Už je to tu. Bezpečnosť v dobe cloudovej je iná

FIRMY

Ešte donedávna bol status quo taký, že informačná bezpečnosť sa primárne sústreďovala na problémy s infraštruktúrou inštalovanou v priestoroch spoločnosti. Nasleduje však grandiózna zmena.

Presun do cloudu prináša výhody a ďalšie príležitosti a zároveň riziká, ktoré treba zohľadniť. SNÍMKA: DREAMSTIME

Vostatnej dekáde niektoré spoločnosti aj začali transformačné projekty smerujúce do cloudu, keďže tam videli potenciál, ale tieto iniciatívy boli viac-menej považované za tieňové IT. A to, samozrejme, znamenalo bezpečnostné riziká.

Všetko sa však veľmi zmenilo minulý rok. Rok 2020 bol rokom, keď sa veľká časť organizácií snažila vymyslieť spôsob, ako efektívnejšie pracovať a vytvárať priestor na spoluprácu svojich zamestnancov.

A tu sa jednoznačne ukazuje výhoda cloudu. Zvládnuť takýto prechod bezpečne si však vyžaduje trochu viac než iba objednať si danú službu a začať ju využívať. Ako teda na to?

Vhodné riadenie a kontrola
Posun do cloudu by sa mal udiať bezpečne. A na to je nevyhnutné, aby organizácie dovolili svojim bezpečnostným tímom včas implementovať dostatočné riadenie a kontrolu cloudového prostredia a považovali bezpečnosť za prvoradú pri prechode do cloudu.

Identifikácia súčasného stavu
Pochopiť a kvantifikovať riziká v súčasnej infraštruktúre verejného cloudu je dôležité nielen z hľadiska bezpečnosti, ale aj riadenia efektívneho využívania zdrojov, ktoré sa premieta do nákladov pre organizáciu.

Nečakajte, až sa zlepší situácia na trhu práce
Je luxusom čakať na to, kým sa vytvoria tímy bezpečnostných profesionálov so špecializáciou na cloud, aj keď to by mal byť dlhodobý cieľ. Teraz musíme hľadať cesty, ako redukovať riziká, kým sa tento dlhodobý cieľ stane skutočnosťou.

Cloudová infraštruktúra je viac a viac z pohľadu zákazníka vnímaná ako kód, preto integrujte svoje tímy v súlade s prístupom vývoj – bezpečnosť – prevádzka. Ide o prístup, keď sú všetky tieto oblasti zahrnuté do vývoja, napríklad aplikácie, aby sa včas identifikovali a eliminovali nedostatky a slabé miesta z pohľadu bezpečnosti a prevádzky.

Technológia musí pracovať pre vás
Využitie technológie bez ohľadu na to, akú máte rozsiahlu organizačnú infraštruktúru. Rozhodne nie je efektívne využívať kapacitu špecialistov na to, čo môžete automatizovať s použitím existujúcich alebo modifikovaných pracovných postupov.

Mali by ste využiť akúkoľvek dostupnú technológiu, ktorú ste schopní zakomponovať do existujúcich procesov a riadiť súčasným personálom. Ako nevyhnutná sa ukazuje práve integrácia s infraštruktúrou ako kód.

V praxi sa to realizuje systémom prideľovania úloh v riadení bezpečnostných informácií a udalostí (SIEM) a, samozrejme, kontrolou prístupu založenou na plnených úlohách (RBAC) spojenými s precíznym riadením rolí a zodpovedností.

> Využitie technológie bez ohľadu na to, akú máte rozsiahlu organizačnú infraštruktúru.
>
> **Daniel Suchý,** bezpečnostný špecialista Aliter Technologies

Neverte univerzálnym riešeniam
Nesnažte sa nájsť jeden nástroj, ktorý vie robiť všetko. S tým, ako rastie cloud, tak rastie aj trh s podpornými nástrojmi a nie zriedka sa stretávame s riešeniami všetko v jednom. Kde všetko veľakrát znamená, že nič nie je poriadne.

I keď si to vyžaduje zvýšené úsilie, je potrebné hľadať riešenia, ktoré zodpovedajú vašim požiadavkám a ponúkajú to najlepšie na trhu v danej oblasti. Takýmto spôsobom si viete vyskladať to najlepšie riešenie pre seba.

