti veľkým hráčom ako Google, Amazon či Microsoft 365?

Všetko je o ľuďoch. Spomínané spoločnosti sú ako provideri omnoho väčší, majú viac služieb. No pre veľa malých firiem na Slovensku sú ich služby nedosiahnuteľné, a to aj z dôvodu, že sa nemajú na koho obrátiť v lokálnom jazyku. Musia prísť na portál, kde je všetko v angličtine, a zadanie si vyklikať. Môže sa stať, že zlým kliknutím firme zrazu príde faktúra o 4000 EUR vyššia. A pritom ide len o nepozornosť, omyl. Na Slovensku je pritom 90% malých firiem. Veľký provider je pre nich v istom zmysle nedostupná vec. IT-čkári môžu mať jazykovú bariéru alebo rozsiahlu ponuku cloudových služieb v ponuke globálnych providerov nevedia obsluhovať. Ak niečo spravia zle, môžu poškodiť svoju virtuálnu infraštruktúru v cloude, a to môže mať v konečnom dôsledku dopad na faktúru. A, samozrejme, ak by chceli konzultácie od Googlu alebo Amazonu, tak ich hodinová sadzba sa pohybuje na iných, vyšších úrovniach ako napríklad služba GAMO Cloud.

Aké výhody má priamo GAMO Cloud?

Veľká výhoda GAMO voči nadnárodným providerom je, že komunikujeme so zákazníkmi na priamo a v slovenčine. Kedykoľvek je možné zavolať s požiadavkou, my navrhneme riešenie, a následne môžu byť aplikácie prenesené k nám do cloudu. Naše služby sú o dostupnosti, väčšej rýchlosti a blízkosti k ľuďom, o plnej súčinnosti. Často sa nám stáva, že zákazník chce ísť do cloudu, ale nevie ako na to. Oslovia nás a začína spoločná debata. Zisťujeme, čo prevádzkujú, či sú aplikácie, ktoré potrebujú mať, lokálne alebo je to softvér, ktorý riadi nejaké výrobne linky a podobne. Následne sa zvažuje, čo je vhodné a dostupné preniesť do cloudu. Naše data centrum je

v Bratislave, a máme zákazníkov z celého Slovenska, ale aj z iných krajín Európskej únie.

Prečo potom cloudové služby nevyužíva viac firiem na Slovensku? S akými obavami sa ako cloud konzultant u klientov stretávate?

Paradoxne to nie sú len financie. Keď sa rozprávame s IT ľuďmi vo firmách, majú obavu, že ich chceme nahradiť. To je ale nevedomosť. My nenahrádzame ľudí, ani na to nemáme ľudské zdroje, snažíme sa s lokálnymi IT ľuďmi kooperovať a spolupracovať. Zabezpečujeme výpočtový výkon, dostupnosť aplikácií, aby mali väčšiu škálovateľnosť, kvalitu, aby systém vždy fungoval bez výpadkov a podobne. Aby už nemuseli investovať do nákupu nového hardvéru, ktorí majú pod stolom.

Pomáha v argumentácii výhoda v dlhodobom šetrení finančných prostriedkov?

Väčšina z finančných riaditeľov rozumie logike, keď sa investičné náklady zmenia na prevádzkové, čo prechod do cloudu prináša. Takisto je kľúčovým argumentom fakt, že pri cloude si v prípade potreby môžete väčší priestor alebo výkon okamžite kúpiť a aj využívať. A naopak. Zákazník teda naozaj platí len za to, čo reálne použije. Ak má nadbytok HW zdrojov, jednoducho ich zníži a bude platiť menej, ak potrebuje pridať, tak si zakúpi viac. To iste platí aj pri SW licenciách.

Budúcnosť cloudových služieb teda vidíte vo svetlých farbách?

Vo veľmi svetlých. Vkladať investície do hardvéru a kupovať ho sa v dnešnej dobe oplatí len veľkým firmám. Na Slovensku by v cloude fungovalo bez problémov 90% spoločností. Dôvodom, prečo tam ešte nie sú, môže byť vlastníctvo a užívanie hardvér v záruke či so životnosťou. Tá je 5, 6, niekedy 7 rokov. A keď má firma 3-ročný hardvér, zatiaľ nebude migrovať do cloudu. V budúcnosti však áno. No ak niekto začína budovať podnik teraz, jednoznačne odporúčam cloud, nie vlastné železo. V budúcnosti budú dokonca firmy využívať aj dva cloudy, dvoch providerov súčasne. Aby mali záruku, že keď sa jednému niečo stane, na ten druhý sa môžu spoľahnúť. Keď si vybavíme slovo cloud, nebude sa už spájať len s infraštruktúrou, ale bude zahŕňať služby umelej inteligencie či machine learning. Cloud tu teda bude stále, len sa bude neustále vyvíjať, pridávať nové funkcie a služby.

Jana Kohárová
jana.koharova@gamo.sk

Komu sú určené Kubernetes?

Kubernetes je ideálnou platformou pre hosťovanie aplikácií v cloude. Predstavuje zaujímavé riešenie ako ľahko nasadiť nové aplikácie respektíve upraviť už existujúce. Pomáha riešiť škálovateľnosť, životný cyklus a dostupnosť aplikácií, čím ich robí efektívne a dobre prispôsobiteľné.

Kormidelník kontajnerových lodí

Technológia Kubernetes bola vyvinutá v spoločnosti Google a v súčasnosti ju spravuje organizácia Cloud Native Computing Foundation. Je to open source systém na orchestráciu kontajnerov za účelom automatického nasadzovania a správy aplikácií v multiplatformovom a multicloudovom prostredí. Názov je anglickým prepisom starogréckeho slova κυβερνήτης (kubernétés), označujúceho kormidelníka lodí. Je to veľmi výstižné pomenovanie, pretože Kubernetes robia podobnú činnosť ako kormidelníci kontajnerových lodí.
Pre človeka, ktorý nie je odborníkom na IT, je to veľa nových pojmov v dvoch vetách. Pod výrazom kontajner v kontexte softvéru rozumieme nezávislý spustiteľný balík softvéru, obsahujúci všetko potrebné k fungovaniu na akejkoľvek platforme. Kontajnery izolujú softvér od svojho okolia, čím sa dosiahne, že aplikačný softvér bude v akomkoľvek prostredí, do ktorého bude aktuálne nasadený, bežať vždy rovnako.

