A kórházügyi menedzsment aktuális kérdései 2017-ben (5. rész): Adatvédelem az egészségügyben
Praxisberichte – Zu aktuellen Fragen des Krankenhausmanagements 2017 Projekte Positionen Perspektiven
Verband der Krankenhausdirektoren Deutschlands e.V.,
2017. október (100 p.)

Kulcsszavak: információtechnológia, digitalizálás, adatvédelem, Németország

A kiadvány nem érhető el Interneten, de azt a Német Kórházigazgatók Szövetsége érdeklődés esetén elektronikus vagy nyomtatott verzióban rendelkezésre bocsátja.

Adatvédelem az egészségügyben

A megtámadottak

A *Deutsches Krankenhaus Institut (DKI)* 2012-ben – egy nem nyilvános tanulmányban – a kórházak biztonságát elemezte. 2014-ben aztán a *Cetus Consulting* közzétette a 150 orvostechnikai szakember, informatikai vezető, gazdasági igazgató és ügyvezető igazgató részvételével készített kutatás eredményeit. Minden második megkérdezett biztonsági incidensekről és üzemzavarokról számolt be.

2016-ban a *PricewaterhouseCoopers (PwC)* a *Szövetségi Információtechnikai Biztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik – BSI)* megbízásából felmérte a szabványoknak megfelelő szoftvereket és hardvereket, amelyek korlátozzák a nem kívánatos termináloknak a hálózathoz való csatlakozását. A felmérés szerint a portok távkarbantartás céljából való megnyitását, pl. orvostechnikai eszközök esetén, „gyakran nem ellenőrizték rendszeresen”. A nem engedélyezett adathordozók azonosítására szolgáló intézkedéseket, valamint a merevlemezek kódolását még nem alkalmazzák minden területen. Az e-maileket, „ha egyáltalán kódolják”, ezt csak a külső kommunikáció esetén teszik meg és az interjúk szerint a kép nem egységes. Végül az adatoknak egy széleskörű azonosítási és hozzáférési eljárás segítségével történő biztosítása „(még) nem elterjedt”.

Peter Schaar korábbi szövetségi adatvédelmi megbízott 2013-ban arra figyelmeztetett, hogy hogy azok az információtechnológiai rendszerek, amelyek még a hozzáférés differenciált védelme, az aktivitások naplózása és a személyi adatok törlése alapkövetelményeinek sem felelnek meg, nem alkalmazhatók jogszerűen és kockázati tényezőt jelentenek. A kórházvezetők a Polgári Törvénykönyv és a társasági törvény szerint is személyes felelősséget viselnek.

A támadók

A titkosszolgálatok minden információt feldolgoznak, érdeklődnek a célszemélyek egészségi állapota iránt, amihez felhasználják a fitnesz-csuklópánton levő adatokat. A bűnözők 650.000 tételnyi betegadatot kínálnak eladásra 700.000 USD ellenében, a kábítószerfüggők az őket nem tetszésük szerint kezelő orvosok életére törnek. Az Egyesült Államokban már több halállistát azonosítottak, amelyek az Interneten véletlenszerűen kiválasztott polgárok adatait tartalmazták.

Az EU adatvédelmi rendelete

2018. május 25-én hatályba lép az EU adatvédelmi rendelete, amely szerint „Bármely személy, aki e rendelet megsértése miatt valamilyen anyagi vagy nem anyagi kárt szenved, kártérítésre jogosult a felelősök vagy az adatfeldolgozók részéről.” Ezzel kapcsolatban akár 10 millió EUR vagy az éves jövedelem 2%-ának megfelelő bírság róható ki, attól függően, hogy mely összeg magasabb.

Annak érdekében, hogy a kórházak jobban felmérhessék a kockázatokat, a Szövetségi Információtechnikai Biztonsági Hivatal az Interneten közzétette a kórházi információtechnológia kockázatelemzésének kézikönyvét (*„Risikoanalyse Krankenhaus-IT“ – RIKRIT-RISIKEN*).

Az *Információtechnológiai Biztonsági Szakmai Szervezetek Szövetségének (TeleTrusT – Bundesverband IT-Sicherheit e.V.)* ügyvédei és technikusai 64 oldalas dokumentumban írták le, hogy mit értenek „a technika jelenlegi állásán” az adatvédelem és az információtechnológiai biztonság területén. ***Martin Schallbruch, a Szövetségi Belügyminisztérium információtechnikai osztályának korábbi vezetője,*** az információtechnológiai biztonsági törvény egyik társszerzője szerint előfordulhat, hogy a dokumentum által bevezetett definíció gyorsan elterjed a felügyeleti szervek, az ügyészek és a bírók körében.