UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Kybernetická bezpečnosť v zdravotníckych zariadeniach

(metodika pre subjekty verejnej správy)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

ÚVOD

Kybernetické útoky predstavujú v dnešnom digitálnom svete závažný celospoločenský problém a vážne ohrozujú fungovanie a činnosti nielen veľkých firiem, ale aj stredných či malých spoločností, jednotlivcov a fyzické osoby nevynímajúc. Počet útokov v kybernetickom priestore neustále narastá, pričom ich podoba je čoraz nenápadnejšia a útočníci využívajú akékoľvek slabé miesta v zabezpečení takmer okamžite. Útoky sú cielené nielen na vládne inštitúcie, finančné služby, či výrobný priemysel, ale bohužiaľ aj na oblasť zdravotníctva a zdravotnícke zariadenia, akými sú veľké nemocnice alebo aj malé ambulancie. Väčšina kybernetických útokov, ktoré smerujú na oblasť poskytovania zdravotnej starostlivosti je zameraná na krádež informácií o pacientoch alebo na zašifrovanie takýchto údajov v informačných systémoch poskytovateľov zdravotnej starostlivosti s následným požadovaním výkupného za ich dešifrovanie, prípadne aj za ďalšie nezverejnenie uniknutých citlivých údajov.

Zdravotnícke zariadenia sa prechodom na elektronické zdravotníctvo stali efektívnejšie v poskytovaní služieb zdravotnej starostlivosti, pričom sa nevyhnutne musia spoliehať na množstvo softvérových aplikácií a systémov, ktoré musia byť prevádzkované v rámci ich počítačových sietí. To im umožňuje realizáciu rôznych činností, ako sú napríklad spracúvanie zdravotných záznamov pacientov, prevádzka laboratórií, lekární, operačných plánov, ale aj manažment sterilizácie zdravotníckeho vybavenia, organizáciu stravovania, skladových zásob či technickej prevádzky a mnohých ďalších s prevádzkou zdravotníckeho zariadenia súvisiacich činností. Dnes už nemocnice nedokážu efektívne fungovať bez informačných a komunikačných technológií. Mnohé zariadenia a prístroje navyše využívajú na prenos údajov bezdrôtové siete, čo zvyšuje nároky na zabezpečenie kvalitnej a bezpečnej sieťovej infraštruktúry.

V nemocničných sieťach prebieha riadiaca komunikácia, ktorá zabezpečuje fungovanie diagnostických, liečebných, ale aj ďalších podporných zariadení a prístrojov, od ktorých závisí zdravie, ale aj životy pacientov. Útoky na takúto infraštruktúru preto dokážu oveľa viac než len získať citlivé údaje. Dokážu vážnym spôsobom narušiť každodennú prevádzku zdravotníckych zariadení. Dnes už nielen veľké nemocnice, ale aj malé zdravotnícke zariadenia, či individuálni poskytovatelia zdravotnej starostlivosti musia prijímať potrebné kroky a opatrenia na zabezpečenie svojich aktív, keďže tieto sa čoraz častejšie stávajú terčom kybernetických útokov. Na rozdiel od iných priemyselných odvetví, dopad kybernetických útokov tu má nielen ekonomické, ale najmä život ohrozujúce následky. Aj preto je nevyhnutné, aby investície smerovali nielen do služieb poskytovania zdravotnej starostlivosti, ale aj do ich zabezpečenia v online, resp. kybernetickom priestore. Nedostatočná pozornosť zo strany správcov nemocníc v tejto oblasti je pochopiteľná, keďže títo sa zameriavajú primárne na starostlivosť o pacientov a nie na kybernetické problémy, ktorým sa v minulosti nemuseli venovať. Navyše zadlženosť zdravotníckych zariadení v našich podmienkach má za následok, okrem iného aj to, že sa na obnovu IT vybavenia vynakladá len minimum prostriedkov z ich rozpočtov, a zastarané a nezabezpečené zariadenia tak zvyšujú riziko ich možného zneužitia.

Na ochranu zdravotníckych zariadení a citlivých údajov pacientov našťastie myslí a aj legislatíva v oblasti kybernetickej bezpečnosti. Nemocničné informačné systémy (NIS) a zdravotnícke zariadenia predstavujú takzvanú kritickú infraštruktúru, t. j. infraštruktúru, bez ktorej spoločnosť nie je schopná plniť niektoré zo svojich základných funkcií. Pre vysokú hodnotu citlivých údajov, ako sú zdravotné záznamy, osobné či finančné údaje pacientov a pre potenciál narušiť poskytovanie životne dôležitých služieb sú zdravotnícke zariadenia a ich systémy častým cieľom kybernetických útokov. Aj preto, sú na

Slovensku prevádzkovatelia NIS zaradení medzi prevádzkovateľov základných služieb, a to podľa Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

1 PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centrá vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Nemenej dôležitým výstupom projektu je doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu a možnosť poskytovania **expertných činností** pre akreditované CSIRT tímy v SR za účelom rýchlejšej a adekvátnejšej reakcie na kybernetické bezpečnostné incidenty.

2 KYBERNETICKÁ BEZPEČNOSŤ V ZDRAVOTNÍCKYCH ZARIADENIACH

2.1 ÚVOD

Kybernetické útoky predstavujú v dnešnom digitálnom svete závažný celospoločenský problém a vážne ohrozujú fungovanie a činnosti nielen veľkých firiem, ale aj stredných či malých spoločností, jednotlivcov a fyzické osoby nevynímajúc. Počet útokov v kybernetickom priestore neustále narastá, pričom ich podoba je čoraz nenápadnejšia a útočníci využívajú akékoľvek slabé miesta v zabezpečení takmer okamžite. Útoky sú cielené nielen na vládne inštitúcie, finančné služby, či výrobný priemysel, ale bohužiaľ aj na oblasť zdravotníctva a zdravotnícke zariadenia, akými sú veľké nemocnice alebo aj malé ambulancie. Väčšina kybernetických útokov, ktoré smerujú na oblasť poskytovania zdravotnej starostlivosti je zameraná na krádež informácií o pacientoch alebo na zašifrovanie takýchto údajov v informačných systémoch poskytovateľov zdravotnej starostlivosti s následným požadovaním výkupného za ich dešifrovanie, prípadne aj za ďalšie nezverejnenie uniknutých citlivých údajov.

Zdravotnícke zariadenia sa prechodom na elektronické zdravotníctvo stali efektívnejšie v poskytovaní služieb zdravotnej starostlivosti, pričom sa nevyhnutne musia spoliehať na množstvo softvérových aplikácií a systémov, ktoré musia byť prevádzkované v rámci ich počítačových sietí. To im umožňuje realizáciu rôznych činností, ako sú napríklad spracúvanie zdravotných záznamov pacientov, prevádzka laboratórií, lekární, operačných plánov, ale aj manažment sterilizácie zdravotníckeho vybavenia, organizáciu stravovania, skladových zásob či technickej prevádzky a mnohých ďalších s prevádzkou zdravotníckeho zariadenia súvisiacich činností. Dnes už nemocnice nedokážu efektívne fungovať bez informačných a komunikačných technológií. Mnohé zariadenia a prístroje navyše využívajú na prenos údajov bezdrôtové siete, čo zvyšuje nároky na zabezpečenie kvalitnej a bezpečnej sieťovej infraštruktúry.

