HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
24. – 26. NOVEMBRA 2023

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Zdravotníctvo a aj my pod útokom

TÉMA

V zdravotníctve na Slovensku pracuje vyše stotisíc ľudí, sú tu desiatky profesií a k tomu rôznorodý ekosystém dodávateľov. Cena bezpečnosti tu stúpa, nech si to vysvetľujete akokoľvek.

Napriek technológiám sú najslabším ohnivkom v kyberbezpečnostnej reťazi – ľudia. FOTO: DREAMSTIME

Martinská univerzitná nemocnica zažila masívny kybernetický útok. Patrí medzi najväčšie na Slovensku, má množstvo špecializovaných pracovísk a v brandži je uznávaná za svoju afinitu k digitalizácii. V prípade úspešného útoku hrozí kolaps národných rozmerov.

Môžete si vydýchnuť. Tento phishingový útok bol iba test.

Poháňa ich zodpovednosť

„V zdravotníctve predstavuje najväčšie riziko strata a odcudzenie pacientskych údajov," upozorňuje Ivan Kocan, riaditeľ Univerzitnej nemocnice Martin. A hneď dodáva, že výpadok informačných systémov, prípadne ich dysfunkcia ohrozujú pacientov a zhoršujú prácu zamestnancom vytváraním zbytočných stresových situácií.

Preto ako štatutár vníma Ivan Kocan potrebu riešenia kyberbezpečnosti nielen kvôli legislatívnym povinnostiam, „ale aj v kontexte dnešnej doby, keď sa zväčšujú riziká pre zamestnanca a pacienta. Našou úlohou je tieto riziká predvídať a minimalizovať".

Nerozprávajte, robte

Rýchlosť je významný faktor v kyberbezpečnosti a zdá sa, že lepšie to využívajú útočníci. Žijeme v dobe, keď umelá inteligencia rýchlejšie urobí phishingový útok, ako sa vo väčšine organizácií dohodne manažér kybernetickej bezpečnosti s vedením.

Martinskí zdravotníci preto nelenili a vybrali si na phishingový test platený nástroj. Chceli kvalitný priebeh a dobrý report. Nasledovala analýza prostredia, vytypovanie účastníkov testu, výber vhodného termínu a vytvorenie obsahu phishingových e-mailov.

Ako sa robí útok

V deň D dostali zamestnanci administratívy mail, že v zdieľanom súbore si môžu pozrieť mimoriadne odmeny. Stačí zadať osobné údaje. Ruku na srdce – kto by nebol zvedavý?

Doručených bolo 189 správ a priložený odkaz použila takmer tretina používateľov a tretina z nich zadala prihlasovacie údaje. Niektorí používatelia aj viackrát. Správne zareagovalo iba desať používateľov.

Prvé varovanie

Schválne – viete, aký je rozdiel v adrese UNM a UMN? Cena za kybernetický útok.

Prvým podozrivým znakom emailovej správy je adresa odosielateľa. Stačí prehodiť jedno písmenko v poradí a už sa stáva z bežného mailu útočný. Meno reálneho odosielateľa sa dá totiž zistiť z verejných zdrojov, ako je telefónny zoznam alebo faktúry na webe. A uvedené telefónne číslo zvyšuje dôveryhodnosť e-mailu.

Druhé varovanie

Ďalším znakom phishingových správ je naliehanie na používateľa, že je v časovej tiesni. V tomto prípade to bola informácia, že ak používateľ súbor neotvorí do 96 hodín, vymaže sa.

Ak vás e-mail motivuje niečo stiahnuť, zbystrite. Aspoň chvíľku sa zamyslite, či je príloha alebo zdieľaný súbor relevantný pre pracovnú pozíciu používateľa.

Ak už odkaz presmeruje používateľa na úložisko, opäť treba skontrolovať adresu. Žiadne gramatické patvary či generátory názvov tu nemajú miesto.

