HN
obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
26. – 28. JÚLA 2024

Odborná spolupráca
NBÚ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Riziká tu budú vždy. Ako budete s nimi žiť?

TÉMA

Analýza rizík je bolestivá téma, firmy jej často nerozumejú alebo sa jej obávajú. A pritom reálna analýza rizík vám uľahčí rozhodovanie. Upracete vo firme – priority aj kolegov.

Riadenie rizík nie je nová téma a ani nová zákonná požiadavka. FOTO: DREAMSTIME

Profesionálny pohľad na riziko môže byť aj obsiahlejší: „Človek riadi riziká odjakživa aj bez toho, aby si to uvedomoval. Aj vďaka tomu dokázal prežiť rôzne nepriazne osudu a v evolučnom procese sa prepracoval na vrchnú priečku rebríčka!“ Ivan Makatura sa však ako riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti rýchlo vráti k súčasnosti.

Od mamutov k hackerom

V súčasnosti sa nás okrem fyzického týka aj kybernetický priestor. A úplne všetkých – od malých detí až po dôchodcov, verejnej správy aj podnikateľov, služieb aj výroby, malých aj veľkých organizácií, jednotlivcov aj skupín.

Tak, ako kromaňonci v paleolite dbali na prevenciu rizika zašliapnutia mamutom, dnešný Homo sapiens by mal ošetrovať riziká týkajúce sa jeho života v kyberpriestore, farbisto pokračuje Ivan Makatura. A za riadenie rizík bol zodpovedný náčelník kmeňa. Dnes to majú „náčelníci“ dané aj zákonom.

Štatutári budú totiž povinní schváliť opatrenia na riadenie kybernetických rizík s cieľom dosiahnuť súlad so zákonom a dohliadať na ich vykonávanie. Zároveň budú mať osobnú zodpovednosť.

Riadenie rizík je proces

Riadenie rizík je procesom a zároveň aj základným stavebným prvkom bezpečnosti. A prvým krokom v procese je analýza rizík. Ukáže, „kde nás tlačí topánka“ a z toho potom vyplýva ošetrenie rizík.

Michal Srnec, vedúci oddelenia informačnej bezpečnosti Aliter Technologies, oceňuje prínos analýzy rizík pre kyberbezpečnosť aj pre biznis a aktuálne pridáva: „Zo všetkých povinností, ktoré novelizovaný zákon prinesie pre štatutárov a ktoré sú veľakrát diskutované, je práve analýza rizík jedna z tých aktivít, ktorá by mala byť vykonávaná aj bez legislatívnych požiadaviek.“

Ako presvedčiť riaditeľa

Pýtate sa, prečo by finančný alebo akýkoľvek riaditeľ mal chcieť analýzu rizík? Sú na to tri kľúčové dôvody. Bude vedieť, čo všetko treba chrániť, kde sú slabé miesta a kam skôr investovať.

Po poctivej analýze rizík sa často objavia príležitosti, kde ušetriť a ktoré aktíva sú skutočne kritické. Neraz sa odhalia aj zbytočné služby a na druhej strane je to akési potvrdenie, že s dodávateľmi máte dobre postavené služby a cenotvorbu.

Bod nula

Klienti sa Michala Srnca často pýtajú, s čím majú v oblasti informačnej bezpečnosti začať. Jeho odpoveď je opäť – začnite s analýzou rizík, „lebo ak aby ste ju mali, táto otázka by nebola potrebná“.

Analýza rizík je však dokument, ktorý sa nedá kúpiť hotový. Môžete si dohodnúť spoluprácu so špecialistom, ale proces si vyžaduje nevyhnutne spoluprácu na všetkých frontoch. Keď nespolupracujú všetky oddelenia, zostanú slabé miesta v kybernetickej bezpečnosti ako diery v plote.

(Ne)veselá príhoda

Ak samotná organizácia nepomenuje najdôležitejšie procesy, alebo údaje, podporné služby v prípade incidentu nevedia správne určiť, čo treba chrániť alebo urýchlene obnoviť. Opíšme to metaforou – ak ítečkári nevedia pri obnove systémov priority, urobia si vlastné. Čiže po incidente si obnovia mailový server, portál s hrami a intranet, aby videli firemné sviatky.

Zdesili ste sa alebo pobavili? Tento príbeh používa skúsený audítor kybernetickej bezpečnosti na prezentáciách zaneprázdnenému manažmentu.

Hýbeme sa vpred

Skúsenosti kyberbezpečnostných profesionálov boli ešte donedávna iba o tom, že firmy začínajú dobrovoľne riadiť riziká typicky až vtedy, keď už je neskoro.

Za ostatné roky však už vidieť badateľný posun medzi štatutármi od reaktívneho k proaktívnejšiemu postoju. Technický špecialista spoločnosti ESET Július Secký za tým okrem legislatívy vidí aj vplyv pandémie a s tým spojený presun zamestnancov na prácu na diaľku. „V minulosti sa mnohé úlohy zameriavali predovšetkým na dodržiavanie predpisov a reagovanie na incidenty. V súčasnosti sa kladie väčší dôraz na predvídanie hrozieb a budovanie odolnosti.“

Rozpočet nie je bezodný

Od každého lídra sa očakáva návrh rozpočtu pre jeho oddelenie a v oblasti bezpečnosti je táto úloha obzvlášť zložitá. Pre vedenie firmy sú termíny ako inštalácia firewallov, IDS, IPS a XDR systémov, zvyčajne neznáme pojmy. Pri použití technických výrazov sa mnoho top manažérov „stráca“ a naskytá sa pohľad na zívajúce tváre a zasnené pohľady do neznáma.