Rozdiel medzi úspechom a katastrofou
Cloud sa dynamicky vyvíja a veľakrát poskytuje značnú konkurenčnú výhodu pre organizácie, ktoré sú schopné bezpečne ho implementovať a integrovať do procesov. Avšak slovo bezpečne by sa nemalo nikdy vytratiť, pretože toto slovo je veľakrát jediný rozdiel medzi úspechom a katastrofou.

PRAX

Ako si môžu pomôcť obce a malé mestá

Kybernetické útoky za nevyhýbajú ani Slovensku a už vôbec nie mestám a obciam.

„V praxi sa stretávame s phishingovými mailami hromadne rozposielanými zamestnancom, krádežami identity na sociálnych sieťach či hackerskými útokmi na úrady a firmy," upozorňuje certifikovaný audítor kybernetickej bezpečnosti Michal Ďorda zo spoločnosti auditori.it.

Krajina malých obcí
Mestá a obce majú povinnosť urobiť audit kybernetickej bezpečnosti nielen preto, aby mali formálny papier, ale najmä aby chránili bezpečnosť obyvateľov.

„Je však obrovský rozdiel medzi obcou s tisíckou obyvateľov či mestom s desaťtisíc obyvateľmi, alebo bratislavskou mestskou časťou," hovorí na základe skúsenosti z terénu bezpečnostný špecialista Alison Slovakia Miroslav Macko. Technické a personálne vybavenie či bezpečnostné povedomie je diametrálne odlišné, ale povinnosť majú rovnakú.

Samohodnotenie
Preto bolo novelizáciou zavedené samohodnotenie. Účelom je zjednodušiť splnenie zákonnej povinnosti malým a menším poskytovateľom základnej služby. Tým, ktorí majú povinnosť auditu, ale ich informačný systém nepredstavuje úplne sofistikovanú architektúru.

Formulár k samohodnoteniu je od novembra dostupný na webovej stránke Národného bezpečnostného úradu.

Michal Ďorda však upozorňuje: „Samohodnotenie je možné realizovať len za určitých podmienok." Obec musí mať určeného manažéra kybernetickej bezpečnosti a nesmie mať informačný systém III. kategórie.

Náročné úlohy
Zodpovednosť za riadenie kybernetickej bezpečnosti má vždy prevádzkovateľ základnej služby a jeho štatutárny orgán, čiže starostovia a primátori.

Pochopiteľne, úlohy, ktoré si vyžadujú odborné spôsobilosti, je možné realizovať aj využitím dodávateľských služieb. Nie je však možné na dodávateľa preniesť zákonom stanovené povinnosti.

Fakty a dokumenty
Dotazník samohodnotenia na základe aktuálneho stavu vypĺňa manažér kybernetickej bezpečnosti pravdivo a tak, aby bolo možné uvedené tvrdenia v prípade potreby preveriť.

Štátna autorita odporúča pripojiť aj dokumenty podporujúce tvrdenia. Zároveň je potrebné pridať aj plán implementácie opatrení kybernetickej bezpečnosti na nasledujúce obdobie schválený štatutárom.

Vyplnený formulár s plánom implementácie treba podpísať kvalifikovaným elektronickým podpisom a doručiť Národnému bezpečnostnému úradu.

Dobrá robota
Poctivo spravené samohodnotenie spolu s prijatým plánom opatrení a jeho realizáciou dokáže v malej obci zastúpiť náročný audit kybernetickej bezpečnosti.

„Na audite ušetrené prostriedky sa dajú investovať do budovania či zvyšovania bezpečnostného povedomia zamestnancov spolu s procesnými a technickými opatreniami v praxi," uzatvára Miroslav Macko. Práve to, že používatelia nesprávne používajú IT zariadenia, je podľa prieskumov najčastejším vektorom útokov na Slovensku.

Máme viacej ako 2800 obcí a miest, kde žije menej ako desaťtisíc obyvateľov. SNÍMKA: DREAMSTIME

TRENDY

Menia sa pravidlá a dnes rýchlejší vyhrávajú nad silnejšími

Rozšírená a virtuálna realita nám otvára bránu do kybernetického sveta, v ktorom umelá inteligencia dokáže predpovedať budúcnosť alebo vdýchnuť pomyselný život do chladného železa.

