HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 31. JANUÁRA – 2. FEBRUÁRA 2025

Čo nám odhalil kyberútok na kataster?

ANKETA

Január vystavil účet Slovensku o stave kybernetickej bezpečnosti. Či už hovoríme o odbornej alebo širokej verejnosti, dostali sme lekciu. Tento míľnik je už osadený a profesionáli hodnotia jeho význam.

Jaroslav Ďurovka,
riaditeľ, Národné centrum kybernetickej bezpečnosti

Odhalil to, že kybernetickú bezpečnosť, osobitne v organizáciách s takými rozsiahlymi informačnými aktívami, nie je možné podceňovať. Liekom síce môže byť kvalitný systém zálohovania, ale oveľa dôležitejšia je prevencia. A to prevencia komplexná, čo znamená primerane aplikovaná kombinácia bezpečnostných opatrení. Zároveň odhalil, že na Slovensku máme šikovných a ochotných odborníkov na riešenie kybernetických incidentov.

Tibor Szabo,
vedúci Odelenia auditu IT, Všeobecná úverová banka

Veľmi ťažká otázka vzhľadom na málo informácií. Kyberútok možno ukázal na investičný dlh v tejto oblasti, potrebu neustáleho zlepšovania úrovne kyberbezpečnosti aj povedomia spoločnosti. Ale hlavne útok vypovedá o dobe, ktorú žijeme. Kybernetický útok ako jedna z hybridných hrozieb je súčasťou našich životov. Naučme sa dôkladnejšie brániť, uplatňujme dôkladnejšie všetko, čo vieme, lebo máme šikovných ľudí.

Ľubomír Kríž,
manažér kybernetickej bezpečnosti, Slovenská pošta

Incident odhalil, že ešte stále nemáme pod kožou vryté adekvátne reakcie na podobné udalosti vrátane požadovanej komunikácie. A to nielen v kyberútokom zasiahnutej organizácii, ale aj celej komunite kybernetickej bezpečnosti. Všetci vieme, ako by to malo vyzerať, menej je tých, ktorí to vedia aj zabezpečiť. Viacerým hodnoteniam, popri nespornej odbornosti, by pristala tiež malá dávka pokory.

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

Tak ako v hokeji, vo futbale, tak aj tu je zrazu „päť miliónov" kyberbezpečnostných expertov, ktorí presne vedia, čo všetko sa malo urobiť. Po bitke je však každý generál. Nesúďme bez hlbšej znalosti všetkých súvislostí a dôverujme tým, čo to vedia robiť, a držme si všetci palce, aby sa to vrátilo do normálneho stavu čo najskôr. Nikto nevie, kedy sa môže ocitnúť v podobnej situácii, aj keď urobil maximum, čo mohol.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti, Aliter Technologies

Všetko a nič. Myslím si, že pre profesionálov v kybernetickej bezpečnosti neodhalil nič nové. V podstate „len" poukázal na stav mnohých spoločností a inštitúcií, na ktorý dlhodobo poukazujeme vo svojich bezpečnostných analýzach, správach či komentároch. Avšak to, aký mal tento incident vplyv na širokú verejnosť a jej precitnutie ohľadne stavu aktuálnej kybernetickej bezpečnosti, či už v privátnom, alebo vo verejnom sektore – to je už iný príbeh, tam ukázal všetko.

Tomáš Zaťko,
CEO, etický hacker, Citadelo

Je mi to ľúto. Z takéhoto ochromenia sa nedá tešiť. Útok ukázal dvojité zlyhanie štátnej inštitúcie. V bezpečnosti aj v komunikácii. Ako je na tom zvyšok štátu? Ak sa riešenie bezpečnosti nezlepší, ďalšie útoky sú len otázkou času. Tento moment musí byť katalyzátorom zásadnej zmeny v kybernetickej bezpečnosti aj v krízovej komunikácii.

Maroš Rajnoch,
architekt kybernetickej bezpečnosti, Soitron

Dnes už vieme povedať, že bezpečnosť informačného systému ÚGKK SR nebola v najlepšej kondícii. Sme svedkami toho, že vybrané inštitúcie nie sú pripravené na zvládnutie kybernetického útoku. Udalosť nám tiež odhalila, že štát s ťažkosťou komunikuje v kritických situáciach. Po vyšetrení budeme poznať, či išlo o technologický dlh, chýbajúce opatrenie, nevhodné postupy alebo niečo úplne iné.