Vedúci projektov kybernetickej bezpečnosti pre výrobu spoločnosti Mondelēz International Matej Orlický preto nedá na analýzu rizík dopustiť: „Mám takto príležitosť prezentovať riešenia ochrany pred potenciálnymi hrozbami aj mennej technickým členom vedenia firmy v ich každodennom jazyku, a tým sú financie.“

> SPRÁVNE ZOSTAVENÁ ANALÝZA, KTORÁ MÔŽE ZAHŕŇAŤ AJ REÁLNE INCIDENTY Z MINULOSTI, SI ZARUČENE ZÍSKA NÁLEŽITÚ POZORNOSŤ VEDENIA FIRMY.
>
> **Matej Orlický,** vedúci projektov kybernetickej bezpečnosti pre výrobu Mondelēz International

Keď sa už vedenie sústredí

Matej Orlický k zhodnoteniu najbežnejších hrozieb pre firmu vždy pripája aj kvantitatívnu analýzu rizík, ktorá vyjadruje potenciál finančnej straty pri kybernetickom útoku.

Uvádza odhadovanú cenu za implementáciu systému, ktorý by do značnej miery znižoval dané riziko. Nevyhnutné je v tomto prípade demonštrovať finančnú návratnosť prezentovaného riešenia.

Správne zostavená analýza, ktorá môže zahŕňať aj reálne incidenty z minulosti, si zaručene získa náležitú pozornosť vedenia firmy. Pri tejto príležitosti je vhodné vyzdvihnúť aj dosah na renomé firmy a stratu dôvery zamestnancov a kľúčových partnerov. A tie nemožno vyjadriť číslami v excelovskej tabuľke.

Bonus pre kyberkomunitu

To, že analýza rizík neoceniteľne zlepšuje celú oblasť kyberbezpečnosti, zdôrazňuje aj Dominik Procházka, riaditeľ odboru kybernetickej bezpečnosti AGEL SK: „Práve nedávno sme predložili riziká a ich kategorizácie a jedna konkrétna položka sa okamžite dostala do pozornosti manažmentu. Ihneď sme dostali pokyn na riešenie aj schválenie navrhovanej investície potrebnej na zníženie rizika.“

Prínosom pre samotných bezpečákov je aj to, že sa takto stále zlepšujú v efektívnej komunikácii. „Ak budú tieto náročné komplexné bezpečnostné problémy zrozumiteľné aj pre vedenie organizácií, bude to viesť k rýchlejšiemu prijatiu potrebných opatrení,“ uzatvára Dominik Procházka.

UPÚTAVKA NA ANKETU

Anketová otázka pre kyberbezpečnostných profesionálov:

Akú radu by ste dali malej firme?

Odpovede na 10 až 60 sekúnd.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 26. – 28. JÚLA 2024

Akú radu by ste dali malej firme?

ANKETA

Predstavte si firmu v okresnom meste, výrobňu a s dodávkou služieb. Majú účtovníčku, ítečkára a domácich aj zahraničných dodávateľov. Darí sa im, ale vedia, že žijeme náročné časy. Takže majiteľ, váš kamarát, si prišiel po radu. „Mám tu pár tisíc eur. Čo mám urobiť v kyberbezpečnosti?“

Jaroslav Ďurovka,
riaditeľ,
Národné centrum kybernetickej bezpečnosti

Začal by som takto: seba, účtovníčku a zamestnancov s prístupom na internet z firemných počítačov pošli na školenie, ako bezpečne používať internet, e-mail a sociálne siete. Ítečkára pošli na školenie, ako bezpečne administrovať PC, servery a aplikácie. No a konfiguráciu PC, serverov, sieťových prvkov a pripojenia na internet si daj preveriť nezávislou kyberbezpečnostnou firmou alebo audítorom. Potom sa uvidí.

Richard Kiškováč,
generálny riaditeľ,
Elkan

Najprv si spíšte, aké máte procesy výroby, predaja a všetky podporné a nevyhnutné služby. Potom zistite, ako sú naviazané na IT technológie a spracovávané dáta. Tu ti pomôžem identifikovať možné riziká a navrhneme adekvátne protiopatrenia – organizačné a technologické. Potom naplánujeme implementáciu a prevádzku opatrení a, samozrejme, aj ich kontrolu a rozvoj v súlade s aktuálnymi hrozbami.

Peter Dufek,
manažér kybernetickej bezpečnosti,
Penta Hospitals

Či je firma malá alebo veľká, rozhodne nech si kyberbezpečnosť nestavia ad hoc, ale systémovo. Moje odporúčanie je začať oslovením odbornej bezpečnostnej firmy. Tá preskúma aktuálny stav zabezpečenia, súpis dôležitých aktív, identifikuje hrozby, riziká, dosahy a stanoví priority a kroky na ochranu.

