HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
22. – 24. MARCA 2024

Odborná spolupráca

NBÚ

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Incident má v sebe ničivý adrenalín

Za posledné obdobie sú bezpochyby tie najzávažnejšie incidenty spojené s ransomvérom. FOTO: DREAMSTIME

TÉMA

Kybernetický bezpečnostný incident potrápil už nejednu organizáciu v našich končinách. Niektorí to priznávajú, iní sa trápia potichu. Dosahy sú bolestivé, stoja peniaze, čas aj reputáciu.

Kameru na monitorovanie vstupu sanitiek má asi každá nemocnica na Slovensku. A podobné kamery sú v stovkách firiem.

Zjednodušuje to kontrolu a prístup cez internet môžu využívať bezpečáci aj iní zamestnanci. Aj útočníci.

Taká malá chybička

Ak má kamera alebo jej softvér chybu, pre kybernetických zločincov je to zraniteľnosť, ktorú vedia zneužiť. A tak sa aj v tejto slovenskej nemocnici stalo.

Útočník využil ako „vstupnú bránu“ do vnútornej siete nemocnice kompromitovanú kameru a prostredníctvom nej nasadil nástroje a techniky na prieskum. Bezpečnostný tím spozornel, keď monitorovacie zariadenia zachytili nezvyčajnú aktivitu.

„Útočník sa snažil rýchlo identifikovať otvorené porty a zraniteľné služby na zariadeniach, ktoré sú pripojené k vnútornej sieti,“ opisuje útok člen tímu.

Máme incident!

Rozsah prístupu útočníka sa zisťoval vyšetrovaním, analýzou sieťovej prevádzky a aktuálnym nastavením sieťových zariadení. Kvôli hľadaniu a overovaniu možných napadnutých systémov bola prevádzka nemocnice obmedzená dvanásť hodín. Zasiahnuté systémy sa museli dočasne vypnúť, čo malo vplyv na operácie a zdravotnú starostlivosť.

Po prvotných nápravných opatreniach bola prioritou transparentná komunikácia. Vedenie informovalo zamestnancov o incidente, jeho možnom vplyve na nemocničné služby a zároveň aj o opatreniach na ochranu ich údajov. A okamžite pridalo odporúčania na zvýšenie kyberhygieny.

Najhorší scenár

Pýtate sa, čo by sa stalo, ak by napríklad bezpečnostný tím zlyhal? Útočník by získal prístup do celej siete, mohol by ukradnúť dáta pacientov a zamestnancov, zašifrovať počítače a požadovať výkupné. Informačný systém by padol.

„Nedostupnosť systémov už viac než jeden deň pri väčšej nemocnici je kritický,“ varuje audítor kybernetickej bezpečnosti Michal Ďorda auditori.it. Hrozí chaos a panika, časť prípadov treba určite odkloniť. Nemocnica musí prejsť na papierovú dokumentáciu a obnova systémov by pravdepodobne trvala minimálne desať dní.

Preto medzi inými opatreniami zaviedli v nemocnici aj „prísnejšie politiky pre IoT zariadenia, ktoré sú často prehliadané v bezpečnostných stratégiách.“

Skúška ohňom

Najčastejšie chyby pri riešení incidentu sú panika a chaos. V tom sa profesionáli zhodujú. Takmer likvidačné je, ak sa podcení systém zálohovania a neexistuje krízový plán. Takto stručne zhŕňa skúsenosti za dve dekády bezpečnostný architekt a konzultant Martin Fábry, ktorého už zavolali k nejednému incidentu.

Je to až neuveriteľné, ak ide o incident v chemickej továrni so stovkami zamestnancov. Prežitie firmy tu závisí od vysoko sofistikovaného systému na riadenie a monitorovanie chemických výrobných procesov, ktoré zaisťujú výrobu produktov pre mnoho krajín.

Piatok večer

V roku 2022 sa vo firme, nazvime ju Victim, odohral závažný kybernetický incident v kritickom riadiacom systéme. Kľúčoví pracovníci sa pobrali na víkend a ítečkár, ktorý mal pohotovosť, zaevidoval nefunkčnosť ekonomického systému.

