Útmutató az ügyvédi információbiztonság javításához

dr. Homoki Péter, 2016. január 14.

1 Bevezető

Az ügyvédi törvény szerint az ügyvédet, ügyvédi irodát, alkalmazottait titoktartási kötelezettség terheli minden olyan adatot, tényt illetően, amelyről a hivatásának gyakorlása során szerzett tudomást, beleértve az ügyvéd birtokában lévő olyan iratot is, ami az ügyvédi titkot tartalmaz. E kötelezettség kiterjed az ügyvédi titkot tartalmazó elektronikus iratokat tároló vagy feldolgozó végző személyekre is.[1] Az ügyvédi hivatás etikai szabályairól és elvárásairól szóló 8/1999. (III. 22.) MÜK Szabályzat kimondja, hogy a titoktartásra kötelezett személy az ügyvédi titkot mindenkivel szemben köteles megőrizni (4/3.).

A technika sajnos olyan irányba fejlődik, hogy e kötelezettségünket egyre nehezebb megtartani. Bár a titkok "elkotyogásának" kockázata nem csökkent, mára az első számú veszélyforrássá az vált, hogy jogosulatlan személy valamely titokhoz technikai hiba vagy nem megfelelő kezelés miatt hozzáférhet. Az ügyvédi munkában is hatalmas mértékben megnőtt az elektronikus úton feldolgozott és forgalmazott adatmennyiség, így az ügyvédi titok is. Az ügyvéd úgy kommunikál, ahogyan azt az ügyfele elvárja, tehát nem alternatíva az ügyvéd számára, hogy megmaradjon a papír alapú kommunikációnál. Az ügyvéd csak egyet tehet: minél jobban gondoskodik az ügyfél elektronikus adatainak védelméről.

Egyre több ügyvédi kamara vizsgálja meg, hogy miként tudná ebben az ügyvédséget segíteni. Az Európai Ügyvédi Kamarák Tanácsában (CCBE) az informatikai jogi szakosztály hamarosan elfogad egy műszaki jellegű útmutatót, amely a nemzeti kamarák felé ajánlást fogalmaz meg. Ennek fényében időszerű vált, hogy ezt a kérdést Magyarországon is megvizsgáljuk.

Az alábbiakban először röviden bemutatjuk, hogy milyen fenyegetések érik az ügyvédséget, és milyen irányú változások várhatóak.

Ezt követően az ügyvédek számára általános jellegű javaslatokat fogalmazunk meg az ISO 27000-es szabványcsalád megközelítése alapján, a CCBE IT jogi szakosztályának műszaki útmutatójával összhangban. Végül pedig kiemeljük azokat a biztonsági intézkedéseket, amelyek az ügyvédek körében egyfajta minimum védelmi körnek tekinthető. Ez utóbbinál megpróbáltunk figyelemmel lenni arra, hogy az ügyvédi munka során melyek a tipikus sérülékeny pontok, de egyúttal ne is legyen a szöveg túl technikai vagy túl részletes sem.

2 Miért fontos az ügyvédek számára is az információbiztonság?

Az információbiztonsági tájékoztatásokat célszerű a motiváló (magyarul "rémisztgető") résszel kezdeni.

Manapság az információ biztonságát az információ három tulajdonságának megőrzéseként szokás definiálni, ez az információ **bizalmassága**, **sértetlensége** és **hozzáférhetősége** (lásd ISO/IEC 27000:2009 2.19, NIST CF, 2013. évi L. törvény stb.), ezért az alábbiakban bemutatott példák körében

[1] Lásd az ügyvédségről szóló 1998. évi XI. törvény 8. §.

is kitérünk arra, hogy az adott példában az információ biztonságának mely aspektusa sérül elsődlegesen.[2]

A hazai ügyvédi irodák méretéhez képest egészen nagy ügyvédi irodák is áldozatául estek a "ransomware"-nek nevezett zsaroló vírusoknak (pl. CryptoWall), ahol egy-egy csatolmányként letöltött rosszindulatú alkalmazás titkosítja az elektronikus ügyvédi iratokat, és csak bitcoin-ban fizetett (lenyomozhatatlan) váltságdíj fejében teszi lehetővé a dekódolást (ami aztán vagy sikerül, vagy nem.) Ez a veszély nem csak az ügyvédeket fenyegeti, de számos olyan esetet jelentettek, amikor ügyvédi irodák látták kárát az ilyen támadásnak. Olvashatunk ilyen támadásról az Egyesült Államokból, Kanadából, Angliából és Németországból is.[3] Látható, hogy ebben az esetben az információ "hozzáférhetősége" van veszélyben. (A teljesség kedvéért itt érdemes felhívni a figyelmet arra, hogy erre a félelemre is rájátszhatnak rosszindulatú személyek, amikor valaki azt mondja, hogy rosszindulatú kód támadta meg a gépet, és fontos fájlokat titkosított, amelyet csak nagy költség ellenében lehet helyreállítani – közben meg nem történt semmi ilyen.[4])

Szintén említést érdemelnek azok a támadások, amikor a támadók ügyvédnek adják ki magukat, és úgy próbálnak vagy az ügyvédi irodák munkavállalóitól vagy az ügyfelektől pénzt kicsalni. Akár egyszerűen úgy, hogy a levelezőrendszerhez való jogosulatlan hozzáférést követően a kiküldött elektronikus számla helyett egy olyan számlát küldenek az ügyfélnek, amin egyedül az ügyvédi iroda bankszámlaszáma helyett egy másik számlaszám szerepel. De az is többször előfordult már, hogy a támadó ügyfélnek adja ki magát, és a letéti pénz átutalását egy olyan számlaszámra kérte, ami valójában a támadóé. Ez esetekben vagy az információ tartalmát változtatják meg észrevétlenül félúton vagy az azt küldő fél megszemélyesítésével élnek vissza.

Nem minden támadó érdekelt azonban abban, hogy ilyen körmönfont módon pénz csaljon ki az ügyvédtől. Sok esetben a támadó célja egyszerűen a bizalmas információ megszerzése. Az ügyvédi munkát tekintve az utóbbi időben éppen a bizalmasság tulajdonsága az, amit érintően a kockázatok jelentősen megváltoztak, mert az ügyvédi munka alapját képező egyes kritikus eszközök és azok környezete is jelentősen megváltozott. Szinte minden ügyvéd tárol valamilyen ügyfél adatot távol az irodájától, amely adatot az internet útján érhet el - de nem csak ő, hanem bárki, aki ismeri a hozzáférési azonosítókat.

Az információ bizalmasságát illető támadások körében nagy médiafigyelmet kaptak az ügyvédi munkát érintő titkosszolgálati megfigyelések is, lásd pl. a Prakken D'Oliveira ügyet.[5]

Akár hazai, akár külföldi titkosszolgálatról, bűnüldöző szervek által végzett megfigyelésről van szó, az ügyvédek számára a legnagyobb kockázatot az jelenti, ha egyes állami szervek úgy végezhetnek titkos információgyűjtést, hogy ennek tényéről nincsen megbízható nyilvántartás (a megfigyelésről

---

[2] Hozzátesszük, nem túl lényeges, hogy mikor-melyik sérül. Számunkra fölösleges elméleti vita lenne abba belebocsátkozni, hogy mikor-hol az egyes fogalmak között a határ, és pl. a hitelességet vagy más alternatív tulajdonságot hova illesszük be ezek közé, és egyáltalán a "tulajdonság"-e a helyes megnevezés.

