 DOI: 10.53020/IME-2021-105

Magyar kórházakban előfordult zsarolóvírus támadások esetei

Ransomware attacks in Hungarian hospitals – case studies

Dr. Palicz Tamás[1], Sas Tibor[1], Szabó Zoltán[2], Tóth Tamás[2],
Tisóczki József[3,4], Dr. Bencsik Balázs[5], Joó Tamás[1,6]
[1] Semmelweis Egyetem, Egészségügyi Közszolgálati Kar, Egészségügyi Menedzserképző Központ, Budapest, [2] Semmelweis Egyetem, Egészségügyi Közszolgálati Kar, Digitális egészségtudományi Intézet, Budapest, [3] Pest Megyei Flór Ferenc Kórház,
[4] Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest,
[5] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, Budapest,
[6] Magyar Egészségügyi Menedzsment Társaság, Budapest

Az elmúlt években, de különösen a COVID-19 járvány alatt az egészségügyi intézmények elleni kibertámadások száma jelentősen növekedett. A növekedés hátterében nemcsak az egészségügyi adatok felértékelődése áll, hanem az egészségügy, mint létfontosságú infrastruktúra sérülékenysége is növeli a rendszer kiszolgáltatottságát. A támadások speciális fajtája a zsarolóvírus támadás, amelynek felismerése és megelőzése különösen fontossá vált a mostani időszakban, hiszen a napi működési folyamatok veszélyeztetése, az egyébként is szűkös kapacitások gyors átszervezése a betegek ellátását és biztonságát veszélyeztető kényszerhelyzetet teremthet. A cikk célja, hogy az észlelt magyarországi zsarolóvírus támadások esetein keresztül bemutassa a szükséges teendőket.

In recent years, but especially during the COVID-19 pandemic, the number of cyberattacks against healthcare institutions has increased significantly. The reason for the growth is not only the high value of health data, but also the vulnerability of healthcare as a critical infrastructure increases the sensitivity of the system. A special type of attack is the ransomware virus attack, the detection and prevention of which has become especially important in the current period, as the endangerment of daily operational processes and the rapid reorganization of already decreased capacities can create an emergency situation influencing negatively patient care and safety. The goal of the article is to present the necessary actions in connection with the detected ransomware virus attacks in Hungary.

BEVEZETÉS

A 2021-es év egészségügyi információbiztonsági szempontból meghatározó volt. A COVID-19 pandémia hatására számos területen a digitális technológiák még inkább előtérbe kerültek, a távmunka az egészségügyben is nagyobb teret nyert, miközben információbiztonsági szempontból sérülékenyebbek lettünk. Kórházainkban különösen szenzitív adatokat kezelnek az informatikai rendszerek. A páciensek teljes élettörténete, kórképe nyomon követhető a medikai vagy kórházi informatikai rendszerekben (Health/Hospital Information System – továbbiakban: HIS) megtalálható adatbázisokban, ezért azok védelme különösen fontos ezekben az intézményekben [1]. Az elmúlt években, különösen az egészségügyi adatok értékessége [2], másrészt a 2019. vége óta tartó világjárvány miatt az egészségügyi szolgáltatók irányába jelentősen növekedtek a kibertérből érkezett adatvédelmi incidenst eredményező fenyegetések, amelyeknek közel 30%-a zsarolóvírus támadás [3].

A zsarolóvírusok olyan speciális rosszindulatú kódok, amelyek egy gépre vagy egy hálózatba bejutva az ott lévő állományokat titkosítják, ezáltal a felhasználó általi hozzáférést akadályozzák meg. Ahhoz, hogy a felhasználó hozzájuthasson a működés szempontjából fontos fájlokhoz, a zsarolóvírust működtető kiberbűnözői csoport váltságdíjat kér el. Ennek összege néhány tízezer eurótól akár milliós nagyságrendig is terjedhet. A legújabb zsarolóvírusok, és az ezeket akár szolgáltatásként működtető csoportok képesek arra is, hogy a zsarolóvírus bejutását követően adatszivárgás révén az érzékeny adatokat kimásolják, majd annak érdekében, hogy nagyobb legyen a fizetési hajlandóság, ezen adatokat akár publikálják is [4].

Az ilyen jellegű támadások számának növekedése mögött az áll, hogy magas befektetési megtérüléssel megvalósítható zsarolóvírus-támadások az egyébként is leterhelt egészségügyet még jobban terhelik, így nagyobb esély van a zsarolási díj kifizettetésére, hiszen a betegek élete, és az adott intézmény jó hírneve érdekében hajlandóak fizetni az egészségügyi szolgáltatók [5].