Peter Matej,
manažér kybernetickej bezpečnosti, eMsec

Pre znalých problematiky kyberútok na kataster potvrdil to, čo vedeli: útoky na kritickú infraštruktúru nemajú dosah len na samotnú obeť. Obeťami sa stávajú aj sekundárne a terciárne subjekty závislé od služieb obete. Že schopnosť zvládnuť incident si vyžaduje tím skúsených ľudí, vysoké nasadenie, dostupné zálohy a jasnú komunikáciu. Prekvapením pre mňa bol exponenciálny nárast množstva „odborníkov".

Eduard Hertl,
obchodný riaditeľ, skupina CYLLIUM

Vzhľadom na vplyv útoku na bežný život si musíme uvedomiť, že kybernetická bezpečnosť sa týka nás všetkých, a musíme k tejto téme pristupovať zodpovedne. Odporúčam spracovať a pravidelne testovať komplexné plány kontinuity činností pre efektívne zvládnutie krízových situácií.

Ivan Kopáčik,
bezpečnostný expert, Gordias

Aktuálne kyberútoky dokazujú, že nemenej dôležitá ako technická pripravenosť je aj spoločenská rovina. Ukazuje sa, že pokrivkáva vecná a informačne adekvátna komunikácia zo strany štátu voči verejnosti. Spolupráca (nie improvizácia!) všetkých zainteresovaných strán má tiež priestor na zlepšenie. A v neposlednom rade je dôležité vyvodiť poučenia do budúcnosti a prijať nápravné opatrenia.

Benjamin Würfl,
obchodný zástupca Eviden, Eviden Slovakia

Útok na kataster jasne ukázal stav IT bezpečnosti, ktorý na Slovensku pretrváva. Zároveň poskytol priestor a šancu tieto nedostatky odstrániť tým, ktorí na ne vo svojich organizáciách upozorňovali, ale neboli vypočutí. Zvýšime našu pozornosť na zraniteľnosti, patchovanie alebo vzdelávanie IT?

Jaroslav Ušiak,
prodekan pre vedu a výskum, Fakulta politických vied a medzinárodných vzťahov UMB Banská Bystrica

Tento útok na kataster odhalil, že kybernetická bezpečnosť Slovenska pripomína domček z kariet – na prvý pohľad stabilný, ale stačí malý vánok a všetko sa rozsype. Ukázal nám, že v digitálnom svete sa neoplatí spoliehať na náhodu, a dnes už aj kataster zistil, že pravidelné zálohovanie nie je možnosť, ale nutnosť. Ale za akú cenu...

Tomáš Hettych,
viceprezident, ISACA

Ukázali sa slabiny v pripravenosti na krízové situácie. Incident nestačí riešiť len technologicky, ale občas je oveľa dôležitejšie o ňom správne komunikovať. Súčasťou krízových plánov by mal byť aj efektívny plán komunikácie.

Pavol Vrabec,
manažér kybernetickej bezpečnosti, Univerzitná nemocnica Martin

Úspešný útok na kataster demonštroval, že kyberbezpečnosť sa bez výnimky dotýka každého z nás a je potrebné o tom hovoriť, a to nielen vtedy, keď sa incidenty vyskytnú. Proti kyberútočníkom nie je jednoducho nikto imúnny. Verím, že tento incident dal mnohým zainteresovaným osobám podnet na zamyslenie. Dúfam, že útok bude transparentne vysvetlený, aby sme sa z neho mohli poučiť v budúcnosti.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť, Západoslovenská energetika

Obávam sa, že kyberútok odhalil realitu stavu kybernetického prostredia vo väčšine verejných inštitúcií na Slovensku. Veľmi chcem veriť, že to bolo skutočné varovanie pre mnohých zodpovedných aj v iných organizáciách, a začnú konať. Pre verejnosť je to praktická ukážka toho, čo znamená narušenie princípu CIA – dôvernosti, integrity a dostupnosti dát. A tam sa už končia všetky vtipné a amatérske odporúčania.

