HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 24. – 26. JÚNA 2022

Partneri špeciálnej prílohy:

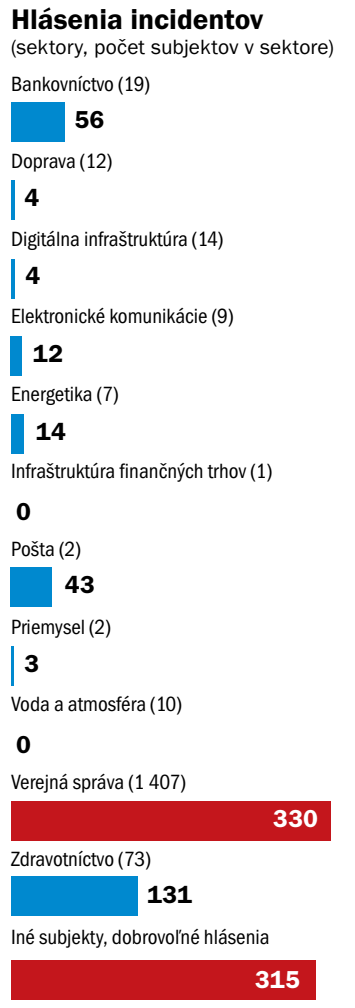
ALISON

ALITER TECHNOLOGIES

Veľa ohrození, málo ľudí a peňazí

Bezpečnosť v zdravotníctve je úloha na 24 hodín na každý deň a pre všetkých. SNÍMKA: DREAMSTIME

Hlásenia incidentov
(sektory, počet subjektov v sektore)



Zdroj: Správa o kybernetickej bezpečnosti Slovenskej republiky 2021, NBU

TÉMA

Kybernetická bezpečnosť je pre život v treťom tisícročí esenciálna a všadeprítomná. V zdravotníctve je však doslova „otázkou života a smrti".

Zdravotníctvo tohto storočia

Nie je to iba skrinka s liekmi a všadeprítomná obrazovka. Okrem diagnostických a monitorovacích zariadení pripojených do siete sú to aplikácie, informačné systémy, dátové toky medzi laboratóriami a nemocnicami, spracovanie údajov pacientov aj masívna komunikácia.

Téma kybernetickej bezpečnosti nasledovala elektronizáciu a digitalizáciu systémov a pracovných postupov v praxi. Vladimír Ježík, prezident Asociácie laboratórií Slovenska, to zhrnul jasne: „Ešte pred niekoľkými rokmi sme písali všetky správy v nemocniciach na písacích strojoch a teraz sú už všade počítače."

Ako sme na tom?

Správa o kybernetickej bezpečnosti v Slovenskej republike za rok 2021 charakterizuje zdravotníctvo ako sektor, ktorý je vystavený kybernetickým hrozbám viac ako iné odvetvia. Podpísala sa na tom pandemická situácia a úroveň ohrozenia zvýšila aj aktuálna geopolitická situácia.

Sektor zdravotníctva tak trápi aj zastaraná infraštruktúra a nedostatok kvalifikovaných IT odborníkov, keďže ťažko konkuruje iným odvetviam.

Zvyšujú sa aj riziká, ktoré predstavuje dodávateľský reťazec. „V sektore je množstvo dodávateľov rôznych zariadení, dnes už väčšinou pripojených na sieť, aj veľa dodávateľov špecializovaných služieb," upozorňuje Rastislav Janota, riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT.

Spoločná slabina

Členovia Asociácie nemocníc Slovenska sa zhodujú v tom, že kybernetickú bezpečnosť vnímajú vážne. „Opatrenia sú nutné, povedomie používateľov je však nízke," uviedli v oficiálnom stanovisku.

Martin Hromádka, riaditeľ Psychiatrickej nemocnice P. Pinela v Pezinku, to potvrdzuje z vlastných, aj sprostredkovaných skúseností. Najväčšiu slabinu vidí vo veľmi nízkej počítačovej gramotnosti. „Používatelia sú náchylní reagovať aj na najjednoduchšie a úplne evidentné pokusy o získanie prístupu k osobným údajom, akými sú heslá, čísla kariet, PIN kódy a nechajú sa ľahko vyprovokovať k otváraniu odkazov z neznámych zdrojov."

Kriticky nebezpečné e-maily

Upozorňuje na to aj Terezia Mezešová, vedúca podpory bezpečného vývoja v Siemens Healthineers: „S rozsahom už uniknutých dát na celosvetovej úrovni sa phishingové kampane budú zlepšovať a budú cielenejšie a špecifickejšie, čo nám všetkým skomplikuje ich rozpoznanie."

Zvyšovanie bezpečnostného povedomia sa preto musí priblížiť zdravotníckemu personálu, ktorý je vyčerpaný po pandémii a pod neutíchajúcim tlakom na poskytovanie kvalitnej zdravotnej starostlivosti. „Je to široká škála ľudí s rozličnou každodennou náplňou práce, je dôležité, aby dostali cielené tipy, ktoré hneď môžu začať praktizovať," dodáva Terezia Mezešová.

Tisíce prístrojov

Ak by sme aj všetkých zdravotníkov vycvičili v odolnosti proti phishingovým mailom, ešte stále sú tu koncové zariadenia pripojené do internetu. Často sú nedostatočne chránené alebo bez bezpečnostných záplat. Nejeden audítor kybernetickej bezpečnosti s hrôzou zisťuje, že infraštruktúra je zraniteľná či nesprávne nakonfigurovaná.

Ako brána pre kybernetické útoky fungujú napríklad v troch štvrtinách prípadov routery. Sú to najobľúbenejšie ciele s priemerom vyše päťtisíc útokov za mesiac. Neprekvapí preto odpoveď z Asociácie nemocníc, že každodenné zraniteľnosti patria do trojice faktov, ktorá ich v kybernetickej bezpečnosti desí.