A nikdy, úplne nikdy nezadávajte osobné údaje, prístupové heslá a čísla platobnej karty.

> Zdravotníctvo vnímame ako najviac ohrozený sektor.
>
> **Július Selecký,** Eset

Podozrenie potvrdené

Používatelia, ktorí správne reagovali v phishingovom teste, dostali odmenu. Symbolickú, ale keby išlo o skutočný útok, zachránili by životy. Pričom pripomíname, že išlo o zamestnancov administratívy. Zdravotnícki zamestnanci mali „svoj" phishingový test.

„Test potvrdil, že jednou zo slabín systému je samotný zamestnanec, preto chceme ďalej pokračovať v edukácii zamestnancov, ako takýmto hrozbám čeliť," hovorí Ivan Kocan.

Po teste evidujú administrátori v martinskej nemocnici zvýšený počet hlásení. Súčasne zaviedli školenie kybernetickej bezpečnosti pre nových zamestnancov, implementujú e-learning a začínajú všeobecnú informačnú kampaň v internom newslettri.

Smutné prvenstvo

Phishing je v globálnom hodnotení najčastejší spôsob úvodného útoku v zdravotníctve. Zodpovedá za 16 percent všetkých únikov dát. Hlási to výročná správa prestížneho Ponemon Institute, ktorá monitoruje náklady spojené s únikom dát.

Správa opätovne potvrdzuje, že porušenie ochrany údajov v zdravotníctve patrí medzi najnákladnejšie. Priemerné náklady spojené s porušením sú tu najvyššie zo všetkých odvetví. Výdavky rastú už 13 rokov za sebou, pričom za posledné tri roky sa zvýšili o 53 percent

Rekord, ktorý nikto nechce

Podľa štatistík trvá až 231 dní, kým prevádzkovateľ v zdravotníctve identifikuje narušenie ochrany dát, čo je viac ako priemer. Zároveň zdravotníci zažijú dlhšie obdobia obmedzenia ako následky útoku – priemerne 92 dní v porovnaní so 73 v iných odvetviach.

„Len za prvých deväť mesiacov tohto roka čelila jedna zdravotnícka organizácia v globále až 1 613 kyberútokom týždenne, pričom útoky sú multifaktorové a vysoko komplexné," varuje Tomáš Vobruba z Check Point Software Technologies. Problémom zdravotníctva na Slovensku je veľa zariadení a rôzneho softvéru, a tým aj potreba rôznych špecialistov. Ítečkári pritom riešia aj servis tlačiarní, zabudnuté heslá, aktualizácie softvéru a na bezpečnosť im zostáva málo času.

Opatrenie na dosah

Július Selecký z Esetu hovorí, že kedysi chodili po príklady kyberútokov do sveta, dnes si už vystačíme aj na Slovensku: „Zdravotníctvo vnímame ako najviac ohrozený sektor."

Toho roku doplnili malý kúsok do bezpečnostnej skladačky, čo definitívne potvrdzuje trend od produktov a riešení k službám kybernetickej bezpečnosti.V riešeniach Esetu sa už nachádza nástroj na vyhľadávanie zraniteľností a ich zaplátanie.

Účinná ochrana môže byť aj systém, ktorý pošle do laboratória vzorku hrozby. Tam sa cielene „nakazia", analyzujú vzorku a zákazníkovi pošlú report, ktorý môže použiť v správe alebo v hlásení.

Pri ochrane sa dá spoliehať už iba na súbor technológií, kde je ťažisko na rýchlosti a komplexnosti. Výhodou riešenia je, že technológie sú integrované a netreba ďalšie inštalácie.