Nemzetközileg számos olyan példa fordult elő 2020-ban, amelyek alapján felhívták a figyelmet arra, hogy a zsarolóvírus támadásokkal, különösen azok megelőzésével, nagyon komolyan kell foglalkoznia az egészségügyben dolgozó valamennyi szereplőnek.

A Nemzeti Kibervédelmi Intézet (NKI) 2020-ban – a jelentési kötelezettségek ellenére – csak négy zsarolóvírus támadásról szerzett tudomást. Ezek részletes feldolgozása kiér-

tékelése időt vesz igénybe, azonban annak érdekében, hogy az ágazat számára tanulságokat tudjunk megfogalmazni, két korábbi esetet feldolgoztunk.

Jelen publikáció célja, hogy a konkrét kórházi zsarolóvírus támadásokon keresztül mutassuk be annak folyamatát, illetve ahhoz kapcsolódóan a legfontosabb teendőket is megfogalmazzuk.

AZ ESETFELDOLGOZÁS MÓDSZERTANA

Az esetek összeválogatása az NKI, valamint a kórházakban dolgozó informatikusok által ismert esetekre korlátozódott. A feldolgozás során látóterünkbe kerültek olyan esetek is, amelyek egy-egy kórház egy-egy végpontján fordultak elő. Ezek hatása az informatikai rendszerre és a betegellátási vagy a kórházi támogató folyamatokra minimális mértékűek voltak, ezért nem tartottuk bemutatásra érdemesnek azokat. Az esetek kiválasztása kapcsán azokat emeltük ki (két megyei kórház esete), amelyek jellegzetesek és a betegellátási folyamatot befolyásolták, így nem csak az informatikai vagy információbiztonsági tapasztalatok összegezhetők.

Az estek áttekintése három fő szempont menténtörtént:

- hogyan is történt az eset – ennek kapcsán azokat a lehetséges gyenge pontokat próbáltuk feltérképezni, amely egy kórházi működés során a zsarolóvírus támadás kapcsán előfordulhatnak,
- milyen mértékű volt a támadás üzleti jelentősége (business impact analysis) – milyen mértékben érintette a betegellátást (osztályok, egységek, munkatársak száma), volt-e olyan diagnosztikai, terápiás, vagy egyéb adminisztratív folyamat (dokumentálás, időpont szervezés, pénzügyi stb.), amelyet érintett a támadás,
- volt-e olyan tanulsága az adott esetnek, amely más kórházak számára is hasznosítható lehet (azonnali és középtávú teendők, cselekvési tervek stb.)

ESET 1 – MEGYEI KÓRHÁZ

A szervezet rövid bemutatása

A kórház egy teljes megye ellátásáért felelős, több mint 700 aktív ággyal és közel 200 krónikus ággyal. A kórházi rész mellett jelentős óraszámú járóbeteg rendelőintézet is működik.

Az intézmény informatikai osztályán a támadás idején 13-an dolgoztak: az érdemi informatikai és jelentéskészítési munkát összesen 5 mérnök és 5 technikus végezte, emellett az ügyfélszolgálati munkát végző vagy az informatikai rendeléseket bonyolító kolléganők is az osztályhoz tartoztak. Az intézet gépparkjában 11 különálló szerver, a végpontokon 650 db körüli személyi számítógép működött, jellemzően Windows 7-operációs rendszerekkel, de körülbelül 100 db Windows XP operációs rendszerrel működő PC is volt közöttük.

Az esemény és azonnali beavatkozások

2016 áprilisában, egy pénteki napon telefonon jelentkezett az egyik osztály, hogy folyamatosan tűnnek el az asztalról az Excel fájlok és helyettük valamilyen ismeretlen fájl kerül fel. A hívást fogadó azonnal lekapcsolta az összes szervert és értesítette az osztályvezetőket, így minden gépet lekapcsoltak. Életbe lépett a vészhelyzeti terv, mely arra az esetre íródott, ha az informatikai rendszer megáll. Egy gyors szakmai helyzetértékelést követően, rövid jelentésben az informatikai terület meghatározta az esemény súlyosságát és azonnal referáltak a felsővezetésnek. Miközben a menedzsment a tájékoztatással foglalkozott és a sajtóval való kommunikációra koncentrált, az informatika a probléma kezelését tervezte meg.