Stovky aplikácií

Či sme chceli, alebo nie, v čase pandémie sme sa museli s aplikáciami zžiť v zrýchlenom tempe. Kauzu zdravotníckych informácií slovenská verejnosť len tak ľahko nezabudne a odborníci asi nikdy.

> V našom zdravotníctve je toľko vážnych problémov, že otázka bezpečnosti je iba jedna z mnohých.
>
> **Vladimír Ježík,** prezident Asociácie laboratórií Slovenska

Tomáš Bartek, bezpečnostný konzultant Aliter Technologies, tu preto opäť pripomína princíp bezpečnosti: „V systémoch kritickej infraštruktúry, akou je oblasť zdravotníctva, je nevyhnutné dbať na pevné zabudovanie mechanizmov informačnej bezpečnosti už do prvotných fáz vývoja softvéru." Na dosiahnutie požadovanej úrovne ochrany citlivých údajov musia byť tieto mechanizmy trvalo prítomné počas celého cyklu vývoja softvéru, jeho prevádzky a údržby. V skratke, dodržiavať princípy „security by design".

Zákon hovorí jasne

Za kybernetickú bezpečnosť zodpovedá štatutár. Rovnako ako iné organizácie, aj zdravotnícke zariadenia služby kybernetickej bezpečnosti nakupujú, outsourcing však nezbavuje štatutára zodpovednosti.

Na začiatku to boli iba antivírusové programy, ale teraz sú to už sofistikované hardvérové a softvérové zabezpečenia. Všetky systémové kroky v nemocniciach, poliklinikách, diagnostických centrách a ambulanciách sa digitalizujú aj prepájajú medzi sebou, poisťovňami či štátnymi autoritami, a tak vzniká väčšia potreba bezpečnosti.

Najťažšia úloha

V tom, čo je najťažšou úlohou v kybernetickej bezpečnosti v zdravotníctve, sa vzácne zhodujú všetci – dostatočné financovanie.

Technologické aj legislatívne zmeny si vyžadujú veľké investície a tie by mali byť zohľadnené pri plánovaní financovania zdravotníctva. Vladimír Ježík ako jedno z riešení navrhuje využiť aj prostriedky z plánu obnovy, respektíve časť investícií pre digitalizáciu.

Pohľad z druhého brehu

„Sme si vedomí, že zdravotnícky sektor je v oblasti IT mimoriadne podfinancovaný. Zároveň však treba povedať, že zariadenia často nevedia financie efektívne využiť a slepo dôverujú dodávateľom," zdôrazňuje Rastislav Janota.

Nemocnice nakupujú technológie namiesto riešenia urgentných problémov. Nevedia ich identifikovať a riešiť a ani ich dodávateľ túto schopnosť vo väčšine prípadov nemá. Bezpečnostný špecialista Július Selecký zo spoločnosti Eset často v praxi vidí, že je síce nakúpený špičkový hardvér a softvér, ale je zle zapojený alebo neaktualizovaný. „Nie je to len o nákupe technológií. Je to aj o ľuďoch, ktorí sa o ne starajú, a o bezpečnostných politikách."

Sám to nikto nedá

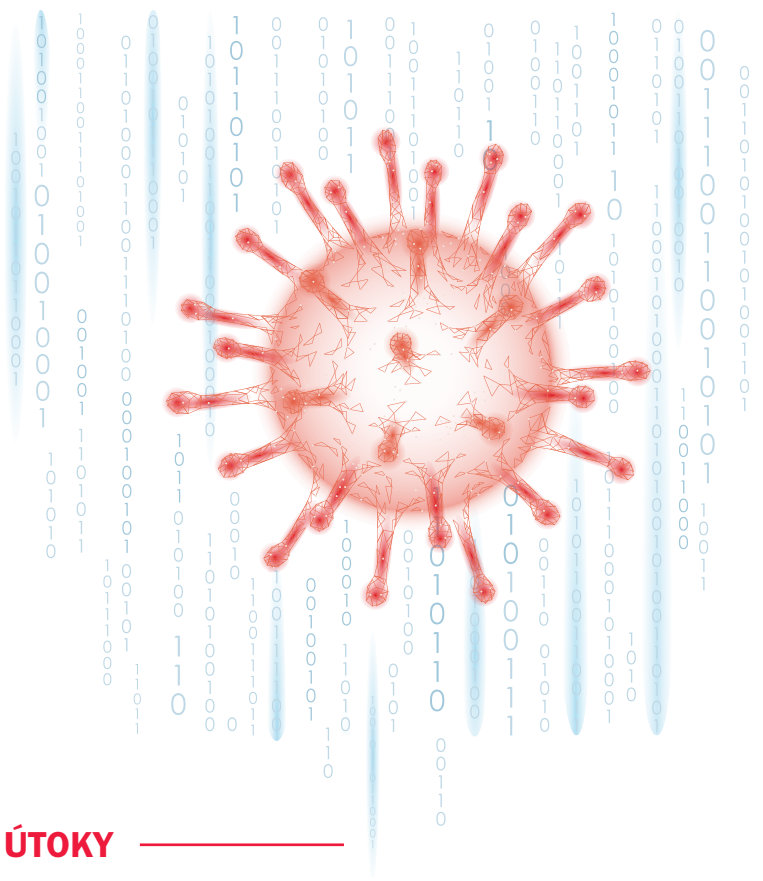
Záverečné slová Vladimíra Ježíka však presahujú tému: „V našom zdravotníctve je toľko vážnych problémov, že otázka bezpečnosti je iba jedna z mnohých." Ak nemáme dostatok lekárov a sestier a nemá kto ošetrovať, ak sú čakacie lehoty na vyšetrenia v mesiacoch, v kybernetickej bezpečnosti potrebujú zdravotnícke zariadenia podať pomocnú ruku.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · eset · Progress | Flowmon · MICRO FOCUS · Qubit · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 24. – 26. JÚNA 2022

Najagresívnejší škodlivý kód k nám ide najjednoduchšou cestou. Taký je tento rok



Správa ESET Threat Report T1 2022 sumarizuje najdôležitejšie štatistiky z detekčných systémov a kľúčové zistenia výskumníkov spoločnosti za obdobie prvého trimestra 2022.