Roman Varga,
manažér kyberbezpečnosti,
Dôvera, zdravotná poisťovňa

Kyberbezpečnosť je neustály proces, nie jednorazová investícia. Investuj do vzdelávania zamestnancov, firewallu a ochrany koncových staníc. Pravidelne zálohuj dáta a aktualizuj softvér. Zavedenie dvojfaktorovej autentifikácie je dnes samozrejmosť a tá ti tiež zvýši bezpečnosť. Vykonávaj audity a penetračné testy. Vytvor si plán na riešenie incidentov a zváž kybernetické poistenie.

Tomáš Hettych,
viceprezident,
ISACA

Dáš to na päť krokov. Začni so základným školením, aby si vedel, čo je to kyberbezpečnosť a aké sú požiadavky. Urob si inventár informačných aktív, aby si zistil, čo vôbec máš. Klasifikuj si aktíva, nech vieš, čo je viac a menej dôležité pre tvoj biznis. Vykonaj analýzu rizík a analýzu dosahov, nech sa rozhoduješ podľa miery rizík. Urob si akčný plán, čo budeš implementovať.

Miroslav Chlipala,
riadiaci partner,
Advokátska kancelária Bukovinský & Chlipala

Vykonajte právny audit internej dokumentácie a zmlúv vo vzťahu k zraniteľnostiam, opatreniam na ochranu údajov a aj k dodávateľom. Ak máte zmluvy a doložky týkajúce sa ochrany údajov, kybernetickej bezpečnosti a odolnosti, aktualizujte ich. Vypracujte interné smernice, aby ste mali pravidlá na predchádzanie a riešenie kybernetických incidentov. Investujte do zmysluplného školenia zamestnancov.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Odporúčam investovať minimálne do školenia zamestnancov, overiť odolnosť firmy pred sociálnym inžinierstvom a otestovať infraštruktúru aspoň testom zraniteľností. A zvážiť väčšiu investíciu do monitorovania bezpečnosti IT infraštruktúry interne alebo externe formou služby.

Andrej Mišura,
partner,
Cyllium

Nájdi si skúseného audítora alebo konzultanta kybernetickej bezpečnosti, spravte analýzu aktuálneho stavu, posúďte riziká a na základe výsledkov aplikujte opatrenia. Efektívne a zmysluplne.

Katarína Kročková,
odborníčka na ochranu osobných údajov,
Kročka & Partners

Najskôr potrebujeme zistiť, aké má spoločnosť prijaté technické a organizačné opatrenia z hľadiska ochrany osobných údajov a kyberbetickej bezpečnosti. Sú totiž úzko prepojené, preto je potrebné posudzovať ich vo vzájomnej spolupráci. Po posúdení súladu opatrení s GDPR by som navrhla dodatočné riešenia.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií,
Volkswagen Slovakia

Odporúčam zaviesť pravidelné vzdelávanie v informačnej a kybernetickej bezpečnosti štatuára firmy aj zamestnancov vrátane tretích strán s prístupom k firemným dátam. Inventarizovať informačné aktíva a IT infraštruktúru firmy vrátane rozhraní na zákazníkov a dodávateľov, realizovať komplexnú analýzu bezpečnostných rizík a nasadiť z nej vyplývajúce opatrenia.

Stanislav Smolár,
manažér oddelenia bezpečnosti,
Soitron

Keďže presne nepoznáme vašu infraštruktúru, začal by som auditom aktuálneho stavu kybernetickej bezpečnosti. V prípade, že nemáte implementované MFA, začal by som určite tým vrátane aktualizácie bezpečnostného perimetra na aktuálne zariadenia. A službu správy siete by som rozšíril na manažovanú bezpečnosť a security operations centre.

Július Selecký,
senior technický špecialista,
ESET

Potešil by som sa, že mám takého uvedomelého proaktívneho kamaráta. Vysvetlil by som mu, že budovanie bezpečnosti je kontinuálny proces, a začali by sme rovno analýzou rizík, aby poznal svoje slabé stránky. Až na základe analýzy by som navrhol vhodné riešenie na zabezpečenie siete, koncových bodov a zálohovania a k tomu prislúchajúce služby, aby mal prostredie monitorované.

Jakub Berthoty,
advokát,
Dagital Legal

Mal by si konečne kúpiť „to GDPR“.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť,
Západoslovenská energetika

Rozhodne si objednaj audit služby na správu siete. Zistíš tak aktuálny stav z hľadiska kyberbezpečnosti, či služba má dostatočný rozsah a adekvátnu kvalitu. S veľkou pravdepodobnosťou skôr nie. Extra financie použi na zvýšenie úrovne bezpečnosti, primerane veľkosti a aktuálnym rizikám biznisu. A investuj do kybervzdelania interného ítečkára.

Ivan Kopáčik,
bezpečnostný expert,
Gordias

„Vyhraď si hodinku času a 10 eur. V týchto horúčavách ma pozveš niekam na pivo a pozhovárame sa. Ak ti mám poradiť, potrebujem ti položiť viacero otázok.“ Zmysluplné rady v tomto prípade sa nedajú vtesnať do odpovede na anketovú otázku. A keďže je to kamarát, chcem byť zodpovedný…

Zuzana Motúzová,
advokátka,
Motúzová & Lacko Advokátska kancelária

Po nedávnom incidente Crowdstrike, ktorý zastavil leteckú dopravu a takmer ochromil celý svet, by som mu zrejme poradila zdvojnásobiť rozpočet.