Čo ďalej

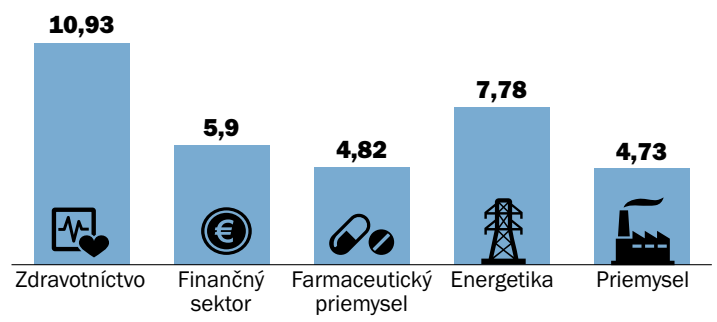
Väčšie zdravotnícke zariadenia sa už pozerajú po službe externého SOC-u, čiže Strediska bezpečnostných operácií. Pre mnohé organizácie je totiž nemožné nájať dostatok kyberbezpečnostných odborníkov, nehovoriac o výške investícií či zdĺhavom obstarávaní technológií, aby si vlastný SOC postavili.

SOC prepája bezpečnostný a prevádzkový monitoring aktív a často umožňuje odhaliť anomálie a udalosti, ktoré by mohli vyústiť do kybernetického bezpečnostného incidentu ešte pred jeho vznikom.

O kyberbezpečnosť v zdravotníctve sa čoraz intenzívnejšie zaujímajú nielen útočníci a národné autority, ale aj pacienti. A na to, aby bolo zdravotníctvo skutočne odolné, už iba antivírus nestačí.

Zdrojové informácie: prednášky na Kongrese Nemocničné informačné systémy 2023

Najvyššie náklady spojené s porušením ochrany údajov v roku 2023 (sumy uvádzané v miliónoch dolárov)



Zdroj: Cost of a Data Breach. IBM Security, Ponemom Insititute

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · auditori.it · CHECK POINT · eset · Progress · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 24. – 26. NOVEMBRA 2023

Koho a čoho sa obávať v zdravotníctve

ANKETA

Kyberbezpečnosť v zdravotníctve je otázkou života a smrti a týka sa všetkých. Oslovili sme obrancov v prvej línii aj tých, ktorí stoja za nimi. Takže koho alebo čoho sa najviac obávať, ak chceme budovať kyberodolné zdravotníctvo?

Milan Pikula,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Namiesto obáv je nutné budovať odolné zdravotníctvo na základe analýzy rizík. Informačné technológie sú kritickým aktívom pre garanciu zdravotnej starostlivosti. Tento sektor dlhodobo zápasí s finančným a personálnym zabezpečením nielen v informatike a kybernetickej bezpečnosti. Následkom sú chýbajúce opatrenia od základov, ako segmentácia siete a zálohovanie – tvárou v tvár reálnym incidentom. Pozornosť si preto zaslúžia reálne hrozby a investície do ľudí či opatrení.

Jozef Zoričák,
vedúci oddelenia informatiky
Národný ústav pľúcnych chorôb

Keď sa hovorí o zdravotnom stave, pacient často počuje slová lekára: prevencia, nepodceňovať riziká, preventívne prehliadky. Pri problematike kyberbezpečnosti sa manažment a zdravotný personál správa podobne ako zlý pacient a tieto rady podceňuje. Stihne napraviť manažér kybernetickej bezpečnosti a oddelenie IT tento neželaný stav skôr, ako nastane poučenie z vlastnej chyby?

Roman Čupka,
hlavný konzultant
Progress a CEO Synapsa Networks

Obávajme sa nekompetentných politických rozhodnutí.