A probléma vizsgálatakor az derült ki, hogy annak hátterében egy, a titkárság által megnyitott e-mail állt. Az e-mail Moszkvából érkezett egy „mezei” felhasználótól, amelyet tovább már nem lehetett visszakövetni. Utólagosan a fertőzés menete az alábbiakban valószínűsíthető: a moszkvai felhasználó letöltött több „ajándék” programot, amelyben olyan rosszindulatú programok (trójai programok) is voltak, melyek a háttérben kinyitották a gépén azokat a kapukat (portokat), amelyek más külső szerverekkel való kommunikációt tették lehetővé. Ezt a felhasználó nem vette észre. A támadó a moszkvai felhasználó gépét felhasználva küldte el a zsarolóvírust a világba.

Az informatikai részleg által meghatározott kezdeti lépések kulcsfontosságúak voltak: a gyors tájékozódás mellett az azonnali teendők meghatározását és a probléma felderítését tűzték ki célul:

- Tájékozódtak a környékbeli kórházaknál, hogy találkoztak-e már a problémával, illetve milyen megoldási javaslatuk van az adott problémára;
- Létrehoztak két belső munkacsoportot (Szerver és Kliens csoportok), amelyek a diagnosztikai és a terápiás teendők kapcsán specifikusan és koncentráltan tudtak egy-egy hardware, software és felhasználói csoporttal foglalkozni.

A Szerver csoport a leválasztott szervereket izolálta, így egyesével meg tudta vizsgálni azok állapotát és meg tudta határozni a helyreállítási sorrendet, figyelembe véve a rendszerek prioritását: Medikai rendszer (ez internet nélkül is működött), Diagnosztikai rendszer, Tűzfal és internet oldali belépési pontok, Levelező szerver, Fájl szerverek, Mentések, Gyógyszer rendszerek, Gazdasági rendszer, Internet.

A Kliens csoport a végpontokat vizsgálta a teljes intézményben és az alábbiakat tette:

- Informatikai vírusvédelem a kórházi végpontokon: a meglevő kereskedelmi alkalmazás használatával megpróbálta megtalálni a vírust, azonban ebben az esetben nem volt képes azt kiszűrni, így a megelőzésre sem volt esély.
- Olyan szoftvert kellett keresni, amely képes megtalálni a vírust, így a végpontok teljeskörűen ellenőrizhetővé váltak.

- A vírusra jellemző sajátosságok meghatározása, és egy közös tudástár kialakítása. Az operatív csapat ösztönösen alkalmazta azt a megoldást, amely ilyen helyzetekben szükséges: SitRoom (situation room) létrehozása, ahol a szakemberek és a döntéshozatalra feljogosított vezetők együtt tekintik át az aktuális helyzetet, és hozzák meg az operatív döntéseket. Ez az „eszköz" (pl.: az ismeretek központi, flipcharton történő rögzítése) alkalmas volt arra is, hogy az érdeklődő kórházak is megismerhessék a legfontosabb tudnivalókat, és akár be is kapcsolódhassanak a probléma feltárásába és megoldásába.
- Azon helyek és felhasználók azonosítása, akik nem megfelelően lépnek be a rendszerbe (nem a saját belépést használták), mert ezeken változtatni kellett.