V nemocničných sieťach prebieha riadiaca komunikácia, ktorá zabezpečuje fungovanie diagnostických, liečebných, ale aj ďalších podporných zariadení a prístrojov, od ktorých závisí zdravie, ale aj životy pacientov. Útoky na takúto infraštruktúru preto dokážu oveľa viac než len získať citlivé údaje. Dokážu vážnym spôsobom narušiť každodennú prevádzku zdravotníckych zariadení. Dnes už nielen veľké nemocnice, ale aj malé zdravotnícke zariadenia, či individuálni poskytovatelia zdravotnej starostlivosti musia prijímať potrebné kroky a opatrenia na zabezpečenie svojich aktív, keďže tieto sa čoraz častejšie stávajú terčom kybernetických útokov. Na rozdiel od iných priemyselných odvetví, dopad kybernetických útokov tu má nielen ekonomické, ale najmä život ohrozujúce následky. Aj preto je nevyhnutné, aby investície smerovali nielen do služieb poskytovania zdravotnej starostlivosti, ale aj do ich zabezpečenia v online, resp. kybernetickom priestore. Nedostatočná pozornosť zo strany správcov nemocníc v tejto oblasti je pochopiteľná, keďže títo sa zameriavajú primárne na starostlivosť o pacientov a nie na kybernetické problémy, ktorým sa v minulosti nemuseli venovať. Navyše zadlženosť zdravotníckych zariadení v našich podmienkach má za následok, okrem iného aj to, že sa na obnovu IT vybavenia vynakladá len minimum prostriedkov z ich rozpočtov, a zastarané a nezabezpečené zariadenia tak zvyšujú riziko ich možného zneužitia.

Na ochranu zdravotníckych zariadení a citlivých údajov pacientov našťastie myslí a aj legislatíva v oblasti kybernetickej bezpečnosti. Nemocničné informačné systémy (NIS) a zdravotnícke zariadenia predstavujú takzvanú kritickú infraštruktúru, t. j. infraštruktúru, bez ktorej spoločnosť nie je schopná plniť niektoré zo svojich základných funkcií. Pre vysokú hodnotu citlivých údajov, ako sú zdravotné záznamy, osobné či finančné údaje pacientov a pre potenciál narušiť poskytovanie životne dôležitých služieb sú zdravotnícke zariadenia a ich systémy častým cieľom kybernetických útokov. Aj preto, sú na

Slovensku prevádzkovatelia NIS zaradení medzi prevádzkovateľov základných služieb, a to podľa Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

2.2 NIEKTORÉ ZNÁME PRÍPADY KYBERNETICKÝCH ÚTOKOV NA ZDRAVOTNÍCKE ZARIADENIA

Prečo je kybernetická bezpečnosť v zdravotníctve dôležitá?

Podľa správy Európskej agentúry pre kybernetickú bezpečnosť (ENISA) z októbra 2025 patrí z pohľadu odvetví zdravotníctvo medzi päť najčastejších cieľových sektorov NIS2 v EÚ (NIS2 aktualizovaná verzia smernice NIS - *Network and Information Security*). Spoločne s verejnou správou, dopravou, digitálnou infraštruktúrou a energetikou tak patria k najrizikovejším a najohrozenejším sektorom.

Snahou útočníkov je získať prístup k nemocničnému počítaču, serveru s informačným systémom nemocnice, alebo iným sieťovým zariadeniam a aktívnym medicínskym prístrojom a využiť ich na vykonávanie škodlivých aktivít. Napríklad, útočník môže rozposlať škodlivý kód alebo škodlivý softvér ako súčasť e-mailovej správy, ktorý po spustení infikuje niektorý z počítačov v nemocničnej sieti a následne sa môže šíriť aj na ostatné zariadenia, vrátane medicínskeho vybavenia a prístrojov, ktoré nemusia byť dobre chránené, t. j. používajú už nepodporované verzie operačných systémov, nemajú antivírusovú ochranu, aplikované najnovšie aktualizácie softvérových produktov a pod. K najčastejším aktivitám útočníkov aj v prostredí zdravotníckych zariadení patrí skenovanie a mapovanie ich počítačovej siete, získavanie fyzického prístupu k aktívnej medicínskej technike, doručovanie škodlivého softvéru (malware) prostredníctvom elektronickej pošty, dodávateľské reťazce, cez ktoré môže do nemocnice prísť skrytý softvér, alebo škodlivý kód, krádeže zariadení, monitorovanie bezdrôtových signálov, ale aj hrozby zvnútra a to tak úmyselné, ako aj neúmyselné.

Závažnosť problému kybernetických útokov je možné dokumentovať na reálnych prípadoch, ktoré už v nedávnej minulosti poskytovanie zdravotnej starostlivosti ochromili. Napríklad, v máji 2017 sa útočníkom podaril kybernetický útok pomocou ransomware WannaCry na britskú národnú zdravotnú službu, a ktorý mal devastačný dopad na nemocnice naprieč celým Spojeným kráľovstvom. Podľa odhadov stál tento útok britskú národnú zdravotnú službu takmer 92 miliónov libier. Útočníci využili zraniteľnosti v starších verziách operačného systému Windows, cez ktoré infikovali najmenej 16 zdravotných stredísk a desaťtisíce počítačov, čo viedlo k zrušeniu takmer 20 000 návštev pacientov a ochromilo viac ako 1 200 diagnostických zariadení.

V roku 2018 sa uskutočnil kybernetický útok na najväčšiu zdravotnú sieť v Singapure SingHealth. Útočníkom sa podarilo získať prístup k osobným údajom viac ako 1,5 milióna pacientov, pričom uniknuté údaje obsahovali napríklad aj informácie o predpisovaných liekoch. Vyšetrovania po útoku odhalili infekciu škodlivým softvérom na jednom z počítačov, ktorú útočníci použili na získanie prístupu k databáze pacientov.

Univerzitná nemocnica Charles-Nicolle v severofrancúzskom Rouene sa v roku 2019 taktiež stala obeťou ransomvérového útoku. Škodlivý softvér infikoval až šesťtisíc počítačov naprieč piatimi budovami, ktoré komplex nemocnice pokrýva. Zdravotnícky personál musel kvôli incidentu čeliť problémom pri počítačovom spracovaní lekárskych predpisov, správ alebo posudkov. Incident sa dotkol aj komunikácie medzi opatrovateľmi a rôznymi nemocničnými službami.

Ďalší z útokov, ktorý sa odohral v roku 2020, bol cielený na sieť zdravotníckych zariadení Universal Health Services, ktorá prevádzkuje viac ako 400 nemocníc a kliník v USA. Sieť nemocníc bola opäť napadnutá ransomvérom, pričom útok paralyzoval všetky IT systémy naprieč Spojenými štátmi, čo

spôsobilo veľké problémy a oneskorenia v poskytovaní zdravotnej starostlivosti. Spoločnosť Universal Health Services vykázala dopad útoku vo výške 67 miliónov dolárov.