Tomáš Zaťko,
CEO,
etický hacker,
Citadelo

Nájdi dôveryhodného partnera s kvalitnými skúsenosťami v kyberbezpečnosti. Najmi etických hackerov na odhalenie slabých miest. Vytrénuj svoj tím, aby sa stal ľudským firewallom, ľudia sú vždy najslabším článkom. Vytvor dlhodobý plán a vynakladaj peniaze podľa plánu, nie naraz. Buď ostražitý.

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies na Slovensku

Ešte rýchlejšie ako technológie sa vyvíjajú formy kyberútokov. Pár desiatok tisíc eur na úvod je možno dobré, ale na bezpečnosť sa musíme pozerať z dlhodobého hľadiska a plánovať ju. Keď si uvedomíme, že najzraniteľnejším článkom v celej sústave sú ľudia, investícia do nich by na úvod mohla byť to správne.

Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Pri dnešnej realite slovenských malých a stredných výrobných firiem by odporučenie malo asi takéto poradie dôležitosti – investuj do modernizácie IKT, začni efektívne a bezpečne zálohovať, urob serióznu analýzu aktuálneho stavu vrátane svojich dodávateľov a dovzdelávaj zamestnancov. A zároveň sa začítaj do svojej bezpečnostnej dokumentácie a tam určite nájdeš zoznam opatrení, ktoré ostali len na papieri.

Ivan Makatura,
generálny riaditeľ,
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Od kvalifikovaného dodávateľa objednať profesionálne zhodnotenie existujúcej informačnej architektúry firmy, posúdenie zraniteľností a analýzu rizík. Ak je firma povinnou osobou zo zákona, nezabudnúť ani na audit kyberbezpečnosti. Na základe získaných informácií potom spolu s dodávateľom a s ítečkárom rozhodnúť o implementácii primeraných bezpečnostných opatrení. A potom nezaspať na vavrínoch.

Jozef Zoričák,
vedúci oddelenia informatiky,
Národný ústav pľúcnych chorôb Vyšné Hágy

Základom je analýza a interný audit. Budete vedieť, aká je aktuálna úroveň kyberbezpečnosti. Overte si, aké máte povinnosti podľa smernice NIS2. Výsledok analýzy a odhalenie kritických miest určí, kde sa prioritne použije interný balík peňazí. Radím vám aj overiť si možnosti zapojenia sa do výziev EÚ pre stredné podniky. A osobu zodpovednú za kyberbezpečnosť máte?

Ján Adamovský,
riaditeľ bezpečnosti,
Slovenská sporiteľňa

Jožko, zorganizuj skvelý teambuilding. Zábavnou formou poukážeme na hrozby kybernetickej bezpečnosti, ktorým firma aj zamestnanci ako súkromné osoby čelia. Nauč ich, ako im nepodľahnúť a ako na ne reagovať. Potom si daj spraviť krátku analýzu stavu technológií a zvýš ich bezpečnosť. A odlož časť peňazí a toto znova zopakuj o pol roka. Aby sa z toho stala pravidelná činnosť a nielen jednorazový výstrel do tmy.

Peter Bukovinsky,
šéf IT bezpečnosti,
Eviden Slovensko

Ak chce majiteľ firmy ostať čo najviac nezávislý, mal by zistiť a obstarať rozumnú kombináciu pravidelných školení, nákupu špeciálneho hardvéru a softvéru a nájmu služieb kyberbezpečnosti. S akceptáciou rizika závislosti by stačil nájom komplexných služieb kyberbezpečnosti, kde je zahrnuté všetko uvedené, ale pre voľbu dobrého a trvácneho poskytovateľa treba riadnu mieru erudovanosti a asi aj intuície.

Roman Čupka,
hlavný konzultant,
Progress a CSO Istrosec

Hovoríš niekoľko desiatok IT zariadení a vo výrobe priemyselná technológia? Predpokladám, že na zabezpečenie používate len sieťový firewall a antivírus na počítačoch. Najvhodnejšia pre vás je profesionálna manažovaná služba. Posúdi sa stav bezpečnosti, vytvorí dokumentácia, implementujú opatrenia, robí sa dohľad aj riešenie incidentu v prípade vzniku. Mesačné náklady sú fixné a v tomto prípade aj výhodnejšie než investícia do interného bezpečáka.

Tibor Szabo,
vedúci oddelenia auditu IT,
Všeobecná úverová banka

Vidím, že si ešte neinvestoval do bezpečnosti. Začnime tým, čo si vo firme najviac ceníš. Urob si zoznam aktív, ohodnoť ich a urobíme analýzu, čo by sa stalo, keby si o tieto informácie, dáta, softvér a hardvér prišiel alebo by ich niekto poškodil. Keď budeš mať business impact analýzu hotovú, potom sa budeme baviť o adekvátnych a účinných bezpečnostných opatreniach. Určite sa ti bude lepšie spávať.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti,
Aliter Technologies

Už samotná otázka naznačuje, že je nutné začať od základov. Kybernetická bezpečnosť nie je jednorazová aktivita. Nedá sa odbiť jediným „quick fix“ riešením. Je nutné postupovať od základov a systematicky. Podľa môjho názoru je najlepšie začať s analýzou rizík, teda upratať si pred vlastným prahom, identifikovať tie najväčšie riziká a tie systematicky ošetrovať.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 26. – 28. JÚLA 2024

Aktuálne fakty o našej bezpečnosti

ANALÝZA

Správa o kybernetickej bezpečnosti ESET Threat Report H1 2024 mapuje digitálne hrozby od decembra 2023 do mája 2024.