Összegzés, tanulságok

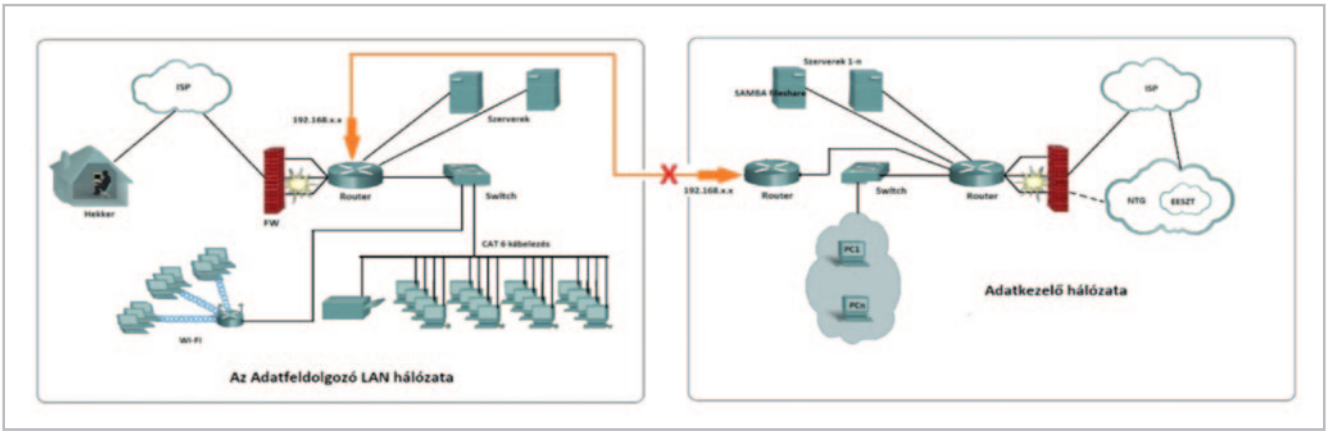
- A fertőzés pénteken munkaidőben történt, így a három nap a hétvégén elég volt a hiba elhárításához. Ez jelentős többlet feladatot jelentett, illetve az informatikai csoport számára működési kockázat volt, azonban a teljes szervezetet és a szervezet kritikus üzleti folyamatát (betegellátás, és azok belső támogató folyamatai) tekintve összességében szerencsés volt az időzítés.
- Sikeres volt az elhárítás, amelynek a sikertényezői az alábbiak voltak:
  - Megfelelően felkészült vezetői és szakértői kapacitás állt rendelkezésre (tudták kinek kell szólni, aki tudta mit kell tenni).
  - Az adatok többségéről megfelelő mentések voltak, így azokat vissza lehetett állítani és a rendszerek működőképesek maradtak.
  - A nem mentett adatok a támadás során nem sérültek, így nem történt betegadat vesztés, illetve egyéb adat sem tűnt el.
  - A tapasztalatok gyors, transzparens feldolgozása biztosította az intézményen belüli és azon kívüli adat- és információáramlást, amely révén külső szakértelem is bevonásra kerülhetett, illetve más kórházakon is lehetett segíteni.
- Rövid és középtávú beavatkozások:
  - A menedzsment támogatásával előírták a kliensek/végpontok szigorúbb működését és annak ellenőrzését.
  - A tűzfal beállítások kapcsán szigorúbb szabályokat vezettek be, és a továbbiakban ezek szerint üzemeltették a szervereket.
  - A wifi rendszereket a gépek speciális hálózati azonosítójára (MAC cím) szűrték, megszűntek a mindenki által igénybe vehető wifi elérések.
  - Szabályzatokat felülvizsgálták, és több esetben szigorítást vezettek be a felhasználói magatartás kockázatainak csökkentése érdekében.
  - Oktatták a kollégákat, amelyek kifejezetten a pszichológiai megtévesztés (social engineering) módszertan csapdáira építettek.
  - A külső informatikai szállító ingyenes továbbképzést biztosított az informatikának az információbiztonság területén.

ESET 2 – MEGYEI KÓRHÁZ

A szervezet bemutatása

A megyei kórház fekvő- és járóbeteg területi ellátási kötelezettsége megközelíti az 1,5 millió főt, mindezt hozzávetőlegesen 800 aktív ágyon végzi a kórház. A kórház informatikai osztályán az üzemeltetési feladatokat szerver és kliens oldalon hat fő látta el (1 fő szakirányú mérnök, 2 fő felsőfokú OKJ-s szakképesítéssel rendelkező és 3 fő szakközépiskolát végzett munkatárs). Hozzávetőlegesen 30 szerver és 450 kliens gépet kellett nonstop üzemeltetnie a kórház informatikai osztályának.

Az egészségügyi ellátás folyamatos biztosítása érdekében a kórház több közreműködővel kötött szerződést, amelyek szakmai-diagnosztikai ellátást biztosítottak, vizsgálatokat végeztek a kórház számára (pl.: képalkotó diagnosztika, laboratóriumi vizsgálatok stb.). Az adatfeldolgozók önálló informatikai rendszereket üzemeltettek saját szerver és kliens gépekkel, önálló internetes kapcsolatokkal és szolgáltatókkal.



1. ábra
Az incidensben érintett adatfeldolgozó és az adatkezelő átnézeti kapcsolati sémája (Forrás: saját szerkesztés)

A vizsgálatkérések, majd az eredmények visszaadása is Server Message Block (SMB) fájlmegosztásokon keresztül zajlott az incidens időpontjában. A kórház és a közreműködők hálózata jellemzően 1-1 routeren keresztül volt összekötve (lásd 1. ábra).