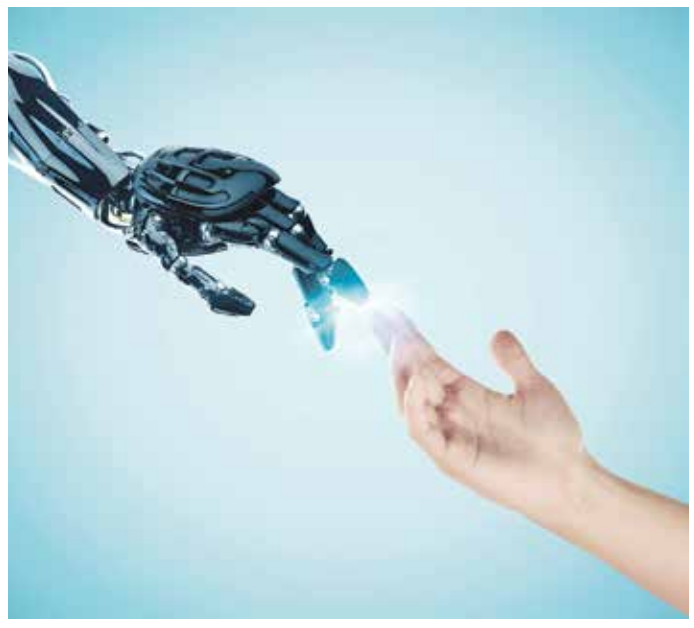
Robotika je novým odvetvím, ktoré nám sľubuje blahobyt. Najväčšími hrozbami sa stávajú útoky hackerov, ktorých sa môžeme obávať aj vo fyzickom svete. Získanie veľkých dát predstavuje ohromné bohatstvo a matematici sú znovu v kurze. Nové platidlá negarantujú banky hmotným bohatstvom a ani rezervami.

Yuval Harari, profesor histórie na Jeruzalemskej univerzite, predpovedá novú éru vývoja človeka – Homo deus, kde technológie budú súčasťou človečenstva.

Áno, život menia technológie, ktoré sa dostávajú aj na menej očakávané miesta, akými sú umenie, šport, výchova. Kto adoptuje nové technológie, prežije. Ochránia vás napríklad pred sofistikovanými kybernetickými útokmi hackerov, ale aj pred primitívnym útokom vandalov.

Predstavte si technológiu, ktorá by chránila váš príbytok tak, že umožní vstup len známym osobám. O neznámej osobe by vás proaktívne informovala a dvere by sa otvorili len overenej osobe. V prípade, že by sa v okolí objavili viaceré neznáme osoby, dostali by ste počet a opis osôb.

Mám na mysli nový technologický startup priamo z MIT, za ktorým stojí slávna investičná skupina Sequoia. Investori, ktorí stáli pri úspechu firiem ako Apple, PayPal, Oracle, Instagram, LinkedIn, WhatsUp, Zoom či Cisco Meraki, sa najnovšie rozhodli podporiť firmu Verkada.



Umelá inteligencia je na ceste stať sa hlavnou technológiou budúcnosti. SNÍMKA: DREAMSTIME

Verkada je systém, ktorý využíva umelú inteligenciu na spracovanie zvukového a obrazového záznamu nielen na detekciu, ale hlavne na prevenciu pred nebezpečenstvom. Jeho integrácia na alarmy, senzory, kamery a manažment vstupu vytvára nepreniknuteľnú bariéru pre podozrivé osoby alebo vozidlá.

Predstavte si proaktívne vyhľadávanie ľudí na základe farby trička alebo pohlavia, vozidlá zas na základe továrenského typu. To všetko bez nutnosti vytvárania dátového centra a drahých serverov, diskových polí, switchov alebo firewallov.

Pamätám sa na jeden príklad, kde zákazníkovi ukradli zlodeji „poolové" auto. Služobné vozidlo, ktoré si zamestnanec mohol na deň požičať, stálo počas karantény v garáži. Samozrejme, všetko zabezpečené, pod kamerou. Službukonajúci bezpečnostný operátor si ani nevšimol v húfe malých obrazoviek na monitore, že sa niečo deje. O krádeži sa dozvedeli až po skončení karantény.

Teraz si predstavte systém, ktorý by vám poslal notifikáciu hneď, ako si do auta sadá neznáma osoba a odchádza.

Thomas Friedman vo svojej knihe Zem je plochá napísal, že naše storočie nebude priať silným tak, ako diktovala história. Budúcnosť praje pripraveným, ktorí dokážu rýchlo adoptovať najnovšie technológie. **Andrej Aleksiev**