Július Selecký,
senior technický špecialista, ESET

Laickej verejnosti ukázal, aký môže mať kybernetický útok vplyv na chod štátu a bežných občanov. Slovensko sa pýši kvalitnou legislatívou v oblasti kybernetickej bezpečnosti, ktorá je uznávaná aj v medzinárodnom kontexte. Avšak na to, aby táto legislatíva plnila svoj účel a prinášala reálne výsledky, je nevyhnutné, aby sme ju nielen deklarovali, ale aj dôsledne dodržiavali v praxi.

Róbert Mramúch,
manažér oddelenia kybernetickej bezpečnosti, MH Teplárenský holding

Fatálna výpoveď o zlom stave základných služieb štátu a o tom, ako kolektívne nevyžadujeme zodpovednú správu vecí verejných. Oblasti, ktoré majú byť výkladnou skriňou, sú dlhodobo zanedbávané a finančne aj odborne podvyživené. Ale máme šťastie – z EÚ prišla smernica NIS2, ktorá prikazuje nápravu a zaväzuje štatutárov konať. Držím Slovensku palce, čaká nás ešte veľmi veľa práce.

Jaroslav Oster,
predseda správnej rady, Preventista.sk

Potvrdila sa realita, o ktorej sa sa vo svete cybersec hovorí už dávno – podceňovanie všetkých úrovní riadenia bezpečnosti. Ukázala sa dôležitosť kvalitne nastaveného reputačného manažmentu, vývoj prvých dní potvrdil, že zle nastavená krízová komunikácia dokáže vytvoriť podhubie pre vznik teórií a „overených právd" všetkého druhu. Na strane druhej táto udalosť otvorila takú prepotrebnú diskusiu o stave KB štátnych a samosprávnych inštitúcií.

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

Pre mňa z tohto incidentu neplynie ponaučenie, ale potvrdenie faktu, o ktorom dávno viem: že od predsedu vlády až po traktoristu Joža v krčme v Hornej Dolnej tu máme samých odborníkov na kybernetickú bezpečnosť. A na hokej. A na makroekonómiu. Žiaľ, k veciam, ktorým absolútne nerozumejú, sa vyjadrujú aj inak príčetní ľudia. Možno sa to stane aj v tejto ankete. Nepotrebujete kvalifikáciu. Len názor.

Richard Kiškováč**,**
generálny riaditeľ, Elkan

Odhalil, že byrokraticko-akademická bezpečnosť sa iba málo stretáva s realitou v praxi a žije si svoj virtuálny svet. Ukázal aj to, že nasávanie právomocí sa deje bez akejkoľvek zodpovednosti za konečný výsledok a napriek komplexnosti neexistuje žiadna koordinácia, iba zmes vlastných záujmov a nekonečného alibizmu. Zistili sme, že tím nevyhrá ligu ani pod hrozbou sankcií, ani tak, že zakúpime zlaté kopačky hráčom, ktorí neexistujú.

Tomáš Valenta,
riaditeľ, Check Point Software Technologies na Slovensku

Nemyslím si, že kyberútok niečo odhalil. Mojim kolegom, mne a ďalším bezpečákom potvrdil to, čo vieme a o čom neustále hovoríme. Pre firmy, inštitúcie, ich riaditeľov a majiteľov, ale aj pre verejnosť je to ďalší varovný prst a impulz k posunu do reálnych riešení. Vlastne jednu vec to predsa len odhalilo – ako nie sme pripravení na tieto situácie z hľadiska komunikácie. Tá bola po útoku žalostná.

Jana Puškáčová,
vedúca špecialistka IT bezpečnosti, Slovnaft

Žiadna kampaň na budovanie bezpečnostného povedomia by nemala taký dosah ako kyberincident v spojitosti s katastrom. Bežní občania zaradili do slovníka slovíčko ransomvér a na vlastnej koži zažili jeho dôsledky. Útočníci získali argumenty, prečo zálohovať, plátať starý softvér a testovať obnovu dát zo zálohy. Biznis zistil, aký význam má komunikácia a načo je dobré riadenie kontinuity podnikania. Bezpečáci vedia zdôvodniť, prečo treba plány na obnovu po katastrofe a aký môže byť prínos procesu, ako reagovať na kybernetický incident. A top manažment sa presvedčil, že správna otázka naozaj nie je „či", ale „kedy" by sa organizácia mohla stať obeťou kybernetického útoku.

