HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 25. – 27. OKTÓBRA 2024

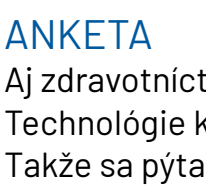
Opakujeme to znova. Ide o život!

ANKETA

Aj zdravotníctvo prešlo do kyberpriestoru. Technológie kontrolujú naše zdravie a aj život. Takže sa pýtame, čo je akútnym problémom, a teda pálčivou úlohou kyberbezpečnosti v zdravotníctve.

Adrian Kmeťko,
vedúci oddelenia IT,
Stredoslovenský ústav srdcových a cievnych chorôb Banská Bystrica

Kyberbezpečnosť je aktuálna téma vo všetkých oblastiach. Obzvlášť by sa malo prihliadať na oblasti, kde ide o život človeka. Toto je potrebné si uvedomiť a tak k tomu aj pristupovať. Odhliadnuc od nedostatku finančných prostriedkov, žiadne technické zariadenie nedokáže absolútne eliminovať chyby človeka, a preto si myslím, že vzdelávanie a zvyšovanie povedomia na všetkých úrovniach je tou pálčivou úlohou.



Milan Haliena,
vedúci odboru informatiky,
FNsP J. A. Reimana Prešov

Najakútnejším problémom kybernetickej bezpečnosti v zdravotníctve je zvýšenie bezpečnostného povedomia u zdravotníckych pracovníkov, pretože najkritickejším článkom v reťazci kybernetickej bezpečnosti je človek. Pri bezpečnostne vzdelanom a skúsenom pracovníkovi je aj práca manažérov kybernetickej bezpečnosti a pracovníkov zabezpečujúcich prevádzku informačných technológií omnoho jednoduchšia.

Zuzana Motúzová,
advokátka,
Motúzová & Lacko Advokátska kancelária

Bezpečnosť zdieľania a spracúvania dát pacientov na účely diagnostiky a liečenia. Ale taktiež si myslím, že by sme mali uvažovať aj o rizikách použitia generatívnej AI do budúcnosti.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC,
Soitron

Kybernetická bezpečnosť v zdravotníctve je iba pomaly sa zotavujúci pacient. Technologický dlh je prekážkou pri preventívnych opatreniach, nedostatok odborníkov a podfinancovanie brzdia terapiu. Inak povedané, ani za uplynulý rok sa stav nezmenil a dôsledky môžu byť aj naďalej fatálne – doslova.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Okrem získania financií na riešenie kybernetickej bezpečnosti z napätých zdravotníckych rozpočtov považujem za akútny problém ochranu citlivých zdravotníckych údajov tak, aby tieto ochrany čo najmenej obmedzovali zdravotníkov pri výkone ich náročnej práce a boli pre nich „neviditeľné“ a používateľsky prívetivé.

Stanislav Priščák,
IT špecialista,
Východoslovenský ústav srdcových a cievnych chorôb

Trápia nás najmä slabé bezpečnostné personálne kapacity. Máme desiatky zdravotníckych systémov a je nás tu na ne iba limitovaný počet. Slabinou celého systému je povedomie zdravotníckych pracovníkov, ktorí bezpečnosť považujú za druhoradou prioritu, a preto ich musíme neustále presviedčať o dôležitosti kyberbezpečnosti.

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies na Slovensku

Nemocnice, polikliniky a ordinácie sú preplnené rôznymi zariadeniami pripojenými do internetu. V tom lepšom prípade si ešte správca pamätá, kde sú a kedy sa im končí životnosť. V tom najhoršom prípade tam už útočník potichu kontroluje sieť a sťahuje citlivé údaje. Bezpečnosť a správa IoT zariadení sú dennodennou výzvou kyberbezpečnosti v zdravotníctve.

Tomáš Hettych,
viceprezident,
ISACA

Podceňovanie a bagatelizácia požiadaviek kyberbezpečnosti, prípadne orientácia len na papierovú a technologickú bezpečnosť. Samozrejme, že problémom sú aj finančné zdroje a ich efektívne využitie. Pálčivou úlohou je analýza rizík a dosahov. Obe analýzy ukážu kritické procesy, zraniteľnosti a hrozby zdravotníckych zariadení.