Rýchlosť a škálovateľnosť

Aplikácie by sa v multiserverovom a multicloudovom prostredí dali presúvať zároveň s virtuálnymi strojmi (Virtual Machine). No na rozdiel od virtuálneho stroja, ktorý obsahuje aj operačný systém, kontajnery obsahujú len aplikácie a komponenty potrebné pre svoje fungovanie. Vďaka tomu sú kontajnery podstatne menšie. Presun 1000-krát menších súborov je pri vyrovnávaní záťaže medzi jednotlivými servermi - či už fyzickými alebo virtualizovanými, alebo vo vlastnej serverovni či v cloude - oveľa rýchlejší, a zároveň menej zaťažujúci sieťovú vrstvu.
Aby aplikácie mohli naplno využiť výkon klastra virtuálnych serverov, Kubernetes tento klaster orchestruje. V podstate ide o vyrovnávanie záťaže, monitorovanie priradenia prostriedkov a ich škálovanie. Kubernetes tiež umožňuje aplikáciám, aby sa v prípade problémov samy opravovali prostredníctvom automatického reštartovania alebo replikácie kontajnerov. Z toho vyplýva, že Kubernetes

Jana Kohárová
jana.koharova@gamo.sk

je ideálnou platformou pre hosťovanie aplikácií v cloude, hlavne tých, ktoré vyžadujú rýchle škálovanie, prípadne častejšie úpravy a aktualizácie.
Najväčšou výhodou technológie Kubernetes je, že automaticky rieši nasadzovanie kontajnerov, sleduje ich dostupnosť a aktuálne požiadavky na výkon, a snaží sa efektívne využiť dostupnú kapacitu serverov. Kubernetes nad nimi vytvára abstraktnú vrstvu, takže všetky prepojené servery sú dostupné ako jeden stroj.

Nezničiteľná infraštruktúra

Nakoľko kontajnerové aplikácie sú oddelené od infraštruktúry, pri spustení v prostredí Kubernetes sú jednoducho prenosné. Dajú sa presúvať z firemných serverov do hybridných a cloudových prostredí, aj medzi jednotlivými cloudmi, pri zachovaní ich konzistencie naprieč prostrediami.
Týmto sa infraštruktúra zákazníka stane takmer nezničiteľná. V prípade nefunkčnosti niektorého kontajnera pod správou Kubernetes sa okamžite automaticky spustí nový identický kontajner a aplikácie zostanú funkčné.
Kubernetes spoľahlivo a efektívne rieši aj problémy súvisiace s predvídateľným i nepredvídateľným nárastom požiadaviek na výkon, napríklad u e-shopov v období nákupných špičiek, alebo ak predávate vstupenky na veľké podujatie. Ak aplikácia a jej kontajnery nestíhajú, vytvorí sa klon kontajnera, čiže ďalší identický kontajner, a dočasne sa zvýši výkon. Keď sa po nejakom čase záťaž vráti do normálu, nadbytočné kontajnery sa zrušia a za výpočtový výkon, ktorý sa nevyužíva, už netreba platiť.

Automatizovaná prevádzka

Veľkou výhodou systému Kubernetes je jeho efektívna prevádzka v hybridnom prostredí, čiže u poskytovateľov verejných cloudových služieb, v privátnych cloudoch, aj v IT infraštruktúre vo vlastnej serverovni. Možno si veľmi jednoducho zvoliť, kde bude bežať aká pracovná záťaž, prípadne ju podľa potreby operatívne presúvať, a vybrať pre kontejnery s aplikáciami prostredie, ktoré bude z hľadiska nákladov najefektívnejšie.
Automatizovaná správa kontajnerov s aplikáciami odbremení aj vysoko kvalifikovaných IT špecialistov spoločností od rutinných činností súvisiacich s prevádzkou, a títo sa môžu naplno venovať produktívnym činnostiam, napríklad vývoju a optimalizácii aplikácií. Kubernetes zároveň umožňujú aj vysokú pružnosť týkajúcu sa uvádzania nových, prípadne vylepšených aplikácií, a v prípade potreby je možné sa jednoducho vrátiť k staršej, osvedčenej verzii. Takáto schopnosť operatívne reagovať na požiadavky zákazníkov je v ére súčasného dynamického biznisu veľkou konkurenčnou výhodou.

Článok v plnom znení a rozsahu čítajte na platformofinvention.sk

Mne sa to nemôže stať!?

Rekonštrukcia kyberútoku na slovenskú výrobnú spoločnosť so 70-ročnou úspešnou históriou

Je utorok, 13. apríla 2021, 6. hodina ráno. Zamestnancovi výrobného podniku sa začína klasický pracovný deň. Zapína počítač – a okamžite sa všetko mení. Na obrazovke svieti oznam od kyberútočníka: „Počítač je zakryptovaný, kontaktujte ma do 24 hodín.“ Zjednodušene povedané: systém napadol heker a za navrátenie dát chce výkupné.

Nielen vo svete, ale aj na Slovensku sú útoky na súkromné spoločnosti aj štátne inštitúcie na dennom poriadku. Niekde idú kybernetickí útočníci na istotu, inde to len skúšajú a čakajú, ktorá akcia sa vydarí. Škody úspešne napadnutých spoločností sú následne obrovské. Prichádzajú o státisíce eur najmenej v štyroch rovinách: v prerušení činnosti, v nutnosti technickej obnovy systémov, na zmluvných pokutách pre obchodných partnerov, a nezriedka aj pri zaplatení výkupného. Neželaným dôsledkom navyše býva strata dôvery zákazníkov a reputácie.

V nasledujúcom článku prinášame rekonštrukciu útoku na slovenskú výrobnú spoločnosť, ktorý sa vďaka rýchlemu hľadaniu odborných riešení manažmentu, vysokému nasadeniu lojálnych zamestnancov, a v neposlednom rade včasnej a otvorenej komunikácii ku klientom, blíži k úspešnému finále.

Prvé kroky spoločnosti po útoku

Vráťme sa k osudnému 13. aprílu 2021.

> *„Šlo o najčernejší deň v 70-ročnej histórii našej spoločnosti,“ zhodujú sa dnes manažéri podniku.*

Zamestnanec, ktorý odkaz od útočníka našiel, kontaktoval IT manažéra firmy. Jeho prvá telefonická reakcia bola: „O ktorý server ide?“ Už predtým mali skúsenosť s individuálnym zašifrovaním, a vždy ho hravo zvládli. Odpoveď zamestnanca však znela: „Obávam sa, že o všetky.“

Pôvodne klasický pracovný deň sa tak vo výrobnom podniku zmenil na súbeh dramatických udalostí, vyžadujúci nasadenie všetkých vnútropodnikových zložiek vrátane top manažmentu.

V prvom rade bolo potrebné vypnúť všetkých 38 serverov, vrátane počítačov a tlačiarní, z dátovej siete. Tie, čo sa napadnutým vírusom opätovne nanovo naštartovali alebo zasekli, bolo nutné „natvrdo“ vytiahnuť zo skriniek elektrického napätia. „Vtedy sme všetci pochopili, že náprava bude trvať dlhšie ako odstávka pri údržbe,“ spomína IT manažér.

