HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 31. OKTÓBRA – 2. NOVEMBRA 2025

Pri útoku sme rukojemníci všetci

ANKETA

Epidémie, ochorenia, či úrazy nás ohrozujú už tisícky rokov. A potom sme vstúpili do digitálnej éry. Tak sa pýtame profesionálov: Aké kybernebezpečenstvo na nás číha v zdravotníctve? Hovoríme o celom sektore aj o nás všetkých, lebo všetci sme jeho klientmi.

Jaroslav Ďurovka,
riaditeľ, Národné centrum kybernetickej bezpečnosti

Zdravotníctvo patrí medzi odvetvia, ktoré sú intenzívne vystavované kybernetickým hrozbám. Zdravotnícke zariadenia využívajú rôznorodé technológie a systémy s nerovnakou úrovňou ochrany, čo z nich robí lákavý cieľ pre útočníkov. Tých láka vysoký potenciál finančného obohatenia sa, keď využívajú falošnú dilemu, v ktorej proti sebe stoja finančná strata a ohrozenie ľudských životov. Bezpečnejšie zdravotníctvo však možno budovať postupnými krokmi. Pomôcť môže aj Európsky plán kybernetickej bezpečnosti nemocníc a zdravotníckych zariadení, ktorý je už v štádiu realizácie.

Miroslav Havelka,
lektor kybernetickej bezpečnosti, Laudeo

Príklad pre všetkých? Tak si predstavte si, že v žiadnej lekárni si nebudete môcť vyzdvihnúť e-recept. Alebo že sa o svojom zdravotnom stave ráno dočítate na webe.

Jakub Berthoty,
advokát, Dagital Legal

V zdravotníckom systéme by nemal „každý vidieť všetko". Prístup k zdravotným záznamom pacienta by interne mal mať len ten zdravotnícky personál, ktorý ho skutočne potrebuje. Napríklad preto, že pacienta ošetruje. Za nedostatky v internom riadení prístupov už bolo v zahraničí udelených naozaj veľa pokút podľa GDPR. Uvidíme, aké nedostatky vzídu z kontroly verejných lekární, ktoré mal tento rok v pláne kontrol Úrad na ochranu osobných údajov SR.

Viktor Balušeskul,
manažér kybernetickej bezpečnosti, Univerzitná nemocnica L. Pasteura Košice

K najväčším nebezpečenstvám v zdravotníckom sektore patrí enormný nárast počtu ransomvérových útokov. Môžu spôsobiť obmedzenie, v horších prípadoch až celkový výpadok poskytovania zdravotnej starostlivosti a tiež odcudzenie a následné zneužitie citlivých pacientskych údajov. Tieto útoky sú vedené čoraz sofistikovanejšie, často aj s využitím umelej inteligencie, čo značne zvyšuje pravdepodobnosť ich úspešnosti.

Ivana Lysinová,
audítorka kybernetickej bezpečnosti, Cyllium

Zdravotnícke zariadenia patria k takzvaným mäkkým cieľom, čiže k miestam s veľkou koncentráciou ľudí a nízkou úrovňou zabezpečenia. Najzraniteľnejšie sú z pohľadu fyzickej bezpečnosti koncových zariadení. A neuzamknutý počítač, pri ktorom nik nie, nie je v zdravotníckych zariadeniach ničím výnimočným.

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

Toho, čo hrozí zdravotníctvu, nie je málo. Ransomvér, ako tomu bolo v lete v Nymburku, phishing a sociálne inžinierstvo a aj útoky na dodávateľské reťazce. Príčiny sa notoricky opakujú - nedostatok kvalifikovaného personálu, zastaralé systémy, oklieštené rozpočty. A najväčšie bezpečnostné riziko sú koncoví používatelia, ktorých prioritou je pacient a nie počítač.

Lenka Gondová,
prezidentka, ISACA

Najväčším rizikom v zdravotníctve je kombinácia starých IT systémov, slabého riadenia kyberbezpečnosti a personálu pracujúceho pod tlakom. S digitalizáciou a umelou inteligenciou prichádzajú nové hrozby. Stačí jediný kvalitne pripravený phishingový e-mail či nezabezpečené zariadenie a môže byť ochromená nemocnica aj ohrozené životy pacientov.