V lete 2021 sa odohral útok, kedy sa útočníci sponzorovaní iránskou vládou rozhodli zaútočiť na Detskú nemocnicu v Bostone. Našťastie útok bol zastavený rýchlou reakciou federálnych orgánov (FBI), no upriamil pozornosť aj na geopolitickú oblasť. Nebolo to však prvý a jediný krát, čo sa Detská nemocnica v Bostone musela brániť rozsiahlemu kybernetickému útoku. Oveľa horší dopad mal útok v roku 2014, kedy sa nemocnica bránila masívnemu a dlhotrvajúcemu distribuovanému útoku odmietnutia služby (DDoS - *Distributed Denial of Service*) zo strany hackerskej skupiny Anonymous.

V roku 2022 bola kybernetickým útokom zasiahnutá detská nemocnica SickKids so sídlom v Toronte v Kanade. Útočníci sa aj v tomto prípade zamerali na paralyzovanie činností nemocnice formou ransomvérového útoku. Útok mal síce ovplyvniť len niekoľko klinických a korporátnych systémov, no aj tak zapôsobil na poskytovanie zdravotnej starostlivosti. Horšie na tom bola Parížska nemocnica, od ktorej útočníci požadovali 10 miliónov dolárov po tom, čo ransomware napadol jej systémy. Pacienti, ktorí potrebovali liečbu, museli byť posielaní do iných nemocníc a operačné výkony boli odkladané.

V roku 2024 francúzska nemocnica Simone Veil so sídlom v Cannes oznámila, že sa stala obeťou kybernetického útoku. K útoku sa prihlásila ransomvérová skupina LockBit a zverejnila ukradnuté údaje z nemocnice v objeme 61 GB. Nemocnica potvrdila, že údaje sú skutočné. V Rumunsku bolo zasa najmenej 25 nemocníc odrezaných od online služieb po tom, čo útok ransomvéru znefunkčnil ich nemocničný informačný systém. Útok zasiahol produkčné servery nemocničného informačného systému, v dôsledku čoho prestal fungovať. Navyše súbory a databázy s údajmi pacientov a správy nemocníc boli zašifrované. Okrem týchto nemocníc bolo ďalších 79 zdravotníckych zariadení preventívne odpojených od služieb internetu. Podľa dostupných informácií sa útočníci dostali do systému prostredníctvom vzdialeného pripojenia, ktoré využívala jedna z dodávateľských spoločností. Rumunské kybernetické úrady uviedli, že kľúčové údaje boli krátko pred útokom zálohované, čo znížilo dopad útoku.

Toto je len niekoľko rezonujúcich, ale reálnych prípadov, ktoré potvrdzujú, že problematike kybernetickej bezpečnosti v zdravotníctve je potrebné venovať náležitú pozornosť. Útočná aktivita môže byť vo všeobecnosti rozdelená do štyroch skupín, a to na základe toho, na čo je zameraná. Môže to byť útok na sieťový server, klientsku pracovnú stanicu, samotnú počítačovú sieť alebo medicínske vybavenie. Staršie aktívne medicínske vybavenie je často nemožné zabezpečiť modernými bezpečnostnými prvkami, preto sa IT oddelenia zameriavajú najmä na ochranu siete, serverov a klientskych pracovných staníc. Ak sa už raz nejaký škodlivý kód dostane do siete, potom je každé zariadenie v lokálnej sieti ohrozené kompromitáciou a aktívne medicínske prístroje v danom uzle siete môžu byť veľmi pravdepodobne priamo manipulované tak, aby prijímali a vykonávali škodlivé aktivity, a to aj na pozadí svojej regulárnej činnosti, t. j. bez vedomia používateľa. Je potrebné si uvedomiť, že útočníkovi postačuje odhaliť jedno slabé miesto v reťazci zabezpečenia, ktoré vie takmer okamžite využiť na realizáciu svojho útoku. Preto by pozornosť nielen IT oddelenia, ale aj všetkých zamestnancov daného zdravotníckeho zariadenia mala byť sústredená na dôsledne dodržiavanie všetkých známych bezpečnostných opatrení a postupov.

2.3 KROKY ÚTOČNÍKOV ZAMERANÉ NA ZBER INFORMÁCIÍ V MANAŽMENTE ZDRAVOTNEJ STAROSTLIVOSTI

Ako útočník zisťuje informácie o zdravotníckom zariadení, jeho sieti, vybavení a systémoch?

Komplexná zdravotná starostlivosť je dnes zabezpečovaná tímom lekárov rôznych špecializácií a odborným zdravotníckym personálom, ktorí sa všetci spoliehajú na rôzne medicínske prístroje a vybavenie určené na diagnostiku a liečbu pacientov. Takáto spolupráca je možná len vďaka elektronickým zdravotným záznamom, v ktorých sa uchováva veľké množstvo lekárskych správ a klinických informácií. Prístup k nim majú oprávnení používatelia prostredníctvom informačných systémov nemocníc alebo zdravotníckych zariadení. Vďaka interoperabilite informačných systémov (aj z pohľadu rôznych výrobcov alebo krajín) je možné tieto informácie medzi zdravotníckymi zariadeniami elektronicky vymieňať, samozrejme pri dodržaní všetkých bezpečnostných a legislatívnych predpisov. Okrem benefitov súvisiacich s elektronickým spracovaním štruktúrovaných dát zdravotnej starostlivosti, sú takéto citlivé informácie častým terčom krádeží alebo predmetom na požadovanie výkupného. Útočníci okrem odcudzenia údajov môžu taktiež získať priamu kontrolu nad pripojenými medicínskymi prístrojmi, ktoré sú spojené s informačnými systémami nemocníc, a ktoré do záznamov, napríklad žiadaniek na vyšetrenie a výsledkov vyšetrení, dokážu posielať výsledky, ktorých dôvernosť, integritu alebo dostupnosť môže útočník narušiť a tak aj ovplyvniť liečbu pacientov. Útočník sa môže dostať k aktívnym medicínskym prístrojom, ktoré priamo interagujú s pacientom a poskytujú mu nejakú formu zdravotnej starostlivosti, alebo k pasívnym medicínskym prístrojom, ktoré sa síce nepoužívajú na poskytovanie liečby, ale monitorujú napríklad zdravotný stav pacienta a v prípade potreby kontaktujú záchranné zložky. Narušenie činnosti takéhoto vybavenia by mohlo taktiež viesť k poškodeniu zdravia pacienta.

Výhody digitalizácie služieb v zdravotníctve sú zrejmé a prinášajú obom stranám, t. j. poskytovateľom zdravotnej starostlivosti ako aj pacientom množstvo výhod, vrátane efektívnosti a dostupnosti. Na druhej strane, je nesmierne dôležité zabezpečiť aj primeranú úroveň ochrany a bezpečnosti, ktorú sa útočníci snažia prekonať či narušiť vykonávaním rôznych aktivít tak, aby na konci dňa získali prístup k sieti, ukradli údaje o pacientoch alebo až prevzali kontrolu nad zdravotníckymi prístrojmi a vybavením. Procesy, ktoré útočníci využívajú na dosiahnutie svojho cieľa obsahujú nasledovný rámcový postup.

