



Hírek

Detektor Plusz magazin



Termékmonitor

Pályázat

Szakcikk

Kapcsolat

Hírlévé



January & February Product Test

Pyronix



Civil Körözési Rendszer



Keresés

OK

Hírek

Hírek

Az egészségügyi létfontosságú rendszerelemek sajátosságai az I. Nemzeti Kiberverseny tükrében

Hekktartamásért Európai Unió és Ukrán egészségügyi intézményeket. A támadás során egy ransomware segítségével titkosították a medikai informatikai rendszerek adatait (betegek személyes- és a kezelés során addig keletkezett minden adatát) és csak bitcoinban megfizetett váltásdíj fejében oldják fel a titkosítást. Ezen túl a támadók hibajelenségeket képesek generálni olyan orvostechikai eszközökben, amelyek távoli elérése hálózaton keresztül lehetséges, így üzemzavar keletkezett több gyógyszeradagolóban, infúziós pumpában is. Így lehet összefoglalni az I. Nemzeti Kiberverseny forgatókönyvének alapvetését. A megmértetetésen ezen forgatókönyv alapján kellett a csapatoknak az Európai Unió döntéshozóinak tanácsadó testületként komplex, több alternatívát tartalmazó krízisintervenciós csomagot összeállítaniuk.

A helyzet aktualitását a számos nemzetközi példa mellett a 2016-os évben két magyarországi egészségügyi intézményt ért, a betegadatokat és így a betegellátást közvetlenül érintő ransomware támadás is alátámasztja.

Bár a verseny – elnevezéséből adódóan – egy kibertámadás elhárításáról szól (annak nemzeti szinten és a nemzetközi együttműködés szintjén történő kezeléséről) a nyertes csapat anyagának erőssége többek között abban is rejlett, hogy ugyanilyen részletességgel dolgozta ki az egyébként megtámadott ágazat továbbműködésének feltételrendszerét, mely a komplex kríziskezelés elengedhetetlen feltétele.

A nyertes csapat tagjaként és Hazánk egyik legnagyobb egészségügyi szolgáltatójánál a biztonsági terület felelős vezetőjeként rendkívül tanulságos volt ebből az aspektusból is áttekinteni a magyar egészségügyi „kiberképességeit”, az egészségügyi válsághelyzeti tervezés és üzemeltetési biztonság területeit ezen aspektusból is.

A javasolt krízisintervenciós csomag – az egészségügyi ellátórendszer válsághelyzeti működésének lehetőségeire, üzemeltetésbiztonsági kérdéseire vonatkozó részének – értelmezéséhez, annak a következőkben történő kifejtéséhez tisztázni szükséges egy-két alapvetést, melyek szerint:

- 2016. év végén megkezdődtek az egészségügyi ágazatban is a nemzeti létfontosságú rendszerelemek (LÉR) – korábbi terminológia szerint kritikus infrastruktúraelemek – kijelölései;
- A kijelölések a területi ellátási kötelezettség mérete, a tevékenység átvételére alkalmas intézmények közelsége, illetve az adott intézmény – akár speciális képességeiből adódó – működéséhez fűződő kiemelt egészségpolitikai érdekek szempontrendszer alapján történt;
- A LÉR-ek üzemeltetői Üzemeltetői Biztonsági Terv (ÜBT) készítésére kötelezettek, mely során fel kell mérniük az informatikai jellegű üzemeltetési kockázatokat is. Ennek során nagy hangsúlyt kapnak a medikai informatikai rendszerek és a hálózatra kötött orvostechikai eszközök üzemeltetési kockázatai, mint a LÉR-en belüli kritikus infrastruktúraelemek;
- Ezzel együtt ezen intézmények az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá kerültek, melynek köszönhetően kockázatelemként az alapján rendszereiket biztonsági osztályba, a szervezetüket biztonsági szintbe kell sorolni és az ezen osztályokhoz/szintekhez tartozó követelményeket meghatározott időn belül teljesíteniük kell;
- Emellett, amennyiben egy rendkívüli esemény miatt az ellátás fenntartásához szükséges kapacitás helyben nem áll rendelkezésre az egészségügyért felelős miniszter, a védelmi bizottság elnöke vagy az egészségügyi államigazgatási szerv egészségügyi válsághelyzetet hirdethet. Ebben az esetben a fekvőbetegellátók aktivizálják az Egészségügyi Válsághelyzeti Terveiket, illetve a további kapacitásnövelés érdekében további erő, eszköz (szakszemélyzet, illetve pl. az Állami Egészségügyi Tartalék készletei) vezényelhető, csoportosítható át.