Az ábrából kitűnik, hogy a VLAN alkalmazása nélküli LAN-ban a szegmentálást a különböző IP range-ek alkalmazásával tudták biztosítani, a samba megosztások ezen keresztül üzemeltek, az adatcserék ezeken keresztül bonyolódtak, mely az incidens észlelésekor fizikailag megszakításra került.

Az érintett adatfeldolgozó LAN hálózatában Wi-Fi megoldást is alkalmazott, mely nagymértékű sérülékenységet képviselt, azonban jelen incidens esetén nem volt releváns.

Az esemény és azonnali beavatkozások

A kórház egyik alvállalkozója 2018. december 13-án, pénteken délelőtt jelezte, hogy a titkársági számítógépen tárolt adatállományok titkosítása miatt nem fér hozzá állományokhoz, majd ez rohamosan terjedt át további 11 db munkaállomásra és 9 óra 36 perckor a kiszolgáló szerverre, amely egyébként egy normál munkaállomás volt, szerver célokra használva.

Adott reggelen az incidenst elszenvedő adatfeldolgozó értesítette a kórház informatikai üzemeltetését, hogy a hálózata és a gépek nagyon meglassultak. Ezt azonban nem vélte nagyobb problémának, hiszen korábban is előfordult hasonló. Ilyen esetekben jellemzően egy, a fizikai kábelhossz miatt beépített switch került újraindításra, mely fizikailag a kórház egyik rackszekrényében helyezkedett el, mint „idegen” eszköz, de funkcionalitásában az adatkezelő hálózatában üzemelt. Tekintettel arra, hogy a többszöri újraindítás sem segített a probléma elhárításában, ezért az adatfeldolgozói szerver vizsgálata történt meg, ahol megtalálták a lassulás okát. A támadás tényét a zsarolóvírus által küldött képernyőüzenet tette számára egyértelművé, lásd 2. ábra. A fotón az egyik munkaállomás képernyőképe látható: a malware titkosította a szerveren található állományokat. A támadás a kórház által üzemeltetett informatikai rendszereket nem érintette, annak ellenére, hogy egy úgynevezett fájlmegosztásos szolgáltatással az alvállalkozó és a kórház informatikai rendszerei a támadás időpontjában össze voltak kötve.

2. ábra
Az első szemmel látható információ a megvalósult ransomware támadásról (Forrás: saját készítés)

Minden informatikai infrastruktúrát üzemeltető rémálma egy ilyen vagy hasonló információhordozó üzenet megjelenése. Az esemény észlelését követően az alábbi azonnali lépések és intézkedések történtek a kárcsökkentés, illetve a mielőbbi helyreállítás érdekében:

- Az adatfeldolgozó vezetője azonnali értesítést küldött a saját munkatársainak, hogy azonnal kapcsolják ki a munkaállomásokat.
- Haladéktalanul értesítették a Kórház informatikai vezetőjét a tapasztaltakról.
- A Kórház által használt hálózati tartomány és az adatfeldolgozó informatikai hálózatának fizikai összeköttetését azonnal megszakították, a két hálózatot izolálták.
- Az adatfeldolgozó szervere és összes kliens gépe leállításra került.
- Telefonos bejelentések, intézkedések megtételére került sor a kórház felsővezetése felé (főigazgatója, készenlétes kórházvezető), az Országos Katasztrófavédelmi Főigazgatóság (OKF), mint incidenst vizsgáló hatóság irányába, az Állami Egészségügyi Ellátó Központ (ÁEEK), mint fenntartó, valamint a kórház informatikai infrastruktúrájának korszerűsítésében részt vevő harmadik fél felé. 2019. január 1-től ez a hatáskör átkerült az NKI-hez, az OKF eljáró hatósági illetékessége átmenetileg megmaradt, majd 2020. július 1-jétől valamennyi feladat az NKI hatáskörébe került.
- A kórház fizikai és virtuális szerverein egy azonnali antivírus vizsgálat került elindításra, illetve minden szerveren és végpontokon ellenőrzésre került az EndPoint védelem futása, azt nem írta-e felül egy esetleges vírusscript.
- Megvizsgálták az SMB portok tilthatóságát, de mivel a fájlszerverek ezt használták, ezek tiltása működési zavart okozott volna, így ezeket nem tilthatták.
- Az adatfeldolgozó azonosította az egyik fertőzött gépen a file kiterjesztést, mely az OKF részére továbbításra került : „*.id-00cd6f7.(denisnapi1982@aol.com).adobe”

