GDPR: megfelelés az egészségügyben

Interjú Kocsis György szolgáltatásmenedzserrel

Mint ismert, az Európai Parlament és Tanács 2016/679. számú rendeletében szabályozta a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását. Az Általános Adatvédelmi Rendelet (General Data Protection Regulation, GDPR) egységes jogi keretek közé tereli a személyes adatok kezelését az Európai Unió teljes területén, alkalmazása 2018. május 25-től kötelező. A GDPR-nak való megfelelésről az egészségügyben, és a betegellátó intézményeknek nyújtott testreszabott támogatás lehetőségeiről nyilatkozott lapunknak Kocsis György, az Asseco Central Europe Magyarország Zrt. GlobeNet üzletágának szolgáltatásmenedzsere.

– Milyen aspektusból közelíti meg vállalatuk a GDPR rendeletnek való megfelelést?

A GDPR megfelelést mi elsősorban az adatokhoz való hozzáférés átgondolt, szakmailag indokolt szabályozásában, az adatkezelések abszolút ismeretében, nyilvántartásában, ellenőrizhetőségében, az esetleges kompromittálódás tetten érhetőségében, az „incidens" helyrehozásában, következésképpen a hozzáférési, ellenőrzési és védelmi folyamatok javításában látjuk. Vitathatatlannak tartjuk, hogy a feladat első fele – amely alól kivételt képeznek természetesen a papíralapú adatkezelések – informatikai eszközök nélkül nehezen, a feladat második fele pedig egyáltalán nem valósítható meg. Ebből a megfontolásból kiindulva, mi – a piacon megjelent számos tanácsadó, felkészítő metodikával szemben – az alkalmazott medikai rendszer képességeire alapozott, de azon nyilvánvalóan túlmutató, a teljes kórházi informatikai rendszert, szabályozást, eszközjellemzőket, felügyeleti és védelmi megoldásokat átvilágító auditot, újratervezést és támogatást helyeztük a felkészítő projektjeink fókuszába.

A WEB SÖTÉT OLDALA

– Milyen kihívásokkal szembesültek a partnerkórházak informatikai infrastruktúrájának felmérésekor?

Úgy gondolom, nem mondok újat azzal, hogy a magyar egészségügyi ellátórendszerben nagymértékű informatikai elmaradottság tapasztalható. Ez alatt nem csak az elavult, lelassult, le-leálló computerek tömegét értem, hanem azt a felhasználói magatartást is, amelyet a kórházakban a számítógépeket kezelő személyzet tanúsít. Gondolok elsősorban arra, amikor átadják egymásnak a belépési adataikat. Kivételt képeznek azok az orvosok és szakdolgozók, akik vagy már eltöltöttek néhány évet külföldi kórházakban, vagy a képzésük kapcsán, illetve mindennapos tevékenységük során professzionális módon kezelik a computert, a tabletet és általában az okos eszközöket. Számukra természetes, hogy informatikai eszköztár szolgálja ki az orvosokat: minden, a képalkotóktól, laboratóriumokból és egyéb vizsgálóhelyekről beérkező információ azonnal elérhető, ami egyébként is alapkövetelmény lenne a mai modern egészségügyben.

– Említene néhány, a helytelen adatkezelésre jellemző példát?

Ha például az orvos hozzáférést ad az adminisztrációt részben helyette elvégző nővérnek, vagy az otthonról hozott pendrive használatával akaratlanul, de vírusfertőzésnek teszi ki nem csak a saját számítógépét, hanem az egész kórházi hálózatot. Nem beszélve a nyitva hagyott computerekről, amelyekbe boldog-boldogtalan betekinthet, vagy – ilyen esettel is találkoztunk – a monitorra emlékeztetőül kiírt jelszóról. Olyan kórházban is jártunk, ahol több éve nem támogatott operációs rendszer futott a gépeken, amelyek nem voltak hálózatba kötve, így a központi vírusvédelem és jelszó-policy szóba sem jöhetett. Szinte óhatatlan, hogy mindennek előbb-utóbb valamilyen biztonsági incidens lesz a következménye. Nemrégiben Portugáliában például komoly – több százezer eurós – bírságot szabott ki a helyi adatvédelmi hatóság egy kórházra, ahol a jogsértést feltáró vizsgálat során 985 olyan felhasználót találtak, akik orvosi hozzáféréssel rendelkeztek, holott az intézményben csak 296 orvos dolgozik. Sajnos a botrányok korszakát éljük, és már Magyarországon is megjelentek a zsaroló vírusok. Egy hazai kórház informatikai rendszerét anonim támadók blokkolták, bitcoinban, azaz digitális fizetőeszközben követelve tetemes összeget a feloldás fejében. A felügyeleti hatóság és a biztonsági cégek természetesen nem javasolják az ilyen típusú díjak megfizetését, de bizonyos esetekben – akár presztízs okból, akár a tényleges adatvesztési probléma miatt – a károsultak mégis hajlandóak eleget tenni ezeknek a követeléseknek. Az ún. dark-web – a digitális világ sötét oldala – mindig előttünk jár egy lépéssel: a haszonlesők és bűnözők nagyon hatékonyan használják a digitális technológia eszközeit az információk megszerzésére, ellopására és azok felhasználásával különböző súlyú visszaélések elkövetésére. Tavaly és tavalyelőtt például megtámadták az esztek központi egészségügyi rendszerét, betörtek a norvégok államigazgatási rendszerébe levő levelező rendszerekbe, támadás érte az ukrán állami szerveket és a szlovák külügyminisztériumot. Néhány évvel ezelőtt a brit nemzeti egészségügyi szolgálat (National Health Service) rendszerét is leblokkolták. A magyarországi központi rendszereket még nem érte ekkora volumenű támadás, de sosem az a kérdés, hogy megtörténik-e, hanem inkább az, hogy mikor? A megelőzés és a felkészülés pedig éppen ezért, nagyon időszerű már.