[3] http://blog.michgehl.de/it-panne-des-monats-februar-loesegeld-oder-daten-weg/, http://www.cbc.ca/news/canada/british-columbia/ransomware-hackers-pose-threat-to-b-c-law-firms-1.2898490, http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security

[4] Lásd pl. https://discussions.apple.com/docs/DOC-8071 vagy az alábbi, tanulságos eset: http://www.wsj.com/articles/SB10001424052748703957804575602993406810012.

[5] http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/HU_newsletter_46pdf14_1448977757.pdf.

nincsenek a bíróság számára hozzáférhető adatok). Így lehetőségük nyílik e szerveknek arra, hogy egy megfigyelést csak akkor vegyenek nyilvántartásba, ha az így szerzett adatot bíróság előtt fel akarják használni.

Ettől függetlenül annak is jelentősen megnőtt a kockázata, hogy államinak nem minősülő nagyobb privát szervezetek (pl. szervezett bűnözői csoportok) vagy akár az érdekellentétben álló közeli hozzátartozók is jogosulatlan hozzáférjenek bizonyos ügyvéd-ügyfél kommunikációhoz.[6]

Ma elképzelhetetlen, hogy egy ügyvéd ne ismerje a papír alapú iratkezelés alapjait, és minden ügyvédnek tudnia kell, hogy miként tudja beazonosítani a bírósági, hatósági és ügyfeles iratokat, és miként gondoskodjon azok biztonságáról. Lehet, hogy egy adminisztrátor vagy szerződő partner végzi az iratkezelést és a postázást, de az ügyvéd feladata, hogy elmagyarázza az igényeit és ellenőrizze a feltételek betartását. Ugyanígy elengedhetetlenné válik az is, hogy az ügyvéd az elektronikus iratokról, és általában az informatikai eszközei biztonságáról gondoskodjon. Nem kell feltétlenül a technikai részleteket ismernie, de azt igenis tudnia kell, hogy milyen intézkedések biztosítják a megfelelő szintű információbiztonságot. Az információbiztonság megfelelő tudatossága, fontosságának megértése, megfelelő prioritásként kezelése elválaszthatatlan része az ügyvédi működésnek.

3 Az ügyvédi információbiztonság javasolt megközelítése

3.1 Áttekintés

Általánosságokat meg lehet fogalmazni az ügyvédi működés informatikai hátteréről: minden országban kritikus az ügyvéd szinte folyamatos, emailbeli és telefonos elérhetősége. Vagy azt, hogy ritkán konfigurálják és működtetik a saját weboldalaikat, webszolgáltatásaikat. De részleteket a technikai és az ügyvédi működés sokfélesége miatt még a hazai viszonylatban is lehetetlen megfogalmazni. Még az egyéni ügyvédek megbízható védelmére sem lehet általános biztonsági receptet adni, nemhogy a jelentősen eltérő méretű ügyvédi irodákra. Ahány szoftver, eszköz és egyedi konfiguráció, annyi eltérő típusú informatikai kockázat és kockázatkezelés.

Maga az információbiztonság is nagyon sok tényezőt érintő, sokféle ismeretet igénylő terület, sok szinten lehet vizsgálni. Alacsony szintű technikai paraméterektől kezdve nagyvállalati méretű folyamatok szabályozásán át az információbiztonsági megfelelőség értékelésének kérdéséig sok minden ide tartozik.

Szem előtt kell tartanunk, hogy nehezen beszélhetünk megfelelő szintű információbiztonságról, ha annak csak egy-egy részterületét ragadjuk ki. Két példa erre: egy több felhasználós környezetben hiába védjük megfelelő jelszavakkal a gépeket, ha emellett a felhasználók nincsenek egyedileg azonosítva. (Hasonlóan ahhoz, hogy hiába szigorú a felelősségi szabály egy pénztárossal szemben, ha egy adott időpontban két pénztáros is hozzáférhetett ugyanahhoz a kasszához, és nem tudjuk, hogy melyik.) Ugyanígy hiába titkosítunk egy üzenetet akár a feladótól a címzettig, ha a küldő vagy fogadó végberendezéshez illetéktelenek is hozzáférhetnek. Tehát ha csak egyes részterületeket veszünk figyelembe, akkor könnyen lehet, hogy csak a biztonság hamis illúzióját kapjuk meg.

A fentiekre figyelemmel a jelen útmutatóban célszerű, ha először bemutatunk egy általánosabb információbiztonsági megközelítést, ami alapja lehet egy megfelelő információbiztonsági tudatosság

[6] További riasztó esetek kiváló példatára az angol-walesi solicitor szabályozó hatóság IT biztonsági jelentése, lásd https://www.sra.org.uk/risk/resources/online-crime-legal-business.page.

kialakításának. Egy olyan vázat kellene adni, amire aztán alappal lehet felaggatni a számtalan lehetséges biztonsági intézkedést, és ezeket megvalósító piaci megoldásokat.

3.2 A szabványok szerepe az információbiztonság terén

Az általánosabb megközelítést illetően azt láthatjuk, hogy az ügyvédi tudás megszokott forrása, a jogszabályok, nem sok érdemi segítséget nyújtanak nekünk. A bevezetőben hivatkoztunk az ügyvédi törvény irányadó általános kötelezettségére. Ezen túlmenően személyes adatot is tartalmazó iratok esetén hasonlóan általános útmutatást találhatunk az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 7. § (2) és (6) bekezdésében,[7] egyéb védett adatok (pl. banktitok) esetén az ágazati törvények előírására is.[8]

Ezek a jogszabályi előírások az általánosság olyan szintjén maradnak, amelyekhez közvetlenül nem kapcsolhatunk sem technikai, sem szakmai standardokat, legjobb gyakorlatokat, hatóságok vagy bíróságok által elfogadott zsinórmértéket. Az IT biztonság területén ilyen közvetítő-részletező tartalmat a szabványosítás eszközei adnak.

Számos előnnyel jár, ha az IT biztonság témáját az ügyvédek esetén is a tárgybeli informatikai szabványokra építve próbáljuk megközelíteni:

a) Az IT biztonsági szabványra épülő információbiztonsági megközelítést már más iparágakban és szakmákban is jó ideje használják. Számos más szakma vagy iparág van, amely egy vagy több szempontból hasonlít az ügyvédi működéshez, így az ő IT biztonsági tapasztalataikat, az általuk alkalmazott kockázatkezelési technikákat magunk is hasznosítani tudjuk. Vagy össze tudjuk magunkat hasonlítani azzal, hogy pl. a közjegyzők információbiztonsági tudatossághoz képest mi hol állunk.

b) Mivel az IT biztonsági szabványokat az ügyfeleink is ismerhetik, alkalmazásával egyszerűen és hihetően alá tudjuk támasztani, hogy az ő adataik biztonsága számunkra is fontos. Persze egy IT biztonsági szabvány követése, alkalmazása, önmagában nem biztosíték semmire, hiszen láthatjuk, hogy a technikai nagyvállalatok is milyen gyakran elszenvedői különféle adatvédelmi incidenseknek. De éppen az ilyen nehezen elkerülhető helyzetekben a legfontosabb, hogy legyen mire hivatkoznunk, hogy mi azért kellő gondossággal jártunk el.

Mondhatjuk, hogy az "elvárhatóság" mércéjét éppen a minél széles körben alkalmazott IT biztonsági szabványokkal tudjuk kitölteni.