> Najčastejšie chyby pri riešení incidentu sú panika a chaos.
>
> **Martin Fábry,** bezpečnostný architekt a konzultant

Skupina nie veľmi šikovných kybernetických pirátov získala prístup k sieti prostredníctvom otvoreného portu do internetu. Bol „tajný“ a mal slúžiť vyvoleným administrátorom na pohodlnú vzdialenú správu IT systémov.

Cez tento nezabezpečený kanál útočníci odoslali škodlivý softvér k obeti a zašifrovali ním kritické IT systémy, ktoré nepriamo, ale okamžite ohrozili výrobné procesy.

Nebezpečenstvo výbuchu

Dôsledkom útoku bola séria výpadkov IT systémov a dočasné odstavenie výroby vo vysoko výbušnom prostredí. Interná reakcia na incident bola chaotická a firma povolala externých špecialistov. Kľúčovým pri minimalizovaní následkov sa stal až krízový tím a rýchla reakcia.

„Našťastie, útočníci nerozumeli prevádzkovým technológiám, aby mohli vykonať devastujúci útok,“ hodnotí incident Martin Fábry. V každom prípade Victim bola paralyzovaná na niekoľko týždňov, a to nielen ekonomicky, ale aj sociálne, pretože zamestnancov kybernetický útok značne fyzicky a mentálne vyčerpal.

Hrá sa o čas

Detekcia a analýza sú len prvými krokmi, aby sa zmenšili dosahy incidentu a odstránili zraniteľnosti alebo chyby. Tu je najdôležitejších prvých 48 hodín.

Skutočný boj, či už z pohľadu ľudských zdrojov, alebo financií, nastáva potom. Obnova systémov, zmeny konfigurácie a zabezpečenia infraštruktúry si môžu vyžiadať stovky hodín. „Zálohy sú mnohokrát fuč, poprípade poškodené útokom. Ide sa 24 hodín denne, nespí sa,“ hovorí skúsený odborník na kybernetickú bezpečnosť Roman Čupka.

Nezažiješ, neuveríš

Pokiaľ organizácia nemá k dispozícii kvalitný tím s „veliteľom“ riešenia incidentu, hrozí riziko kumulovania chýb. A nečudo. Veď do obnovy infraštruktúry a informačných systémov vstupuje množstvo dodávateľov a otázky zamestnancov, zákazníkov a médií neustávajú.

Tím kvalitných „incident responderov“ musí mať skúsenosti s riešením incidentov na pravidelnej báze, silné technické znalosti, zručnosti v komunikácii, projektovom riadení, znalosť s konfiguráciou IT systémov, forenznou analýzou, nasadzovaním nápravných opatrení, zabezpečením nastavovania správnych politík a testovaním odolnosti infraštruktúry. A to všetko v hybridnom prostredí a počas riešenia incidentu.

Pripravujte sa posadnuto

Ak sa náprava po incidente neurobí dostatočne kvalitne a nechajú sa nezabezpečené zadné dvierka či konfiguračné chyby, o pár mesiacov sa môže čierny Peter ujsť organizácii znova. Nie je ani výnimkou, že pri nasledujúcom incidente väčšie organizácie vymenia celú IT infraštruktúru. Tie menšie zas ukončia činnosť. Proste ich to zruinuje.

Martin Fábry pripomína aj nevyhnutné kroky na zlepšenie celkovej kybernetickej bezpečnosti. Zahŕňa to revíziu a aktualizáciu bezpečnostných protokolov, zvýšenie povedomia o kybernetických hrozbách a investície do moderných technológií na prevenciu a detekciu útokov.

Pre zmiernenie dosahov potenciálnych incidentov Roman Čupka odporúča posúdenie odolnosti organizácie v rámci implementácie bezpečnostných opatrení. Táto investícia sa vyplatí, pretože ak nastane incident, rapídne sa znížia časové a finančné nároky na jeho riešenie.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 22. – 24. MARCA 2024

Našli bod zlomu, odkiaľ sa nedá vrátiť

ANKETA

Čo také sa v živote stáva, aby sa človek začal vážne zaoberať kybernetickou bezpečnosťou? Bezpečnostní profesionáli hovoria o svojich rozhodnutiach a motivácii, delia sa o skúsenosti a ich inšpirácia sa dotýka aj nás.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti
Aliter Technologies