TESTRE SZABOTT TÁMOGATÁS

– A kórházakat meglehetősen felkészületlenül érte a GDPR rendeletben foglaltaknak való megfelelési kötelezettség. Hogyan látott neki az Asseco Magyarország Zrt. egészségügyi üzletága a kórházak felkészítésének?

Mindenekelőtt fontosnak tartom elmondani, hogy a Magyarországon közel százötven alkalmazottat foglalkoztató vállalatunk egészségügyi üzletága – a GlobeNet – hosszú évek óta piacvezető pozíciót foglal el az egészségügyi informatika területén. A cégünk által kifejlesztett MedWorkS rendszer a legelterjedtebb kórházi informatikai rendszer (HIS) Magyarországon. Az Állami Egészségügyi Ellátó Központ (ÁEEK) felügyelete alá tartozó mintegy száz egészségügyi intézmény 40 százaléka a mi rendszerünket használja, így beszállítóként meglehetősen nagy rálátásunk van a magyar kórházak informatikai infrastruktúrájára. Magasan kvalifikált munkatársaink a nap huszonnégy órájában azon dolgoznak, hogy nonstop informatikai támogatást nyújtsanak a felhasználóknak. Nem csak magának a rendszernek a biztosítása és az ahhoz kapcsolódó támogatás tartozik a szolgáltatásaink körébe, hanem a rendszeres oktatás is. A kórházak működésében a teljes informatikai rendszer 80 százalékban a gyógyítási folyamatokat és a medikai rendszerrel kapcsolatos feladatokat fedi le. Ily módon, HIS beszállítóként napi szinten ismerjük a kórházak működését eszközoldalról és felhasználók viszonylatában is. A GDPR-ra való felkészülés körébe beletartozik az ügyviteli, levelezési és iktatási rendszerek áttekintése is, ám ez a tevékenység mindössze a feladatok 20 százalékát tette ki. Természetesen mi magunk is komoly tanulási folyamaton estünk át, de a munkába külső szakértőket – szakjogászokat, információbiztonsággal foglalkozó cégeket – is bevontunk. Így állt össze az a partnerkör, amely képes volt biztosítani a várhatóan nagy mennyiségű igény egyidejű kiszolgálását. Közreműködő partnereink részt vettek a kórházak bejárásában, aminek eredményeképpen elkészülhettek a felkészülési szintet rögzítő auditjelentések. Ezekben a meglehetősen terjedelmes dokumentumokban rengeteg hibát és helytelen működést tártunk fel. Második lépésként intézkedési – más néven cselekvési – tervet készítettünk arra vonatkozóan, hogy milyen prioritási sorrendben melyek a legfontosabb teendők az intézmények GDPR megfeleltetéséhez. Ennek az intézkedéssorozatnak az egyik eleme a felhasználói magatartás javítása oktatással, szabályozással, kontrollokkal és adatvédelmi szimulációs gyakorlatokkal, másik fő komponense az informatikai támogatottság európai szintre való emelése volt. Mivel – mint említettem – nagyon erős a digitális fenyegetettség a világban, fontosnak tartottuk a kórházak menedzsmentjének tájékoztatását arról, hogy milyen informatikai fejlesztések szükségesek az intézményükben a hatékonyabb védelem kialakítása érdekében.

– Ön az IME 2018 májusában megtartott Országos Egészségügyi Infokommunikációs Konferenciáján előadásában a bizalmasság, sértetlenség és rendelkezésre állás sérülékenységét elemezte. Összefoglalná röviden, hogy mit takar ez a „bűvös hármas”?