Az esemény kezelése szempontjából érdemes a két különböző típusú támadásra adott reakciókat külön-külön kezelni, hogy a végkövetkeztetésnél újra összeérhessenek majd a szálak.

Ezek alapján tehát:

- A medikai informatikai rendszerek adatainak zárolása:

Egy ilyen típusú esemény bekövetkezésekor az addig az intézményben bármikor is kezelt betegek előzményadatai, a már felvett és kezelés alatt álló betegek minden rögzített adata, így alapadatai, körélménye, a már elkészült diagnosztikai vizsgálatok eredményei nem lennének láthatóak a kezelést végző személyzet számára. Tehát a már kezelés alatt álló betegek vizsgálatait meg kell ismételni, azokat és a körélményeket ismételt papíralapon rögzíteni szükséges, illetve ezek intézményen belüli logistikájáról, a sértetlenség, bizalmasság, rendelkezésre állás alapjaitól ez esetben is gondoskodni kell. Bár a magyar egészségügyben több, a kezelés során keletkező adatot (lázlap, gyógyszerelési lap) jellemzően a medikai informatikai rendszerek mellett, külön papíralapon is vezetnek, az adminisztrációs és diagnosztikai terhek jelentősen növekednének, melyek extrém terheléssel járó időszak az első 48-72 óra.

Ezen időszakban extrém módon és ez után is jelentős mértékben megnő az adminisztratív és diagnosztikai területek humán erőforrás-kapacitás igénye, mely túlnyomórészt a betegellátási területen dolgozókat terheli. Ezen kívül az adminisztrációs eszközökre is fokozott igény mutatkozik. Felméréseink alapján elmondható, hogy a „békeidő”, normál üzemmenet szerinti működés során a fekvőbetegellátás területén a humán erőforrás-kapacitás jelenleg a szakmai minimum 70-80%-a környékén mozog átlagosan.

Fentiek alapján kijelenthető, hogy egy nagyszabású az Európai Uniót, illetve Magyarországot országos

ELŐFIZETÉS

2017. I. félévi Biztonságttechnikai Szabványlisták

MACH-TECH

IPAR NAPJAI

2017. május 9-12.

OKTATÁS

Folytatjuk oktatássorozatunkat, megújult programokkal és feltételekkel!

ASPECTiS
DISTRIBUTION • SERVICES
www.aspectis.hu



SCHRACK



Hirarchívum

Partnerek

Belépés

Legyen Ön is partnerünk
Felhasználási feltételek

Termékmonitor

Adat és információvédelem
Elektronikus jelzéstechika (135)
 Gépjárművédelem
 Kommunikációtechnika
 Mechanikus biztonságvédelem
 Szolgáltatások
Tűzvédelem technika (5)
[Adatfeldolgozási tanácsadás, és revízió](#)
[Adathozzáférés elleni védelem](#)
[Adatkiszugárzás elleni védelem](#)
[Beszéd-, és jeltitkosító eszközök](#)
[Biztonsági szoftverfejlesztés](#)
[Dokumentum - megsemmisítő készülékek](#)
[Lehallgatás elleni eszközök](#)
[Villámvédelem](#)
[Audió és videó kaputelefonok](#)
[Azonosító eszközök](#)
[Behatolásjelzők \(9\)](#)
[Beléptető rendszerek \(2\)](#)
[CCTV biztonsági rendszerek \(35\)](#)
[Inteligens épület felügyeleti rendszerek \(2\)](#)
[Kapcsolóórak, őrző ellenőrző rendszerek](#)
[Kapu és ajtónyitás vezérlő rendszerek](#)
[Kártyakészítő eszközök](#)
[Kül- és beltéri figyelőrendszerek \(42\)](#)
[Kültéri objektumőrző rendszerek \(8\)](#)
[Lakásriasztók \(12\)](#)
[Riasztóközpontok \(9\)](#)
 Robbanóanyag - keresők
 Személy és csomagvizsgáló eszközök (3)
 Személyi riasztó, segélyhívó eszközök,
 pánikkapcsolók (1)
 Távfelügyeleti rendszerek (11)
 Áruvédelmi rendszerek (1)
 Autóriasztók GPS rendszerek
 Gépjármű távfelügyeleti rendszerek, elfogó szolgálattal
 Gépjárművek biztonsági

sztinten érintő támadás esetén mindenképpen, de akár kisebb mértékű támadás esetén sem kerülhető el az egészségügyi válsághelyzet kihirdetése. Ebben az esetben a LÉR kijelölések alapján szükséges a rendelkezésre álló erőket és eszközöket átcsoportosítani, melyek által az ellátás biztonsága országos szinten biztosítható.