Roman Body,
riaditeľ pre digitálne technológie, cloud a modernú infraštruktúru, Eviden Slovakia

Ohrozenie IT systémov v zdravotníctve môže mať priame a okamžité dopady na zdravie a životy obyvateľov aj na chod štátu ako celku, keďže ide o najkritickejšie služby. Nemocnice zamestnávajú ľudí s rôznou úrovňou kvalifikácie a preto najväčšie nebezpečenstvo spočíva v ich zneužití. Človek je najslabším článkom a preto je mimoriadne dôležité systematicky sa venovať vzdelávaniu a školeniu.

Tomáš Valenta,
riaditeľ, Check Point Software Technologies na Slovensku

Technologické riešenia a umelá inteligencia dokážu v kybernetickej bezpečnosti postaviť výnimočnú ochranu. Obávam sa ľudskej zákernosti a zlomyseľnosti.

Ivan Makatura,
predseda, Asociácia kybernetickej bezpečnosti

Lekári často zdôrazňujú, že prevencia je pre život dôležitejšia než liečba. Alebo sa práve rozprávame o kybernetickej bezpečnosti? V oboch prípadoch platí: čím menej zraniteľností, tým zdravší systém.

Ján Benka,
audítor kybernetickej bezpečnosti, Soitron

Zdieľané účty sú v zdravotníctve stále bežnou no veľmi rizikovou praxou najčastejšie na úrovni ambulantného zdravotníckeho personálu. Znemožňuje to určiť, kto vykonal konkrétny úkon a vystavuje systém riziku zneužitia či úniku zdravotných údajov. Výzvou je preto nájsť riešenie s rovnováhou medzi bezpečnosťou a komfortom použitia, napríklad zaviesť jednoznačné identity používateľov a použiť praktické formy prihlásenia ako čipové karty, biometria, passkeys prípadne skrátiť trvanie relácie, ktoré zdravotníkov nebrzdia pri výkone starostlivosti.

Ivan Kopáčik,
bezpečnostný expert, Gordias

Úplne postačuje spomenúť „bežné nebezpečenstvá". Únik citlivých zdravotných údajov, útoky ransomvérom paralyzujúce nemocnice, manipulácia s výsledkami vyšetrení či zneužitie IoT zariadení. Ako to môže ohrozovať zdravie a životy pacientov netreba ďalej rozvádzať...

Marián Daníšek,
IT manažér, Penta Hospitals

Zdravotníctvo čelí rastúcemu počtu útokov na citlivé dáta, pričom chýbajú IT bezpečnostní odborníci. Slabé povedomie zamestnancov, zastaraná infraštruktúra a nástup umelej inteligencie zvyšujú riziká. Kyberbezpečnosť je otázkou života a najzraniteľnejší článok je človek.

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

Aj zdravotnícky systém ako aj všetky tie ostatné je zraniteľný súčasnými kybernetickými hrozbami. Riziko straty dát, ich publikácia či neoprávnené pozmenenie hrozí poškodením zdravia alebo dokonca fatálnymi následkami. Je dôležité sledovať vývoj hrozieb a reagovať protiopatreniami, či už technologickými podľa ekonomických možností organizácie, ale hlavne, ako už bolo veľakrát povedané vzdelávaním používateľov, ktorí zostávajú v celom procese najzraniteľnejším prvkom.

Štefan Pilár,
advokát, AK Signum

Zdravotníctvo je čoraz viac závislé od technológií, no systémy sú prevažne zastarané a navzájom nekompatibilné. Ďalšou závislosťou sú dodávatelia s rôznou úrovňou zabezpečenia, bez adekvátneho procesu riadenia rizík a náležitej kontroly. A kde začať s výpočtom ohrození? Kritickým je používateľ, ktorý vníma kyberbezpečnosť ako prekážku v nerušenej práci a úprimne sa usiluje o výnimky zo zavedených kyberpravidiel.