A bizalmasság elve azt jelenti, hogy egy adott személy adataihoz csak azok férhetnek hozzá, akiket ő erre felhatalmaz, illetve akiknek a közfeladat ellátása kapcsán törvényben előírt kötelezettségük, hogy megismerjék az adatait. Az egészségügy tipikusan az a terület, ahol sérülhet a bizalmasság elve. Ha például olyan személyek is be tudnak lépni a kórházi rendszerbe, akiknek nincs ahhoz joguk, vagy a váróteremben szabadon hagyott számítógép monitorát valaki lefotózza. Még a papír alapú dokumentáció esetén is sérülhet ez az elv. Gondoljunk csak arra, amikor a laborleletünket bárki számára kiadják, meghatalmazás hiányában is. Akkor is illetéktelenek kezébe juthatnak az egészségügyi adataink, ha vírustámadás éri az adott kórházi rendszert. Ez utóbbi eset arra példa, hogy milyen könnyen sérülhet a sértetlenség elve. A rendelkezésre állás azt jelenti, hogy az egészségügyi ellátórendszerbe belépő beteg adataihoz gombnyomásra hozzá kell férnie az őt ellátó orvosnak, hogy gyorsan informálódhasson a páciens korábbi kezeléseiről, gyógyszerelésről, esetleges gyógyszerérzékenységéről. Ezeknek az adatoknak az adatkezelője az egészségügyi intézmény, amelynek vezetője személyesen felel azért, hogy csak az arra feljogosított személyek férhessenek hozzájuk. Az állampolgárok azzal, hogy belépnek az ellátórendszerbe, ráutaló magatartást tanúsítanak, azaz automatikusan feljogosítják az adott intézményt az egészségügyi adataik kezelésére. Ugyanakkor joguk van ahhoz, hogy megtiltsák az általuk megnevezett személyek – például elvált házastárs, élettárs, stb. – hozzáférését. Mi minden partnerünknek azt javasoljuk, hogy vezesse be az ISO-27100 minőségbiztosítási rendszert, amelynek egyik fontos eleme az információbiztonság, és kritériumként foglalja magában a bizalmasság – sértetlenség – rendelkezésre állás hármasát.

– Milyen egyéb módon teremthető meg a kórházi információs rendszerek biztonsága?

A mi szakértői közösségünk, módszertanunk, megoldásaink és támogatási szolgáltatásaink ezt hivatottak szolgálni. A GDPR auditon és intézkedési terven túlmenően elérhető áron kínálunk olyan IT-támogató rendszert (NetWorkS), amely lehetővé teszi a teljes géppark rendszerezését, távfelügyeletét és távmenedzselését is. Ma már igénybe vehető továbbá olyan szakértői teamek közreműködése is, amelyek a vírusvédelem specifikus, nagy szaktudást igénylő feladatát 24 órán keresztül végzik, szoftveres segítséggel monitorozva a rendszerben zajló folyamatokat. Ilyen ún. Security Operation Center (SOC) működik például az államigazgatásban. A Kormányzati Eseménykezelő Központ (GovCERT-Hungary), mint a magyar kormányzat információ-megosztó és incidenskezelő szervezete végzi az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, továbbá közzéteszi a felismert és publikált szoftver sérülékenységeket. Mindenki figyelmébe ajánlom a központ szabadon hozzáférhető hírleveleit, amelyekben folyamatosan informálja az olvasókat a világban felmerülő kibertámadásokról.

GDPR: MISSION POSSIBLE!

– Hogyan értékeli a partnerkórházakban elvégzett, GDPR felkészítéssel kapcsolatos munkát?

Nyolc kórházat készítettünk fel, négyet teljes körűen, azaz auditot, intézkedési tervet és szoftvermegoldást is nyújtottunk. A másik négy intézmény esetében igény szerint hol auditot, hol intézkedési tervet, hol szoftvermegoldást biztosítottunk. Olyan kórház is felkért minket a GDPR-ra való felkészítésre, amelyik nem a mi HIS rendszerünket használja, de bízott a szaktudásunkban, és hozzánk fordult segítségért. A kezdeti ijedtséget követően a partnereink megértették a folyamat jelentőségét, örömmel vették a tanácsainkat, és igyekeznek követni az általunk kijelölt utat. Kórházi partnereinkkel együtt gondolkozunk, együtt dolgozunk, és együtt előzzük meg a bajt, és ha mégis megtörténne, akkor együtt hozzuk azt helyre.

– Az alábbiakban néhány egészségügyi intézmény képviselőjének a véleményét adjuk közre arról, hogy milyen tapasztalatokra tettek szert az Asseco Magyarország GlobeNet üzletágával folytatott együttműködés, a GDPR-ra való felkészítés során.