Zaujímanie sa o kybernetickú bezpečnosť, respektíve cesta k nej je pre každého unikátna. Pre mňa to bol zmysel pre detail a túžba rozlúsknuť, ako IT veci fungujú za oponou. Pre niekoho to však môže byť kariérny zlom, keď je do tejto pozície doslova „vhodený“. Pre iných zasa postupná cesta premeny, na konci ktorej je profesionál. Tak či onak sa v komunite kybernetickej bezpečnosti tešíme z nových kolegov, akoukoľvek cestou sa k nám pridajú.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Kybernetická bezpečnosť je pre mňa náročná práca na vysokej úrovni. Vždy bola a bude súčasťou IT riešení a života firiem. Dokonca aj predtým, ako sa stala atraktívnou agendou, ku ktorej sa dnes hlásia aj podivuhodné subjekty. Kyberbezpečnosť považujem za organickú súčasť nášho portfólia už jednu dekádu a okrem toho nás to extrémne baví.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Ako bankový informatik som sa s požiadavkou na ochranu dát stretával už s rozvojom počítačových sietí. Štart mojej bezpečáckej kariéry však vyvolala až novelizácia zákona o bankách pred tridsiatimi rokmi. Tá donútila banky zaviesť procesy informačnej bezpečnosti. Aj táto skúsenosť podčiarkuje, že regulácia je štandardne dôvodom, prečo sa organizácie zaoberajú bezpečnosťou. Škoda, že dôvodom nie je uvedomenie si rizík.

Michal Sekula,
bezpečnostný konzultant
Eviden Slovakia

Pôvodne som sa venoval technologickým službám s vysokou dostupnosťou, no neustále som sa stretával s otázkou ich bezpečnosti. Otázka, ako sa proti nim efektívne brániť, ma zaujala natoľko, že som už pri kybernetickej bezpečnosti zostal. Kyberbezpečnosť je sama osebe veľmi zaujímavá téma a zároveň sa čiastočne prekrýva s mojím predchádzajúcim zameraním, takže voľba bola jasná.

Ivan Kopáčik,
bezpečnostný expert
Gordias

Pred 30 rokmi, keď som popri štúdiu začínal v kyberbezpečnosti, to bola možnosť zažiť sci-fi v realite. Zistil som, že virtuálny priestor a kyberútoky nie sú len na filmovom plátne, ale aj v realite. Bol to nový svet a mohol som si vybrať, či budem na strane „dobrých“ alebo „zlých“. Pre začínajúceho systémového administrátora to bolo, samozrejme, jasné.:)

Marián Illovský,
audítor kybernetickej bezpečnosti
Auditori.it

Vidím minimálne dve životné situácie, keď sa každý človek začne, teda mal by sa začať vážne zaoberať kybernetickou bezpečnosťou. Po prvé, keď sa sám stane terčom alebo obeťou kybernetického útoku. Druhým vážnym dôvodom je, keď ako rodič zodpovedá za kybernetickú bezpečnosť svojich detí.

Dominik Procházka,
riaditeľ odboru bezpečnosti
AGEL SK

Pre mňa osobne je to nekonečná zvedavosť, túžba pomôcť a vzdelávať sa. Ako systémy fungujú? Ako spolu komunikujú? Ako môžem ochrániť celú sieť a sledovať, čo sa deje?

Miroslav Chlipala,
riadiaci partner
BCH Advokáti Chlipala

Prelomový moment nastal, keď som priamo zažil, ako kybernetický útok spôsobil klientovi problémy a škody. Strata dát a poškodenie reputácie boli nepríjemné a bolestivé. Staré stratégie už nestačili na ochranu v tomto dynamickom prostredí. Začal som sa obávať o bezpečnosť vlastných aj klientskych dát a uvedomil som si potrebu konať proaktívne a chrániť ich pred kybernetickými hrozbami.

Pavol Vrabec,
manažér kybernetickej bezpečnosti
Univerzitná nemocnica Martin

Úprimne povedané, kybernetickej bezpečnosti som sa začal venovať takpovediac full time po tom, ako som u zákazníka riešil ransomvérový útok. A neboli to teda príjemné chvíle. O to viac, že útočník sa snažil zašifrovať aj zálohy dát. Na druhej strane to bola situácia, z ktorej som si odniesol jedinečné skúsenosti a zároveň motivačný moment, na základe ktorého som sa začal tejto téme intenzívne venovať.