Maroš Trnka,
vedúci odboru IT, Vodohospodárska výstavba

Ak vynecháme časť so šifrovaním a za predpokladu, že útočníci boli v katastri dlhšie, tak mohli (útočníci) napríklad manipulovať s údajmi o vlastníctve a meniť ich, čo by mohlo v extréme viesť napríklad k podvodným predajom nehnuteľností či pozemkov nezistených vlastníkov, a to by bol celkom iný typ problému. Prečo niekto útočí na štát, kde je predpoklad na zaplatenie výkupného minimálny? Uvidíme.

Roman Varga,
manažér kyberbezpečnosti, Dôvera, zdravotná poisťovňa

Odpoveď je rozprávka Cisárove nové šaty. Kyberodborníci dlhodobo upozorňujú, že cisár je nahý! Žiaľ, ten náš „cisár" sa dlhodobo obklopuje neschopnými radcami. Ak by to bral vážne, systematicky by sa budovala kyberobrana v tomto našom štáte a zmenšoval by sa technologický dlh. Na problémy v sektore zdravotníctva upozorňujeme už dlhodobo. Podobnú skúsenosť ako kataster s ransomvérovým útokom majú až dve percentá ambulancií.

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

Kyberbezpečnosť je stále podceňovaná, hoci sa neustále ukazuje ako kľúčová pri ochrane dát. Rovnako tak aj kataster narába s citlivými údajmi, ktoré mohli alebo môžu byť zneužité. Ďalším „kameňom úrazu" bola aj následná nedostatočná komunikácia smerom k verejnosti. Žiaľ, vznikali tak rôzne teórie a vynorilo sa množstvo „odborníkov" na kybernetickú bezpečnosť, predovšetkým v oblasti zálohovania.

Ako sa dnes útočí ransomvérom

TRENDY

Ransomvérové útoky prebiehajú od jednoduchých emailových príloh až po sofistikované služby na čiernom trhu.

Kybernetický zločin sa transformuje na výkonný aparát, ktorý zasahuje všetky oblasti ekonomiky a života. FOTO: DREAMSTIME

Mnohí si pod ransomvérovým útokom predstavujú jednoduchý scenár: niekto otvoril prílohu v e-maile, ktorá obsahovala nebezpečný spustiteľný súbor. Po kliknutí na súbor sa začne šifrovacia rošáda. Dnes je však situácia omnoho zložitejšia.

Zločinecký ekosystém

Ransomvérová scéna prešla za posledné roky dramatickým vývojom. Namiesto jednoduchých „klikačiek“ na škodlivé prílohy sa čoraz častejšie stretávame s premyslenými postupmi, ktoré môžu prebiehať celé týždne.

Kyberzločinci totiž vybudovali dynamické a agresívne ekosystémy. Existuje dodávateľský reťazec kyberkriminálnikov, kde sa predáva a kupuje prístup, zdieľajú sa informácie o potenciálnych cieľoch a ich zraniteľnostiach a využívajú sa profesionálne nástroje. Ransomvérové kampane tak fungujú ako moderný biznis.

Áno, ale

Áno, phishing a podvodné prílohy stále predstavujú bežný a veľmi častý spôsob šírenia, respektíve kompromitácie ransomvérom.

Je však dôležité uvedomiť si, že súčasné ransomvérové kampane často využívajú aj sofistikovanejšie techniky. Sú to útoky na neaktualizované a zraniteľné systémy, zneužitie protokolov na diaľkovú správu zariadení či nákup odcudzených prihlasovacích údajov.

Škodliví aktéri často vykonávajú laterálne pohyby v sieti, pričom postupne získavajú najvyššie systémové oprávnenia a kradnú citlivé informácie. Dá sa teda povedať, že operácie sa tak viac podobajú aktivitám skupín pokročilých hrozieb APT (Advanced Persistent Threat) skupín, kde sa útočníci snažia zostať v sieti čo najdlhšie neodhalení.

Služba ako každá

Jedným z hlavných dôvodov rapídneho nárastu množstva ransomvérových útokov je služba Ransomware-as-a-Service (RaaS), keď autori škodlivého kódu poskytujú platformu iným kriminálnym skupinám. Títo „partneri“ potom vykonajú samotný útok a delia sa o zisky.