Footprinting

Footprinting, teda stopovanie, predstavuje spôsob, akým útočníci spravidla začínajú svoju analýzu cieľovej nemocničnej siete. V podstate sa jedná o prieskum, v rámci ktorého útočníci zhromažďujú dostupné informácie o sieti, systémoch, ale aj používateľoch. Hlavným účelom je zistiť čo najviac informácií o cieli útoku, vrátane identifikácie potenciálnych zraniteľností, ktoré by mohli využiť. Informácie sú zhromažďované kombináciou rôznych techník, medzi ktoré patrí napríklad skenovanie sieťovej infraštruktúry, identifikácia zariadení, operačných systémov a verzií týchto systémov, hľadanie kontaktných údajov na zamestnancov, ktoré by mohli byť použité na útoky v rámci sociálneho inžinierstva. Aby sa útočník dozvedel čo najviac o nemocnici, snaží sa prehľadávať všetky materiály dostupné na internete. Často navštívi danú nemocnicu, preskúma bezdrôtové signály a komunikáciu, nazrie do kontajnerov a vytvára si detailný obraz o nemocnici a jej medicínskom vybavení. V prípade, že identifikuje typ alebo výrobcu zariadenia, ktoré chce napadnúť, dohľadá si návody na obsluhu a údržbu, ktoré sú často dostupné online, a ktoré bohužiaľ zvyčajne obsahujú aj informácie o predvolených heslách. V minulosti dokonca niektorí výrobcovia odporúčali, aby si zdravotnícke zariadenie ponechalo predvolené heslo, aby ich technici mohli ľahšie testovať, či vykonávať údržbu

daného zariadenia. Toto je však zjavná zraniteľnosť, ktorá významne uľahčuje napadnutie takéhoto zariadenia. Preto by mali byť predvolené heslá vždy zmenené ako prvé.

Aby útočníci získali to čo potrebujú, zameriavajú sa na získavanie údajov používateľských účtov v počítačovej sieti. Používajú na to rôzne počítačové programy, ktoré prehľadávajú internetové zdroje, vrátane komunikačných a textových služieb a zhromažďujú e-mailové adresy, názvy domén, obsah okamžitých správ, diskusných fór a diskusných skupín, adresáre webových sídiel odborných spoločností, medicínske webové stránky a celý rad ďalších online dostupných zdrojov. Dolovaním veľkého množstva údajov a zdrojov tak dokážu zhromaždiť potrebné informácie o cieľovej nemocnici. Útočníci však analyzujú aj informácie o dodávateľoch, veľmi často vo vzťahu k IT produktom, aby pochopili úlohy a zodpovednosti jednotlivých zamestnancov. Takéto informácie vedia následne použiť na to, aby sa vydávali za niekoho z dodávateľskej spoločnosti. Útočníci často využívajú odpočúvanie komunikácie, aj súkromnej, alebo nainštalujú softvér na snímanie obrazovky či zaznamenávanie informácií zadávaných z periférnych zariadení počítača (klávesnica, myš, kamera). Treba si uvedomiť, že útočníci nezanedbávajú žiadne informácie, ktoré odhalia. Patria sem aj zdanlivo neškodné informácie o narodeninách zamestnanca, povýšení a kariérnom raste, dovolenkách, miestach pohybu a pod. Ak sa útočníci nemôžu fyzicky dostať do nemocnice, snažia sa napadnúť aj mobilné zariadenia zamestnancov, cez ktoré by si mohli vytvárať virtuálne modely jej interiéru. Pomocou malvérových aplikácií, ktoré sú väčšinou nainštalované prostredníctvom trójskych koňov, tak získavajú citlivé informácie, lokalizačné údaje či snímky priestorov.

Skenovanie

Ak útočník získa dostatočné množstvo potrebných informácií o cieľovom zdravotníckom zariadení, prehľadáva, ktoré zariadenia sú dostupné z internetu (napríklad pomocou hackerských nástrojov na odhaľovanie sietí, ako sú napríklad Shodan, Nmap, Wireshark, Metasploit, Nessus, Burp Suite, John the Ripper, OpenVAS a pod.). Pomocou nástrojov vyvinutých na testovanie a analyzovanie bezpečnosti siete, identifikovanie zraniteľností a zneužívanie slabých miest v sieťach a systémoch, sú útočníci schopní nájsť IP adresy zariadení a spustiť skenovanie portov tak, aby identifikovali, ktoré operačné systémy nemocnica používa a podľa toho zistili ako môžu získať prístup do jej siete. Žiadne zo zariadení nemocnice by preto nemalo byť voľne prístupné z internetu (teda pre nemocnicu zvonku).

V momente keď útočníci zistia, ktoré softvérové aplikácie bežia v sieti cieľovej nemocnice, môžu vyvinúť špecifickú sadu nástrojov na zneužitie známych zraniteľností. Veľmi pravdepodobne útočníci spustia útok pomocou preskúmavania adresného priestoru počítačovej siete nemocnice, aby našli bezpečnostné diery, ako sú napríklad neopravené zraniteľnosti. Útočníci tiež monitorujú komunikáciu v nemocničnej sieti, dekódujú protokoly a skúmajú hlavičky a sieťový prenos, len aby získali potrebné informácie. Dokonca sa snažia použiť databázy známych prihlasovacích údajov, aby overili či sa takto nedostanú do slabo zabezpečeného systému, v ktorom niekto nezmenil predvolené nastavenia alebo podcenil potrebu používania originálnych a silných hesiel.

Enumerácia

Enumerácia predstavuje proces systematického skúmania cieľa a získavania informácií. V tomto štádiu sa útočníci pozerajú hlbšie do nemocničných počítačových sietí, keďže už našli a identifikovali servery, alebo iné sieťové zariadenia, určili konkrétne operačné systémy, ich aktualizácie, používaný aplikačný softvér a zistili aj to, kto sú používatelia. Všetko v takzvanom pasívnom režime monitorovania sieťovej prevádzky. Do veľkej miery využívajú aj to, že ešte stále veľa používateľov neinštaluje aktualizácie

a bezpečnostné záplaty pre známe zraniteľnosti, a to aj keď sú jednoducho dostupné. Kľúčom k získaniu neoprávneného prístupu pre útočníkov je teda znalosť toho, z čoho sa nemocničná sieť skladá. Snažia sa získať prístupy ku konfiguračným súborom, ktoré obsahujú údaje o systéme, ale napríklad aj používateľské mená a heslá na správu a ovládanie systémov. Takýto prístup im totiž umožní prepísať súbory v napadnutom zariadení a napokon aj získať správcovský prístup.

Útočníci sa preto snažia použiť spyware (špionážny softvér), ktorý je nenápadne nainštalovaný v nemocničnej sieti, a ktorý tajne zhromažďuje potrebné informácie, prípadne ich aj posiela na iné zariadenia, samozrejme bez súhlasu a vedomia nemocnice. Spyware môže aj prevziať kontrolu nad počítačovým systémom bez vedomia používateľov. Väčšinou sa však používa na monitorovanie a zaznamenávanie aktivít používateľov (keylogger), či zobrazovanie kontextových reklám, pričom jeho prítomnosť je zvyčajne pre používateľa dobre skrytá, aby ho nebolo možné odhaliť. Útočníci však využívajú najmä to, že spyware dokáže zhromažďovať takmer akýkoľvek typ údajov, vrátane osobných a citlivých údajov, zvykov pri prehliadaní internetu, prihlasovacích údajov používateľov, informácií o bankových účtoch a pod. Môže však tiež zmeniť nastavenia počítača, presmerovať webové prehliadače na podvodné stránky, vykonávať neoprávnené zmeny v nastaveniach iných softvérov a pod. Spyware sa zvyčajne nešíri ako iné vírusy alebo červy, pretože infikované systémy sa vo všeobecnosti nepokúšajú kopírovať softvér do iných počítačov.