Slovensko v skratke

1. Phishingový podvod HTML/ Phishing.Agent trojan

Ide o škodlivú HTML prílohu imitujúcu prihlasovacie okná do populárnych služieb, ktorá sa bežne šíri prostredníctvom e-mailov s cieľom získať od obetí citlivé údaje.

Viac ako 18 % detekcií

2. Hrozba JS/ Agent trojan

Tento škodlivý JavaScript kód dokáže kompromitovať zle zabezpečené, no legitímne webové stránky, často postavené na publikačnom nástroji WordPress, ktoré využívajú pluginy s bezpečnostnými zraniteľnosťami. Napadnuté stránky sú nebezpečné v tom, že dokážu infikovať zariadenia návštevníkov bez toho, aby si z nich obete čokoľvek stiahli.

Takmer 11 % detekcií

Celkový počet hrozieb zostal v porovnaní s predošlým polrokom nezmenený.

Najrozšírenejšou hrozbou zostáva phishing.

Rapídne pribúdajú škodlivé aplikácie, ktoré sa vydávajú za nástroje umelej inteligencie.

3. Downloader PowerShell/ TrojanDownloader. Agent trojan

Škodlivý softvér typu downloader využíva PowerShell skripty na sťahovanie a inštaláciu ďalšieho malvéru do počítača. Masovo sa šíri prostredníctvom e-mailov s prílohou formátu.bat. Text jedného zo zachytených e-mailov nasvedčuje, že útočníci sa zamerali na firmy či podnikateľov: „Ahoj, v prílohe nájdete našu novú objednávku. Zašlite nám prosím proforma faktúru na platbu. S pozdravom/Best regards.“

Viac ako 7 % všetkých detekcií

Zneužívanie napodobenín generatívnych nástrojov umelej inteligencie

Infostealer Rilide Stealer sa zameriava na krádež prihlasovacích údajov. Operuje ako rozšírenie prehliadača, ktoré si obeť nainštaluje po kliknutí na Facebook reklamu propagujúcu falošnú službu generatívnej AI.

Nárast 133 %

Trendy vo svete

Temná stránka umelej inteligencie

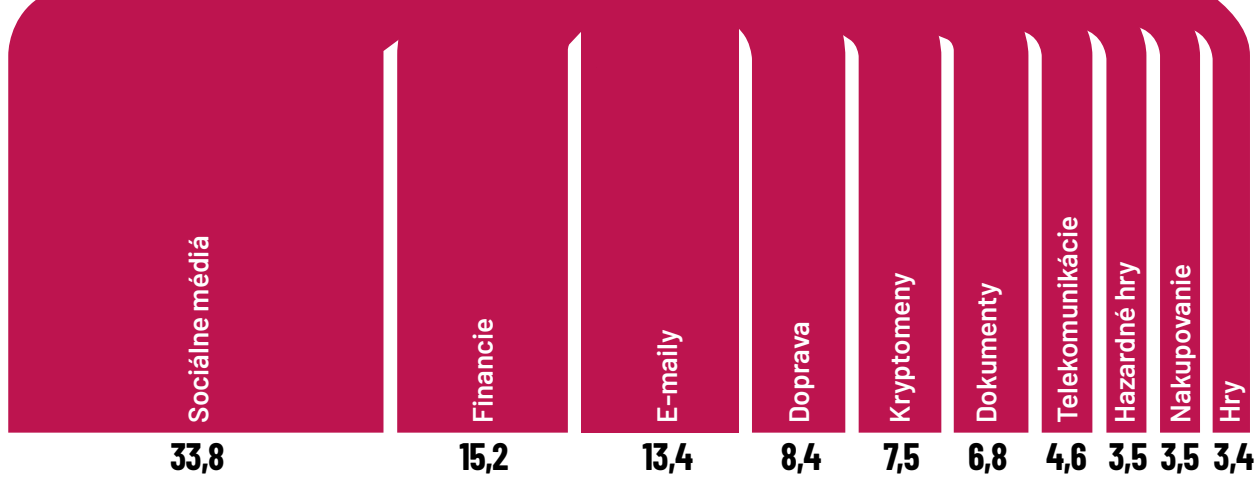
Útočníci používajú nový mobilný malvér GoldPickaxe na to, aby kradli údaje z rozpoznávania tváre a vytvárali z nich deepfake videá. Videá následne používajú na overovanie podvodných finančných transakcií. GoldPickaxe má verzie pre Android aj iOS a škodlivé aplikácie vie lokalizovať.

Herný svet pod útokom

Herní nadšenci, ktorí sa rozhodli vydať mimo oficiálneho ekosystému herných vývojárov, sa stávajú obeťami kybernetických útokov. Niektoré cracknuté hry a nástroje na četovanie v online multiplayer hrách skrývali malvér. Napríklad infostealer RedLine Stealer zaznamenal niekoľko prudkých nárastov spôsobených kampaňami v Španielsku, Japonsku a Nemecku. Počet detekcií v porovnaní s predchádzajúcim obdobím sa zvýšil o tretinu.