Összegzés, tanulságok

Ennek az esetnek az alábbi főbb tanulságai vonhatók le:

- A fertőzés ez alkalommal is pénteken történt.
- A sikeres támadás következtében 2017. február és 2018. december között keletkezett elektronikus adatok kerültek titkosításra, ezért azok nem voltak elérhetőek, azonban az összes adat papíron rendelkezésre állt. A rendszer

helyreállításáig az adatkezelő papír alapú üzletmenetet folytatott.
- Az incidens kapcsán, annak bejelentését követően, az OKF és az NKI is vizsgálatot folytatott. Az adatfeldolgozónál kialakított informatikai rendszer hiányosságai, az incidens kapcsán rendelkezésre álló rendkívül csekély mennyiségű információk alapján egyik hatóság sem tudta egyértelműen feltárni a támadás részleteit, ugyanakkor sikerült segítséget nyújtaniuk az adatok egy részének visszaállításában.
- A meglévő adatok alapján valószínűsíthető volt, hogy a zsarolóvírus az adatfeldolgozó titkársági gépéről került be a cég hálózatába, onnan gyorsan terjedt a hálózat többi elemére, és így szinte valamennyi munkaállomására és szerverére. Az adatfeldolgozó szerverén tárolt adatok titkosítása az első gép megfertőzését követően kb. 6 perc elteltével kezdődött meg.
- A támadás a kórház által üzemeltetett informatikai rendszereket nem érintette, annak ellenére, hogy a támadás idején egy ún. fájlmegosztásos szolgáltatással a közreműködő és a kórház informatikai rendszerei össze voltak kötve.
- A mielőbbi üzletmenet visszaállítása érdekében az adatfeldolgozó a munkaállomásokban lévő háttértárolókat törölték és az operációs rendszereket újratelepítették vagy új háttértárolókat építettek be, illetve komplett gépeket cseréltek.
- A sikeres támadás következtében az adatfeldolgozó rendszerében elektronikus adatvesztés történt. Az érintett klienseken tárolt adatok megsemmisültek, biztonsági mentések korábban nem készültek a kliensekről. A szerverben lévő háttértárolók egyike tönkrement, a másik adathordozó teljes tartalma titkosításra került, ami jelen ismeretek szerint nem visszaállítható. Az itt található naplóadatokhoz kizárólag akkor lehet hozzájutni, ha a ransomware dekódolási eljárása nyilvánosságra kerül.
- A 2017. február előtt keletkezett adatok mentésből visszaállíthatók voltak. Ugyanakkor meg kell jegyezni, hogy az elektronikusan tárolt adatoknak papír alapú változata teljeskörűen rendelkezésre állt, azonban ezek ismételt elektronikus rögzítése nagy munkát jelentett. A fentiek miatt betegadat vesztés nem történt.
- Az alvállalkozó rendszere a fertőzést követő 3. naptól ismét használhatóvá vált, az összes munkaállomást az incidenst követő hét csütörtöki napjától tudták használni.

A bemutatott esetek tanulságai, következtetések

A fent bemutatott esetek – habár ezek az egészségügyben ténylegesen előforduló zsarolóvírus incidenseknek is csak a töredékét jelentik – azonban vannak olyan megállapítások, amelyeket már ez alapján is meg lehet tenni.