Bežne sa totiž ich server obnovoval zo záloh v priebehu jedného až dvoch dní, po napadnutí sa však aj po skúšobnom zapnutí servera údaje šifrovali ďalej. Čo s tým?

Okamžitou reakciou manažmentu bol, pochopiteľne, hnev proti útočníkovi. „Prečo práve naša firma? Pre koho môžeme byť ako terč zaujímaví,“ spomína na čierny deň člen vedenia spoločnosti. IKT infraštruktúra, systémy, zariadenia, tok informácií do výroby, mailová komunikácia, všetko, čo mali priamo naviazané na IT, zrazu nefungovalo. „Predstavte si, že máte vypnutú sieť, ktorá je kontaminovaná, máte kontaminované servery, a zisťujete, nakoľko zasiahnuté boli aj vaše zálohy.“

Každý jeden človek vo firme mal pocit, že sa ocitol v bode nula. Isté bolo len jedno: spravodlivo rozčúlení členovia manažmentu sa zhodli a dohodli, že v žiadnom prípade nebudú nikomu nič platiť.

„Zároveň sme si uvedomili, že hnev nepomôže, že treba konštruktívne uvažovať, nastaviť stratégiu a situáciu postupnými krokmi riešiť. Všetkým nám bolo jasné, že najdôležitejšie je udržať výrobu, ktorá je z hľadiska produkcie, príjmov aj záväzkov spoločnosti kľúčová. A to aj za cenu, že sme sa pri riadení činností museli vrátiť k papieru a ceruzke,“ spomína na prvé hodiny čierneho dňa člen vedenia výrobného podniku. „Bolo to nesmierne ťažké.“

Prvé odporúčania špecialistov

Technici najskôr uvažovali o možnosti pripojenia cez Windows zariadenia na NAS-ko v serverovni. Ide o úložné zariadenie umožňujúce firmám bezprácne skladovať a chrániť veľké objemy dát. Aj tu však hrozila možnosť, že dôjde ku prenosu škodlivých kódov či ku spusteniu šifrovania. Spoločnosť sa preto obrátila na poskytovateľa konzultačných služieb, IT firmu GAMO.

Prvé odporúčanie konzultanta znelo: skontrolovať zálohy cez linuxové zariadenie. „Šli sme postupne, hromady súborov, ktoré sme prechádzali, boli vždy úplne alebo čiastočne zašifrované. A vieme, že ak je niečo na virtuálnom serveri čiastočne šifrované, už tam môže byť vložený neviditeľný škodlivý kód. V takomto prípade by sme z tohto servera nemali nič používať,“ komentuje vtedajšiu situáciu vedúci IT napadnutej spoločnosti.

Obrátili sa teda na lídra na trhu v oblasti bezpečnostných riešení. Ten síce ransomvérové útoky na viaceré slovenské spoločnosti registroval, ale konkrétne

> *„Plán, že všetko obnovíme zo záloh, nefungoval. A čas nám bežal.“*

riešenie daného stavu nemal. „Čiže plán, že všetko obnovíme zo záloh, nefungoval. A čas nám bežal.“

Jednou z nádejí v záchrane časti dát boli kazetové pásky. „Zálohovali sme ich na tieto nosiče približne pred polrokom. Dúfajúc, že by na nich mohli byť využiteľné informácie, sme pásky za posledných päť rokov poslali nášmu konzultantovi,“ pokračuje IT manažér.

Tie prešli v GAMO pomocou robotizovaného zariadenia prácnou kategorizáciou. Proces postupného pretočenia pások a nájdenia súvislostí v záznamoch trval viac ako tri týždne.

Spoločnosť paralelne hľadala aj iné spôsoby riešenia.

Rýchly prechod do cloudu

Keďže bola celá infraštruktúra napadnutého podniku zašifrovaná, hľadalo sa prostredie, ktoré postaví informačný systém rýchlo a bezpečne späť na nohy. Ideálnym riešením bol cloud. Manažment podniku už na druhý deň konzultácií so špecialistami zvolil túto novú cestu fungovania a vyžiadal si službu pre všetky servery.

Technickí pracovníci krok za krokom prechádzali čo ešte možno zachrániť. Našla sa napríklad databáza výrobného systému z predošlého dňa. Skúškou zistili, že nie je kontaminovaná, ale iba poškodená silným vypnutím servera. Opravili sa poškodené transakcie, nainštalovala sa MS SQL prázdna databáza a pri importe bola dodaná databáza bez prípony, bez zašifrovania. „Ak by nebola databáza v poriadku a nesedeli kontroly všetkých jednotiek vnútri, databázový systém by ju neprijal. Keď sa však očistili transakcie a databáza bola korektne importovaná, prešla testovaním a následne bola poslaná do cloudu,“ približuje IT manažér podniku.

„Zachránené databázy a dáta najdôležitejších systémov firmy sme vložili do dvoch diskov,“ približuje krízový moment jeden z vrcholových manažérov podniku. Zo stredného Slovenska ich bolo nutné urýchlene doručiť do Bratislavy, aby ich technici GAMO oživili do cloudového prostredia. „Bol to zvláštny pocit, že na dvoch diskoch máte zrazu celé bohatstvo firmy, ktorú budujete 70 rokov. Nie je to hala, ktorá sa dá postaviť, nie sú to stoje, ktoré môžete kúpiť. Sú to dva disky, s ktorými neviete, čo máte robiť. Tie dáta tam niekde boli, no bolo potrebné ich vydolovať,“ spomína s tým, že ich mal „celú noc, namiesto manželky, ktorá bola mimo domu, uložené pri sebe v posteli“.

Do Bratislavy vyrazil veľmi skoro ráno. „Hlavou mi vírili rôzne myšlienky a pracovné povinnosti – no všetky prebíjalo vedomie, že veziem vo svojom aute doslova možno jedinú záchranu pre firmu. A predstavte si, že nesiete niečo, čo má pre vás nevyčísliteľnú hodnotu, a potom si tieto vaše aktíva preberie na dohodnutom mieste človek, ktorého ste nikdy predtým nevideli. Ktorý si ich ako nič uloží do svojho ruksaku – a odíde... Stojíte tam a rozmýšľate, či ste práve urobili správne rozhodnutie,“ usmieva sa top manažér dnes.

Sanovanie výroby a pomoc dodávateľov

Vedenie sanovalo výrobu a hľadalo spôsoby ako a kde je možné získať dáta a databázy pre tri najdôležitejšie systémy – Výrobný systém, Výkresy a Technickú prípravu výroby.

Paralelne popri tých prioritách v spolupráci s dodávateľmi získavali nové aj zapožičané zariadenia pre spracúvanie údajov zo zachránených a nepoškodených databáz. Šťastím v nešťastí bol dodávateľ, ktorý mal päť rokov starú databázu z nadstavby systému, čo umožnilo nahliadnutie do starých položiek. Po odsúhlasení technikov sa jednotlivé technologické postupy a kusovníky tlačili na papier a posúvali do výroby.