---

[7] 7. § (2) … köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(6) Az … adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

[8] Egyelőre nem várható, hogy bármilyen általános IT biztonsági jellegű kötelezettséget jogszabály vagy általánosan kötelező uniós jogi aktus előírna. Az új általános adatvédelmi rendelet tervezete sem fog e téren alapvető változást hozni, és a hálózati és információ biztonsági irányelv uniós jelenleg ismert tervezete (koncepciója) sem lesz az ügyvédekre irányadó. Azonban már jelenleg is komoly IT biztonsági szabályozás irányadó például az állami szervekre Magyarországon, lásd a 2013. évi L. törvényt.

3.3 Az ügyvédi munka számára jelentős információbiztonsági szabványok

Melyek ezek az IT biztonsági szabványok, amikre érdemes odafigyelnünk? Az ügyvédek számára a NIST FIPS 800-53 számú kiadványa és a kiberbiztonsági keretrendszere,[9] valamint az ISO 27000 alapokra építő nemzetközi szabványok bírnak kiemelt jelentőséggel.[10]

A NIST és az ISO 27000 szabványcsaládban is sok hasonlóságot láthatunk, ám a részleteket illetően már jelentős eltéréseket találhatunk. Bár a hazai 2013. évi L. törvény és végrehajtási rendeletei a NIST FIPS 800-53 kontrolljaira építenek, ugyanakkor az európai ügyvédek körében is inkább az ISO 27000 szabványcsaládra építő kezdeményezések fognak várhatóan teret nyerni.[11]

Erre utalnak a CCBE-ben hamarosan véglegesítésre kerülő egyeztetések is, de az is, hogy a privát szervezetek számára ez a szabvány biztosít viszonylag olcsó és jól kommunikálható tanúsítási (független harmadik felek általi igazolási) lehetőséget (azaz egy megfelelőségi "plecsnit").[12]

Persze ezt ne értsük úgy, hogy majd a jövőben minden ügyvédi praxisnál elvárás vagy ajánlott volna az ISO 27001 szabvány szerinti tanúsítottság (ez teljességgel értelmetlen volna az ügyvédi praxisok nagy részét kitevő egyéni ügyvédeknél, ahol az alkalmazottak száma is minimális.) Az ISO 27000 szabványcsaládnak abból a szempontból van jelentősége, hogy mi legyen a fentebb említett általános megközelítés, a szóhasználat (terminológia), és milyen lehetséges kontrollokat, kockázatkezelési részterületeket, csoportosításokat használjunk.

Maga az ISO 27000 és 27001 szabvány önmagában nem túl informatív, azonban az ISO 27002 számú, gyakorlati kézikönyvként működő szabvány már a technikailag érdeklődő ügyvédek számára is hasznos olvasmány lesz.[13] A szabványcsaládba tartozik még számos, jóval részletesebb szabvány is, pl. a kiberbiztonság vagy az alkalmazási biztonság terén, de ezek alapvetően szakembereknek szólnak.[14]

---

[9] A NIST az Egyesült Államok szövetségi szabványügyi szervezete. Lásd NIST FIPS Cybersecurity Framework és NIST Special Publication 800-53 Revision 4, April 2013, Security and Privacy Controls for Federal Information Systems and Organizations.

[10] Természetesen ezen kívül is számos, nemzetközileg elismert információbiztonsági szabvány van, de ezekkel ügyvédek csak kivételesen és érintőlegesen találkozhatnak, pl. a Common Criteria, magyarul Közös szempontrendszernek nevezett szabvány leginkább termékek IT biztonsága szempontjából bír jelentőséggel, vagy a COBIT, amelynek fókusza nem kizárólag az IT biztonságra terjed ki, hanem alapvetően nagyvállalati működés informatikai szempontú megfelelő irányítottságára stb.

[11] Ügyvédi körben egyelőre a francia ügyvédek nemzeti kamarai szervezete által megfogalmazott ajánlásokat érdemes megnézni, ez ingyenes regisztráció után francia nyelven elérhető itt: http://cnb.avocat.fr/downloads/ebarreau-prive_t9248.html.

[12] A NIST FIPS 800-53 az USA szövetségi információs rendszerek részére, azaz állami célokra lett kidolgozva, de ettől függetlenül a részletes kidolgozottsága miatt ajánlásai, javasolt kontrolljai-szabályozó eszközei más területeken is útmutatásul szolgálnak. Lásd például kifejezetten a kisvállalatok számára megfogalmazott, ingyenesen hozzáférhető tanulmányt: NIST Small Business Information Security: The Fundamentals, http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf

[13] Sajnos az ISO 27002 aktuális kiadása magyar nyelven még nem érhető el, csak angolul, az ISO 27001:2014 jelzésű, magyar nyelvű szabványt nem a területtel való ismerkedésre találták ki.

[14] Pl. ISO 27031-27034-es szabványok.

Az ISO 27000 szabványcsalád alkalmazását illetően kiadtak már kifejezetten kisvállalkozások számára szóló kézikönyvet is.[15]

3.4 Az ISO 27001 szabvány működési mechanizmusának bemutatása

Ez egy bevezető jellegű útmutató, ezért eltekintenénk az ISO 27001 vagy ISO 27002 szabványok tartalmának pontos ismertetésétől. Célszerű inkább a szabvány megközelítését bemutatni, segítve annak megértését, hogy mi a működésének a váza, és hogyan illeszkednek ehhez az egyes biztonsági célok és intézkedések, valamint az ezeket megvalósító informatikai termékek.

Ennek az útmutatónak nem célja, hogy elmagyarázza egy irányítási rendszer működését vagy kiépítését, és a folyamat minden lépését érthetővé tegye. Mint mondtuk, a hazai praxisméreteket tekintve ez nem életszerű. A cél pusztán az, hogy ügyvéd megérthesse a szabvány működésének logikáját, mert csak így tudjuk megvizsgálni, hogy egyáltalán milyen területet fedtünk le már biztonsági intézkedéssel, és mit nem. Éppen ezért számos, a szabvány szempontjából lényeges pontról nem is ejtünk szót, és noha az információbiztonság a papír- és elektronikus iratokat egyaránt lefedi, mi érdemben csak az elektronikus vonatkozásokra fókuszálunk (IT biztonság).

A szabvány a megfelelő információbiztonság kialakítása, fenntartása, javítása érdekében két alapelvet állít a középpontba:

a) legyen egy dokumentált formában is vizsgálható **irányítási rendszer** (szabályzati rend, folyamatok, szervezeti felépítés, kézikönyv stb.), amely a "tervezés, végrehajtás, ellenőrzés, beavatkozás" klasszikus, minőségirányításban is ismert modelljét (plan-do-check-act) követve, a folyamatos javítás szándékával ténylegesen működik az adott szervezetben;

b) tudatosítsuk az **információbiztonsági kockázatok kezelését**, mégpedig a biztonsági kockázatok felmérése és javítása útján.

Első lépésként javasoljuk, hogy a praxis - figyelembe véve az ügyfélkörét, múltbeli működését, a személyzetének képességeit - azonosítsa be a legfontosabb információs "értékeiket", erőforrásait, vagy ahogyan a szabvány mondja, **vagyontárgyait**.[16] Ez alatt értjük az ügyféliratokat, a fontosabb belső nyilvántartásokat (pl. ügyfél adatbázisokat, főkönyvet, tárgyalási naplót), a működés szempontjából leginkább kritikus, külsős szolgáltatásokat (pl. internethez való hozzáférést, jogi adatbázisokat, bírósági vagy más weboldalakat stb.), de a szabvány ide sorolja az embereket, a szakmai jó hírnevet is.