Najčastejšie kanály pre phishingové podvody

(v percentách)



Zdroj: ESET Threat Report H1 2024 mapuje digitálne hrozby zachytené bezpečnostnými riešeniami spoločnosti ESET od decembra 2023 do mája 2024.

Mega rozšírený, mega zraniteľný

Skupina útočníkov Balada Injector je notoricky známa zneužívaním zraniteľností WordPress pluginov. V uvedenom období kompromitovala viac ako 20-tisíc webových stránok, pričom telemetria spoločnosti ESET zaznamenala viac ako 400-tisíc detekcií.

Ransomvérová scéna stratila kráľa

Globálna operácia Chronos zosadila z piedestálu ransomérový gang Lockbit. Stalo sa tak vo februári 2024 a bola to spolupráca orgánov činných v trestnom konaní. Aj keď boli neskôr zaznamenané dve pozoruhodné kampane LockBit, zistilo sa, že boli „iba“ výsledkom použitia uniknutého LockBit buildera útočníkmi, ale tí neboli členmi gangu.

Celý život je riziko. A sme tu

EXPERTÍZA

Krátky slovník slovenského jazyka definuje riziko ako možnosť či nebezpečenstvo straty, neúspechu alebo škody. Podľa zákona o kybernetickej bezpečnosti je riziko miera kybernetického ohrozenia.

Riziká sa učíme v bežnom živote zvládať skúsenosťami. FOTO: DREAMSTIME

Pre študentov bezpečnosti
Pri výučbe rád vysvetľujem riziko na príklade. Predstavte si, že šoférujete naprieč horským priesmykom a všetko okolo je zasnežené. Už teraz sa bojíte, aby ste nedostali šmyk. Vtom sa pred vami objaví plne naložený kamión, ktorý sa prešmykuje na mieste a nevie sa pohnúť.

Musíte zastaviť. Hrozí, že už sa nerozbehnete. A kamión sa môže navyše zviezť priamo do vášho auta. Stav, v ktorom sa nachádzate, je rizikom.

Ešte jeden príklad
V kalendári je Medarda, pravidelne vonku prší a vy sa ráno chystáte do práce, kam sa pravidelne prechádzate, lebo to trvá 20 minút svižnou chôdzou. Pri dverách máte, tak ako vždy, odložený dáždnik a premýšľate, či si ho zobrať, alebo nie. Existuje teda nenulové riziko premoknutia do nitky pri vašej dnešnej ceste do práce.

Poďme do praxe
Dnes už každý z nás riadi svoje osobné riziká a niekedy za nás túto úlohu preberú iné organizácie. Markantným príkladom sú riziká, ktoré vyhodnocuje banka, keď žiadame o úver.

Riadenie rizík v informačnej a kybernetickej bezpečnosti nie je v ničom iné. Dokonca táto doména je ešte viac o riadení, pretože sa tu snažíme preventívne zavádzať bezpečnostné opatrenia. A ak už bezpečnostný incident nastane, tak cez vybrané opatrenia sa snažíme čo najviac minimalizovať jeho dosah.

Začiatok ľahší, ako sa zdá
Prvým krokom je samotná analýza rizík, kde identifikujeme všetky potenciálne riziká. Na pomoc prichádzajú profesionálne služby a metodiky, kde sú zoznamy známych hrozieb, zraniteľností a aj formy dosahu.

Tu treba upriamiť pozornosť na analýzu rizík založenú na udalostiach, ktoré spôsobí útočník alebo používateľ. Rizikom môže byť napríklad DDoS externý útok na perimetrové zariadenia organizácie a následkom možné znefunkčnenie webových služieb.

Obohrané a pritom riešiteľné
Na Slovensku v organizáciách často chýba expertíza alebo funkcia bezpečnostného analytika či špecialistu riadenia rizík, ktorí by vedeli pripraviť kvalitnú a aplikovateľnú metodiku na výkon analýzy rizík.

Preto sa Národný bezpečnostný úrad chopil úlohy a pripravil vzorovú metodiku analýzy rizík. Je dostupná na ich webovej stránke, jej aplikovanie však bude stále vyžadovať expertov. Ich úlohou bude aplikovať niektorú z metodík a správne určiť úroveň identifikovaných rizík.

Posúdenie rizík
Posúdenie rizík sa dá robiť kvalitatívnou metódou, keď analytik určí škály a hodnoty – napríklad nízka, stredná a vysoká úroveň. Väčšinou tu však ide o subjektívne hodnotenie.

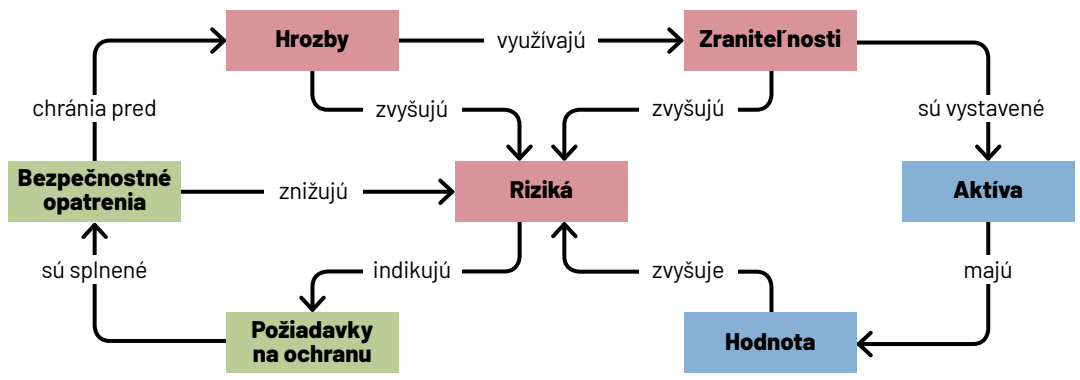
Matematicky presnejšie je kvantitatívne určenie rizík. Pravdepodobnosť sa určí v percentách, čo vyjadruje výskyt danej hrozby v predošlom období početnosťou bezpečnostných udalostí a incidentov.