Adrian Kmeťko,
administrátor IT systému
Stredoslovenský ústav srdcových a cievnych chorôb

Obávať sa je potrebné všetkého, čo by mohlo ovplyvniť poskytovanie zdravotnej starostlivosti. Keďže naše informačné systémy úzko súvisia s podporou týchto činností, je nutné ich sledovať a riešiť každú anomáliu. Či už sú to vonkajšie vplyvy, alebo činnosť našich vlastných zamestnancov. Preto je dôležité sa v dnešnej dobe tejto téme čoraz viac aktívne venovať a hlavne školiť našich zamestnancov, ako týmto hrozbám predchádzať.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies

Pri uvedomení si toho, v akom stave je kyberbezpečnosť v našom zdravotníctve, by som sa obával všetkého a bohužiaľ aj toho najhoršieho. Mali by sme už riešiť sofistikované veci, ale pritom dnes vo veľkej časti rezortu budujeme bezpečnosť od základov. Máme tu reálne hrozby, kde ide o život.

Daniel Slezák,
IT technik
Národný ústav detskej tuberkulózy a respiračných chorôb

Moderné zdravotníctvo je závislé od informačných technológií a systémov – uľahčujú diagnostiku, liečbu, správu údajov a výskum, čo znamená, že kyberhrozby môžu mať fatálne následky. Najväčšie kyberhrozby sú nevenovanie pozornosti samotnej kyberbezpečnosti v inštitúciách a nedostatok financií. Zaistiť bezpečnosť je kľúčové pre zabezpečenie zdravia pacientov a udržanie dôvery verejnosti v zdravotný systém.

Pavol Vrabec,
manažér kybernetickej bezpečnosti
Univerzitná nemocnica Martin

Najväčším problémom je nedostatok kvalifikovaných zamestnancov a veľmi obmedzené finančné prostriedky. Tomu bohužiaľ zodpovedá aj celkový stav kyberbezpečnosti v zdravotníctve, ktorý nie je dobrý. Pozitívom je, že v poslednom období sa táto téma začala konečne „brať vážne“ a venuje sa jej viac pozornosti. Úspešný kybernetický útok na nemocnicu môže mať okrem finančných aj veľmi vážne dosahy na zdravie a životy našich pacientov.

Ján Poremba,
špecialista kybernetickej bezpečnosti AGEL SK

V zdravotníctve je veľa rôznych bezpečnostných rizík, ale veľmi často sa stáva, že zlyháva práve ľudský faktor. Ešte stále nie je v povedomí ľudí dostatočne ukotvená potreba dodržiavať bezpečnostné pravidlá ako prostriedok predchádzania bezpečnostným incidentom.

Július Selecký,
senior technický špecialista
ESET

Drucker, Kalavská, Pellegrini, Krajčí, Heger, Lengvarský, Palkovič, Dolinková. Toto je zoznam osôb poverených riadením rezortu zdravotníctva len za posledných päť rokov. Kyberbezpečnosť v zdravotníctve je koncepčná záležitosť. Správne nastavenie smerovania v oblasti kyberbezpečnosti je často závislé od kontinuity.

Roman Varga,
manažér kyberbezpečnosti
DÔVERA zdravotná poisťovňa

Očakávate, že sa najviac obávam hackerov, ransomvéru alebo iných kyberhrozieb? V skutočnosti sa najviac bojím ľudí, ktorí zdravotnícke technológie používajú. Tých, ktorí majú slabé heslá, zdieľajú osobné a zdravotné údaje s kýmkoľvek, klikajú na podozrivé odkazy alebo prílohy, ignorujú bezpečnostné aktualizácie a upozornenia a nevedia, ako sa zachovať v prípade kybernetického incidentu. Preto musíme zvýšiť povedomie a vzdelanie o kyberbezpečnosti medzi personálom, pacientmi, dodávateľmi, regulátormi aj verejnosťou.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC
Soitron

Ak by kybernetická bezpečnosť v zdravotníctve bola pacient, leží na traumatológii v ťažkom stave. To, že vôbec javí známky života, možno pripísať len mimoriadnej starostlivosti oddaných jednotlivcov na IT oddeleniach, ktorí mnohokrát pracujú nezištne nad rámec svojich ostatných povinností a snažia sa o „zázraky“. Pri hľadaní príčin je síce ľahké diagnostikovať dlhodobý nedostatok financovania a zanedbávanie zo strany manažérov, ale netreba zabudnúť, že celý sektor rieši aj oveľa väčšie a naliehavejšie problémy. Bohužiaľ, kým sa to nezmení, terapia pokračuje (aspoň) rôznymi náplasťami.