Ha van egy ilyen listánk, gondoljuk végig, hogy milyen komolyabb veszélyek fenyegethetik az egyes "információs vagyontárgyakat", mi a gyenge pontjuk? És mivel járhat, ha sérülne a bizalmasságára, sértetlenségére vagy elérhetőségére (rendelkezésre állásuk) vonatkozó valamely követelmény? Mekkora lenne az időbeli kiesés, az anyagi kár vagy a presztízsveszteség, amivel ez járna? (Ki lehetne-e mindezt pl. pénzbeli egyenértékkel fejezni?) Próbáljunk meg az ilyen nemkívánatos eseményeknél a "*becsült* kár" összegén az esemény bekövetkeztére is becslést adni.

---

[15] Lásd pl. Edward Humphreys: ISO/IEC 27001 for Small Businesses: Practical Advice, ISO, 2010.

[16] Az angol "asset" hivatalos magyar fordítása a szabványban vagyontárgy. Sem az eredeti angol, sem a magyar fordítás szerint szakkifejezésnek jól láthatóan semmi köze a szó domináns jelentéséhez.

Természetesen mind a kockázatok beazonosításához, mind azok elemzéséhez szükség lesz informatikai ismeretekre is, de a nemkívánatos következmények miatt e folyamatban is elengedhetetlen az ügyvédi részvétele.

Ha ezt a fajta kockázatelemzést el tudjuk végezni legalább néhány vagyontárgyra, lesz egy összehasonlítási alapunk. Ez az alap segíthet abban, hogy eldönthessük, melyek azok a kockázatok, amelyekkel együtt tudunk élni, figyelemmel azok bekövetkezésének valószínűségére és az intézkedések költségére is. Meg lehet-e esetleg változtatni úgy a működési folyamatokat, hogy az adott kockázat valószínűsége csökkenjen? Át lehet-e hárítani a kockázatot külső felekre?

A 27001-es szabvány "**intézkedésnek**" (control) nevezi azokat az eszközöket, amelyek segítségével a kockázatot csökkenteni lehet, legyen az szabályozási vagy tisztán műszaki természetű. Ezen szóba jöhető intézkedések sajátos csoportosítása, felsorolása és széles körű alkalmazása az, ami miatt igazából megéri ezzel az információbiztonsági szabvánnyal foglalkozni, hiszen ez egy "közös nyelvet" ad. A legújabb, ISO/IEC 27001:2013 szabvány[17] 14 csoportot fogalmaz meg, amelyen belül 35 intézkedési célhoz mintegy 113 különféle intézkedést nevesít, mint pl. "biztonsági határzónát kell használni, hogy védjék az információt és az információfeldolgozó eszközt magába foglaló területeket" (A.9.1.1).

Ehhez képest a 27002-es szabvány azért is hasznos gyakorlati útmutató, mert érthető magyarázatokat (bevezetési útmutatókat) is ad ahhoz, hogy ezt az adott "intézkedést" miként kellene megvalósítani.[18]

Természetesen e körben ne technikai útmutatókra gondoljunk, de arra ez a 27002-es szabvány már elegendő, hogy értelmesen összehasonlíthassuk, melyik szervezetnél milyen információbiztonsági intézkedések működnek, és mire érdemes esetleg több hangsúlyt fektetni, hol van szükség erősebb kontrollokra.

Így ha az ügyvédek számára egy "informatikai higiéniai minimumot" szeretnénk meghatározni, akkor szintén ebből a csoportosításból, terminológiából érdemes kiindulni. Az útmutatónk következő fejezetében erre teszünk kísérletet.[19]

4 Az ügyvédek számára javasolt minimum biztonsági intézkedések köre

Az ISO 27001 szabvány működési alapelemeinek bemutatása után érdemes áttérnünk az egyes javasolt intézkedésekre, de kerülve a túlzott technikai részleteket. A lista természetesen jóval szélesebb lehetne, de próbáltunk a leglényegesebb pontokra fókuszálni, egyrészről figyelemmel arra, hogy az ügyvédi munka során számos szabályozási intézkedés megléte triviális, másrészről figyelemmel a már többször említett tipikusa kis szervezeti méretekre. Az egyes biztonsági

---

[17] Magyarul MSZ ISO/IEC 27001:2014 számon adták ki.

[18] Sajnos az MSZ ISO/IEC 27001:2014-as szabványhoz tartozó 27002-es szabvány még nem lett magyar nyelven kiadva, így a legutolsó magyar nyelven elérhető tárgybeli szabvány az MSZ ISO/IEC 27002:2011, ami a 2005-ös ISO/IEC 27002:2005 fordítása, az pedig a 27001:2005-ös szabvány intézkedéseit magyarázza. Egyébként a szakkifejezések fordításának nehézsége miatt annak, aki teheti, inkább az angol nyelvű változat használatát javasolom.

[19] Szándékosan nem beszéltünk e fejezetben a minden irányítási rendszer elválaszthatatlan részét képező, az irányítási rendszer fejlesztésével, kiértékelésével, átvizsgálásával kapcsolatos lépésekről – ezek nem speciálisan az információbiztonsághoz kötődnek, hanem minden irányítási rendszerhez.

intézkedéseket 2013-as kiadású szabvány szerinti azonosítóval jelöltük, az intézkedések magyar megnevezésével.[20]

8.1.1. – Vagyonleltár

A 3.4. pontban már megmagyaráztuk, hogy a „vagyontárgy" szónak sajátos jelentése van az információbiztonság területén. Jelenthet információ típusú vagyontárgyat (ügyfélirat, ügyfél adatok, pénzmosási és JÜB-adatok nyilvántartását stb.), szoftver vagyontárgyat (alkalmazásokat, rendszerszoftvereket, egyedi fejlesztéseket stb.), fizikai eszközöket, sőt, ide tartoznak a köz- és egyéb szolgáltatások, alkalmazottak és irodai tagok vagy az iroda jó hírneve is. Tegyük hozzá azért, hogy az ügyvédi praxis számára alapvetően a vagyonleltárban az információ a legértékesebb, ezért elsődlegesen erre összpontosítsunk.

Ezek egy része különféle analitikus nyilvántartásban már szerepelni fog, és itt nem is az a lényeg, hogy még egyszer leírjuk. Vegyük számba, hogy a praxis működése során mely vagyontárgy az, aminek kiesésére és pótlására érdemes előre felkészülni, és melyik kiesése van kihatással egy más vagyontárgy használatára. Emiatt e lista nem csak felsorolás, hanem egy fontossági osztályozás is egyben.

E leltár önmagában nem túl hasznos, de előfeltétele a 3.4. pontban leírt kockázatfelmérés elvégzésének, valamint a 17.1.1. számú információbiztonsági folytonosság tervezésének is.

8.2.1. – Az információ osztályozása

Ez az intézkedés már nem minden vagyontárgyra, csak az információkra vonatkozik. Csak azért érdemes kiemelni, mert az ügyvédi működés szempontjából kritikus kérdés az ügyfél és nem ügyfél adatok (iratok) megkülönböztetése, továbbá az ügyfelekkel kapcsolatos információkon belül is pontos további kategóriák felállítása és azok következetes alkalmazása (így az iratok azonosítása, kategorizálása irattári tételek, ügyek, akták stb. szerint). Ez természetesen az információbiztonság kérdésén túl már az iratkezelés területére vezet át minket, de ugyanúgy alapja mindkettő területnek.