Prebehla inštalácia ďalších troch počítačov a offline tlačiarne, aby pracovníci mohli kopírovať výkresy a konštruktéri mohli pripraviť výrobu v papierovej forme na ďalší týždeň.

Podarilo sa zachrániť aj ďalšie výkresy zo zálohovaných pások, ktoré sa importovali do SharePointu a potom kopírovali do Wordu.

Tento proces bol však zdĺhavý a sprevádzaný každodenným tlakom.

Bezpečnostných opatrení v cloude GAMO je hneď niekoľko. Prvým je samotné dátové centrum, z ktorého cloudové služby fungujú. Vďaka svojej konštrukcii a fyzickému i objektovému zabezpečeniu pôsobí navonok ako nedobytná pevnosť. Poskytovateľ garantuje bezpečie a ochranu všetkých dát. GAMO Cloud je vybudovaný na technológii SDDC od VMware s maximálnym dôrazom na bezpečnosť. Jeho zabezpečenie spĺňa štandardy TIA 942 pre úroveň Tier III. Ako prvý slovenský cloudový poskytovateľ získalo GAMO prestížny certifikát CSA Star udeľovaný za najkomplexnejšiu bezpečnostnú previerku. Tu už nie je potrebné riešiť prevádzku, údržbu, ani režim nepretržitej dostupnosti serverov.

Nastavenie správnej komunikácie

Výrobná spoločnosť rýchlo pochopila dôležitosť každého jedného rozhodnutia a zostavila krízový tím odborníkov. Tvorili ho manažment napadnutej spoločnosti a odborníci z GAMO, každý mal presne určené kompetencie i úlohy.

Keďže Exchange server bol vypnutý, obchodníci a nákupcovia začali so zákazníkmi komunikovať prostredníctvom súkromných mailov a telefonických kontaktov. Okrem nich žiadna iná elektronická komunikácia neexistovala.

„Smerom ku GAMO sme už mali pripravenú požiadavku na prechod z Exchange servera do cloudu na Office 365. Po týchto udalostiach bolo nutné, aby nám spoločnosť GAMO urýchlila realizáciu – inštaláciu prvej sady e-mailov v M365," približuje vtedajší posun IT manažér. Do týždňa dostali prvú sadu mailov a začali postupne komunikovať prostredníctvom nich. „To bol signál aj pre našich zákazníkov, že začíname žiť. Postupne sme rozbiehali aj ďalšie servery v cloude."

Neprišli tak ani o jedného zákazníka či dodávateľa. „A to predovšetkým správne nastavenou otvorenou komunikáciou dovnútra aj von. Nebyť ochoty zo strany dodávateľov, ústretovosti zo strany zákazníkov a rýchlemu spojeniu sa so špecialistami, mohlo to dopadnúť úplne inak," dodáva člen vedenia výrobného podniku.

Zamestnanec = základ dobrej spoločnosti

Čo sa týka zamestnancov, ani tam nedošlo k podceneniu komunikácie v krízovej situácii. Spoločnosť ich v tom čase mala približne 350 a pracovali v nej celé rodiny. Problém reálne nevznikol, ale mohol. Výpadok dochádzkového aj mzdového systému či internetbankingu, na ktorý sa každý manažér spolieha pri spracúvaní a vyplácaní miezd, môže poriadne skomplikovať život.

Nevyplatenie peňazí mohlo navyše reálne ohroziť existenciu rodín v regióne. „Tu sa preukázala lojalita a súdržnosť našich zamestnancov. Boli ochotní pracovať nadčasy, za čo som nesmierne vďačný. Naša spoločnosť vždy dbala na prorodinný prístup a to nám v tejto zložitej situácii veľmi pomohlo," vyzdvihuje svoj tím ľudí člen vedenia spoločnosti.

Oceňuje aj prácu mzdovej pracovníčky, ktorá vo firme pracuje 20 rokov. Tá napriek tomu, že mala podklady ku mzdám v informačnom systéme, vo zvyku „starej školy" všetko pre kontrolu aj tlačila.

„Ďalším šťastím bolo, že naša spoločnosť nemá vysokú fluktuáciu. Kolegyňa z tímu si pamätala, ako sa mzdy vyplácali pred informačnými systémami – pomocou mincovky," objasňuje ďalší krok riešenia člen vedenia spoločnosti. No spraviť mincovku pre viac ako tristo ľudí, rozpočítať, koľko bankoviek a mincí na výplaty treba, a následne nahlásiť banke výber v hotovosti, vôbec nebolo jednoduché. „Potom bolo nutné aj celú sumu rozdeliť, ‚nasáčkovať' presne to, čo konkrétnemu zamestnancovi patrí, a nezanedbateľný problém bol aj s bezpečnosťou. Naše zamestnankyne na tom robili vo dne v noci a nešlo o malé sumy. Aj toto sú veci, na ktoré musí človek myslieť, keď zhasne celý systém."

Samozrejmosťou boli denné a pravidelné stretnutia riaditeľa podniku s vedúcimi výroby pre informovanosť všetkých svojich ľudí.

Komunikácia s útočníkom

Na začiatku spoločnosť rázne odmietla zaplatiť výkupné. Uvedomovali si však dôležitosť niektorých serverov, preto sa s kyberútočníkom pokúsili vyjednávať.

„Niektoré dáta sa nám podarilo zachrániť, skúsili sme vyjednávať len o zaplatení tých, ktoré nám nefungujú. Tiež sme žiadali, aby nám útočník na ukážku poslal dôkaz, že ich vie aj dešifrovať. Odpovede od neho boli veľmi strohé. Náš systém mal dokonale zmapovaný a ak sme ho požiadali, aby nám na ukážku dešifroval nejaký server, dodal najmenej dôležitý, testovací, ktorý sa po chvíli zašifroval späť," spomína IT manažér.

V závere útočníkovi nezaplatili nič. „Našli sme človeka, ktorému sa podarilo obísť šifrovanie záloh aj u ostatných serverov, ktoré sme potrebovali."

Vyhli sa tak aj problému so zákonom. Kyberútočníci spravidla požadujú výkupné vo forme kryptomeny, s čím je spojený problém zapísania transakcie do účtovníctva legálnou cestou. Vtedy vzniká riziko pokuty z daňového úradu, keďže nie je možné preukázať, na čo boli peniaze použité. Žiadny útočník totiž na tieto služby faktúru nevystaví.

„Kyberútočník je obyčajný kriminálnik a dáta sú mu ukradnuté. To, o čo mu ide, sú peniaze napadnutej spoločnosti.