– „Derült égből villámcsapásként éltük meg a GDPR megfelelés kötelezettségét, nehezen fogtuk fel, hogy egyáltalán mi is az ezzel kapcsolatos feladatunk. Mivel a kórházunkban működő, meglehetősen magas átlagéletkorú 350 számítógép karbantartását mindössze három informatikus kolléga végzi, lehetetlen küldetésnek tűnt, hogy az egyiküket átképezzük, és erre a feladatra állítsuk rá. Hamar átláttuk, hogy a GDPR-hoz szükséges ismeretanyagot nem lehet néhány nap alatt elsajátítani, és a feladat ellátása nem pusztán informatikai, hanem speciális jogi tudást is igényel. Az Asseco Magyarország profi szakértőket delegált hozzánk, akik átvilágították az egész intézményt, és olyan intézkedési tervet tettek le az asztalra, amelynek mentén lépésről lépésre haladhatunk tovább. A felkészülés fél évet vett igénybe és sok munkával járt, de nagyon jó eredménnyel zárult, ezért sikertörténetként éltük meg.” (Szabó István informatikai vezető, Albert – Schweitzer Kórház – Rendelőintézet, Hatvan)

– „Nem ért minket váratlanul a GDPR megfelelési kötelezettség, hiszen ismertük az idevonatkozó, 2016-ban meghozott jogszabály rendelkezéseit. A fenntartóval folytatott előzetes egyeztetések eredményeképpen arra jutottunk, hogy olyan tapasztalt partnert keresünk a feladat elvégzésére, aki az ehhez szükséges tanúsítvánnyal és megfelelő tapasztalattal rendelkezik, mert ez biztosítékot jelent számunkra arra vonatkozóan, hogy meg tudunk felelni ennek a jogszabályi kötelezettségnek. Mivel a kórházunknak értelemszerűen nem volt erre felkészült csapata, fontos szempont volt az is, hogy a fejlesztési folyamat ne jelentsen jelentős pluszterhet a dolgozóink számára. Közbeszerzési kiírásunkra a legelőnyösebb ajánlatot kórházunk korábbi partnere, az Asseco Zrt. nyújtotta be, amelynek munkatársai jól ismerték intézményünk működését. A vállalat által opcióként megjelölt lehetőségek közül a komplex szolgáltatási csomagot választottuk, mert célszerűbbnek ítéltük meg, ha ezt a sokrétű feladatot egy hozzáértő csapat végzi el, mintha az auditot követően magunkra vállalnánk ennek a folyamatnak a további menedzselését. Mindössze néhány hónapot vett igénybe a felmérés, melynek végeztével az Asseco Zrt. egy igen részletes auditjelentést készített számunkra. A kórházbejárás során a cég munkatársai maximálisan alkalmazkodóak voltak, igyekeztek úgy dolgozni a háttérben, hogy ne zavarják az intézményünk elsődleges feladatát képező betegellátás menetét, és a munkálatok ne okozzanak fennakadást a mindennapi gyógyításban. Időközben elkészült a további teendőket kijelölő javaslatcsomag is, amelynek bizonyos elemei a közeljövőben kerülnek megvalósításra. Nagyon sikeres, produktív és hatékony együttműködést folytattunk, amely közel sem zárult le, hiszen a továbbiakban is számítunk az Asseco Zrt. támogató közreműködésére. (Dr. Havasi Katalin orvos-igazgató, Csongrád Megyei Egészségügyi Ellátó Központ, Hódmezővásárhely-Makó)

Boromisza Piroska

NÉVJEGY

Kocsis György 1982-ben szerezte meg üzemmérnöki diplomáját a Könnyűipari Műszaki Főiskolán. 2015-ben INFOTA online marketingképzésen vett részt, 2018-ban Gill&Murray Certified DPO képesítést szerzett. 2014-2016 között az IntelliMed Hungária Kft. cégvezetőjeként dolgozott, és az orvosszakmai társaságok kommunikációs rendszerének megújításával, új célrendszerek fejlesztésével foglalkozott. 2016-2017 között az Enterprise Communications Kft. kiemelt ügyfélmenedzsereként dolgozott, majd 2017-től az Asseco CE Magyarország Zrt. GlobeNet üzletágának szolgáltatásmenedzsere, NOCaaS (NetWork Operation Center as a Service) projektfelelőse. Feladata az egészségügyi IT infrastruktúra távfelügyeleti és monitoring rendszertámogatás bevezetése, GDPR projektek menedzselése, kiemelt ügyféltámogatás, és a MedWorkS HIS rendszer tudástárának terjesztése, bővítése.