SOFTVÉR

113-násobný nárast detekcií nebezpečného a sofistikovaného malvéru Emotet

Znovuzrodenie malvéru Industroyer, ktorý útočí na rozvodne vysokého napätia

Výrazne pribudol **špionážny softvér na Android** zariadeniach

Rozmohli sa sofistikované škodlivé schémy na vykrádanie krypto-peňaženiek v zariadeniach s operačnými systémami Android aj iOS

ÚTOKY

12 percent* výskytu ransomvéru na svete bolo detekovaných v Rusku, čím sa táto krajina stala najväčším globálnym terčom týchto útokov

Pribudli amatérske ransomvéry a wipery, čím autori vyjadrujú podporu jednej zo strán rusko-ukrajinského konfliktu a útoky realizujú ako osobnú pomstu

Prudko poklesli útoky cez protokol na vzdialenú správu, prvýkrát po dvoch rokoch neustáleho rastu

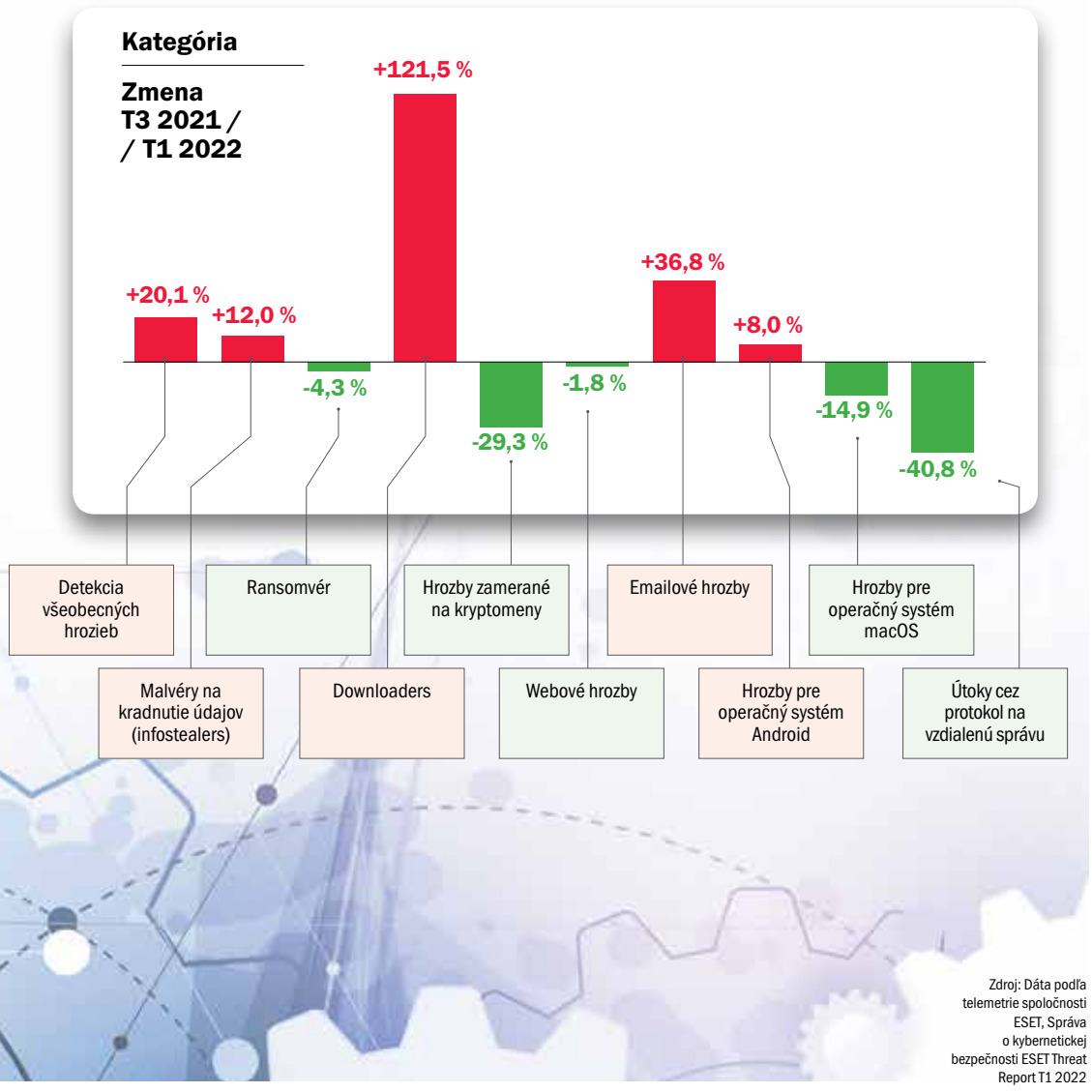
Poklesli hrozby spojené s nelegálnou ťažbou kryptomien

KAMPANE

Kategória hrozieb, ktoré sa k nám dostávajú **e-mailom, vzrástla o 37 percent**

V marci a apríli sa masívne šírili spamové kampane na báze malvéru Emotet používajúce škodlivé Microsoft Word dokumenty

Online priestor zaplavili phishingové a podvodné kampane a falošné zbierky, ktoré zneužívali solidaritu s Ukrajinou



Zdroj: Dáta podľa telemetrie spoločnosti ESET, Správa o kybernetickej bezpečnosti ESET Threat Report T1 2022

KOMENTÁR

Čo myslíte, ako je na tom váš lekár s IT bezpečnosťou? Mizerne

Sedím v čakárni a rešpektujem, že jednou z mnohých povinností za ostatné dva roky je aj naďalej používanie FFP2 respirátora pri návšteve ordinácie lekára. Tak si ho poslušne nasadím správne či šibalsky tesne pod nos a minúty začnú plynúť. Pravidlá treba dodržiavať.