Stanislav Priščák,
IT špecialista
Východoslovenský ústav srdcových a cievnych chorôb

Čo sa týka kyberbezpečnosti v zdravotníctve, je veľkou výzvou kontinuálne dovzdelávanie už aj tak pracovne vyťaženého zdravotníckeho personálu, ktorého je na Slovensku nedostatok. Neznalosť aktuálnych rizík v oblasti kyberbezpečnosti môže zapríčiniť ľudskou chybou povolený prístup k citlivým údajom, ktoré môžu takto uniknúť alebo sa ich digitálna podoba nenávratne stratí.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Bude to už obohraná pesnička. Ransomvér, malvér, phishingové útoky a podobne. Hlavne však nedostatok finančných zdrojov, ktoré zdravotníctvo primárne potrebuje na svoj výkon. IT a bezpečnosť je to posledné, čo vedenie trápi. Pri rozhodovaní sa medzi nákupom defibrilátora alebo bezpečnostného softvéru je vopred jasné, kto je víťaz.

Marian Daníšek,
manažér IT infraštruktúry
Penta Hospitals

Neustále rastie počet kybernetických útokov na zdravotnícke zariadenia, ktoré sú lákavým cieľom, pretože spravujú citlivé pacientske dáta. Útoky môžu ohroziť zdravie či životy ľudí, takže útočníci často žiadajú vysoké výkupné. S príchodom umelej inteligencie bude intenzita a sofistikovanosť týchto útokov stúpať. V zdravotníctve zúfalo chýbajú odborníci na IT bezpečnosť. Problémom je tiež nízke povedomie o kyberbezpečnosti u zamestnancov, zastaraná a zložitá IT infraštruktúra.

Miroslav Odor,
manažér informačnej a kybernetickej bezpečnosti
Ministerstvo zdravotníctva SR

Vzhľadom na stav sektora predstavujú najvýznamnejšiu hrozbu ransomvérové útoky, ktoré vedú k obmedzeniu poskytovania zdravotnej starostlivosti. Ak chceme budovať odolné zdravotníctvo, musíme zlepšiť stav, v ktorom sa nachádza. Systémovým riešením budovania odolného zdravotníctva je zvyšovanie bezpečnostného povedomia, cesta cloudového prostredia, podpora vedenia a vyčlenenie dostatočných financií.

Martin Dzurilla,
vedúci IT oddelenia
Univerzitná nemocnica – Nemocnica svätého Michala

Obávajme sa najviac zdravotníkov samotných. Najväčšie riziká vznikajú aktivitou koncových používateľov. Ich správanie a vyhodnocovanie každodenných digitálnych aktivít v rutinnej práci sú kľúčové v rámci rizík. Aplikačné nástroje kyberbezpečnosti a osveta sú iba zmiernením rizík samotných. Zastávam jednoduché riešenia – používať zdravý sedliacky rozum či základné pravidlá kyberbezpečnosti. V jednoduchosti je krása.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ENISA nedávno vydala štatistiku, v ktorej porovnáva typické hrozby s motiváciou útočníkov. Zdravotné záznamy a lekárska elektronika stúpajú na rebríčku potenciálnych cieľov. Štátni zriaďovatelia zdravotníckych zariadení sú však naďalej pasívni a kyberbezpečnosť zostáva na poslednom mieste priorít. Pri pokračujúcom podceňovaní problematiky zo strany lekárskych komôr sa budem lekárov báť čoraz viac.