Mapovanie siete

Po získaní konfiguračných údajov, údajov o dostupných zariadeniach a správaní ich používateľov sú útočníci schopní určiť topológiu nemocničnej počítačovej siete, a teda „nakresliť“ veľmi podrobné rozloženie zariadení v sieti a vizualizovať si celkové sieťové prostredie. Takáto mapa siete vytvorená útočníkmi (za predpokladu, že sa do nemocničnej siete dostali), býva veľmi pravdepodobne aktuálnejšia ako mapa samotného IT oddelenia nemocnici, pretože útočníci zistil to, čo sa tam aktuálne a skutočne nachádza. Mapa siete IT oddelenia (ak nie je využívaný kontinuálny monitoring) často zobrazuje iba to, čo si IT zamestnanci zaevidovali, prípadne si myslia, že sa tam nachádza, pričom používatelia (ak mali oprávnenia) alebo dodávatelia mohli na zariadeniach vykonať konfiguračné zmeny. Mapa siete, ktorú si vytvorili útočníci však obsahuje aj nebezpečné zariadenia, ktoré zamestnanci nesprávne nakonfigurovali, alebo aj tie, ktoré nainštalovali dodávatelia zariadení bez autorizácie, aby mohli svoje zariadenia monitorovať na diaľku. Ktorékoľvek z týchto zariadení vedia útočníci použiť na spustenie útoku, ktorého cieľom je narušiť bezpečnosť zariadení a služieb poskytovaných v nemocničnej sieti.

2.4 RIZIKÁ KYBERNETICKEJ BEZPEČNOSTI V NEMOCNIČNÝCH SIEŤACH A INFORMAČNÝCH SYSTÉMOCH

Čo môže byť ohrozené v zdravotníckom zariadení?

Medzi hlavné riziká, ktoré ohrozujú kybernetickú bezpečnosť služieb spojených s poskytovaním zdravotnej starostlivosti a evidenciou zdravotných záznamov v informačných systémoch zdravotníckych zariadení patria:

- **Ohrozenie dôvernosti dát** vplyvom úniku elektronických zdravotných informácií z elektronických zdravotných záznamov (EHR - *Electronic Health Record*) a osobných údajov pacienta. Tieto dáta sú na čiernom trhu vysoko cenené pre potenciál na krádež identity alebo poistné podvody.

- **Ohrozenie integrity dát** prostredníctvom možnosti neoprávnenej manipulácie s údajmi, napr. zmeny výsledkov laboratórnych testov alebo zdravotných záznamov.
- **Dopad na dostupnosť a kontinuitu starostlivosti**, keďže útoky môžu viesť k výpadku kritickej infraštruktúry, nedostupnosti systémov a dát, čo môže viesť napríklad k zrušeniu termínov vyšetrení, oneskoreniu procedúr, alebo dokonca k ohrozeniu zdravia alebo života pacienta (napríklad pri zmene dávkovania liekov alebo nefunkčnosti diagnostických/chirurgických zariadení).
- **Finančné straty a straty reputácie**, ktoré sú spojené s nákladmi na obnovu napadnutých systémov, pokutami za porušenie ochrany údajov (napríklad GDPR), súdnymi spormi a poškodením dobrého mena inštitúcie.
- **Zraniteľnosti medicínskeho vybavenia** (prístrojov a zariadení). Zariadenia internetu vecí (IoT), ako sú respirátory, anestéziologické stroje, infúzne pumpy alebo monitorovacie systémy, môžu byť zneužité a útočníci môžu nad nimi prevziať kontrolu alebo narušiť ich správne a spoľahlivé fungovanie.
- **Zraniteľnosti dodávateľského reťazca**. Útoky na dodávateľov a subdodávateľov zdravotníckeho softvéru, zariadení alebo služieb, ktorí majú prístup k systémom nemocnice.

2.5 METÓDY KYBERNETICKÝCH ÚTOKOV NA SYSTÉMY ZDRAVOTNEJ STAROSTLIVOSTI

Ako útočník získava prístup do siete a systémov nemocnice?

Ako sme už v úvode tohto textu naznačili, zdravotníctvo je oblasť, ktorá býva najviac ovplyvnená kybernetickými útokmi, keďže na rozdiel od bankovníctva, priemyslu, či iných odvetví, je tu najmarkantnejší dopad na zdravie a životy pacientov. Spôsoby útokov sú však podobné a v čase sa menia, tak ako je to vidieť aj v správach Európskej agentúry pre kybernetickú bezpečnosť ENISA. Na nasledovnom obrázku je uvedený prehľad najväčších kybernetických hrozieb pre zdravotníctvo v roku 2024, tak ako ich uvádza portál terranovasecurity.com.

Obr. č. 2.1 – Najväčšie kybernetické hrozby pre zdravotníctvo evidované v roku 2024.
Zdroj: https://www.terranovasecurity.com/blog/most-dangerous-healthcare-cyber-attacks

Phishing

Útočníci sa spoliehajú pri získavaní informácií o svojich potenciálnych obetiach na to, že zdravotnícke zariadenia a ich zamestnanci sú pod neustálym tlakom tak zo strany pracovného prostredia, ako aj zo strany pacientov. Takéto prostredie je následne ideálnym miestom pre aplikovanie techník phishingu, pretože niektorí zamestnanci si pred odoslaním informácií v zápale práce a časovej tiesne veľmi pravdepodobne neoveria všetky detaily komunikácie. Najbežnejším typom phishingu v zdravotníctve je emailový phishing. Útočníci pri ňom používajú pokročilé techniky sociálneho inžinierstva, aby presvedčili svoje obete k tomu, aby im spravidla dobrovoľne a neuvedomelo poslali citlivé informácie. Takéto informácie už následne dokážu odpredať alebo použiť na krádež identity. Najlepším tipom ako nenaletieť takémuto typu podvodu je vždy dôsledne kontrolovať pôvod akéhokoľvek e-mailu. Phishingové správy pochádzajú väčšinou z falošných adries alebo adries, v ktorých je podobný, ale nesprávny názov domény.

Únik údajov

V porovnaní s inými odvetviami trpí zdravotnícky priemysel veľkým počtom únikov údajov (*Data Breach*), pričom denne dochádza v priemerne k 1,76 únikom. Napriek prísnym požiadavkám na ochranu zdravotných záznamov a informácií o pacientoch, väčšina zdravotníckych zariadení stále zaostáva v implementácii bezpečnostných kontrol, čo uľahčuje prácu útočníkov. Jedným z najväčších únikov údajov v histórii je únik údajov spoločnosti Tricare (program zdravotnej starostlivosti poskytujúci služby aktívnym vojakom, ich rodinným príslušníkom a vojenským dôchodcom), ku ktorému došlo v septembri 2011, keď boli ukradnuté elektronické záznamy takmer 5 miliónov pacientov. Únik nastal po krádeži záložných pások elektronických zdravotných záznamov, ktoré boli ukradnuté z auta osoby zodpovednej za prepravu záložných pások medzi zariadeniami. Na zabezpečenie ochrany pred únikmi údajov (nielen pacientov) musia inštitúcie aplikovať monitoring aktivít v rámci inštitúcie, ale aj v rámci siete svojich dodávateľov a tretích strán.