V čakárni siahnem po spoločníkovi na „dlhé zimné večery", po mobilnom telefóne. Prečítam, čo som doma nestihol, a začínam premýšľať, čo ďalej. Preskenujem Wi-Fi, pripojím sa. Som „bezpečák" už viac ako desať rokov a nedá mi to.

Odolám nutkaniu zisťovať, či je zariadenie v súlade s STN EN 60601 a či neovplyvňuje lekárske prístroje pozapájané naokolo.

Predstava, že ma práve diagnostikujú a niekto si popritom sťahuje update aplikácií v telefóne, ktoré môžu ovplyvniť meranie, ma máličko vyrušuje. Lebo čo sa týka bezpečnosti, ja som v čakárni pravidlá dodržal, FFP2 mám. Tak pochopiteľne čakám, že pravidlá bude dodržiavať aj druhá strana.

Pravidlá sú tu však na to, aby sa porušovali. A tak ich overujem. Predsa len WiFi nie je jediné zariadenie pripojené v tejto malej sieti, ktorá pokrýva ordináciu a čakáreň.

S veľkou pravdepodobnosťou sieť spravuje jednoosobová eseročka, ktorá zároveň prevádzkuje aj IT systém. Tento systém nielenže spracúva moje osobné údaje, ale je od neho závislý aj môj život. A to doslova.

Bingo, mám to, vidím tlačiareň, dva počítače. Predstava, ako posielam na tlačiareň pozdrav: „AU, AU, bolí ma bruško..." ma síce rozveselí, ale smiešne to nie je. Toto ma desí. Elementárne bezpečnostné pravidlá evidentne neboli aplikované.

Sedím, naďalej mám nasadený respirátor a premýšľam, ako je to v tejto sieti s mojou digitálnou zdravotnou dokumentáciou – aké je spracovanie, uchovávanie či miera zabezpečenia. V tejto chvíli ma už trápi, kto má schopnosť detegovať situáciu, keď sa niekto nepozorovane pozerá na obsah, ktorý by mal zostať súkromný.

Ešte stále som v čakárni, aj respirátor mám a premýšľam, ako by sa tejto situácii dalo predísť. Neočakávam, že IT personál, prípadne bezpečnostný špecialista sú súčasťou tímu ordinácie, ale zachovanie dôvernosti údajov je kľúčové. Preto musíme hľadať cestu, ako zvýšiť povedomie o bezpečnosti.

Metodika a priebežné vzdelávanie sú jednou z ciest, ako sa vyrovnať s bezpečnosťou stoviek slovenských ordinácií. Nástroje aj technológie sú k dispozícii, avšak bez pravidelného opakovania zostanú len nákladovou položkou.

Som rád, že môžem uviesť dobrý príklad. Občianske združenie Slovenský pacient spolupracuje s organizáciami rôzneho typu a prvá výzva na lepšie zabezpečenie pri spracovaní informácií prišla už v roku 2016. S využitím technológií, nastavením metodiky práce a pravidelným opakovaním inštrukcií splnili požiadavky zadávateľa. Nielen formálne, ale aj prakticky. A získané zručnosti zúročili aj v čase dištančnej práce.

Veď už len nastavenie mena a hesla k počítaču a ich pravidelná zmena sú rovnako dôležité, ako keď prechádzam cez cestu a najskôr sa pozriem vľavo a potom vpravo.

Mario Minarovský
konzultant informačnej bezpečnosti CREDIBILIS

Keď sa stretávajú lekár, bezpečák a zákon

Audit prináša zúčastneným stranám vzácny objektívny pohľad zvonku. FOTO: DREAMSTIME

> Prvým rozhodnutím po audite bolo personálne posilnenie tímu.
>
> **Peter Dufek,** manažér kybernetickej bezpečnosti ProCare a Svet Zdravia

PRAX

Audity kybernetickej bezpečnosti v zdravotníctve sa v uplynulých mesiacoch uskutočňovali v čase pandemických opatrení a extrémnej záťaže. Nastal však čas zhlboka sa nadýchnuť, vyhodnotiť skúsenosti – a nečakať, že situácia sa zlepší bez záznych krokov.

Zákon nepustí

Nemocnice, laboratóriá a špecializované pracoviská patria medzi poskytovateľov základných služieb a podľa zákona sa na ne vzťahuje povinnosť urobiť audit kybernetickej bezpečnosti a správu dodať národnej autorite. Národný bezpečnostný úrad k začiatku roka evidoval 49 doručených auditov v sektore zdravotníctva.

V súčasnosti prebiehajú ďalšie audity, ale ešte stále ich chýba niekoľko desiatok. Ako však zdôrazňuje zodpovedný úrad, cieľom auditu nie je kontrola ani postihy. Cieľom je predovšetkým náprava podľa auditových zistení.

Potvrdí to každý audítor

Skúsenosti audítorov by sa dali zhrnúť do jednej mantry – každá organizácia bude len taká bezpečná, aký význam a dôležitosť kybernetickej bezpečnosti pripisuje manažment organizácie. Ako potvrdzuje audítor kybernetickej bezpečnosti Marián Illovský, je nesmierne dôležité, ak vedenie prikladá tejto problematike veľký význam.

Či už nad zariadeniami visí legislatívna povinnosť, alebo sa čoraz viac medializujú útoky na nemocnice v Českej republike a okolitých krajinách, audit kybernetickej bezpečnosti má nespochybniteľné postavenie v činnosti organizácií.

Verzia 1.0

V minulých mesiacoch stáli pred povinnosťou auditu kybernetickej bezpečnosti desiatky zdravotníckych zariadení a s nimi desiatky audítorov. Keďže audítor je vysokokvalifikovaná a certifikovaná autorita, pribúda ich iba veľmi pomaly. Ich povinnosti sú rozsiahle a špičkoví audítori zbierajú skúsenosti roky.