- A kórház vezetésének tisztában kell lenni azzal, hogy napjainkban az informatikai eszközök nagy száma, a hálózatba kötés, és az internet nyíltsága miatt az elektronikus információbiztonság a kórházi működés és a betegbiztonság szempontjából kritikus tényező.
- Az informatika és az információbiztonsági képzettségét naprakészen kell tartani, és ez a szervezet valamennyi szereplőjére igaz. Természetesen más ismeretekkel és készségekkel kell rendelkezni a gyógyító folyamatokban dolgozó munkatársaknak, mint a támogató folyamatokban rendelkező munkatársaknak.
- Az informatikai beszállítók megbízhatósága felértékelődött, különös tekintettel arra, hogy a támadások egy részét a biztonsági szempontból nem megfelelően tervezett és fejlesztett informatikai alkalmazásokon keresztül hajtják végre. A fejlesztések mellett az üzemeltetési biztonság is kulcsszerepet játszik (7x24 óra, megfelelő backup, és megfelelő fizikai, logikai, szoftveres, és egyéb védelem szükségessége).
- A biztonság növelése érdekében szükség esetén támogatókat, külső cégeket, tanácsadókat is szükséges alkalmazni. Az egészségügyi intézmények esetében kiemelt szerepe van az állami szereplőknek: Belügyminisztérium, Nemzeti Kibervédelmi Intézet, Országos Kórházi Főigazgatóság, egyetemek és kiberbiztonsággal foglalkozó szakértő cégek.
- Egy zsarolóvírus támadás kapcsán értelemszerűen felmerül a fizessünk vagy ne fizessünk kérdése. Ezzel kapcsolatosan a Nemzeti Kibervédelmi Intézet – összhangban a Szövetségi Nyomozó Iroda (Federal Bureau of Investigation, FBI) ajánlásával – azt ajánlja, hogy ne fizessen a megtámadott szervezet. Ez azonban bizonyos egyedi esetekben, helyzetekben módosulhat: attól függően, hogy milyen adatokat, és milyen mértékben érint a támadás, milyen zsarolóvírussal van dolgunk, valamint milyen backupok állnak rendelkezésre, illetve, hogy milyen üzleti folyamatot érint vagy érinthet az adott támadás [6].

Mint minden változás, változtatás kapcsán, ezen a területen is az egyik legfontosabb, hogy az ágazati, intézményi vezetői elkötelezettsége megfelelő legyen, és felismerjék: a XXI. században a betegek biztonságának már nem csak azok a klasszikus területein kell jól teljesíteni az intézménynek, mint amit a XIX. vagy XX. századi tudásunk határozott meg (pl kézhigiéné, betegátadás, stb.). Ez a XXI. században az informatikai fejlődés miatt kiegészült az elektronikus információk biztonságával is. Ahogy az Amerikai Orvosszövetség (American Medical Association) 2019 októberében megfogalmazta: „Cybersecurity in healthcare is not a technical issue, it is about patient safety!” vagyis „A kiberbiztonság az egészségügyben nem egy technikai kérdés, hanem a betegbiztonságról szól” [7].

IRODALOMJEGYZÉK

[1] Tisóczki J: Informatikai infrastruktúrák biztonsága a hazai egészségügyi ellátásban. Jelenkori Társadalmi és Gazdasági Folyamatok. 2019, 14: 137-51. https://doi.org/10.14232/jtgf.2019.3.137-151

[2] Bodó AP, Palicz T, Joó T (Szerk: Deák V) Az IBTV. gyakorlata. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2020 pp 21-31 (ISBN: 978-963-498-358-3)

[3] Nearly 30% of cyberattacks on hospitals in 2020 were ransomware, report finds. https://www.beckershospitalreview.com/cybersecurity/nearly-30-of-cyberattacks-on-hospitals-in-2020-were-ransomware-report-finds.html (megtekintve: 2021.02.25.)

[4] Ransomware attack on mailing service exposes info of 20,000+ Oregon clinic patients. https://www.beckershospitalreview.com/cybersecurity/ransomware-attack-on-mailing-service-exposes-info-of-20-000-oregon-clinic-patients.html (megtekintve: 2021.01.24.)

[5] Palicz T, Sas T, Tisóczki J, Bencsik B, Joó T: „Pénzt vagy életet!"– Zsarolóvírusok az egészségügyi informatikai rendszerekben, Orv Hetil, 2020, 161: 1498–1505. https://doi.org/10.1556/650.2020.31788

[6] Ransomware https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (megtekintve: 2021.02.28.)

[7] American Medical Association. Patient safety: the importance of cybersecurity in health care. https://www.ama-assn.org/media/21676/download (megtekintve: 2020. 05.15.)

A SZERZŐK BEMUTATÁSA

Dr. Palicz Tamás 1993-ban szerezte orvosdoktori diplomáját a Debreceni Egyetemen, majd 1998-ban belgyógyász szakorvos lett. 2003-tól dolgozik vezetőként, kezdetben a Semmelweis Egyetem Stratégiai és Működésfejlesztési Főigazgatóság főigazgató-helyetteseként, majd 2005-től a Kútvölgyi Klinikai Tömb orvosi igazgatójaként szerzett tapasztalatot az egészségügyi szervezetek vezetésében. 2010 és 2013 között a Nemzeti Fejlesztési Ügynökség Humánerőforrás-programok Irányító Hatóságát (HEP IH) irányította. 2015 végétől a Semmelweis Egyetem Egészségügyi Menedzserképző Központ stratégiai igazgatóhelyettese. Fő érdeklődési területe az egészségügyi szervezetek folyamatközpontú menedzsmentje, szervezeti változások vezetése és projektmenedzsment. Az utóbbi években az egészségügyi digitális átalakulása kapcsán foglalkozik az egészségügyi szervezetek kiberbiztonságával.