Martin Zajíček,
manažér kybernetickej bezpečnosti,
Medirex

Zdravotníctvo ako také rieši problém s nedostatkom financií, s ich neefektívnym využívaním či neustálymi zmenami financovania. Výsledkom je okrem iného zastaralá, často už nepodporovaná infraštruktúra. Pálčivou úlohou kybernetickej bezpečnosti v zdravotníctve je „bojovať“ o obmedzené zdroje a hľadať efektívne riešenia. Na to je potrebné zrealizovať analýzu prostredia a priorizovať jednotlivé kroky podľa rizikovosti jednotlivých oblastí kybernetickej bezpečnosti.

Marian Daníšek,
manažér IT infraštruktúry,
Penta Hospitals

Zdravotníctvo má obmedzený budget na IT bezpečnosť a nedostatok skúsených interných špecialistov zodpovedných za kyberbezpečnosť. Priorizácia prevádzkových potrieb – rýchlosť, zdieľanie informácií nad informačnou bezpečnosťou. Nezabezpečené zdravotnícke zariadenia a systémy, ktoré súvisia s technologickým rozvojom IoT, AI a pripojením do internetu. A nad tým všetkým prepracovaný a slabo vyškolený personál.

Michal Sekula,
bezpečnostný konzultant,
Eviden Slovakia

Zvyčajnou odpoveďou je, že sú to nedostatočné finančné a ľudské zdroje. Zdroje však zodpovedajú prioritám a povedomiu pracovníkov v zdravotníctve, predovšetkým tých, ktorí o tom rozhodujú. Zastaranosť IT prostredia a aplikácií, citlivosť dát a veľké dosahy v prípade narušenia chodu nemocnice sú lákadlom. Nárast množstva kyberútokov v zdravotníctve a úspešnosť phishingových kampaní je skôr dôsledkom ako príčinou.

Roman Čupka,
hlavný konzultant,
Progress a CSO Istrosec

Keby som chcel byť vtipný, poviem, že najväčší problém sú zrušené Zajacove „dvadsaťkorunáčky“. Mladšia generácia tento vtip pravdepodobne nepochopí. Alebo to bude pre nich rovnako náročné, ako keď má tá staršia generácia veľkého množstva presluhujúcich lekárov porozumieť principiálnej potrebe bezpečnosti v dobe digitálnej transformácie.

Roman Varga,
manažér kyberbezpečnosti,
Dôvera zdravotná poisťovňa

V ambulanciách na základe nedávneho prieskumu je to nedostatočné vzdelávanie v oblasti IT bezpečnosti, nedostatočné zálohovanie a obnova dát, neschopnosť identifikovať bezpečnostné incidenty a hrozby a používanie súkromných emailov na pracovné účely. Riešením je zaviesť pravidelné praktické školenia, bezpečné automatizované zálohovacie systémy, ochranu na detekciu a reakciu na kybernetické incidenty a politiku používania výhradne pracovných e-mailov s dvojfaktorovou autentifikáciou.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti,
Aliter Technologies

Podľa môjho názoru je to dlhodobá nedostatočná priorita kybernetickej bezpečnosti. Zdravotníctvo v niektorých regiónoch Slovenska čelí doslova existenčným problémom, preto investície smerujú primárne do zabezpečenia prevádzky pre starostlivosť o pacientov. Kybernetická bezpečnosť je preto často prehliadaná, čo zvyšuje riziko únikov citlivých dát a výpadkov v dôsledku kyberútokov, ako to vidíme v zahraničí.

Michal Ďorda,
partner,
Cyllium

Jedným z opakujúcich sa problémov je presvedčiť každého nového riaditeľa o potrebe investícií do bezpečnosti a pokračovania rozbehnutých projektov skrz možné vysoké dosahy na prevádzku zdravotníckych zariadení v prípade výskytu bezpečnostných incidentov. Kto by už len na nás útočil.;) Časté výmeny vedení spôsobujú nesystematické riadenie bez zásadných reforiem a neefektívne financovanie.

Ondrej Kubovič,
špecialista na digitálnu bezpečnosť, ESET

Jednou z najväčších výziev v zdravotníctve je už roky ochrana pred ransomvérom, ktorý dokáže vyradiť kritické systémy v kľúčových momentoch, a tým ohroziť nielen chod zariadenia, ale aj životy pacientov. Predísť alebo aspoň zachytiť takéto prípady v ranom štádiu nie je jednoduché, no je to možné, ak má nemocnica dobre zmapované svoje IT prostredie, udržiava ho aktualizované a monitoruje v ňom potenciálne podozrivé aktivity.

Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Primárne problémy sú štyri. Hlboko podfinancovaný rezort, vďaka čomu je kybernetická bezpečnosť vnímaná ako okrajový problém. S financiami úzko súvisí stav IKT. V treťom rade nedostatočne školení používatelia s radom nesprávnych návykov. A štvrtým problémom je aktuálny celospoločenský problém – nedostatok kvalifikovaných odborníkov pre riadenie kybernetickej bezpečnosti. Úlohou je rozmotať tento gordický uzol.

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

Peniaze. Presnejšie – ich nedostatok. Chýba investičný rozpočet na modernizáciu sieťovej a bezpečnostnej infraštruktúry. Chýba prevádzkový rozpočet na zaplatenie odborníkov a kvalitných odborných služieb. Diagnóza je však nesprávna – pretože akútny problém už dávno prerástol do chronického.

Miroslav Chlipala,
advokát,
Advokáti Chlipala

Zdravotnícke zariadenia by mali aktívne participovať na tvorbe právnych predpisov a presadzovať realistické termíny na implementáciu. Synergia s inými právnymi predpismi by zabránila aj zbytočnému administratívnemu zaťaženiu. Zariadenia by mali spolupracovať, vymieňať si skúsenosti a spoločne hľadať riešenia. Akútnym problémom kyberbezpečnosti je ochrana citlivých zdravotných údajov aj zabezpečenie kontinuity poskytovania zdravotnej starostlivosti

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

Úlohou je primeraná regulácia „správania“ k dátam, spôsob ich zabezpečenia a ochrany. Keďže zavádzanie nástrojov kyberochrany informačných systémov sa stáva štandardom, je nevyhnutné sa intenzívnejšie zameriavať na slabé miesta. Jedným z nich je interný zamestnanec. A preto prácu s koncovým používateľom vo forme edukácie a zvyšovania jeho informačného povedomia vnímam ako trvale aktuálnu tému..

Milan Zorvan,
vedúci oddelenia IT,
FNsP F. D. Roosevelta Banská Bystrica

Akútnym problémom u nás, ako aj v celom zdravotníckom sektore je nedostatok kvalifikovaného personálu. Ďalším problémom v zdravotníctve je narastajúci počet kybernetických útokov, ktoré ohrozujú bezpečnosť pacientskych údajov, a tým poskytovanie zdravotníckych služieb. Ochrana dát, zvyšovanie povedomia o kyberbezpečnosti medzi personálom sú hlavné výzvy, tomu je potrebné sa urýchlene venovať.

Ivan Kopáčik,
bezpečnostný expert,
Gordias

V slovenských podmienkach sú bohužiaľ akútnejšie problémy ako kyberbezpečnosť. Vo všeobecnosti sú však aktuálne kyberbezpečnostné problémy súvisiace so zdravotníctvom v niekoľkých rovinách – útoky na systémy ako ransomvér, phishing, DDoS, zneužitie pokročilých technológií – AI, ochrana zdravotníckych zariadení, ktoré sú dostupné cez počítačovú sieť. V každej rovine má slovenské zdravotníctvo akútne úlohy.

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

Zdravotníctvo spracúva a disponuje veľmi citlivými osobnými údajmi. Je potrebné ich chrániť pred kybernetickými útokmi, ktoré by mohli napríklad paralyzovať prevádzku nemocníc/ambulancií, ohroziť životy pacientov, zmeniť nastavenia liečebných prístrojov. V neposlednom rade môžu byť zneužité a poškodiť súkromie pacienta či reputáciu nemocníc či ambulancií.

Richard Kiškováč,
generálny riaditeľ,
Elkan

Zdravotníctvo je jedinečný segment kyberpriestoru s vlastnými hrozbami a rizikami a na ich riešenie je potrebný koncepčný a strategický prístup. Formálne stanovenie povinností legislatívou nepostačuje. Akútnym problémom je preto absencia jednotnej koncepcie kyberbezpečnosti. Mala by byť flexibilná a zohľadňovať špecifické potreby rôznych zariadení. Prispelo by to k reálnemu zvýšeniu úrovne kyberbezpečnosti aj k efektivite vynakladaných zdrojov.