Na druhej strane sú tu rôznorodé zdravotnícke zariadenia. Predstavujú kolosy s viacerými subjektmi, ale aj inštitúcie rozložené na pár poschodiach, no so špecifickým poslaním.

Napríklad v sieti nemocníc Svet zdravia bolo v čase výkonu auditu jedenásť poskytovateľov základnej služby registrovaných ako prevádzkovateľ základnej služby na NBÚ. Celková dĺžka auditu tu bola takmer tri mesiace. Podľa Petra Dufeka, manažéra kybernetickej bezpečnosti ProCare a Svet Zdravia, bolo najvýznamnejšou skúsenosťou v sieti práve praktické oboznámenie sa s výkonom auditu.

Najvýznamnejšie skúsenosti

V mnohých zdravotníckych zariadeniach išlo o vôbec prvé posudzovanie zhody formou auditu. Samotný audit je systematický, nezávislý a zdokumentovaný proces a je objektívnym posúdením miery, do akej sa splnili vopred definované bezpečnostné požiadavky. Priebeh auditu tak ovplyvňuje celú organizáciu.

Aj podľa skúsenosti Petra Dufeka si audit vyžiadal spoluprácu množstva oddelení – IT a HR tímu, špecialistov kvality, prevádzkových zamestnancov a, samozrejme, manažéra kybernetickej bezpečnosti.

Preskúmanie všetkých oblastí si vyžadovalo presné dodržiavanie auditového harmonogramu, jeho rozsahu, zdrojov a účasť na mieste v auditovaných subjektoch.

Predtým a potom

Audit kybernetickej bezpečnosti v organizácii sa nekončí odovzdaním auditovej správy. Kybernetická bezpečnosť je komplexný a systematický proces. Nikdy sa nekončí a zohľadňuje prevádzkové odlišnosti každého subjektu. Predstavuje cyklus budovania a udržiavania celého ekosystému opatrení a procesov.

Bezprostredne po získaní výsledkov auditu sa stanovili záväzné opatrenia a harmonogram odstránenia nedostatkov. Ako uvádza Peter Dufek, prvým rozhodnutím organizácie po doručení správy auditu kybernetickej bezpečnosti bolo personálne posilnenie tímu IT bezpečnosti v spolupráci s manažmentom.

Je zrejmé, že zmena od povedomia ku kultúre kybernetickej bezpečnosti v organizácii nie je jednoduchá. Marián Illovský preto kladie dôraz na postupné a cieľavedomé vzdelávanie v kybernetickej bezpečnosti. Iba takéto spojené aktivity na všetkých „frontoch“ pomôžu ochrániť organizáciu pred kybernetickými hrozbami.

ŠTÚDIA

Útočníci prenikli do siete, nemocnica reaguje

Pravdepodobnosť, že ransomvérový útok zasiahol alebo zasiahne slovenskú nemocnicu, je takmer stopercentná. Možnosť, že obeť útoku zverejní prípadovú štúdiu, je takmer žiadna. Tak sa na to pozrime cez aktuálnu udalosť vo svete.

Útok a obrana

Zdravotné stredisko Yuma Regional Medical Center (YRMC) v Arizone oznámilo, že sa stalo obeťou ransomvérového útoku, pri ktorom útočníci získali aj údaje približne 700-tisíc súčasných aj bývalých pacientov.

Len čo bol incident identifikovaný, systémy boli prepnuté do režimu offline, aby sa zabránilo ďalšiemu neoprávnenému prístupu. Stredisko okamžite informovalo aj orgány činné v trestnom konaní a na vyšetrovanie si najalo forenzných analytikov, aby určili povahu a rozsah útoku.

Vyšetrovanie však už v tejto fáze potvrdilo, že útočníci získali prístup k systémom medzi 21. a 25. aprílom a pred zašifrovaním súborov exfiltrovali rozsiahle súbory. Počas útoku fungovali systémy strediska s použitím záložných procesov a postupov, čo spôsobilo určité oneskorenie služieb, ale väčšina pokračovala podľa plánu.

Všetci dotknutí pacienti dostali oznámenia, kde ich zdravotné stredisko informovalo o rozsahu incidentu. Odcudzené údaje obsahovali mená pacientov, čísla sociálneho poistenia, informácie o zdravotnom poistení a čiastočné zdravotné informácie.

Postihnutým osobám zároveň stredisko ponúklo bezplatné služby monitorovania kreditu a ochrany pred krádežou identity.

V oznámeniach aj vyhláseniach Yuma Regional Medical Center zdôrazňuje, že do systému elektronických zdravotných záznamov sa útočníci nedostali. Súčasne však manažment potvrdil ďalšie bezpečnostné opatrenia, aby zabránil útokom.

Ak nie je zaplatené výkupné, ransomvérové útoky často vedú k zverejneniu ukradnutých údajov. V tomto prípade však zdravotné stredisko odmieta potvrdiť, či sa na platbe dohodlo.

Komentár

V súčasnosti si už prevádzkovatelia uvedomujú hodnotu dobrého mena na trhu a v prípade kybernetického incidentu sa obávajú aj straty reputácie.

Na druhej strane, ak nebudeme tieto udalosti a incidenty komunikovať, budeme žiť vo falošnej nádeji, že sme v bezpečí. Preto v prípade arizonskej nemocnice pacienti aj médiá ocenili otvorenosť a rýchlosť komunikácie. Z profesionálneho hľadiska to hodnotím ako učebnicový incident handling.

V čase incidentu sa totiž postihnuté zdravotné stredisko mohlo oprieť o bezpečné a kvalitné zálohovanie dát. Nespochybniteľný je kvalitný interný a externý tím a v neposlednom rade mali určite kvalitný záložný plán aj postup, ako sa vrátiť do prevádzky.

Ak by sa niečo takéto stalo na Slovensku, je tu zákonná povinnosť hlásiť incident Národnému bezpečnostnému úradu, a ak by išlo o únik údajov, aj Úradu na ochranu osobných údajov. Obe inštitúcie okamžite uvádzajú do pohotovosti mechanizmy na pomoc a varovanie ďalších potenciálne zasiahnutých subjektov.