- Orvostechnikai eszközök üzemzavara:

Ebben érintettek lehetnek aktív eszközök (pl.: gyógyszeradagolók, infúziós pumpák), illetve állapotkövetésre használt eszközök is (pl.: különböző monitorok, melyek a nővérpultba „közvetítik” a jeleiket). Hazánkban jellemzően az utóbbi területen terjed erősebben a high-tech eszközök alkalmazása. Az alkalmazásuknak megfelelően a beteg ellátásába üzemzavarukkal beavatkozhatnak közvetlenül, vagy fals pozitív/fals negatív jelzések generálásával közvetett módon is.

Ezen esetben az érintett eszközöket a működésből ki kell vonni, azokat korábbi technikai színvonalat képviselő/tábori eszközökkel szükséges kiváltani. Amellett, hogy ezen, a kiváltásra alkalmas, tartalék eszközök rendelkezésre állása erősen véleményes, alkalmazásuk – érthető módon – további humán erőforrás bevonását indokolja.

Ezen erő-eszköz átcsoportosítás szintén a LÉR-ek mentén történhet és az érintettek számától függően nagy valószínűséggel szintén az egészségügyi válsághelyzet kihirdetését tenné szükségessé.

**A jövőbe tekintő módon szükséges azonban feltennünk a kérdést:
 Miként előzhető meg egy ilyen támadás?**

Tekintettel arra, hogy a ransomware általában email útján, az ismeretlen feladótól jött, rossz magyarsággal írt emailek csatolmányának feleltlen megnyitásával, a BYOD eszközök szabályozatlan használatával, a szervezeti hálózat korlátozás nélküli és feleltlen internetelérése során a felhasználó által jut be a szervezet rendszerébe, a legkézenfekvőbb megoldás, napjaink slágertémája (mely ennek ellenére a szakmán kívül kevés „központi” figyelmet élvez) a biztonság tudatosság fejlesztése. Emellett azonban nem mehetünk el azon tapasztalati tény mellett sem szóltanul, hogy bár az emberek többsége készségszinten használja mobiltelefonján a közösségi médiát és ehhez kapcsolódóan különböző alkalmazásokat, a digitális írástudatlansága mégis megmutatkozik, amikor egy számítógépen alapvető műveleteket, egy e-learning oktatást, egy e-közigazgatáshoz kapcsolódó ügyintézt, vagy egyszerűen egy többszintű bejelentkezést kell megvalósítani. Véleményem szerint az informatikai biztonság tudatosság fejlesztése során sokszor az alapokig visszanyúló oktatásra van szükség. Ezeken túl természetesen a megelőzésben ugyanilyen fontos szerepe van létfontosságú hálózatok, kritikus elemek fizikai és logikai védelmének, illetve a szabályozott módon és a tevékenységhez igazodó gyakorisággal történő biztonsági mentéseknek, azok tárolási módjának, körülményeinek.

Összegzőképpen elmondható, hogy egy, a versenyben vázolt kibertámadás kivédése, illetve bekövetkezése esetén az egészségügyi ellátórendszer működésének fenntartása, a védekezés és a következmények kezelése humán erőforrás és technikai oldalról is jelentős kihívások elé állítja a kritikus infrastruktúraelem üzemeltetőjét, mely jelentős anyagi megterheléssel jár, az egészségügyi ellátórendszer esetében pedig jelentős humán erőforrás-kapacitás többletet igényel.

Akár egészségügyi, akár biztonsági szakemberekkel beszélgettem munkám során, hajlamosak voltunk mintegy kézlegyintéssel elintézni, megszokásból, már-már természetességéből adódóan szinte ignorálni azt a tényt, hogy az egészségügy erőforráshiányos állapotban van anyagi- és humán erőforrás téren is. Pedig az üzembiztonság komplex rendszerében, a munka-, tűz-, vagyon-, környezet- és polgári védelem, illetve informatikai biztonság szakmai szempontrendszerének vizsgálata mellett, azok bázisaként kizárólag ezen alapvetések tudatosulásával és kezelésével optimalizálhatóak a biztonsági intézkedések és azok költségei. Ha ezeket megszokásból egy legyintéssel elintézzük, akkor nem csak a biztonsági intézkedések arányosságának és gazdaságosságának oltárán áldozunk, de sem az üzemeltetési biztonsági, sem a válsághelyzeti tervezés nem kerül racionális alapokra, így azok alkalmazhatósága erősen megkérdőjelezhetővé válik.

Mészáros István

2017.05.03 15:00:14 | [Vissza](#)| [Impresszum](#) |