Sas Tibor vegyészmérnökként végzett, majd több informatikai végzettséget is szerzett, jelentős tapasztalatokkal rendelkezik az elektronikus közigazgatás területén. Az általa vezetett TIOP 2.3.1. projekt tervezte az EESZT-t és fejlesztette ki az EESZT szoftver alkalmazásait (pl. eRecept). Jelenleg az ajkai Magyar Imre Kórház informatikai és kontrolling osztályvezetője. Az ország első kórházi zsarolóvírus támadását sikeresen kezelte és adatvesztés nélkül állította helyre a kórház működését. Több kórházban oldott meg hasonló problémákat. Szakmai tapasztalatait az oktatásban is kamatoztatja.

Tóth Tamás a Semmelweis Egyetem Digitális Egészségtudományi Intézetben dolgozik tanársegédként. Doktori kutatásának fókuszában a digitális technológiák, elektronikus egészségügyi megoldások betegekre, szakemberekre és az orvos-beteg kapcsolatra gyakorolt hatásának vizsgálata áll. 2009-ben a Semmelweis Egyetemen informatikus egészségügyi menedzser diplomát szerzett. A Neumann János Számítástudományi Társaság Orvosbiológiai Szakosztályának tagja.

Szabó Zoltán Attila villamosmérnök és közgazdász, közel 26 éve az infokommunikációs szektorban tevékenykedik. Pályafutását 1995-ben a MATÁV Rt.-nél kezdte, majd 2001-ben a GTS-DataNet Távközlési Kft.-nél folytatta. 2010 és 2014 között a Nemzeti Hírközlési Informatikai Tanács (NHIT) alelnöke. 2012. február 6. és 2019. január 1. között a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ Zrt.) vezérigazgatója és az igazgatóság tagja, emellett 2012-2015 között a PRO-M Zrt. igazgatóságának elnöke. A NISZ Zrt.-nél eltöltött évek alatt részt vett az új közigazgatási infokommunikációs modell kidolgozásában, illetve több, az egészségügyet érintő informatikai projektben. 2019. január 1-től a belügyminiszter politikai főtanácsadója, mellyel párhuzamosan 2019. július 1-től 2019. október 15-ig az e-Health koordinációért felelős miniszteri biztosi feladatokat látta el.

Tisóczki József okleveles mérnöktanár, mérnök informatikus, a Pest Megyei Flór Ferenc Kórház Informatikai és Finanszírozási osztályának vezetője, a kórház elektronikus információs rendszereinek biztonságáért felelős vezető. Végzettségét a Budapesti Műszaki és Gazdaságtudományi Egyetemen szerezte, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD-hallgatója. Kutatási területe a létfontosságú egészségügyi rendszerelemek biztonságos IT üzemeltetése, a technológia és a felhasználói biztonságtudatosság kapcsolatának vizsgálata. A Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal által kiírt Kooperatív Doktori Pályázat egyik nyertes pályázója 2020-ban. Oktatóként menedzsment, projektmunka és digitális írástudás tárgyak előadója.

Bencsik Balázs a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetének igazgatója.

Joó Tamás közgazdász és okleveles egészségpolitikai szakértő. 2011-2016 között kutatóként, gazdasági elemzőként, illetve projektvezetőként az államigazgatás különböző szintjein dolgozott. Kutatóként és projektmenedzserként részt vett az Országos Egészségfejlesztési Intézet 2012-es, a dohányzás társadalmi terheit felmérő kutatásában, valamint a népegészségügyi termékadó bevezetését értékelő hatásvizsgálatok elkészítésében (2012, 2015). Jelenleg a Semmelweis Egyetemen senior egészségügyi közgazdászaként hazai és nemzetközi finanszírozású projektek előkészítésében és végrehajtásában vesz részt. Az utóbbi években kiemelten foglalkozik az egészségbiztonság komplex megközelítésével és az azokat befolyásoló tényezőkkel (dohányzás, kiberbiztonság stb.).