Druhou zložkou je určenie dosahu v súvislosti s reputačnými, legislatívnymi, prevádzkovými alebo život ohrozujúcimi dosahmi.

Každá metóda určenia hodnoty rizika má svoje „za a proti“, a teda sú aj rôzne používané v rôznych organizáciách.

Najhoršie riešenie
Často sa v praxi stretávame s tým, že organizácia vedie v katalógu rizík iba jedno všeobecné ICT riziko. Vtedy doň analytik vloží všetky možné úmyselné aj neúmyselné, aj prírodné hrozby.

Informačná a kybernetická bezpečnosť



Upozorňujem, že sa tu môžu zlúčiť rôzne riziká do jedného a chýba tu adekvátna rozlišovacia schopnosť. Ak organizácia nevie identifikovať príslušné riziká, je možné, že nevie ani adresovať adekvátne bezpečnostné opatrenia. Tento postup je preto neefektívny na riadenie zdrojov.

Inšpiratívny prístup
Ako audítor si pamätám na klienta, kde analýza rizík nebola vo veľkých IT aplikáciách a nástrojoch a ani len v obyčajných excel tabuľkách. Bola urobená v stromovej štruktúre a zakreslená s identifikovanými hrozbami a zraniteľnosťami.

Pod „listami“ v tejto myšlienkovej mape boli aj úrovne pravdepodobnosti rizika a dosah na vopred definovanej škále.

Táto evidencia a zobrazenie analýzy rizík ma veľmi zaujali a presvedčili, že jeho autor rozumie procesu a aj prínosu riadenia rizík.

Čo nás čaká
Skúsené organizácie nezabúdajú ani na posúdenie rizík plynúcich z dodávateľských reťazcov. Navyše, bezpečnostné opatrenia v oblasti riadenia rizík tretích strán sú už zahrnuté aj v aktuálnych smerniciach NIS2, DORA a v európskej regulácii budú aj ďalej pribúdať.

Čo teda s identifikovanými vysokými rizikami? Nastavte si plán zvládania rizík, aplikujte adekvátne bezpečnostné opatrenia v súlade s legislatívou a bojujte so známymi, ale aj s novými hrozbami. Tie sa budú objavovať každý deň.

Michal Ďorda,
partner pre expertné služby,
Cyllium

PORADŇA

Výsledky sú, teraz nasledujú opatrenia

Výsledkom dobre vykonanej analýzy rizík je zoznam opatrení, ktoré treba prijať, a rozpočet na ich implementáciu – časový, finančný či personálny.

Tu bude priestor pre špecializované firmy, ktoré dokážu vyhodnotiť, ako s kombináciou dostupných zdrojov dosiahnuť čo najlepší výsledok.

Môže ísť o kyberbezpečnostné opatrenia ako nasadenie monitorovacieho softvéru, zavedenie dvojstupňovej autentizácie či implementácia riešení na prevenciu úniku dát. A niekedy stačí niečo omnoho jednoduchšie.

Môže to byť aj u vás
V jednej spoločnosti, ktorá prichádzala do styku s citlivými osobnými údajmi, neustále riešili, prečo sa tieto dáta dostávajú von v rozpore s prijatými politikami.

Ukázalo sa, že jeden zo zamestnancov nestíhal svoju prácu cez pracovný čas, tak si citlivé údaje jednoducho prekopíroval a poslal do súkromného mailu, aby na nich mohol pracovať aj doma. Stačil jeden preklep v adrese a únik týchto údajov mohol organizáciu zničiť.

Niekedy je tak riešením aj jednoduché nastavenie procesných opatrení – napríklad, že sa vyhodnotí a obmedzí prístup k rôznym údajom na jednotlivých dôveryhodných pracovníkov.

A preto nezabúdajte
Každý štatutár organizácie by si však mal uvedomiť, že najslabším článkom každej bezpečnostnej stratégie je človek. Ešte skôr ako spoločnosť investuje do rôznych softvérových a hardvérových opatrení na zvýšenie kybernetickej bezpečnosti, mala by sa zamerať na pravidelné školenie personálu.

Reč teraz nie je o bezpečnostných pracovníkoch či zamestnancoch IT oddelení, ale o úplne bežných zamestnancoch. Bez zvyšovania ich povedomia o bezpečnostných hrozbách môže ísť o premrhané prostriedky.

Čísla napovedia
Do základnej výbavy každej organizácie by mali v súčasnosti patriť osvetové aj vzdelávacie aktivity. Práve analýza rizík by vám mala dať odpoveď na to, kde stačí osveta vo forme informácií a ktorí zamestnanci by mali prejsť vzdelávaním.