Marek Zeman,
generálny riaditeľ, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

V zdravotníctve sa všetci bojíme útokov, ransomvéru čo ničí dáta, útočníkov odstavujúcich nemocnicu počas operácie. Nazerajme na zdravotníctvo ako na komplex, obsahujúci rôznorodých dodávateľov, zastarané, nechránené systémy, pričom je potrebné zabezpečovať bezpečnosť dát a procesov a systémov. Riešiť je potrebné všetko, ale začať musíme od rozumného plánu a zoznamu ohodnotených rizík.

Timea Tomčová,
manažérka útvaru IT architektúra a IT bezpečnosť, Union

Subjekty zdravotníckeho systému dnes chránia nielen zdravie pacientov ale aj informačné systémy a dáta. Kybernetické útoky môžu narušiť poskytovanie zdravotnej starostlivosti rovnako vážne ako epidémie – ohrozujú dostupnosť údajov aj samotný výkon liečby.

Anton Berežňák,
vedúci oddelenia IT prevádzky a technického rozvoja, Operačné stredisko záchrannej zdravotnej služby SR

Vymenovávať formy kybernebezpečenstva v zdravotníctve nie je podstatné, keďže možné vektory útokov sú známe alebo sú odvoditeľné od technologického zázemia. Za hlavné riziká považujem zamestnanca a zanedbanie adekvátneho technologického rozvoja. Mitigácia rizík musí byť jedným z kľúčových krokov zodpovednej organizácie, aby dopad na kontinuitu doručovania služieb nebol fatálny.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti, Aliter Technologies

Najväčšie riziko predstavuje únik citlivých zdravotných údajov. Ide o kombináciu extrémne citlivých informácií sústredených na jednom mieste a často nedostatočne chránených. Zdravotníctvo navyše bojuje s podfinancovaním, čo z kyberbezpečnosti robí „luxus", na ktorý sa často zabúda. Až do chvíle, keď je neskoro.

Miroslav Chlipala,
advokát, Advokáti Chlipala

Poskytovatelia zdravotnej starostlivosti sú často prevádzkovateľmi základnej služby a preto musia plniť povinnosti v oblasti riadenia rizík, hlásenia a riešenia incidentov. Implementácia adekvátnych bezpečnostných opatrení vyžaduje množstvo času a významne zasahuje aj do rozpočtu. Najväčšie riziká vidím v nedodržaní právnych požiadaviek na ochranu informačných systémov a osobných údajov.

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

Vždy a úprimne sa vyľakám, keď mi prídu výsledky od lekára cez Gmal a nezaheslované. Môže za to nevedomosť, ľahostajnosť, alebo časový stres? Dvakrát do roka vzdelávam lekárov v ochrane osobných údajov a nevzdávam to a stále im opakujem zásady. Obávajme sa katastrofického incidentu v zdravotníctve takých rozmerov, ako bol kataster. Je to najhorší možný spôsob, ako si uvedomiť naliehavosť situácie.

Ondrej Krajč,
kyberbezpečnostný architekt, ESET

Veľkou hrozbou v zdravotníctve nie je len nedostatok nástrojov a financií, ale aj falošná ilúzia zabezpečenia. Často nastáva takzvaná „papierová bezpečnosť". Riešenia sú síce zakúpené, ale nikto ich aktívne nemonitoruje. Ignorované varovania a zanedbané konzoly sú pritom rovnako nebezpečné ako odomknutá serverovňa alebo neaktualizované záplaty zraniteľností.

Tomáš Zaťko,
etický hacker, CEO, Citadelo

Hromadný únik zdravotnej dokumentácie - v zahraničí sa to už stalo. Paralýza zdravotníckeho systému na hodiny či dni - ochutnávku sme už mali aj na Slovensku. Úmrtia v dôsledku nefunkčnosti systémov. Vyhasnuté životy, ktoré vyhasnúť nemuseli. Veľmi si prajem, aby to tam nezašlo. A zároveň ďakujem všetkým bezpečákom v zdravotníctve, lebo aj vďaka nim sa to zatiaľ nestalo.