Ransomware

Tento typ útoku na jedny z najcitlivejších informácií v živote každého človeka, ktoré sú spracúvané v zdravotníctve je založený na škodlivom kóde alebo škodlivom programe, často stiahnutom prostredníctvom trójskeho koňa, ktorý infikuje počítače a zašifruje všetky údaje v napadnutých zariadeniach. Útočníci následne na všetkých infikovaných počítačoch zobrazia správu so žiadosťou o výkupné za dešifrovanie informácií v týchto zariadeniach. Takéto vírusy sú čoraz komplikovanejšie a sofistikovanejšie, a je preto takmer nemožné ich odstrániť. Aj preto je im potrebné predchádzať a zastaviť ich skôr než sa do zariadenia dostanú. Takéto škodlivé kódy či programy sú často súčasťou phishingových útokov. Preto je potrebné zamestnancov nemocníc upozorňovať na to, aby nikdy neklikali na odkazy v podozrivých správach, aby nesťahovali a neotvárali súbory z neznámych zdrojov a už vôbec nespúšťali neoverené aplikácie. Tu je dôležité kontrolovať tak URL adresy, či sú legitímne, ako aj nespúšťať neznáme .EXE či .VBA súbory.

DDoS útoky

Distribuované útoky odmietnutia služby (DDoS - *Distributed Denial of Service*) sú založené na princípe „preťaženia“ danej služby, t. j. predstavujú typ kybernetického útoku, pri ktorom sa útočníci snažia narušiť alebo znefunkčniť webovú stránku, sieť alebo inú online službu tým, že ju preťažia veľkým množstvom falošných alebo nevyžiadaných požiadaviek. Často tento útok zahŕňa hromadné požiadavky na server (napríklad PING - *Packet InterNet Groper*, ktorý umožňuje preveriť funkčnosť

spojenia medzi dvoma sieťovými rozhraniami), čo spôsobí jeho zlyhanie a znefunkčnenie po celú dobu útoku. Takéto útoky môžu mať závažný dopad, ak sa použijú na kritickú infraštruktúru a základné služby národného významu, ako sú aj systémy zdravotníckych zariadení. Aj krátke prerušenie prevádzky systému v urgentných situáciách môže viesť ku fatálnym následkom pre pacienta. Útočníci opäť väčšinou požadujú výkupné za zastavenie DDoS útokov a „uvoľnenie" napadnutého systému. Odporúča sa používať primeranú technologickú obranu na strane IT oddelení spravujúcich dané systémy.

Hrozby zvnútra

Hrozby zvnútra, alebo takzvané insider hrozby predstavujú významné riziko aj v zdravotníckych zariadeniach, keďže v nich pracuje veľké množstvo zamestnancov na rôznych pozíciách, s rôznym vzdelaním a s rôznymi oprávneniami. Väčšina rizík zo strany vlastných zamestnancov môže byť znížená zabezpečením dostatočnej informovanosti a školeniami v oblasti kybernetickej bezpečnosti, aby sa predchádzalo neúmyselným hrozbám. Neinformovaní zamestnanci totiž môžu svojim neodborným správaním alebo neznalosťou niektorých procesov nevedomky uľahčiť útočníkom krádež údajov alebo inštaláciu škodlivého softvéru, ako sú vírusy a botnety na zariadenia v nemocničnej počítačovej sieti. Na zmiernenie tohto problému je potrebné implementovať komplexné školiace programy, ktoré vzdelávajú zamestnancov o dôležitosti bezpečnosti údajov a rizikách spojených s prístupom k údajom a fyzickým pripojením k systémom. Významným proaktívnym prístupom býva integrácia opatrení na prevenciu straty údajov, ktoré dokážu monitorovať a kontrolovať pohyby údajov a upozorňovať na akékoľvek nezvyčajné aktivity, ktoré by mohli naznačovať bezpečnostnú hrozbu.

Internet vecí

Koncepcia vzájomného prepájania zariadení, objektov a ľudí v počítačových sieťach priniesla fenomén internetu vecí (IoT - *Internet of Things*), čo umožňuje bez ľudského zásahu zbierať, vymieňať a analyzovať dáta z rôznych oblastí. Mnohé prepojené zariadenia sú vybavené senzormi a softvérom, prinášajú automatizáciu, zlepšujú efektivitu a poskytujú nové možnosti aj v oblasti zdravotnej starostlivosti. Môže ísť o zariadenia určené na monitorovanie vitálnych funkcií, pohybu pacientov, ale aj sofistikované chirurgické operačné vybavenie. Internet vecí tak priniesol nové možnosti v zdravotníctve, ale súbežne s tým otvoril priestor významným kybernetickým bezpečnostným hrozbám, ktoré ponúkajú možnosti šírenia ransomvéru, únikov údajov, DDoS útokov a pod. Ochranu pred útokmi prostredníctvom internetu vecí je potrebné zvyšovať aktualizovaním najnovšími bezpečnostnými záplatami a implementovaním robustných autentifikačných protokolov. Na úrovni správy počítačovej siete je dôležité zabezpečiť segmentáciu siete.

Dodávateľský reťazec

Ak útočníci vyhodnotia, že je pre nich náročné alebo až nemožné sa dostať do dobre zabezpečených systémov zdravotnej starostlivosti, potom sa môžu zamerať na menej bezpečné prvky obsiahnuté v dodávateľskom reťazci, cez ktoré sa následne dostanú k svojmu cieľu. Útočníci si totiž veľmi dobre uvedomujú aké široké je rozpätie dodávateľov a subdodávateľov rôznych služieb pre zdravotníctvo. Potom k úspešnému kybernetickému útoku postačuje už len odhalenie slabého miesta, často nedbanlivosti dodávateľského reťazca alebo tretích strán. Napríklad digitálnou transformáciou systémov do cloudových riešení sa zvýšili aj bezpečnostné hrozby pre takto spravované zdravotné záznamy pacientov. Tu je dôležité aplikovať mechanizmy pre pochopenie cloudových služieb

a zabezpečenie toho, aby poskytovatelia tretích strán implementovali vyspelé bezpečnostné programy.

2.6 OCHRANA PRED ÚTOKMI

Ako chrániť siete a systémy nemocnice?

Snáď najzjavnejším krokom, ktorý je možné vykonať na predchádzanie útokov na nemocničné siete a systémy v nej prevádzkované, je znížiť úroveň rizika v najslabších miestach reťazca ich každodenného používania. K takýmto miestam určite patria zamestnanci, teda používatelia zariadení a služieb, ktorí často uprednostňujú pohodlie pred bezpečnosťou. Aj preto býva prvým krokom v prevencii kybernetických útokov zabezpečenie náležitej informovanosti zamestnancov o potenciálnych hrozbách, ktoré možno očakávať v súvislosti s ich prácou v digitálnom priestore nemocnice. Každý zamestnanec by preto mal absolvovať základné školenie v oblasti kybernetickej bezpečnosti a osvojiť si tak návyky, ktoré prispejú k zvyšovaniu bezpečnosti zariadení a systémov nemocnice, a teda aj k bezpečnosti a spoľahlivosti poskytovanej zdravotnej starostlivosti. Vychádzame z toho, že drvivej väčšine kybernetických útokov sa dá predchádzať. Na druhej strane stopercentná bezpečnosť neexistuje, ale vieme realizovať opatrenia, ktoré môžu, a aj by mali aktívne prispievať k minimalizácii rizika kybernetických útokov na zdravotnícke zariadenia. Tieto opatrenia **na strane IT oddelení a manažmentu nemocnice** vo všeobecnosti vychádzajú zo zabezpečenia fyzického prístupu k aktívam nemocnice, odstránenia známych sieťových zraniteľností a monitorovaní prístupov k sieti a systémom nemocnice.