> *„Kyberútočník je obyčajný kriminálnik a dáta sú mu ukradnuté. Spoliehať sa na to, že dáta vráti späť, je naivné."*

Spoliehať sa na to, že firma získa dáta späť, je naivné," hovorí k tomu špecialista na kybernetickú bezpečnosť Ľubomír Kopáček.

Prioritou útočníka zvyčajne je, aby dáta zašifroval, a nikoho nezaujíma, či ich dokáže aj dešifrovať. Dešifrovanie časti dát „na ukážku" je absolútne nedôveryhodné a nevypovedá o ničom. „Ďalším argumentom prečo neplatiť je fakt, že ak zaplatíte a neurobíte zároveň perfektné ‚vyčistenie' napadnutých systémov, môžete s istotou počítať, že rovnaký incident sa čoskoro zopakuje," uzatvára špecialista.

„Súhlasíme, že treba dbať na dôkladnú kontrolu a vyčistenie systémov. Prísne sme dodržiavali postup obnovy ‚prelomených' záloh serverov, s veľkou opatrnosťou sme vykopírované databázy

systémov najskôr skontrolovali, a až potom ich opäť použili," dopĺňa tému IT manažér výrobného podniku.

Aj keď nezaplatíš, stojí útok tisíce

Hoci predmetná napadnutá spoločnosť kriminálnikovi nezaplatila nič, náklady kybernetického útoku odhaduje na približne pol milióna EUR. Iba technické náklady so službami ju stáli 142-tisíc EUR. Zvyšok tvorili predovšetkým mzdy a práca ľudí, ktorí museli pracovať nadčasy. Taktiež museli prijať okolo 30 nových pracovníkov, aby dobehli časové sklzy pri výrobe.

V sume navyše nie je započítaný stres, logistika a len zdanlivo čiastkové „maličkosti". V kovidovom období napríklad nebolo jednoduché zohnať technológie. Na jar 2021 prebiehalo niekoľko útokov súčasne a systém, že v jeden deň odíde objednávka a na ďalší deň kuriér prinesie techniku, neplatil. „V prvom momente sme sa snažili kúpiť NASko. Keď bolo konečne na sklade, poslali sme do Bratislavy - bez cenových ponúk, iba na základe telefonátov - auto, aby sme získali jedno z posledných. Bolo to v piatok, a v sobotu už ďalšie zariadenia neboli k dispozícii," opisuje stresujúce obdobie člen vedenia.

Po 4 mesiacoch spia už lepšie, no nie sú v cieli

Hoci sa firme podarilo veľa vecí úspešne rozbehnúť, nie je ešte nainštalované a fungujúce všetko, nie je nasadená ani kompletná infraštruktúra. Podarilo sa však zachrániť tri pilotné informačné systémy pre výrobu.

Všetky ďalšie stupne, ktoré si firma zaumienila technicky zlepšiť, sú v procese realizácie. „Bude to trvať ešte dlho. Potrebné je nahradiť pôvodné firewally novými a bezpečnejšími, zvýšiť povedomie pre užívateľov o odolnosti a správnom používaní zariadení, a podobne. Je to nekonečný príbeh. Technológie sa zlepšujú a útočníci sú stále pred nami," uzatvára IT manažér.

Nahlásiť alebo nenahlásiť útok polícii?

Napadnutá spoločnosť sa s GAMO radila aj o tom, či útok nahlásiť. Tu je odpoveď jasná. Je viac ako nerozumné počúvať útočníka, ktorý vydiera aj tým, že subjekt nesmie kontaktovať políciu či tretiu stranu.

Kyberexpert GAMO Ľubomír Kopáček prízvukuje: „Určite je rozumné incident nahlásiť. Ak je obeť útoku regulovaná zákonom o kybernetickej bezpečnosti a incident je vyhodnotený ako závažný, je to dokonca jej zákonná povinnosť."

Taktiež odporúča podať trestné oznámenie. „Nie, že by polícia dokázala niečo bližšie zistiť a nebodaj vyšetriť, ale je užitočné mať o celej záležitosti úradný záznam." Je to dôležité pre prípadné ďalšie problémy napríklad s daňovým úradom, sociálnou poisťovňou, zdravotnou poisťovňou či inými.

V Európskej únii platia rôzne vyhlášky a zákony hovoriace o postupe v prípade bezpečnostného incidentu. Pri zanedbaní povinností v súvislosti s bezpečnostným incidentom (nenahlásenie alebo neriešenie) môže napríklad úsek správnych deliktov podľa zákona o kybernetickej bezpečnosti uložiť pokutu od 300 EUR do 300-tisíc.

> *„Mlčať pri incidente je nielen nerozumné, ale vo väčšine civilizovaných krajín aj protizákonné a môže to spoločnosť stáť ďalšie peniaze."*

Cloud = správne riešenie a budúcnosť

Napadnutá firma sa v odmietnutí požiadaviek útočníka aj vo všetkých bodoch krízového manažmentu zachovala správne. Nielenže sa už v rannom štádiu riešení obrátila na špecialistov a počúvala ich rady, ale tiež si zachovala dobré meno v komunikácii s dodávateľmi aj zamestnancami.

Jej príbeh je však ukážkovým príkladom, že aj keď pravidelne zálohujete svoje dáta na serveroch, nemáte istotu, že sú naozaj v bezpečí. Aby bola aj vaša spoločnosť chránená, potrebujete odborné riešenia, šité na špecifické potreby každého jedného subjektu. Prechodom do bezpečného cloudu máte istotu, že bude o ňu postarané na najvyššej úrovni. Manažmentu firmy tak odpadá jedna z najdôležitejších úloh moderného podnikania a môže sa 100-percentne sústrediť na svoj core bussines.

Zuzana Omelková
zuzana.omelkova@gamo.sk

Právna zodpovednosť pri cloude je zdieľaná. O čo ide?

JUDr. Tomáš Klinka, právnik
Bukovinsky & Chlipala, s.r.o.

Kto zodpovedá za nelegálny obsah, čo sa v cloude objaví? Aká je zodpovednosť providera v prípade úniku citlivých údajov? Kedy môže zákazník žiadať náhradu ušlého zisku? Kde sa končí zodpovednosť poskytovateľa cloudu a za čo nesie zodpovednosť používateľ = zákazník? To sú otázky, s ktorými sa stretáva každý poskytovateľ cloudových služieb.

Všeobecná odpoveď znie: Súlad s dodržiavaním príslušných obchodných noriem a platných zákonov je v zásade povinnosťou oboch strán.
Hovoríme o takzvanom modeli zdieľanej zodpovednosti. Obojstranný zmluvný vzťah znižuje záťaž zákazníka, keďže Cloud Service Provider (CSP) prevádzkuje, spravuje a kontroluje komponenty hostiteľského operačného systému a virtualizačnej vrstvy až po fyzické zabezpečenie zariadení, na ktorých služba cloudu funguje. Zákazník naopak preberá zodpovednosť a správu hostovaného operačného systému, vrátane aktualizácií a bezpečnostných záplat, a ďalšieho súvisiaceho aplikačného softvéru.
Takéto rozdelenie sa označuje ako Security OF the Cloud a Security IN the Cloud.