Medzi atraktívne a efektívne formy patria aj phishingové testy. Robia sa na mieru každej organizácii a pracovným pozíciám a výsledky dávajú veľmi živý a funkčný obraz o kybernetickej odolnosti organizácie. Či už ide o individuálne zručnosti, alebo celkovú odolnosť. Navyše, opakovanými testmi sa dá merať progres a identifikovať priestor na zlepšenie.

Tomáš Hlavsa,
bezpečnostný riaditeľ
Eviden Czech Republic

VAROVANIE

Čo príde po IT kolapse? Už prišlo. Phishingové útoky

Keď v piatok 19. júla nastal rozsiahly globálny výpadok IT systémov, médiá dostali v ospalom letnom čase chutné sústo. Navyše – zažili sme fenomén čiernej labute.

Tento globálny IT kolaps je dokonalým príkladom fenoménu známeho ako čierna labuť.

Bola to neočakávaná udalosť s rozsiahlymi dôsledkami, ktorá má v retrospektíve logické vysvetlenie, no predvídať jej výskyt je takmer nemožné.

Stalo sa
Výpadok spôsobila chybná aktualizáciou bezpečnostného softvéru CrowdStrike Falcon. Táto aktualizácia ovplyvnila kernel-level ovládač, čo viedlo k takzvanej modrej smrtiacej obrazovke na mnohých zariadeniach s operačným systémom Windows.

CrowdStrike okamžite zareagoval a chybnú aktualizáciu stiahol. Napriek tomu však oprava všetkých postihnutých systémov bude trvať určitý čas. Analytici sa už predbiehajú v odhade škôd a padajú miliardové sumy.

Včera bolo neskoro
Podobné incidenty a výpadky ako ten CrowdStrike väčšinou vedú k zvýšenému záujmu útočníkov. Zameriavajú sa na zneužitie situácie nielen u zákazníkov CrowdStrike, ale aj u všetkých ostatných.

Aj napriek tomu, že CrowdStrike rýchlo identifikoval a nasadil opravu vzniknutého problému, hackeri sa chopili situácie a začali vymýšľať nové útoky.

Prakticky už hneď sa vyskytli prípady, keď sa útočníci vydávali za zamestnancov spoločnosti CrowdStrike a prostredníctvom telefonátov sa snažili zmanipulovať obete, aby vykonali určité kroky na svojich zariadeniach.

Blízka budúcnosť
Určite sa nevyhneme phishingovým kampaniam a podvodným e-mailom, ktoré budú vyzerať ako e-maily z podpory CrowdStrike alebo ako oficiálne správy od CrowdStrike alebo iných dôveryhodných entít.

Cieľom e-mailov je oklamať zákazníkov, aby prezradili citlivé informácie alebo poskytli neoprávnený prístup.

Tieto e-maily môžu obsahovať odkazy na podvrhnuté stránky, ktoré vyžadujú zadanie citlivých údajov alebo inštaláciu škodlivého softvéru.

Prečo čítať pozorne
K dnešnému dňu už existuje pomerne rozsiahly zoznam podvodných stránok, ktoré vznikli v rekordne krátkom čase a slúžia práve na tieto účely.

Škodlivé domény obsahujú v sebe názov „crowdstrike“ či „microsoft“, často v kombinácii so štandardnými označeniami help, fix či helpdesk. Očakávame, že budú pribúdať ďalšie podvodné stránky.

Zvyčajný postup
Okrem iného sa budú zločinci pokúšať „predať“ a nainštalovať zaručene fungujúce skripty, ktoré automatizujú vyriešenie problému s CrowdStrike aktualizáciou. Prípadne vám oskenujú počítač, aby zistili, či je u vás všetko v poriadku. To však môže v konečnom dôsledku namiesto opravy viesť k nainštalovaniu malvéru alebo vytvoreniu nového zraniteľného miesta.

Preto je potrebné proaktívnym prístupom a zvýšenou obozretnosťou minimalizovať riziko nadchádzajúcich útokov zneužívajúcich aktuálnu situáciu.

Trest pre sektor
Udalosť nezostala bez ohlasu na burze. Akcie CrowdStrike klesli o 20 percent a finančné trhy reagovali zakolísaním pri technologických značkách.

Incident zároveň ukázal zraniteľnosť závislosti od jednotného IT riešenia a zdôraznil potrebu posilnenia kybernetickej odolnosti kritickej infraštruktúry. Celá udalosť opäť zdôraznila potrebu strategického prístupu k manažmentu IT a zabezpečeniu robustných aktualizačných procesov.

Míľnik dekády
Crowdstrike výpadok má všetky parametre fenoménu čierna labuť, ako ho spopularizoval Nassim Nicholas Taleb. Použil ho na opísanie extrémnych udalostí, ktoré majú tri základné črty.

Sú nepredvídateľné, čiže ich výskyt je nepravdepodobný a takmer nemožný na predpovedanie. Keď sa vyskytnú, majú dramatický a rozsiahly vplyv. Po samotnej udalosti sa často objavujú vysvetlenia, ktoré jej výskyt ospravedlňujú, no tieto vysvetlenia boli predneznáme alebo prehliadané.

V každom prípade – buďte opatrní a nepoľavujte v pozornosti.

Jozef Bálint,
IT bezpečnostný špecialista
ALISON Slovakia