Opatrenia fyzického prístupu obsahujú napríklad:

- Oddelenie počítačovej siete nemocnice a zariadení v nej pripojených od internetu, t. j. prevádzkovanie lokálnej siete nedostupnej z vonku.
- Zavedenie mechanizmov kontroly fyzického prístupu ku všetkým aktívam nemocnice.
- Zvýšenie ochrany a zabezpečenie uzamykania priestorov a miestností so systémovými prvkami ako sú napríklad aktívne prvky počítačovej siete, servery a pod.
- Vymieňanie kódov, prístupových kariet alebo zámkov po úpravách alebo rekonštrukciách priestorov, do ktorých mali počas týchto prác prístupy zamestnanci dodávateľských firiem.
- Inštalovanie kabeláže počítačovej siete nemocnice v nechránených priestoroch tak, aby bola vedená v bezpečných chráničkách a s kovovou ochranou.
- Používanie viacfaktorového overovania pre kontrolu fyzického prístupu.
- Pravidelné kontroly úrovní zabezpečenia všetkých prístupov a odstraňovanie neaktívnych prístupových práv, napríklad pre zamestnancov, ktorí ukončili pracovný pomer v nemocnici.
- Deaktivovanie všetkých služieb a portov, ktoré nie sú potrebné pre bežnú prevádzku zariadení a systémov.
- Zablokovanie prístupov ku komunikačným a vstupno-výstupným portom, cez ktoré by sa do siete a informačných systémov mohol dostať škodlivý softvér, napríklad USB porty, CD/DVD mechaniky a ďalšie konektory a rozhrania.
- Používanie zdrojov napájania trvalej prevádzky pre všetky kľúčové počítačové zariadenia.

Opatrenia na zníženie sieťových zraniteľnosti obsahujú napríklad:

- Nastavenie spoločných bezpečnostných úrovní na všetkých zariadeniach v sieti nemocnice.

- Zakázanie vzdialených prístupov k zariadeniam a systémom mimo nemocničnej siete a to vrátane dodávateľov zariadení.
- Nepripájanie prenosných zariadení do počítačovej siete nemocnice. V prípade, že je to nevyhnuté je potrebné pred pripojením zabezpečiť otestovanie na prítomnosť škodlivého softvéru a spywaru.
- Nepoužívanie bezdrôtového ovládania zariadení ak je možné priame káblové pripojenie.
- Nainštalovanie softvérovej ochrany na servery, ovládacie konzoly a zariadenia s pridelenou IP adresou, aby zamestnanci nemohli či už úmyselne alebo neúmyselne nainštalovať škodlivý softvér z USB zariadení.
- Monitorovanie koncových bodov a periférií IT zariadení (USB, CD/DVD, RJ-45 a pod.), aby nemohli byť použité na narušenie bezpečnosti.
- Udržiavanie aktuálneho zoznamu povolených zariadení a služieb na nich prevádzkovaných.
- Vypnutie všetkých nepoužívaných portov a nezabezpečených komunikačných protokolov.
- Vyžadovanie silných hesiel na všetkých systémoch, vrátane tých, ktoré nie sú považované za kritické, ale cez ktoré by mohlo dôjsť k bezpečnostnému incidentu.
- Zmena predvolených prihlasovacích údajov na všetkých zariadeniach.
- Implementácia dvoj a viacfaktorového overovania na všetkých systémoch a pre všetkých používateľov.
- Pravidelné zmeny hesiel.
- Segmentácia siete na zabezpečenie rôznych typov zdrojov (prístupové systémy, klientske stanice informačného systému, kamerové monitorovacie systémy a pod.).
- Pravidelné aktualizácie a inštalácie najnovších bezpečnostných záplat na všetkých zariadeniach v sieti nemocnice.
- Používanie ochrany pred škodlivým softvérom v reálnom čase, aj lokálne skenovanie siete v reálnom čase.
- Pravidelné analýzy hrozieb pre celú infraštruktúru nemocnice s cieľom pochopenia a vyhodnocovania aktuálnych rizík.
- Monitorovanie stavu a využívania pamäte, CPU či sieťového pripojenia každého kybernetického aktíva pre včasné odhalenie podozrivých aktivít.
- Časté aj neohlásené testovanie zraniteľnosti siete voči kybernetickým útokom.
- Šifrovanie súborov uložených na klientskych staniciach a serveroch, vrátane šifrovania logovacích súborov a záznamov o aktivite siete.

Opatrenia na monitorovanie prístupov do siete nemocnice obsahujú napríklad:

- Nepretržité monitorovanie každej aktivity v počítačovej sieti nemocnice a uchovávanie logovacích súborov pre potreby kontroly. Kontroly logovacích súborov by mali byť pravidelné a zamerané na zisťovanie toho, či neobsahujú nevhodné alebo podozrivé akcie alebo prístupy. Pozornosť je potrebné venovať nielen jednotlivcom s vyššími oprávneniami.
- Dokumentovanie všetkých prístupov a prístupových práv personálu, dodávateľov, zmluvných strán, partnerov v dodávateľskom reťazci a pod. Ani administrátori by nemali mať prístup k celému obsahu informačného systému a nemali by používať zdieľané či predvolené heslá.
- Zavedenie mechanizmov prísnej kontroly a oddelenia povolení pre priamy prístup k zariadeniam a službám.

- Monitorovanie systémov a sietí, ku ktorým používatelia pristupujú, aby mohli byť odhalené prípadné podozrivé aktivity.
- Udržiavanie situačného povedomia o pracovnej sile a vyhodnocovanie kontraproduktívneho pracovného správania, ktoré by mohlo byť v rozpore s legitímnymi činnosťami nemocnice alebo poukazovať na možné riziko ohrozenia bezpečnosti z vnútra nemocnice – insider.
- Predchádzanie nadmernej závislosti na jednom zamestnancovi a zabezpečenie zastupiteľnosti, resp. rovnocennej náhrady pre vykonávanie jeho agendy.
- Vyžadovanie osobnej zodpovednosti a obmedzenie prístupu v prípade porušenia pravidiel bezpečnostných politík.
- Používanie metód detekcie narušenia na odhalenie príznakov útokov alebo anomálií, ktoré by mohli naznačovať, že sieťový útok môže prebiehať alebo sa už vyskytol.
- Používanie skenerov zraniteľnosti siete na posúdenie vhodnosti konfigurácie počítačovej siete nemocnice.
- Používanie digitálneho podpisu na jednotlivé logovacie súbory a na zaručenie toho, že sú úplné a nezmenené.
- Odstraňovanie všetkých nepotrebných a nepoužívaných používateľských účtov, ktoré už nie sú potrebné pre prevádzku systémov a ich služieb.
- Zabránenie prenosu alebo zdieľania používateľských poverení (účty, heslá) formou otvorených textov.
- Zavedenie metód ochrany pred neoprávneným prideľovaním privilégií používateľom.
- Implementácia bezpečnostných záplat a opatrení, aj v súčinnosti s dodávateľmi, na zabránenie zneužitia všetkých známych metód na obídenie autentifikácie používateľa (zadné vrátka).
- Zamedzenie viacnásobných súbežných prihlásení s rovnakými používateľskými povereniami, neumožnenie aplikáciám uchovávať prihlasovacie informácie, nepoužívanie žiadnych funkcií automatického dopĺňania prihlasovacích údajov a nikdy nepovoľovať anonymné prihlásenia.
- Obmedzenie komunikácie medzi rôznymi segmentami sieťového zabezpečenia.
- Používanie detekcie škodlivého softvéru a umiestňovanie podozrivých infikovaných súborov do karantény (namiesto automatického odstránenia), aby mohli byť následne analyzované.
- Overovanie či sa prihlasovacie údaje po nainštalovaní softvérových opráv nevrátili na predvolené hodnoty.
- Používanie antivírusových programov na všetkých zariadeniach a ich pravidelné skenovanie.
- Zakázanie e-mailových klientov alebo služieb okamžitých správ (*instant messaging*) na ktoromkoľvek uzle počítačovej siete nemocnice.
- Vytvorenie jasných pravidiel postupu v prípade podozrivej aktivity.