Security OF the Cloud

CSP je zodpovedný za ochranu infraštruktúry, na ktorej bežia všetky poskytované služby. Infraštruktúra je zložená z hardvéru, softvéru, sietí a zariadení, na ktorých sú cloudové služby prevádzkované.

Security IN the Cloud

Zákazník je zodpovedný za správu, obsah a legálnosť svojich údajov, platforiem, aplikácií, klasifikáciu svojich aktív a adekvátne používanie nástrojov na uplatňovanie príslušných oprávnení a prístupov.

Presné vedenie hranice medzi zodpovednosťou zákazníka a CSP závisí najmä od konkrétne zvoleného obchodného modelu (IaaS, PaaS alebo SaaS).

Kto zodpovedá za nelegálny obsah, nahratý v cloude?

V zmysle tzv. modelu zdieľanej zodpovednosti zodpovedá za legálnosť obsahu výlučne zákazník. CSP nemá reálnu technickú možnosť kontrolovať a ovplyvniť obsah, nahratý v cloude, keďže za štandardných okolností nemá prístup k nahratému obsahu. Za nelegálny obsah pritom považujeme akékoľvek súbory, aplikácie, dokumenty, audio a video, softvér či iné digitálne položky, ktorých držba či vytváranie kópií sú v rozpore s právnym poriadkom riadiacim zmluvný vzťah medzi CSP a zákazníkom.
Výslovné vylúčenie zodpovednosti CSP v obdobných prípadoch obsahujú zmluvné podmienky pravdepodobne všetkých relevantných CSP.
Jedinou výnimkou v tomto ohľade je situácia, keď sa CSP dozvie o nelegálnosti obsahu ukladaného v cloude alebo mu odstránenie obsahu nariadi súd. V takých prípadoch sa dokonca musí zákazník zodpovedať smerom k CSP, najmä ak by došlo k ohrozeniu reputácie či dobrej povesti CSP.

Aká je zodpovednosť CSP v prípade, že nastane bezpečnostný incident týkajúci sa aj úniku citlivých osobných údajov?

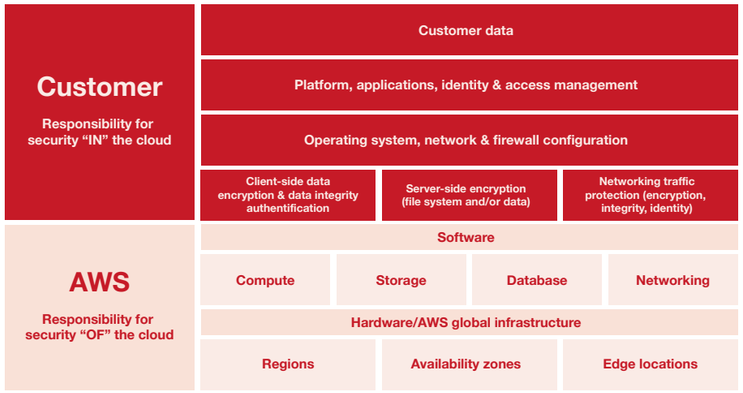
Z hľadiska GDPR je zákazník v postavení prevádzkovateľa a poskytovateľ cloudu v postavení sprostredkovateľa. Voči dotknutým osobám, ktorých osobné údaje v dôsledku bezpečnostného incidentu unikli, zodpovedá primárne zákazník. CSP by zodpovedal, pravdepodobne popri zákazníkovi, len ak by si nesplnil povinnosti, ktoré GDPR ukladá výslovne sprostredkovateľom, alebo ak by konal nad rámec či v rozpore s legálnymi pokynmi zákazníka. V praxi to znamená, že ak si CSP riadne plní všetky svoje povinnosti, na ktoré sa zaviazal v zmluve so zákazníkom, jeho zodpovednosť bude v dôsledku bezpečnostného incidentu nepravdepodobná. V tomto prípade predpokladáme konanie CSP s odbornou starostlivosťou. V režime GDPR je to najmä prijatie primeraných bezpečnostných opatrení podľa čl. 32 GDPR.

Akým spôsobom je riešená výška náhrady škody pri využívaní cloudu?

Zmluvné podmienky pravdepodobne všetkých relevantných CSP obsahujú tiež klauzulu o tzv. limitácii náhrady škody. Takáto limitácia (horná hranica) spravidla predstavuje súhrn zmluvných poplatkov, ktoré poškodený zákazník zaplatil CSP za posledných 6 alebo 12 mesiacov používania cloudových služieb. Aj podľa slovenského práva (Obchodného zákonníka) je možné zmluvne limitovať výšku predvídateľnej náhrady škody. Je však potrebné zdôrazniť, že táto klauzula sa uplatňuje len tam, kde CSP skutočne zodpovedá za škodu, nakoľko samotná skutočnosť, že zákazník využíval alebo nevyužíval cloud, nezakladá žiadny nárok zákazníka na náhradu škody proti CSP.

A čo ušlý zisk? Môže zákazník od CSP žiadať náhradu ušlého zisku v dôsledku napríklad nemožnosti využívať cloudové služby v prípade výpadku služby?

Vo všeobecnosti platí, že ušlý zisk – ako druhá zo zákonom predpokladaných foriem škody popri tzv. skutočnej – je ujmou vtedy, keď u poškodeného nedošlo v dôsledku škodnej udalosti k rozmnoženiu majetkových hodnôt, hoci sa to s ohľadom na pravidelný beh vecí dalo očakávať. Ušlý zisk sa teda neprejavuje zmenšením majetku poškodeného (úbytkom aktív, ako je to u skutočnej škody), ale stratou očakávaného prínosu (výnosu). Nepostačí pritom len pravdepodobnosť rozmnoženia majetku, ale musí byť naisto postavené, že pri pravidelnom behu vecí (nebyť protiprávneho konania škodcu alebo škodnej udalosti) mohol poškodený dôvodne očakávať zväčšenie svojho majetku, ku ktorému nedošlo práve v dôsledku konania škodcu (škodnej udalosti).
Ak by aj tieto podmienky boli, v prípade načrtnutom v otázke, splnené, stále musí byť naplnená aj základná podmienka, že CSP zodpovedá za škodu (ako sme zdôraznili už v odpovedi na predchádzajúcu otázku). Navyše, obvykle je výška náhrady škody pri poskytovaní cloudových služieb zmluvne limitovaná a ušlý zisk zákazníka zrejme nebude spadať pod tzv. predvídateľný rozsah potenciálnej škody.



zdroj: https://aws.amazon.com/compliance/shared-responsibility-model/

Môže sa CSP zodpovednosti za škodu nejako zbaviť?