Incident treba dôkladne vyšetriť a zdokumentovať a vytvoriť záložné kópie pre forenzných analytikov. Aby sme eliminovali škody, kontrola musí byť dôsledná a musí pamätať aj na „zadné dvierka“, ktoré útočníci často nechávajú v systéme. Útočné techniky sa vyvíjajú exponenciálnou rýchlosťou, a preto všetky zistenia musíme zapracovať do nasledovných opatrení, aby sme minimalizovali riziko.

Boli opísané tony papiera o dôležitosti prevencie v kybernetickej a informačnej bezpečnosti. Pravidelné školenia zamestnancov, tréningy a kontrola dodržiavania štandardov by dnes mali byť rovnako samozrejmé ako školenia bezpečnosti práce či preškoľovanie vodičov.

Miroslav Macko, analytik ALISON Slovakia

RIEŠENIE

Lekár sa má starať o pacienta, alebo sa stále niekam hlásiť?

Tradičný obraz lekára s fonendoskopom na krku sa mení. Stáva sa z neho, či chce, alebo nechce, používateľ aplikácií. A po čase dokonca vyčerpaný používateľ.

Skúsenosti nad zlato

Riešenia v sieti nemocníc Community Health Systems (CHS) v USA sa často prezentujú ako prípadové štúdie kybernetickej bezpečnosti. Táto sieť je jedným z najväčších prevádzkovateľov poskytujúcich urgentnú starostlivosť v USA a zastrešuje 158 nemocníc, ktoré majú spolu 27-tisíc lôžok.

Už samotný pojem odolnosť evokuje masívne nasadenie technológií a sofistikované riešenia. Odolnosť má však svoje opodstatnenie vtedy, ak chráni systémy a ľudí každú sekundu bez toho, aby o nej vedeli, alebo im pridávala ďalšie úlohy.

Trikrát za hodinu

Jedna z kliník v sieti CHS mala napríklad systém, v ktorom zdravotnícky personál používal trinásť rôznych aplikácií a každá z nich si vždy vyžadovala zadanie prihlasovacích údajov. Pri 2 700 používateľoch to predstavovalo obrovské časové nároky na správu týchto identít. Lekári navyše strácali množstvo času opakovaným prihlasovaním sa do rôznych aplikácií až dvadsaťkrát za deň, vždy, keď vyšetrovali pacienta.

Bezpečnosť až po kolaps

Riaditeľ pre informačnú bezpečnosť v sieti CHS sa rozhodol problém riešiť, keď mu takmer skolaboval helpdesk. Neustále boli obrovské problémy s heslami a každý týždeň prišlo na helpdesk dvetisíc dopytov.

Nároky na bezpečnosť znižovali pracovný výkon lekárov, ktorí sa pri práci potrebovali neustále prepínať medzi aplikáciami a systém verifikoval ich identitu. Preto na klinike hľadali spôsob, ako prihlasovanie a odhlasovanie do systémov zvládnuť pomocou jediného hesla.

Aká je úloha

Bezpečnostné oddelenie dostalo úlohu spravovať a zabezpečiť digitálne identity 280-tisíc používateľov a integráciu desiatok aplikácií. A to v zdravotníctve, ktoré je vystavené neustálym zmenám a kvalita starostlivosti o pacientov nesmie byť ohrozená.

Bezpečnostný tím analyzovali aplikácie, ktoré lekári využívajú, pričom plán bol umiestniť ich na úvodnú obrazovku a zabezpečiť prihlasovanie pomocou jediného hesla. Nasledovala komunikácia so zainteresovanými v rámci

FOTO: DREAMSTIME

podniku a vyčerpávajúca analýza realizovateľnosti.

Výsledkom bola mapa správy identít a prístupu.

Nech to rieši systém

Hneď po schválení rozhodnutia bolo implementované riešenie správy identít NetIQ Identity Manager. Spĺňalo aj požiadavku, aby bolo škálovateľné a výkonné.

Zároveň bol systém už pri zavádzaní vybavený automatizáciou pracovných postupov, čo umožňuje používateľom flexibilne prechádzať medzi oddeleniami. Predtým napríklad zdravotná sestra, obvykle pracujúca na treťom podlaží nemocnice, mala prístupové práva len na tomto podlaží. Teraz, ak má zmenu na urgentnom oddelení, dostane dočasné prístupové práva, a to bez obmedzenia jej obvyklých prístupových oprávnení.

Používatelia klikajú

Produktivita sa enormne zvýšili už tým, že zamestnanci sa do systému prihlásia iba raz za deň a potom sa jedným klikom hlásia do všetkých aplikácií v celej sieti.

Systém jedného prihlásenia a samoobslužné funkcie znížili dopyty na helpdesk na polovicu. IT odborníci tak získali viac času na podporu iných technologických požiadaviek. Onboarding používateľov prešiel radikálnou zmenou a vytvorenie účtu nového používateľa sa skrátilo z niekoľkých týždňov na desať minút.

Tým, že sa pracovné postupy automatizovali, radikálne sa skrátil aj čas potrebný na správu jedného používateľa.

Anna Stehlíková, manažérka pre bezpečnostné licencie Čechy a Slovensko, Micro Focus

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 24. – 26. JÚNA 2022

Vedia predvídať, ale nestačí to

ANKETA

Bezpečnostní profesionáli odpovedajú na otázku, akú najťažšiu úlohu dostali v ostatnom čase a čo také prekvapivé sa im stalo, že pri riešení museli zo seba dať to najlepšie.

Ján Grujbár, generálny riaditeľ
Aliter Technologies

Neustále sa snažíme rozširovať tím bezpečnostných špecialistov, aby sme vedeli pružnejšie a rýchlejšie pomáhať svojim zákazníkom. Dlhodobo vnímam, ako veľmi náročné je nájsť nových kandidátov, ktorí by spĺňali naše požiadavky. Ako jedno z riešení vidíme umožniť vstup do sveta kybernetickej bezpečnosti aj úplným začiatočníkom a následne spoločne definovať ich špecializáciu a umožniť ich odborný rast internými a externými školeniami, účasťou na medzinárodných konferenciách a podporou odbornej certifikácie v oblasti kybernetickej bezpečnosti.