Henrich Šnajder,
manažér IT bezpečnosti
Orange Slovensko

Začal som pracovať v kyberbezpečnosti a stalo sa mi to skutočnou životnou výzvou. Každý deň je novou príležitosťou objavovať a porozumieť širokej škále bezpečnostných aspektov. Vzdelávanie a bádanie po nových hrozbách ma stále posúvajú vpred a každým krokom som bližšie k skutočnej odbornosti v tomto dynamickom prostredí. Je to povolanie, ktoré ma napĺňa zmyslom a vášňou pre ochranu digitálneho sveta.

Richard Kiškováč,
generálny riaditeľ
Elkan

Z mojich skúseností je asi najväčším impulzom pre kariéru v kybernetickej bezpečnosti dobrý projekt, ideálne „na zelenej lúke“. Aj spolupráca s inšpiratívnym lídrom či s odborníkom s komplexnými skúsenosťami môže znamenať výrazný kariérny posun a vzbudiť v špecialistovi potrebnú mieru nadšenia pre niektorú oblasť kyberbezpečnosti. Môže to byť taktiež nová pozícia so silnou podporou vrcholového manažmentu.

Roman Čupka,
hlavný konzultant
Progress a CSO Istrosec

Bod zlomu by som rozdelil na dve časti. Ta prvá má súvis so životnou filozofiou a s holistickým prístupom k bezpečnosti ako takej, ktorá je v niektorých jedincoch silne evolučne zakorenená a prirodzene sa premietne z fyzického priestoru do toho digitálneho. Druhá už súvisí s pragmatickým prístupom na zaistenie prostriedkov na samotné prežitie – jednoducho povedané, ide o veľmi žiadaný odbor, nadpriemerne finančne ohodnotený, geograficky rozšírený, s veľkou perspektívou trvalej udržateľnosti do budúcnosti.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies SK

Do kyberbezpečnosti ma zaviedla kariérna cesta v IT a téma ma pohltila. Žiadna iná oblasť v súčasnosti nie je taká komplexná a živá.

Juraj Nemeček,
vedúci oddelenia Sieťovej bezpečnosti
Alanata

Najčastejším dôvodom, prečo začať so štúdiom kybernetickej bezpečnosti, je stať sa obeťou útoku. Rozdiel spočíva v tom, že kedysi vám vírus bral výkon a diskový priestor, dnes vás môže stáť cenné dáta.

Stanislav Smolár,
manažér oddelenia bezpečnosti
Soitron

Buď človeku niečo heknú a zoberie to osobne, alebo sám nájde zraniteľnosti v produktoch, ktoré využíva, a začne ich hľadať vo všetkom, s čím pracuje.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť
Západoslovenská energetika

Bude to znieť čudne, ale hlavnou príčinou toho, že som zmenila kariérnu orientáciu zo softvého HR na tvrdú bezpečnosť, bol návrat z materskej dovolenky. Potrebovala som sa vrátiť do menej hektickej oblasti. Bol to omyl v slove „menej“. Inak je to najlepšie profesijné rozhodnutie, aké som učinila. Kyberbezpečnosť je dynamika, neistota, novosť, rôznorodosť, adrenalín. Všetko, čo pravá vášeň má, a preto ma baví.

Tomáš Zaťko,
etický hacker
CEO Citadelo

U mňa sa to začalo ešte v detstve a oveľa skôr, ako som tušil o pojmoch, ako je hacking alebo kybernetická bezpečnosť. Silným signálom je podľa mňa vášeň pre technológie a smäd po poznaní. Ako to funguje? Ako sa to dá pokaziť? Prečo sa to pokazilo práve takto, keď sa to minule pokazilo inak? Akými spôsobmi sa to dá (u/o)praviť? Takéto otázky sú dobrým štartérom.

Martin Oczvirk,
riaditeľ odboru informačnej bezpečnosti a certifikácie
Úrad na ochranu osobných údajov

Niekto vidí kyberbezpečnosť v technológiách ako niečo nové a zaujímavé a môžete sa tam rozvíjať a aj pomáhať zlepšovať existujúci zanedbaný stav. Najmä ak vie, čo všetko nám hrozí, ak je bezpečnosť zanedbaná. Iní vidia v kyberbezpečnosti príležitosť na trhu a na zárobok – či už legálnym alebo nelegálnym spôsobom.