V slovenskom obchodnom práve je zodpovednosť za škodu konštruovaná ako objektívna, teda sa nevyžaduje jej zavinenie (úmyselné či nedbanlivostné), ako je tomu pri všeobecnej zodpovednosti za škodu podľa Občianskeho zákonníka. Z toho vyplýva, že CSP bude štandardne zodpovedať aj za škodu, ktorú v tomto zmysle nezavinil, ak vznikla v dôsledku porušenia jeho povinností (zmluvných alebo zákonných).
Spravidla jediným spôsobom, ako by sa CSP mohol zbaviť tejto objektívnej zodpovednosti, je tzv. liberácia založená na okolnostiach vylučujúcich zodpovednosť. Za takú okolnosť sa považuje vyššia moc (vis maior), teda prekážka, ktorá nastala nezávisle od vôle CSP a bráni mu v splnení jeho povinnosti - ak nemožno rozumne predpokladať, že by CSP uvedenú prekážku alebo jej následky odvrátil či prekonal, alebo že by v čase vzniku záväzku (uzatvorenia zmluvy) túto prekážku predvídal.

Je CSP poistený v prípade, ak by zákazníkovi vznikla škoda?

CSP býva štandardne poistený pre prípady, keď by za spôsobenú škodu niesol zodpovednosť. Poškodený si potom z poistného plnenia môže nahradiť škodu, ktorá mu poistnou udalosťou vznikla.

Prečo uprednostniť CSP, ktorý podlieha legislatíve Slovenskej republiky?

Pre slovenského zákazníka je vždy výhodnejšie a jednoduchšie, ak je založená právomoc a príslušnosť slovenského súdu, a nie súdu v zahraničí. Tiež je pre slovenského zákazníka výhodnejšie, ak sa zmluva spravuje slovenským právnym poriadkom, nie cudzím (napr. zákonmi štátu Kalifornia a pod.). Z hľadiska záujmu slovenského zákazníka teda ide o najmä o praktickú otázku vymožiteľnosti jeho práv, čo môže byť komplikovanejšie vo vzťahu k CSP, ktorý nie je usadený, tzn. nemá sídlo na Slovensku.

Článok v plnom znení a rozsahu
čítajte na platformofinvention.sk

Zuzana Omelková
zuzana.omelkova@gamo.sk

Je potrebné obávať sa migrácie do cloudu?

Martin Pisák
martin.pisak@gamo.sk

Pýtame sa firiem čo tým prešli a neľutujú

Roman Klamo
Projektový manažér
Global Assistance Slovakia, s.r.o.

Global Assistance Slovakia poskytuje technickú asistenciu vodičom motorových vozidiel pri nehodách alebo poruchách, asistenčné služby fyzickým osobám na cestách v zahraničí, služby spojené s riešením problémov pri užívaní nehnuteľností, ako aj doplnkové zdravotné asistenčné služby ako lekár na telefóne, druhý lekársky názor, personalizovaná onkológia a podobne. Pre svoju činnosť využíva profesionálnu sieť zmluvných partnerov zo Slovenska a ďalších krajín sveta.
„Naším impulzom pre migráciu do cloudového prostredia bola inovácia v podobe zavedenia špecializovanej aplikácie riadiacej asistenčné služby zmluvných partnerov zo siete poisťovní, lízingových spoločností a bánk. Spočiatku sme hľadali dodávateľa hardvérovej infraštruktúry, ale v prospech využitia cloudových služieb hovorilo nielen porovnanie celkových výdavkov oboch riešení, a aj garancia dostupnosti a spoľahlivosti cloudu v nepretržitom režime 24/7.
Migrácia pre nás nepredstavovala až takú veľkú výzvu, keďže poskytovateľ cloudu nám umožnil projekt i jeho funkčnosť otestovať a optimalizovať pred uvedením do ostrej prevádzky. Dnes využívame plne funkčný IT systém a okrem prostredia pre samotnú aplikáciu máme v cloude vytvorené aj testovacie prostredie. Vďaka nemu môžeme zaškoľovať nových operátorov call centra a spolupracujúcich partnerov bez obmedzenia prevádzky.“

Miroslav Staník
IT manažér
Detox s.r.o.

Ak sú kľúčové parametre poskytovateľov cloudu z pohľadu výkonu, architektúry, licencovania a prístupových mechanizmov pre vás vyhovujúce a viac-menej porovnateľné, rozhodujúcim kritériom sa stáva cena. Nové cloudové prostredie, v ktorom prevádzkujete systémy rentabilnejšie ako u konkurenčného poskytovateľa, je nepochybne lákavé. Pokiaľ sa pri migrácii môžete spoľahnúť na kvalifikovanú asistenciu špecialistov, ktorí vás prevedú migračnou stratégiou, určite sa oplatí preniesť aplikácie a systémy z jedného cloudového prostredia do iného. Migrácia vo vlastnej réžii môže byť plná nástrah, a preto rozhodne netreba šetriť na nákladoch a je dobré spoľahnúť sa na pomoc odborníkov.
V našom prípade sme realizovali prechod od jedného providera k druhému a celý proces migrácie riadili špecialisti tretieho poskytovateľa cloudových služieb. Všetky kroky migrácie tak boli vykonané správne, bez komplikácií, a s vopred pripraveným scenárom na hladký priebeh.
Naša spoločnosť DETOX je poskytovateľom služieb odpadového hospodárstva a virtuálnu cloudovú infraštruktúru využívame viac ako 8 rokov. Oceňujeme v nej rýchlosť reakcie na zmeny, možnosť dynamického rozširovania IT infraštruktúry a využívanie zdrojov vtedy, keď ich potrebujeme. Dnes naplno venujeme čas rozvoju systémov a podpore core business-u.

Ľuboš Ziman
Obchodný riaditeľ
Flos Slovakia, s.r.o.

Migrácia serverov do cloudu nás odbremenila od nutnosti denného sledovania stavu serverov a ich prevádzkových parametrov. Core business spoločnosti Flos Slovakia, s.r.o., je dovoz a distribúcia kvetov. Je pre nás dôležité vnímať očakávania klientov, zabezpečiť im široký výber, okamžitú dostupnosť a rýchlu komunikáciu na diaľku v podobe: objednať, zaplatiť, poslať. Všetko musí dokonale fungovať, keďže naše prevádzkové procesy sú závislé od vysokej miery automatizácie a bezvýpadkovosti.
Rozhodli sme sa preto podstúpiť dôkladnú analýzu stavu siete a systémov. Tá nám pomohla získať ucelený pohľad na bezpečnosť, dosiahnutie kontinuity v prípade výpadku niektorej časti, aj na používanie verzií operačných systémov. Súčasťou analýzy bolo aj spočítanie výdavkov na obdobie priemernej životnosti fyzickej infraštruktúry. Jasnou odpoveďou pre budúcu komplexnosť našich služieb i technickú podporu bol vstup do cloudu.
A či sme mali obavy z migrácie? Nie. Podstatné bolo a je vyhradiť si čas na dôkladné naplánovanie procesu prechodu na cloudovú platformu. Na obnovu infraštruktúry aj redizajn celého aplikačného prostredia, ovplyvňujúceho a meniaceho spôsob komunikácie IT administrátora so systémami, aplikáciami a ich koncovými používateľmi. Analýzu potrieb odporúčame vykonať každému záujemcovi o cloud.