Tento obchodný model umožňuje i menej skúseným aktérom prevádzkovať ransomvérové kampane vo veľkom meradle.

Navyše existuje celý rad zločincov, ktorí sa špecializujú výhradne na prienik do sietí – či už cez phishing, útoky hrubou silou na heslá, alebo zneužitie zraniteľností. Takto získaný prístup následne na čiernom trhu predávajú takzvaní Initial Access Brokeri.

RaaS partneri potom už nemusia investovať do prelomenia obrany. Stačí im kúpiť si hotový prístup, napríklad administrátorské účty alebo VPN prístup do firemnej siete, a rovno nasadiť ransomvér.

> SÚČASNÝ OBCHODNÝ MODEL UMOŽŇUJE I MENEJ SKÚSENÝM AKTÉROM PREVÁDZKOVAŤ RANSOMVÉROVÉ KAMPANE VO VEĽKOM MERADLE.
>
> **Michal Srnec,** vedúci oddelenia informačnej bezpečnosti Aliter Technologies

Trojitá hrozba

Ak ste si mysleli, že šifrovanie je to najhoršie, čo sa môže stať, tak ste na veľkom omyle. Kedysi útok spočíval len v zneprístupnení dát – typicky to bolo zašifrovanie súborov, a potom nasledovala požiadavka na výkupné za znovu sprístupnenie dát, teda dešifrovanie.

Dnes útočníci dáta aj odcudzia, aj sa vyhrážajú ich zverejnením. Navyše niektoré skupiny pridávajú multi-extortion taktiky, aby zvýšili nátlak na obeť. Vyhrážajú sa ďalšími DDoS útokmi či kontaktovaním zákazníkov napadnutej spoločnosti.

Dáta nepustia

Podľa reportu Data Breach Investigations spoločnosti Verizon za rok 2023 bol ransomvér súčasťou takmer štvrtiny skúmaných narušení bezpečnosti (24 percent). Medzi najčastejšie vektory prieniku patrili phishingové e-maily, zneužitie zraniteľností a odcudzené prihlasovacie údaje.

Spoločnosť CrowdStrike v Globálnom reporte hrozieb 2023 zdôrazňuje, že útočníci často využívajú prístupy sprostredkované Initial Access Brokermi a len čo získajú prístup do systémov či sietí obete, vedia ho v priebehu niekoľkých hodín rozšíriť na celú firmu.

To, že ransomvér stále patrí medzi najčastejšie formy útokov, potvrdzuje aj správa IBM Security X-Force Threat Intelligence Index 2023.

Nie sme bezbranní

Kombináciou technických opatrení a budovaním bezpečnostnej kultúry môžu firmy výrazne znížiť riziko úspešného útoku. Opatrenia ako segmentácia siete, aktualizovanie systémov, multifaktorová autentifikácia sú dlhoročným základom, ku ktorému sa pridávajú školenia, simulované phishingové testy a table-top cvičenia.

Kľúčom je rozpoznať, že najlepšou obranou je proaktívny prístup – nepodceniť základné opatrenia, pristupovať ku kybernetickej bezpečnosti systematicky a mať jasné plány, ako postupovať pri incidente.

RIEŠENIE

Obnova po ransomvéri: prečo to nie je len o zálohách

Incident katastra upriamil pozornosť verejnosti na kybernetickú bezpečnosť.

Mnohé z diskusií sa zjednodušujú na otázky týkajúce sa záloh: Sú vôbec dostupné? A ak áno, kde sú a aké sú?, a času: Prečo obnova trvá tak dlho a kedy bude všetko späť? Ako odborníci na kybernetickú bezpečnosť máme bohaté skúsenosti z vyšetrovania aj veľkých ransomvérových incidentov a dobre vieme, že odpovede na tieto otázky nie sú jednoduché.

Ransomvérové útoky sú komplexné a obnova často trvá mesiace – prečo?

Ransomvér

Pri ransomvérovom útoku si napadnutá organizácia často všimne, že sa niečo deje, až keď sa útočník rozhodne „odkryť karty“. Zvyčajne to robí až po tom, ako sa vopred dôkladne oboznámi s infraštruktúrou, ovládne ju, exfiltruje dáta a zabezpečí si aj „zadné dvierka“. Aby vedel útok spustiť znova.