Vincent Karovič,
prodekan pre informačné technológie
Fakulta managementu UK v Bratislave

Zlom nastal, keď som začal rozumieť, aké vážne sú hrozby v kyberpriestore a aký reálny a priamy dosah má kyberbezpečnosť na ľudí, riadenie a stratégiu organizácií. Zaujala ma táto multidisciplinárna perspektíva a uvedomil som si, aké je nevyhnutné efektívne riadiť riziká a zabezpečiť ochranu dát a informácií. Kľúčový kariérny moment si spájam s pochopením, že môžem prispieť k bezpečnejším a odolnejším manažérskym prístupom.

Katarína Kročková,
odborníčka na ochranu osobných údajov
Kročka & Partners

Keďže sa špecializujem na ochranu osobných údajov, kybernetická bezpečnosť je prirodzenou súčasťou mojej práce. Často sú to práve osobné údaje, ktoré sú cenným cieľom kybernetických útokov. Zároveň, bez kyberbezpečnosti sú osobné údaje vystavené riziku úniku a zneužitia. Vzájomné prepojenie týchto dvoch oblastí je preto kľúčové na zachovanie dôvernosti, integrity a bezpečnosti v digitálnom svete.

Jaroslav Oster,
predseda správnej rady
Preventista.sk

Je otázne, či musí nastať nejaký zásadný zlom. Možno náhoda, vďaka ktorej sa otázkam bezpečnosti začnete venovať hneď po ukončení vysokej školy, postupne sa do problematiky vnárate viac a viac a tam už to ide samo. Pri tejto otázke je asi dôležité aj to, o ktorej dobe a ktorej generácii kyberbezpečákov sa bavíme. Objem motivačných námetov, ale i zdrojov, ktoré nadchýnajú a posúvajú vpred, je naprieč generáciami neporovnateľný.

Jakub Berthoty,
advokát
Dagital Legal

Viem to porovnať len s ochranou osobných údajov. Ako koncipient som dostal túto tému prakticky za trest, pretože nikto sa jej vtedy nechcel venovať. Neskôr som si však uvedomil, že ide o najtechnickejšiu oblasť práva. Technika typicky odrádza právnikov, ale mňa odmalička priťahuje a vždy ma zaujímalo, ako fungujú autá, lietadlá, stroje, softvér alebo počítače. Práve prepojenie techniky a práva je dôvodom, prečo som si vybral túto špecializáciu.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov
Tatra banka

Svojich študentov vždy učím: programátorov a technikov čochvíľa nahradia programy a stroje. Keď prinesiete akýkoľvek program do firmy, vždy prídu otázky: Je to bezpečné? Neprídeme o dáta? Z tohto pohľadu sú informačná bezpečnosť a risk manažment skôr prirodzený vývoj. Pred sedemdesiatimi rokmi sa sťahovali ľudia z vidieka do miest, do tovární. Teraz sú doma a robia informačnú bezpečnosť a riadia riziká.

Július Selecký,
senior technický špecialista
ESET

Predstavte si, že začnete dostávať ďakovné e-maily za prezentácie, ktoré ste nikdy nemali, na konferenciách, na ktorých ste sa nikdy nezúčastnili, v mestách, ktoré ste si museli vygoogliť. Krádež identity vás práve nominovala na životné ocenenie, ktoré však nežijete. Po tomto všetkom je čas uznať, že kyberbezpečnosť je naozaj dôležitá téma.

Tomáš Loveček,
prodekan pre vedu a výskum
Fakulta bezpečnostného inžinierstva Žilinskej univerzity

Kybernetickou, respektíve akoukoľvek inou bezpečnosťou sa človek môže zaoberať už počas štúdia na vysokej škole. K rozhodnutiu však môžete dospieť aj počas kariérneho rastu, keď vás k tomu privedie náhoda, pozitívny či negatívny zážitok, apetít po zvýšení úrovne poznania alebo – často príkaz priameho nadriadeného. Nech už je impulzom čokoľvek, v úspešnom príbehu sa z povolania stáva poslanie.