Inovačné služby SARIO

Slovenská agentúra pre rozvoj investícií a obchodu už viac ako 4 roky rozvíja pod názvom inovačné služby SARIO svoju vlastnú in-house platformu, ktorá slúži na prepájanie slovenských technologických a inovatívnych spoločností s veľkými firmami doma i v zahraničí.

Cieľom inovačných služieb je systematická podpora investorov s dôrazom na technologické inovácie a podporu zavádzania procesov súvisiacich s tzv. priemyslom 4.0, a zároveň snaha o stále väčšie zapájanie lokálnych technologických spoločností do dodávateľských reťazcov domácich i zahraničných podnikov.

Dôvody, ktoré agentúru SARIO viedli k vytvoreniu tejto platformy, nabrali za uplynulé roky na svojej dôležitosti.
Ide najmä o:

- Škálovanie úspešných technologických riešení “Made in Slovakia” v rámci dodávateľských štruktúr významných (predovšetkým zahraničných) spoločností;
- Čoraz väčšie nákupné (procurement) kompetencie zahraničných spoločností etablovaných na Slovensku;
- Celkový rastúci záujem o tému priemyslu 4.0;
- Zvýšený príliv kapitálovo náročných investícií s vysokou pridanou hodnotou.

Hlavným nástrojom prepájania v rámci inovačných služieb SARIO sú klientovi na mieru šité inovačné semináre a workshopy (v poslednom čase aj virtuálne). Zameriavajú sa na zlepšovanie a zdokonaľovanie rôznych vnútropodnikových procesov najmä na Slovensku, ale aj v zahraničí, a slúžia aj ako obchodný kanál pre slovenských poskytovateľov technologických riešení.

Najčastejšie témy a oblasti, v ktorých podniky vyhľadávajú nové inovatívne riešenia, zahŕňajú automatizáciu, robotizáciu a digitalizáciu výroby či logistiky, jednoúčelové stroje a zariadenia, prediktívnu údržbu, kontrolu kvality, senzoriku, virtuálnu či rozšírenú realitu alebo komplexné IT riešenia v oblastiach kybernetickej bezpečnosti, umelej inteligencie alebo cloudových technológií. SARIO disponuje databázou viac ako 300 slovenských technologických spoločností, ktoré ponúkajú inovatívne riešenia vo vyššie spomenutých oblastiach, pričom táto databáza je neustále aktualizovaná a rozširovaná.

Proces hľadania vhodného riešenia sa začína identifikáciou prioritných oblastí záujmu klienta, na čo SARIO v krátkom čase reflektuje zoznamom vhodných slovenských technologických firiem pôsobiacich v definovaných oblastiach. Nasleduje výberový proces, počas ktorého si klient sám na základe rôznych kritérií a preferencií vyberie užší zoznam firiem, ktorých riešenia a predstaviteľov by rád bližšie spoznal. Následne konzultanti SARIO pripravia dedikované inovačné podujatie, ideálne v priestoroch klienta, ktorého sa zúčastnia predstavitelia vybraných firiem.

V takomto alebo podobnom formáte agentúra SARIO za 4 roky zorganizovala 30 inovačných podujatí, do ktorých bolo zapojených 171 prezentáciami viac ako 90 inovatívnych spoločností zo Slovenska, čo znamená, že mnohé sa zúčastnili viacerých podujatí a prezentovali svoje riešenia pred viacerými klientmi. Z vyššie uvedeného SARIO eviduje doposiaľ až 69 nadväzujúcich stretnutí a 15 pilotných inovačných projektov, keď práve vďaka tejto platforme slovenská spoločnosť dostala zákazku u niektorého z klientov. Pochopiteľne je možné a pravdepodobné, že tieto inovačné semináre priniesli aj ďalšie obchodné príležitosti, kontakty či synergie.

V prípade, že vás inovačné služby SARIO zaujali a chceli by ste sa do nich zapojiť - či už ako potenciálny klient alebo poskytovateľ inovatívnych riešení, neváhajte sa na nás obrátiť na innovate@sario.sk

Marek Kopanický
konzultant a tímlíder pre inovačné služby
odbor investičných projektov, SARIO

Budúcnosť je tu

Nové modely mobility a smart city sú úzko späté s kyberbezpečnosťou

Elektrické autonómne vozidlá vybavené technológiou umelej inteligencie a adaptívnym programovaním. Drony s naprogramovaným cieľom a letovou kapacitou 6 hodín. Robot lekár, ktorý určuje diagnózu.
Fascinujúci balík integrovaných dopravných riešení s novými modelmi mobility, incident management system nielen v IT, ale aj v skutočnom svete, predikcia a automatický alerting vedúci k zlepšeniu dopravnej situácie a kriminality v mestách, znižovanie emisií a zlepšovanie kvality ovzdušia a klímy, boli súčasťou veľtrhu GITEX GLOBAL 2021 v Dubaji, spolu s ukážkami inteligentných riešení smart cities podporovaných 5G sieťou.

GITEX GLOBAL je najvplyvnejším medzinárodným technologickým a startupovým veľtrhom, organizovaným od roku 1981. V októbri 2021 sa na ňom predstavilo viac ako 3000 technologických firiem a 700 startupov zo 100+ krajín sveta s inovačnými víziami, digitálnymi revolúciami a riešeniami z oblasti umelej inteligencie, robotiky, 5G siete a cloud computingu, dátovej ekonomiky, kybernetickej bezpečnosti či blockchainu.
Na festivale budúcnosti skúmala aktuálne svetové trendy s potenciálom vývoja technológií a spolupráce aj naša spoločnosť GAMO.
Nemecká firma Neura Robotics napríklad uviedla do sveta celý rad robotov s kognitívnymi vlastnosťami. Sú schopné myslieť ako človek, počuť, vidieť, a dokonca cítiť.
Realitou už je aj robotický pes, ktorý do nikoho nenarazí a môže sa stať veľkým prínosom pre nevidiacich ľudí.
Náhradu ľudskej sily v gastronómii a službách suplovali onedlho všadeprítomní roboti-čašníci, prinášajúci jedlá a nápoje. A pri ceste okolo na nás nezabudli žmurknúť.

Budúcnosť je tu.

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

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).