V praxi to vyzerá tak, že prístup k systémom je zablokovaný, vaše dôležité dáta sú v rukách útočníka – vy máte dáta zašifrované a čelíte žiadosti o výkupné.

Obnoviť zálohu nestačí

Obnovenie funkčných záloh organizáciu vráti do stavu „tesne“ pred spustením šifrovania. V tom čase však už útočník vaše systémy ovládal. Bez dôkladnej kontroly záloh preto hrozí, že útok vykoná znova.

Obnova sa preto začína pripraveným a aktuálnym Incident response plánom (IRP).

Prvé minúty po útoku

Ešte neviete, čo všetko bolo zasiahnuté. Prioritou je rýchlo zabrániť ďalšiemu šíreniu škôd, a preto izolujete sieť. Jednotlivé segmenty odpojíte od internetu a od seba navzájom. V prípade cloudovej infraštruktúry spravíte „snapshot“ aktuálneho stavu a zamedzíte prístup.

Prvé hodiny „po“

Začína sa operácia, ktorú ste si vopred dobre premysleli a máte ju zdokumentovanú v IRP. Zvolávate Incident response (IR) tím, ktorý bude celý proces riadiť a riešiť. Súčasne sa začína krízová komunikácia – o incidente premyslene informujete zamestnancov, klientov i partnerov, regulátorov, OČTK, prípadne médiá, pretože chaos všetko iba zhorší.

Pre IR tím musíte rýchlo „zohnať“ čisté zariadenia, vybaviť ich potrebnými nástrojmi, dôkladne „hardenovať“ a ochrániť, aby sa pri práci v infikovanom prostredí minimalizovalo riziko ďalšej infekcie. Rovnaký postup sa týka základnej infraštruktúry, na ktorej budú fungovať.

Začína sa mapovanie škôd a zisťuje sa, ktoré systémy, dáta a servery boli zasiahnuté. Zbierajú sa dôkazy, všetko sa dokumentuje a uchováva pre ďalšie forenzné vyšetrovanie. Stanovujú sa priority a rozhoduje, ktoré systémy alebo dáta majú prednosť.

Všetky prístupové údaje sa okamžite nahrádzajú novými, silnými a unikátnymi heslami. Začína sa „hunting“ a IR tím pátra po známkach prítomnosti útočníka.

Počas prvých dní „po“

V nasledujúcich dňoch sa snažíte rýchlo obnoviť prevádzku, ale zároveň zabezpečiť, aby sa incident hneď nezopakoval. Prakticky od nuly budujete novú, bezpečnú sieťovú infraštruktúru. Dôsledne dbáte na segmentáciu a princíp minimálnych nevyhnutných prístupov (least privilege).

Súčasne sa v samostatnej časti infraštruktúry začína obnova systémov. Zálohy sa kontrolujú na prítomnosť škodlivého kódu a dochádza k postupnej obnove dát, operačné systémy a aplikácie sa nanovo inštalujú a dôkladne „hardenujú“. Na nové systémy nasadzujete bezpečnostné nástroje a po celý čas monitorujete, čo sa v nich v reálnom čase deje. Až po dôslednej kontrole presúvate systémy do pripravených nových segmentov.

Paralelne prebieha dôkladná forenzná analýza, ktorej cieľom je identifikovať vektor útoku a zistiť, aké zraniteľnosti boli zneužité. Zistenia použijete na zlepšenie svojej obrany a reakcie v budúcnosti. Nezabúdate na krízovú komunikáciu s relevantnými stranami.

Ďalšie týždne a mesiace

Postupne sa posúvate v procese obnovy. Systémy a služby, ktoré už prešli obnovou, dôkladnou kontrolou a testovaním, uvádzate späť do prevádzky. Každý krok robíte systematicky. Obnova preto trvá dlho – a v realite závisí od mnohých faktorov. No pri väčšej organizácii so zložitými informačnými systémami (ako napríklad kataster) je určite reálne uvažovať o mesiacoch. V horizonte týždňov môžeme očakávať obnovenie čiastkových služieb.