Rastislav Janota, riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Nad útočníkmi v kybernetickej vojne sa zvíťaziť nedá. Ale nesmieme proti nim prestať bojovať. Aj keď v realite bojujeme proti mnohým ďalším problémom. Proti nepochopeniu na rôznej úrovni, nedostatku odborníkov, proti ľudskej lenivosti, proti nedostatku financií, proti ľudom, čo chcú škodiť, proti chybám v technológiách, proti... Je toho veľa. Ale budem bojovať – myslím si, že je to správne, a som rád, že som to dostal ako svoju (najťažšiu) úlohu.

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

Mňa osobne vždy „prekvapí“ zdôvodňovanie financií v rozpočte na bezpečnosť. A zvlášť, ak žiadam zvýšenie.

Tomáš Hettych, viceprezident
ISACA

Posledné dva roky sme stavali štátny kyberbezpečnostný startup na zelenej lúke a takmer nemožných úloh bolo pomerne dosť. Ale aktuálne posledná „mission impossible“ bola autorizácia na poskytovanie kvalifikovaných dôveryhodných služieb. Za tri týždne upraviť dokumentáciu, dohodnúť externý audit, zmeniť certifikáty a podať žiadosť na NBÚ, to bola naozaj poriadna výzva.

Andrej Žucha, generálny riaditeľ
ALISON Slovakia

Prijímanie nových ľudí. Dobrých ľudí si firma nechce púšťať a sľubuje im modré z neba. Priemerní majú očakávania nastavené z predcovidových čias a majú pocit, že keď sa o kybernetickej bezpečnosti stále píše, tak si zaslúžia nezaslúžené podmienky. Chcelo to veľa kandidátov, doslova desiatky stretnutí, ale verím, že sme si nakoniec vybrali dobre.

Marián Trizuliak, architekt kybernetickej bezpečnosti
Západoslovenská distribučná

Najťažšie úlohy neexistujú. Existujú len dôležité alebo zbytočné úlohy. Denne zostávam prekvapený, koľko zbytočných vecí alebo úloh musíme riešiť – nielen v pracovnej, ale aj v súkromnej sfére doma alebo na úradoch.

Roman Varga, manažér kyberbezpečnosti
Dôvera, zdravotná poisťovňa

V stredu som na workshope stál pred riaditeľmi slovenských nemocníc a po všetkých prezentáciách o kyberbezpečnosti som čelil jedinej otázke – kde na to vziať. To ma skutočne prinútilo siahnuť do rezervoára svojich síl, ale odpoveď ešte stále hľadám. Ako prvý krok im však podávame pomocnú ruku v tom, že sa s nimi chceme podeliť o skúsenosti a riešenia, ktoré fungujú.

Richard Kiškováč, generálny riaditeľ
IstroSec

Asi najťažšou úlohou, s ktorou sa borí každý manažér v poslednom období, je riešenie problému, kde nájsť odborníkov na kybernetickú bezpečnosť a ako ich adekvátne zaplatiť a motivovať. Vzhľadom na aktuálnu bezpečnostnú situáciu je ľudská sila to, čo asi najviac chýba v tejto oblasti. Samotné technológie bez odbornej obsluhy nedokážu byť dostatočne efektívne a nenaplnia svoj účel. Zdá sa, že práve nedostatok odborníkov je najväčšou slabinou kybernetickej bezpečnosti v súčasnosti.

Daniel Chromek, riaditeľ informačnej bezpečnosti
ESET

Posledná úloha, ktorej som musel prioritne venovať pozornosť, bolo vydanie usmernenia pre Biden's Executive Order 14028 a následná urýchlená analýza dvoch súvisiacich špeciálnych publikácií organizácie NIST 800-161 a 800-218, aby sme mohli začať pripravovať ESET na podporu predaja produktov a služieb pre vládnych zákazníkov v USA.

Ivan Kopáčik, bezpečnostný expert
Gordias

V poslednom čase mám pocit, že najťažšia úloha je vždy tá, ktorú práve riešim. Kybernetická bezpečnosť prináša každý deň obrovské množstvo nových informácií. Osvojiť si ich a aplikovať pri riešení úloh je čoraz náročnejšie.

Diana Legdanová, vedúca úseku bezpečnosti
Východoslovenská energetika Holding

Ostatné dni mi pripomenuli, že kybernetická bezpečnosť je neoddeliteľná triáda – ľudia, procesy, technológie. Aj napriek špičkovým technológiám a sofistikovaným procesom sú ľudia a vzťahy to najvzácnejšie, čo máme. Ak na to aj občas zabudnem, život mi vždy pripomenie, ako si treba vážiť profesionálnych a férových ľudí okolo seba.

Tomáš Zaťko, CEO, etický hacker
Citadelo

Riaditeľ bezpečnosti sa ma pýtal, ako presvedčiť generálneho riaditeľa, že bezpečnosť nestačí robiť iba „na papieri“. A to je naozaj ťažké. Bez podpory vrcholového manažmentu sa bezpečnosť robiť nedá.

Jana Puškáčová, manažérka útvaru informačná bezpečnosť
MOL IT & Digital Slovensko

Doplniť a poskladať takmer nový tím tak, aby boli naplnené očakávania všetkých zúčastnených strán, a preniesť tímového ducha a pocit spolupatričnosti do online sveta.

Michal Ďorda, audítor kybernetickej bezpečnosti
auditori.it

Presvedčiť zamestnávateľa, že investície do bezpečnosti sú rozumne vynaložené zdroje na zníženie zásadného dosahu. Každé opatrenie, ktoré vychádza z dôkladnej analýzy rizík a zvyšuje vyspelosť organizácie, môže predísť niekoľkonásobne vyšším budúcim stratám a problémom v prípade výskytu závažného kybernetického bezpečnostného incidentu. Držme si palce, aby sme tie naše úlohy všetci úspešne zvládli.