Tomáš Hettych,
viceprezident
ISACA

Zdravotnícky personál je špecifická kategória zamestnancov. Pre nich je najvyššia priorita chrániť zdravie a životy. Kyberbezpečnosť je v ich hodnotovom rebríčku veľmi nízko, čo ukazujú aj výsledky opakovaných auditov, ktoré objektívne hodnotia stav kybernetickej bezpečnosti v organizácii. A aj preto je v tomto sektore najväčšou výzvou následná implementácia opatrení a zvyšovanie povedomia.

Ján Grujbár,
generálny riaditeľ
Aliter Technologies

Kyberbezpečnosť v zdravotníctve čelí paradoxu: významná potreba ochrany citlivých dát a životne dôležitých systémov kontrastuje s celkovými nedostatočnými investíciami. Je, samozrejme, správne, že investície sú apriori sústredené hlavne na klinické vybavenie, no ochrana pred kybernetickými hrozbami by sa nemala odsúvať na poslednú koľaj. Rozšírenie investícií do kyberbezpečnosti je nevyhnutné pre odolné a bezpečné zdravotníctvo a zároveň by to nemalo byť na úkor klinického vybavenia.

Milan Haliena,
vedúci odboru informatiky
Fakultná nemocnica J. A. Reimana Prešov

Zdravotníctvo sa v posledných rokoch čoraz viac otvára smerom do cloudu a cesta späť je nemožná. Potrebujeme, aby naše dáta ostali správne a v bezpečí, preto je potreba venovať sa kybernetickej bezpečnosti pri prevádzke zdravotníckych systémov nevyhnutná. Niekedy je to adrenalínová skúsenosť, no vždy je to intelektuálna výzva a zväčša aj zábava.

Miroslav Chlipala,
riadiaci partner
BCH Advokáti Chlipala

V zmysle Smernice NIS II je zdravotníctvo odvetvím s vysokou úrovňou kritickosti, takže kyberbezpečnosť je tu zákonom potvrdenou nevyhnutnosťou. Každý zdravotník musí pochopiť a rešpektovať svoje povinnosti spojené s kyberbezpečnosťou. Okrem zdravého rozumu a dostatku financií výrazne pomôže vzdelávanie, trénovanie a overovanie správania pri simulovaných hrozbách a incidentoch.

Jaroslav Oster,
predseda správnej rady
Preventista.sk

Dôvody nízkej odolnosti zdravotníckych zariadení sú zrejmé bez hlbšej analýzy. Je to často silne zanedbaná infraštruktúra vyplývajúca z dlhodobého a vážneho podfinancovania. S tým úzko súvisí aj nízka úroveň zavedených bezpečnostných opatrení, a teda úplne logicky a nepopierateľne aj stav bezpečnostného povedomia personálu. A že je dôvod na obavy, potvrdzujú každoročné debaty na kongrese Nemocničné informačné systémy.

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

Ako bývalý „zdravotník“ podčiarknem to, čo pretrváva už desiatky rokov. Prienik alebo ochromenie zdravotných systémov je stále veľkým lákadlom mnohých útočníkov, lebo zdravotné dáta majú svoju cenu. Vysoké pracovné zaťaženie a stres môže spôsobiť, že si zamestnanci nedajú dostatočný pozor. Koľko zdravotníkov by odhalilo v pracovnom návale telefonát z falošného IT oddelenia? Veľkou výzvou pre útočníka by neboli ani voľne dostupné sieťové prvky na chodbách.

Michal Ďorda,
audítor kybernetickej bezpečnosti
auditori.it

Ako audítori kybernetickej bezpečnosti sa stretávame s častou výmenou vrcholového vedenia v nemocniciach, zdravotníckych zariadeniach a iných verejných a štátom riadených organizáciách. Častú výmenu ľudí nasleduje zmena vízie a smerovania organizácie, a teda aj plánov a financovania bezpečnostných opatrení. Nie je nič horšie, ak vám nefunguje kontinuita činností, čo je jedna zo základných domén v informačnej a kybernetickej bezpečnosti.