Hasonlóan ahhoz, hogy a büntetőjogi védői tevékenység egyes területeken fokozottabb törvényi védelemben részesül az egyéb ügyvédi titokhoz képest, indokolt lehet az ügyfeles információkon belül is ezekre külön, magasabb védelmi fokozatot felállítani (akár a büntetőügyekre általában, akár meghatározott tényállásokra).

8.1.3. – A vagyontárgyak elfogadható használata

Ezen intézkedés körében sem cél a teljes körűség, és az, hogy minden egyes létező vagyontárgyra valamifajta szabályzatot előírni. Ugyanakkor nagyon fontos, hogy az alkalmazottal vagy több irodai taggal működő praxisok esetén is legyen egy egyértelmű, írt szabályzat egyrészről a mobil eszközök használatáról, másrészről az internet és az elektronikus levelezőrendszer használatáról, amelyet ha megszegnek, akkor az egyértelműen szerződésszegésnek minősülhessen, és a megfelelő szerződéses jogkövetkezménnyel járhasson.[21]

---

[20] Az intézkedések címénél az angol névből indultunk ki, de annak fordítását a 2011-es magyar fordításból próbáltuk levezetni, így néhány pontban lehet eltérés a hivatalos, 27001:2014-es magyar fordítástól. Az intézkedések sorrendje esetleges.

[21] Nem véletlen, hogy e két szabályzat szükségességére még az angol ügyvédi minőségirányítási rendszer, a Lexcel is kifejezetten utal. Lásd Lexcel International v5, 4.2. és 4.4. számú követelményeit, http://www.lawsociety.org.uk/support-services/accreditation/documents/lexcelv5-standard-brochure/

Itt azért fontos kihangsúlyozni a *leírt* szabályozást, mert aránylag gyakran van szükség a felelősség megállapítására, és számos olyan kockázat van, amelyet nem lehet automatikus intézkedésekkel kivédeni, ám ha bekövetkezik, akkor az okozott kár nem csak anyagilag lehet jelentős, pl. mobil eszközökhöz illetéktelen személyek hozzáférése, levélcsatolmányok vagy weboldalak megnyitásával letöltődő és futó rosszindulatú kód esetén (lásd még a 12.2.1. számú intézkedést).

Az elfogadható használat betartását az is segítheti, ha telepítünk egy tartalomszűrő szoftvert, amely csak egyedi felülbírálással engedi a hozzáférést "kockázatos" témájú oldalakhoz. Persze ugyanakkor az ilyen szoftver a kutatási célú internet használatot is jelentősen megnehezíti az érintett számára.

De lehet akármilyen biztonságos szűrőszoftver és vírusirtó, sohasem lesz fölösleges az a plusz egy védelmi vonal, amit a tudatos és az esemény elkerülésében motivált felhasználó jelent.[22] Ebből a tudatosságot a megfelelő oktatás (lásd a 7.2.2. számú intézkedést) mellett a megfelelő szabályzat tudja elősegíteni (mint a szankcionálást lehetővé tevő motiváció).

(Arról, hogy a mobil eszközök körében melyek a legfontosabb használati szabályok, a 6.2.1. számú intézkedésnél részletesebben kitérünk.)

7.2.2. – Információbiztonsági tudatosság, képzés, oktatás

Az intézkedés címe magáért beszél. Célszerű ennek keretében megismertetni az érintetteket azzal, hogy az esetükben az információbiztonság sérülésének milyen tipikus formája következhet be, az milyen következményekkel járhat a számukra, és milyen biztonsági intézkedések hivatottak ezeket elkerülni, mi az egyes intézkedések célja.

Indokolt összeállítani egy sajátos oktatási „csomagot” az új belépők számára. Célszerű továbbá az üzleti vagy informatikai környezetben bekövetkező nagyobb változások előtt is külön, a változással kapcsolatos tréninggel felkészülni.

Saját érdekünkben ilyen oktatás jellegű tájékoztatásra bizonyos szerződéses partnerek esetén is célszerű, ha sor kerül.

6.2.1. – Mobil eszköz szabályzat

A mobil eszközök, úgymint laptopok, táblagépek és telefonok több szempontból is fokozottabb kockázatnak vannak kitéve (a szintén mobilis adathordozók védelméről külön intézkedés szól). Az ilyen eszközöket a jól kontrollálható irodai környezeten kívül használják, így nagyságrendekkel nagyobb az esélye az eszköz, az eszközön lévő- vagy az eszközzel hozzáférhető irodai információ elvesztésének, megsérülésének vagy jogosulatlan általi hozzáférésnek. Ha egy ilyen eszköz rosszindulatú személyek kezébe kerül, lényegében minden eszközzel megpróbálkozhatnak biztonsági támadást indítani.

Így az érzékeny vagy drága mobil eszközök esetén jóval több védelmi intézkedésre van szükség, mint az irodai környezeten belül. Irodai környezetben nem feltétlenül szükséges a háttértárakat titkosítani, míg egy laptop esetén ez már elvárható intézkedés. Ha nem titkosítjuk, lehet akármilyen erős belépésre használt felhasználói jelszó, kis csavarhúzó segítségével a támadó az adathordozóhoz könnyen hozzájut. Így lehet, hogy a biztonságos jelszó mellett a hálózati erőforrásaink nem kerülnek rögtön veszélybe, de a hordozható eszközön lévő adatok igen.

---

[22] Az adathalászat (phishing) vagy a pszichológiai manipuláció olyan támadási formák, amelyek ellen nem vagy nem lehet csak programokkal védekezni.

Mobil eszközök esetén mindig érdemes az ellopás ellen fizikai védelmi intézkedéseket is tenni. Az ilyen lehetséges eszköz a zsebben is hordozható Kensington-zár, amellyel laptopokat tudunk a „felkapás" ellen védeni (bár a gyenge műanyagok könnyen engednek, ez a legegyszerűbb támadásoknak mégis elejét veheti). Ugyanígy hasznos védelmi intézkedés, ha repülőtéren a mobil eszközöket mindig a kézipoggyászban visszük, és nem adjuk fel a csomagtérbe. (A mobil eszközök gépkocsibeli tárolására vonatkozóan talán külön fel sem érdemes már hívni a figyelmet, annyira triviális.)

Ahogyan a távmunka esetén, úgy a mobil eszközök esetén is indokolt csak olyan hálózati kapcsolatot használni, amely során legalább egy minimális védelmünk van az adatforgalom lehallgatása ellen. Azonban a gyakorlatban ezt mobil eszköz esetén megvalósítani jóval nehezebb.

Nagyszerű dolog a wifi, de nem mindig szabad ügyvédi munkára használni. Ne használjuk ügyfél adatok forgalmazására a védelem nélküli wifit (nyílt wifit), sem olyat, ahol a wifi jelszó mindenki számára jól láthatóan ki van írva, sem olyat, ahol gyanítjuk, hogy már napok óta ugyanazt a jelszót használják.[23] Ha az irodánkban a vendégeknek is szeretnénk wifi hozzáférést adni, az véletlenül se legyen azonos az irodai wifivel, és a kollégáknak is magyarázzuk el, hogy miért ne a vendég wifit használják.