Dominik Procházka, riaditeľ odboru bezpečnosti
AGEL SK

Najťažšiu a zároveň najzaujímavejšiu úlohu, ktorú som dostal, je riadenie kybernetickej bezpečnosti aj pre zahraničnú časť skupiny. Interné audity spoločností, úprava stratégie, zladenie technických aspektov, úprava procesov a príprava na audit. To je len krátky súhrn potrebných činností, ktoré ešte prebiehajú, ale aj napriek nemalému úsiliu môžem konštatovať, že ma stále posúvajú a obohacujú.

Jaroslav Oster, predseda správnej rady
Preventista.sk

Rozmýšľam tri dni a teraz som si úplne istý. Každé zadanie pre forenzného analytika zamerané na vyťažovanie digitálnej stopy prináša vždy nové výzvy. Technologické, odborné, ale omnoho častejšie morálne, keďže digitálna stopa je dnes spätá najmä s dokazovaním nekalých aktivít. Často tak siahnem na hranicu svojich síl, ale rovnako často zisťujem, že vždy sa dá ísť ďalej.

Marek Zeman, vedúci oddelenia bezpečnosti informačných systémov
Tatra banka

Popasovali sme sa s prechodom na technológiu Zero trust. Technológia vyžaduje zmenu náhľadu na prevádzku sietí, zmenu správania jednotlivých zamestnancov aj pracovníkov IT a zmenu procesov a zaužívaných zvykov. Priniesla však väčšiu bezpečnosť siete, slobodu v prihlasovaní do firmy, jednoduchosť a prehľadnosť. Implementovať Zero trust vo veľkej zabehnutej firme, to bola porcia hodná technologického inovátora.

Roman Čupka, hlavný konzultant
Progress Flowmon a CEO Synapsa Networks

Úlohy si zväčša zadávam sám a okrem výchovy detí so správnymi morálnymi hodnotami a starostlivosti o rodinu je v poslednom čase tou najťažšou vybudovanie životaschopnej firmy zameranej na vývoj produktov pre automatizáciu činností v kybernetickej bezpečnosti, ktorá si, verím, nájde zákazníkov po celom svete a budúcim kolegom vytvorí moderné zázemie na slobodnú prácu.

Miloslav Leporis, konzultant bezpečnosti
Tempest

Urobil som si analýzu, čo všetko na odpoveď potrebujem, a zistil som, že práve táto otázka je tá najťažšia úloha, ktorú som za ostatný čas dostal. Len čo akceptujem úlohy, tak idem krok za krokom a nepustím dovtedy, kým ich nesplním. Nič nie je iba biele a čierne, tak proste pracujem.

Ivan Makatura, generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Byť generálnym riaditeľom prináša istú drobnú výsadu, a to, že úlohy si zadávam sám (úsmev). A teraz vážne – myslím si, že som dokázal, ako môže aj vo verejnej správe efektívne fungovať nestranná odborná organizácia, ktorá zamestnáva uznávaných profesionálov – „bezpečákov“ a ktorá na seba dokáže zarobiť aj bez nárokov na peniaze daňových poplatníkov.

Martin Fischer, manažér oddelenia kybernetickej bezpečnosti
Všeobecná zdravotná poisťovňa

Konzistentne a pútavo zvyšovať úroveň povedomia o informačnej bezpečnosti medzi zamestnancami a bežnou populáciou. Nie je jednoduché presvedčiť ľudí, že obeťami zlomyseľného konania útočníka môžu byť aj mimo pracovného času, a preto by sme tiež mali dbať na ochranu svojho súkromia a so zásadami ochrany dát byť zžití či už v pracovnom, alebo súkromnom prostredí.

Stanislav Smolár, manažér oddelenia bezpečnosti
Soitron

Ako zabezpečiť monitoring industriálnej infraštruktúry zákazníka. Znie to ako jednoduchá úloha, ale realita ukázala, že nie každá časť výroby má dostupnú vhodnú kabeláž. Pôvodný plán využiť 4G sieť na transport zberu dát sa tiež ukázal ako nerealistický pre elektromagnetické rušenie.
Nakoniec bol riešením zber dát prostredníctvom WiFi senzorov, ktoré však musel výrobca nasadiť a otestovať špeciálne pre tento prípad.

Štefan Mizerák, manažér oddelenia IT bezpečnosti
NN Životná poisťovňa

Občas nám dá zabrať potreba okamžitej koordinácie aktivít medzi rôznymi oddeleniami, čo si vyžaduje reprioritizáciu ich úloh, lebo bezpečnostné udalosti sa zásadne objavujú v hektickom období.
Napríklad prijímanie opatrení na riešenie Log4Shell v decembri 2021, pričom niektoré výskyty zraniteľnej log4j knižnice sa dali vyriešiť len upgradom aplikácie alebo databázy s veľkým úsilím na strane IT.

Ján Adamovský, riaditeľ bezpečnosti
Slovenská sporiteľňa

Koordinácia kritických činností firmy z pozície krízového manažéra je nesmierne náročná. Ostatné obdobie je bohaté na nepredvídateľné udalosti, ktoré vybočujú z rámca bežných incidentov. Vyžaduje si preto plné nasadenie, schopnosť robiť rýchle rozhodnutia a byť si istý, že každý z kolegov priloží ruku k dielu a zastane svoju rolu na sto a viac percent.

Pavel Nechala, partner
Advokátska kancelária WISE3

Za najťažšie považujem prijatie skutočnosti, že to, čo sa realizovalo doteraz, je iba začiatkom. Ak sme hovorili o upriamení pozornosti na budovanie odolnosti, tak dnes je to adaptívnosť, lebo zmeny prichádzajú v hrozbách, technológiách aj legislatíve.