Z pohľadu **bežných zamestnancov** (nie IT oddelení) je potrebné dbať na neustále zvyšovanie ich povedomia o možných rizikách. Ako sme už uvádzali vyššie, ľudský faktor je často tým najslabším článkom. Zamestnanci na akejkoľvek pozícii by mali dodržiavať:

- **Bezpečné heslá** - používať silné a jedinečné heslá, ktoré sa pravidelne menia a nie sú zdieľané.

- **Opatrnosť** pri otváraní e-mailov a ich príloh. Vždy je potrebné overiť odosielateľa emailu, nikdy neotvárať neznáme e-maily alebo prílohy, ktoré môžu obsahovať škodlivý obsah.
- **Pravidelné školenia** - zúčastňovať sa školení a seminárov o kybernetickej bezpečnosti, aby si boli vedomí najnovších hrozieb.
- **Ochrana prístupov** - nikdy nezdieľať prístupové údaje, každú stratu zariadenia okamžite hlásiť príslušnému IT oddeleniu. Počas voľna alebo práceneschopnosti vždy zamykať počítače a systémy a nenechávať ich voľne prístupné.
- **Oznamovanie bezpečnostných incidentov** - včas hlásiť podozrivé aktivity v systémoch IT oddeleniu alebo bezpečnostnému tímu zdravotníckeho zariadenia.

ZÁVER

Problematika kybernetickej bezpečnosti v systéme zdravotnej starostlivosti už nie je len jej okrajovou záležitosťou, ale v súčasnej digitálnej dobe reprezentuje jeden z kľúčových pilierov moderného zdravotníctva, ktoré má prinášať tak občanom, ako aj samotným poskytovateľom zdravotnej starostlivosti široké portfólio dostupných služieb a s nimi spojených údajov. Samotné zdravotnícke zariadenia sa musia v súbehu s technologickou modernizáciou, nasadzovaním inovatívnych prístrojov a vybavenia, či využívaním elektronickej zdravotnej dokumentácie čoraz viac sústrediť aj na bezpečnostné aspekty, keďže sú pre svoju rozsiahlosť a rozmanitosť činností lákavým cieľom útočníkov. V tomto kontexte je potrebné okrem iného zabezpečiť aj to, aby bola kybernetická bezpečnosť považovaná za neoddeliteľnú súčasť bezpečnosti pacientov. Obdobne ako u iných odvetví, aj v zdravotníctve je jednou z najväčších hrozieb, hrozba v podobe ransomvérových útokov, ktoré dokážu paralyzovať nielen ambulancie či oddelenia, ale aj celé siete zdravotníckych zariadení s nedozernými dopadmi na zdravie či dokonca životy pacientov. Stúpajúcu tendenciu majú aj útoky na dodávateľské reťazce, keďže útočníci si veľmi dobre uvedomujú závislosť zdravotníckych zariadení na poskytovaní tovarov a služieb externými organizáciami. Aby dokázali zdravotnícke zariadenia odolávať kybernetickým hrozbám, musia budovať svoju ochranu na viacerých úrovniach. Znížiť riziko sieťových útokov môžu vhodnou segmentáciou počítačovej siete, kedy navzájom vhodne oddelia jednotlivé časti siete tak, aby v nich boli dostupné len spolu súvisiace prístroje alebo vybavenie. Rovnako je potrebné, aby aplikovali systém riadenia a kontroly prístupov, a aby jednotlivé prístupy vždy odpovedali aktuálnym oprávneniam daných používateľov, pričom všade tam, kde je to možné, je potrebné využívať viacfaktorovú autentifikáciu u všetkých používateľov. Ďalej, pre zabezpečenie kontinuity prevádzky, je potrebné proaktívne vykonávať pravidelné zálohovanie údajov či systémov, pričom jednotlivé zálohy je potrebné izolovať tak, aby prípadný útok nemohol viesť k ich zneužitiu či poškodeniu alebo zničeniu. Procesy zálohovania a obnovy údajov by mali byť taktiež testované v pravidelných intervaloch. V neposlednej miere by zdravotnícke zariadenia mali dbať o to, aby sa ich zamestnanci kontinuálne vzdelávali nielen vo svojom odbore, ale aj v oblasti kybernetickej bezpečnosti. Pre dosiahnutie potrebnej bezpečnosti v oblasti zdravotníctva je teda potrebné klásť dôraz na to, že bezpečnosť už dávno nie je len záležitosťou a zodpovednosťou IT oddelení, ale že sa na nej musia podieľať všetci zamestnanci. Tí svojím zodpovedným konaním a správaním sa v digitálnom priestore zdravotníckych zariadení môžu významne prispievať k predchádzaniu úspešného naplnenia kybernetických útokov.

POUŽITÉ ZDROJE

[1] Ayala L.: Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention. Apress, 2016, ISBN 978-1-4842-2154-9, DOI 10.1007/978-1-4842-2155-6.

[2] Bossomaier T., D'Alessandro S., Bradbury R.: Human Dimensions of Cybersecurity. CRC Press, 2020, ISBN 978-1-138-59040-3.

[3] Brooks C.J., Grow C., Craig P., Short D.: Cybersecurity Essentials. John Wiley & Sons, 2018, ISBN 978-1-119-36239-5.

[4] Cox C.K.: Everyday Cybersecurity: A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity. 2019, ISBN 978-1-7330186-1-6.

[5] ENISA Threat Landscape 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[6] Kolouch J., Bašta P. et all.: CyberSecurity. CZ.NIC, 2019, ISBN 978-80-88168-34-8.

[7] Owens B. How hospitals can protect themselves from cyber attack. CMAJ. 2020 Jan 27;192(4):E101-E102. doi: 10.1503/cmaj.1095841. PMID: 31988158; PMCID: PMC6989022.

[8] Steinberg J., Beaver K., Coombs T., Winkler I.: Cybersecurity All-in-One For Dummies. John Wiley & Sons, 2023, ISBN 978-1-394-15285-8.

[9] Vacca J.R.: Cyber Security and IT Infrastructure Protection. Elsevier, 2014, ISBN: 978-0-12-416681-3.