Természetesen a fenti javaslat igaz az ügyvédi irodák által kínált ingyenes vendég wifire is – nem attól kell félni, hogy ők gyűjtik az ügyfeles adatainkat, hanem attól, hogy illetéktelenek használják e célra a vendég wifijüket. Ugyanígy saját magunk csak akkor kínáljunk az ügyfeleknek wifit, ha megbízhatóan tudunk gondoskodni a megbízhatóságáról és védelméről.[24]

A wifihez képest jóval biztonságosabb a mobilinternet használata, bár kétség kívül ez főleg külföldön nem mindig opció. A legbiztonságosabb, ha ilyen eszközöknél is ún. VPN hálózati kapcsolatot biztosítunk a mobil eszköz és az iroda vagy más érzékeny informatikai erőforrás között.

Végül említsük meg, hogy egyre többször használjuk munkavégzés céljára az okostelefonokat és táblagépeket, mégis az ezeken használt biztonsági intézkedések köre tipikusan jóval szűkebb a laptopokhoz képest, pedig a kockázatuk legalább akkora. Ma már ezekre is telepíthetünk vírusirtót, tűzfalat és rosszindulatú weboldalak elleni védelmet, valamint titkosíthatjuk az adattartalmát – de ezek jellemzően nem képezik az alapkonfiguráció részét, tehát ezeket a szoftvereket külön meg kell vásárolni, telepíteni és konfigurálni kell.

6.2.2. – Távmunka

A mobil eszközöknél leírt kockázatokat javasoljuk a távmunkára is azonos módon alkalmazni. (Nem mobil eszközön végzett távmunka esetén elegendő egy fix fizikai környezetre felkészülni, ez a biztonságos hálózati kapcsolat kiépítése szempontjából könnyebbséget jelenthet, de hogy ez mikor irányadó, nem az ilyen egyszerű útmutatókba tartozik.)

---

[23] A támadó az előre megosztott, de közösen használt jelszavak megadásakor is rögzítheti a támadó a wifi hozzáférési pont és eszközünk közötti kommunikációt, bár nem ugyanolyan egyszerűen, mint nyílt wifi esetén (WPA PSK).

[24] Így a jelszó nélküli vagy egységes jelszavú wifi helyett az alkalmanként kiadott jelszót biztosító rendszer használatával, pl. http://www.zyxel.com/us/en/products_services/uag50.shtml

11.2.1. – A berendezés elhelyezése és védelme

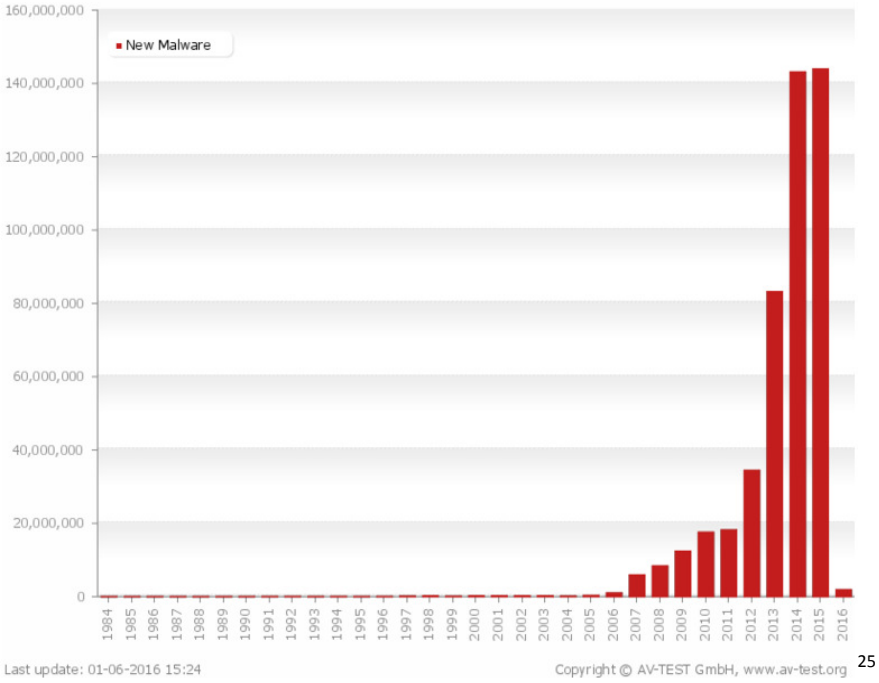
Ide tartoznak többek között azok a triviális, de fontos eszközök, amelyek biztosítják az eszközök villámvédelmét, túláram-elleni védelmét, valamint a tűz- és vagyonvédelmi távfelügyeleti szolgáltatások is. Ide tartoznak azok a szabályok is, amelyek megtiltják az eszközök közelében az étkezést.

9.2.2. – Közműszolgáltatások

Egyes eszközeink esetén az áramingadozás miatti leállásokból való helyreállítás időigénye vagy az adatvesztés kockázata miatt indokolt gondoskodni a szünetmentes tápáram ellátásról.

Bár hazánkban jogilag nem tekintjük közszolgáltatásnak, mégis ezen intézkedéshez sorolják a távközlési kapcsolatok megbízhatóságát is. Ma már annyira olcsó a mobilhálózati internet hozzáférés, hogy a legkisebb ügyvédi irodáknál is megérheti, hogy a nagy sávszélességű vezetékes internet hozzáférésünk mellett mindig legyen készenlétben egy mobilinternet hozzáférés is.

12.2.1. – Védelem a rosszindulatú kódok ellen



[25]

Hogy egy rosszindulatú kódot (malware) minek nevezünk (vírusnak, féregnek, trójainak, backdoornak, rootkitnek stb.), az azon múlik, hogy sokszorosítja-e magát[26] vagy sem, és hogy mindezt milyen hatásmechanizmussal teszi. Valljuk be, ez ügyvédi szempontból technikai részletkérdés.[27]

---

[25] A kép forrása az AV-TEST Malware/Statistics oldala, lásd https://www.av-test.org/en/statistics/malware/.

[26] Az önmagát sokszorosító rosszindulatú kódot nevezik vírusnak vagy féregnek. A vírus és a féreg (worm) között abban volt eredetileg különbség, hogy miként fejti ki a sokszorosító tevékenységét (lásd pl. http://usa.kaspersky.com/internet-security-center/threats/computer-viruses-vs-worms#.VpGHp_nhCUk), de ma, amikor minden hálózatba van kötve, lényegében a magát sokszorosító kódok legjelentősebb része a régi fogalmak szerinti „féreg”.

[27] Akit érdekel, rövid, de jól érthető összefoglalót olvashat erről pl. a következő útmutató 2. pontjában: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

Hatását tekintve felélheti vagy tönkreteheti számítógépes erőforrásainkat, jogosulatlanul adatokat gyűjthet a gépeinkről (bármilyen rosszindulatú célból), kínos üzenetet küldhet a nevünkben partnereinknek stb., egy szóval nagy kárt okozhat.