Napríklad pri rozsiahlom ransomvérovom útoku na írsky zdravotnícky systém v roku 2021 trvala obnova polovice systémov štyri týždne, zvyšok sa obnovoval ďalšie tri mesiace.

P. S. Dôležité!

Nezabúdajme, že aj IR tím tvoria ľUDIA. Každý z nich musí niekedy jesť, piť, nadýchať sa čerstvého vzduchu či vyspať sa. Len tak dokážu títo experti podávať špičkový výkon. Bez fyzického a psychického odpočinku riskujete ich vyčerpanie a prudké zníženie kvality práce. A verte mi, bez nich to „dáte“ asi len ťažko.

Martin Lohnert, riaditeľ centra kybernetickej bezpečnosti void SOC od Soitronu

PORADŇA

Takto to robím ja

Koncom roka ma oslovil jeden z majiteľov firmy Chrum&Chrum a ponúkol mi pozíciu manažéra kybernetickej bezpečnosti. Firma vyrába proteínové tyčinky a špeciálnu výživu a patrí medzi lídrov na trhu. Ponuku som prijal, dnes mám za sebou prvý mesiac.

Moja úloha ako manažéra kybernetickej bezpečnosti je jasná – zabezpečiť, aby všetko od receptov až po zákaznícke dáta zostalo chránené a proces výroby a distribúcie bežal ako hodinky. Na prvý pohľad to znie jednoducho, ale veľmi rýchlo som pochopil, že mám pred sebou veľkú výzvu.

Získavam spojencov

Prvé dni som spoznával, ako firma funguje. Prešiel som si výrobné haly, videl som, ako sa miešajú ingrediencie a rozprával sa s tímami na všetkých úrovniach. V každej diskusii som sa pýtal rovnako: „Čo je pre vás najdôležitejšie? Čo by vás zastavilo v práci?“ Odpovede mi pomohli pochopiť, na čom vo firme naozaj záleží. Od začiatku mi je jasné, že kyberbezpečnosť je tu novinka, bude čo robiť.

Diskusia s vedením

Hneď na začiatku som išiel za generálnym riaditeľom. Vedel som, že ak nezískam jeho podporu, skončil som. Vysvetlil som mu, že ako štatutár nesie zodpovednosť za ochranu údajov aj za plynulosť výroby. Ak budeme PZS – prevádzkovateľ základnej služby, tak tú zodpovednosť má dokonca trestnoprávnu. Na stole som mal plán činností na rok a ukázal som mu, že bezpečnosť nie je len náklad, ale investícia, ktorá môže zachrániť firmu pred katastrofou. Máme spoločný cieľ, aby firma vyrábala aj zajtra. Po chvíľke ticha mi podal ruku: „Andrej, máš moju podporu. Ideme na to.“

Bezpečnostný výbor

Je jasné, že bez zapojenia manažmentu sa nič nepohne. Na porade som navrhol založenie bezpečnostného výboru. Tím som poskladal z ľudí, ktorí vedia, ako firma žije – od IT cez výrobu až po financie. Generálny riaditeľ súhlasil, že bude predsedom. Výbor bude platformou na diskusiu o rizikách, návrhoch riešení a prijímaní strategických rozhodnutí v kyberbezpečnosti. Stretávať sa budeme mesačne a vždy vyhodnotíme, čo sa podarilo a kde máme rezervy. Na prvom stretnutí výboru som im predstavil plán konkrétnych aktivít na každý mesiac.

Začiatok cesty

Viem, že budovanie bezpečnosti nie je o zložitých technológiách, ale o správnych základoch. Ak vedenie pochopí význam bezpečnosti, tieto hodnoty prenesú aj na zamestnancov. Postupne tak môžeme zavádzať konkrétne opatrenia – od analýzy rizík po implementáciu ochranných technológií.

Chrum&Chrum má pred sebou dlhú cestu, ale verím, že to zvládneme. Spolu môžeme vybudovať prostredie, kde budú zamestnanci pracovať bez obáv, kde si zákazníci môžu byť istí, že ich údaje sú v bezpečí a akcionári vedia, že chránime ich investície.

Andrej Mišura, manažér kybernetickej bezpečnosti

Úplnú verziu poradne nájdete v online vydaní v sekcii Kybernetická bezpečnosť