Egy ilyen kód igen sokféle módon kerülhet futtatásra gépeinken. Ma is előfordul a mobil adathordozóról (pl. USB pendrive-ról) telepített rosszindulatú kód, de tipikusabb támadási forma az, amikor távolról keresi a rosszindulatú kód újabb „áldozatát". Ez történhet a korábban megszerzett email címek[28] vagy más gépi kapcsolatok (hálózati szolgáltatások) adatai alapján, de akár úgy is, hogy izgalmasnak vagy hasznosnak ígérkező weboldalakra csalnak gyanútlan böngészőket. Persze a rosszindulatú kódot aktív felderítő munka is nyomra vezetheti (próbálkozás, címek szkennelése stb.). Aztán próba-szerencse alapon találhat a célgépen olyan informatikai sérülékenységet, amely engedélyezi a jogosulatlan kód adott gépen való lefuttatását. [29] (És ne dőljünk be annak, hogy vannak platformok, amelyeken „nincsenek vírusok"[30] – egyszerűen a különbség abból fakad, hogy a legtöbb rosszindulatú kódot meghatározott géptípusra kell írni, ezért kicsi a siker esélye, ha nem kifejezetten az adott géptípusra szabott kód.)

Számunkra a legfontosabb, hogy miként tudunk ellenük védekezni?

A legfontosabb, de önmagában nem elegendő eszköz a vírusirtónak vagy antimalware-nek nevezett program. Abban a kérdésben, hogy melyiket válasszuk a piacon elérhető alkalmazások közül, az áron kívül legalább azt vegyük figyelembe, hogy a jó nevűnek nevezhető, európai független tesztlaborok szerint milyen eredményeket ért el a rosszindulatú kód elleni védekezésben.

Három ilyen tesztlabor oldalt javasolunk, amely rendszeresen közzéteszi eredményeit, és érdemes ebből a szempontból figyelembe venni a javaslataikat – itt is igaz, hogy nem feltétlenül azt kell venni, amit a kiskereskedésekben a legegyszerűbb megvenni, vagy amit a legtöbbször láttunk reklámozni:

https://www.av-test.org/en/antivirus/

http://www.av-comparatives.org/dynamic-tests/

https://www.virusbtn.com/vb100/latest_comparative/index

Javasolom figyelembe venni, hogy egyes termékek forgalmazói a Magyar Ügyvédi Kamarával a tagok számára kedvezményt biztosító megállapodást kötöttek.

Ne feledjük, hogy vírusirtót nem csak számítógépre, hanem bármilyen táblagépre vagy okostelefonra is lehet érdemes is telepíteni, ha azon ügyfél adata vagy értékes ügyvédi információ található.[31]

---

[28] Ezt használják a csatolmányban küldött rosszindulatú kód esetén, vagy ha emailben egy „veszélyes" webes hivatkozást küldenek, amit megnyitva egy fut le a rosszindulatú kód.

[29] Az olyan szoftver sérülékenységet, amit jogosulatlan kód futtatására vagy jogosulatlan információhoz való hozzáférésre lehet használni, „exploit"-nak nevezik.

[30] Pl. az Apple esetén, lásd az erről szóló reklámot: https://youtu.be/sdF5IsyOxU4. Itt is fontos felhívni arra a figyelmet, hogy sokan a malware-vírus különbségtétel erőltetésével akarják ezt a félrevezető információt védeni, ami nem más, mint egy újabb félrevezetés. (Ilyen alapon azt is mondhatnánk, hogy ma már semmilyen új operációs rendszeren nem futnak vírusok.) Lásd még http://www.av-comparatives.org/wp-content/uploads/2015/05/avc_linux_2015_en.pdf.

[31] Lásd az Android eszközökkel kapcsolatos egyik jelentést: http://www.av-comparatives.org/wp-content/uploads/2015/09/avc_mob_2015_en.pdf

Fontos figyelembe venni, hogy a vírusirtó nem tudja kivédeni az összes rosszindulatú kód támadást. A fenti laborok szerinti 99% fölötti detektálási arányokat a jól ismert támadásokkal számolva érik el. Azonban a rosszindulatú kód megjelenése és a vírusirtók adatbázisába történő bekerülése között hosszabb idő is eltelhet. A célzott támadások (hekkelések) esetén az a szokásos taktika, hogy egy-egy olyan, szoftverrel kapcsolatos sérülékenységet használnak ki támadásra (hozzáférésre), ami még vagy nincsen nyilvánosságra hozva, vagy a sérülékenységet még az adott gépen nem javították.[32] A vírusirtók adatbázisába nem a sérülékenység kerül, hanem az azt kihasználó kód (vagy cím), aminek feltétele, hogy valaki a sérülékenység ilyen kihasználását megfelelően bejelentse. (Persze a vírusirtó programoknak az ilyen problémákat is próbálják kezelni, de ennek találati aránya már korántsem olyan megnyugtató.)

Ha mégis megtörtént a fertőzés, és azt a vírusirtó program megnyugtatóan nem tudta megszüntetni, akkor mindenképpen vegyük igénybe szakember segítségét, mielőtt a mentésekből helyreállítjuk a korábbi információkat. A 16.1.2. pontnak megfelelően követeljük meg a felhasználóktól, hogy a rosszindulatú kód futását vagy elhárítását a megfelelő személynek jelentsék.

Nem a rosszindulatú kódhoz tartozó kérdés, de itt érdemes kitérni arra, hogy a szoftver gyártók által támogatott szoftverekben feltárt, a fentiek szerint kihasználható sérülékenységek (exploitok) megszüntetésére a gyártók tipikusan frissítéseket, javításokat ad ki. Ha ezeket a javításokat telepítjük, jelentősen csökkentjük a kitettségünket nem csak a rosszindulatú kódok futtatásának, hanem a rosszindulatú emberek célzott informatikai támadásainak is. Azonban ne feledjük, hogy a frissítések telepítése óhatatlanul nem csak javíthat, hanem sajnos el is ronthat más működő szoftvereket, ezért a nagyobb szervezetek esetén, ahol erre megfelelő erőforrás áll rendelkezésre, mindig indokolt a frissítéseket előbb tesztkörnyezetben (azaz nem az ügyvéd által valódi ügyfelekkel való kapcsolattartásra használt gépen) lefuttatni (erről szól a 12.1.2. számú változtatáskezelés intézkedés is.)

12.3.1. – Információmentés

Mint már többször említettük, az ügyvédi iroda egyik legfontosabb, legkritikusabb „vagyontárgya” az információ. Ezt a szempontot is tükrözi, hogy az egyik legalapvetőbb biztonsági intézkedés az ügyfélre vonatkozó információk sűrű és megbízható mentése.

Ne elégedjünk meg azzal, hogy az információ el van mentve. Gondoskodjunk arról is, hogy le legyen írva a helyreállítás módja. A szoftvereket és beállításait is tartalmazó mentések esetén pedig feltétlenül próbáljuk ki, hogy abból a mentésből valóban egy futtatható rendszer fog helyreállni (ezt a fajta tesztelést indokolt nem csak először, de legalább évente, kétévente elvégezni).

Egy kissé más problémakör jellemzi a hosszú távú mentéseket (archiválásokat). Itt magának az információnak a megőrzésén túl annak olvashatóságának biztosításáról is gondoskodnunk kell (mind hardver, mind futtatási környezet vonatkozásában[33]). Ugyanígy követelmény a hosszú távú mentések

[32] Ún. zero day vulnerability.

[33] Pl. az adott állományt csak egy olyan régi program olvassa, aminek telepítéséhez egy régebbi operációs rendszerre is szükség lesz.

esetén az is, hogy elektronikusan aláírt információk esetén az érvényességi láncot alátámasztó információkat is megőrizzük, érvényesen.[34]

13.1.2. – Hálózati szolgáltatások biztonsága

A hálózati szolgáltatások biztonságának egyik vonatkozásáról a 6.2.1. számú (mobil eszköz szabályozása) intézkedésnél olvashatunk (lásd a vezeték nélküli hálózat kockázatait és a VPN kapcsolat előnyeit).

Itt a tűzfalak fontosságát szeretnénk megemlíteni. A tűzfal kifejezés nagyon sokfajta eszközt és szoftvert jelenthet. Bizonyos tűzfalakat közvetlenül a belső irodai hálózatunk internet csatlakozása elé telepítünk (kisvállalati környezetben gyakori az internet szétosztását biztosító útválasztó vagy más hozzáférési ponttal egybeépített tűzfal), bizonyos tűzfalat pedig közvetlenül a végfelhasználó gépére (ez utóbbi akár az operációs rendszer[35] vagy a vírusirtó szoftver egy mellékes képessége is lehet.)

A tűzfalak azért fontosak számunkra, mert mind a rosszindulatú kódok, mind a célzott támadások körében korlátozza azokat a hálózati kapcsolatok felépítésének, fenntartásának esélyeit, amelyek jogosulatlan kódfuttatást vagy információhoz való hozzáférést (módosítást) eredményeznek.[36]

8.3.2./10.7.2. – Adathordozók selejtezése

Mivel az ügyfél adata az egyik legfontosabb érték, nem szabad megfeledkezni arról, hogy az adatot akkor is védeni kell, ha már nem használjuk. Mind a mobil adathordozók (USB pendrive-ok, külső merevlemezek), mind a gépekbe beépített adathordozók tartalmaznak ilyen adatot, akkor is, ha csak szervizbe adjuk le, és akkor is, ha eladjuk. Ne feledjük, hogy a számítógépen, táblagépen és okostelefonon kívül a nagyobb kapacitású irodai másolók, szkennerek, faxgépek is tartalmaznak ilyen adatot.

Mindegyik adathordozóra igaz, hogy a fájl kitörlésével vagy akár leformázásával nem fogjuk a tárolt adatokat olyan módon törölni, hogy egy határozott szándékkal bíró átlagember ne tudja azt helyreállítani. Amit papír alapon sem tennénk a kukába, azt vagy ne adjuk ki többé a kezünkből, vagy csak gondos, a valódi törlést biztosító műszaki folyamat lefolytatása után (hasonlóan a vírusirtókhoz, itt is javasolom figyelembe venni, hogy egyes termékek forgalmazói a Magyar Ügyvédi Kamarával a tagok számára kedvezményt biztosító megállapodást kötöttek.)

9.2.1. – Használók regisztrálása és deregisztrálása (bejegyzés és bejegyzésmegszüntetés)

Mint fentebb írtuk, gondoskodjunk arról, hogy a felhasználók egyedileg azonosítottak legyenek, mind informatikai értelemben, mind jogilag. Mindenkivel szemben, aki hozzáfér a gépünkhöz, képesek legyünk szükség esetén akár polgári peres eljárást is indítani (természetesen szerződéses partnerek

---

[34] Erről a problémáról az e-cégeljárás kötelezővé válásakor már több írás született, lásd például https://e-szigno.hu/tudasbazis/elektronikus-archivalas.html, https://archivalas.netlock.hu/, http://www.netlock.hu/archer/ vagy http://regi.bpugyvedikamara.hu/elektronikus_archivalas_tajekoztato/.

[35] Lásd pl. a Windows XP és efölötti rendszereket. A beépített tűzfal és a „bővített funkcionalitású" vírusirtó szoftver közötti kölcsönhatásról, azok viszonyáról lásd az alábbi jelentés 16. oldalát http://www.av-comparatives.org/wp-content/uploads/2014/04/avc_fw_201403_en.pdf

[36] Bár vannak más hálózati biztonsági eszközök is (az ún. behatolás észlelő és megelőző rendszerek, angol rövidítéssel IDS és IPS eszközök), de ezek az ügyvédi irodai méretekben egyelőre nem reális megoldások.

munkavállalói esetén ez csak azt jelenti, hogy magával a szerződéses partnerrel szemben tudjunk peres eljárást kezdeményezni.)

Ha valaki többé nem dolgozik már az ügyvédi irodával, nyomban szüntessük meg minden hozzáférését (függetlenül attól, hogy a korábbi email címét megőrizzük, és átirányíthatjuk néhány gyűjtőfiókra).

A rendszergazdai (rendszeradminisztrátori) szintű hozzáféréseket csak a rendszergazdai szintű hozzáférést igénylő célokra engedjük használni, más munkákra véletlenül se. Célszerű lehet az alapértelmezett rendszergazdai felhasználónevet olyanra megváltoztatni, amiből nem nyilvánvaló egy kívülálló számára, hogy az rendszergazdai hozzáférést jelent.

Bár informatikailag egyszerűen végrehajtható probléma, az irodai ügyvitel szervezése szempontjából komplex kérdés, hogy miként tudjuk korlátozni, minden felhasználó csak a feltétlenül szükséges állományokhoz férhessen hozzá, és a legszükségesebb jogosultsággal (mihez ne férhessen hozzá, mihez csak olvasási joggal stb.). Erre általános receptet nem lehet adni, hiszen annyira eltérő, hogy kinél-milyen munkákat végeznek pl. az asszisztensek, titkárnők – de az ilyen kialakított hozzáférési jogokat felhasználói csoportokhoz és ne közvetlenül felhasználói fiókokhoz rendeljük.

9.2.3.. – A felhasználók titkos hitelesítési információinak kezelése (=jelszókezelés) és 9.3.1. – titkos hitelesítési információ használata

A jelszavak megfelelő használata a mai informatikai szokásaink Achilles-ínja. Mindenki tudja, hogy a fő probléma az, hogy nagyon sok felhasználónevünk és jelszavunk van. Nekem például most 115 felhasználónév-jelszó párosom van…

Ekkora darabszám esetén teljesen természetesnek tűnik, hogy mindenki elkezdi azokat több helyen is használni – sőt, az volna nagyon furcsa, ha lenne ember, aki képes lenne 115-fajta eltérő felhasználónevet és jelszót megjegyezni, és ebből mondjuk 5 esetén 60-90 naponként gondoskodni új és új jelszavakról.

Mi lehetünk akármilyen leleményesek a jelszó tartalmával, ha a másik oldalon lévő szolgáltató valami hibája miatt egy ilyen „osztott” jelszó-felhasználónév vagy csak felhasználónév bizalmassága sérül, már az összes „osztott” fiókunk is veszélybe kerül.[37]

Egyetlen megoldás erre jelenleg az ún. jelszókezelő programok és szolgáltatások,[38] vagy az, ha mindent papíron a kezünk közelében tárolunk.

A jelszókezelő programoknak és szolgáltatásoknak is megvan a kockázatuk, hiszen akár a gépünkön tároljuk ezt a „mesterlistát”, akár a felhőben, ezt is megszerezhetik illetéktelenek. Azért hozzá tesszük, hogy ha meg is szerzik ezt az adatot, az adatok tárolása már csak a szolgáltatás és program

---

[37] Mert vannak szolgáltatók, akik a jelszavainkat olvashatóan tárolják (pl. http://plaintextoffenders.com/, de vannak ilyen magyar szolgáltatók is). Ám még akkor is, ha nem olvasható a jelszó, a helyreállítás veszélye így is nagy. Például 2013-ban 38 millió aktív Adobe azonosítót (Adobe ID felhasználónév és jelszó párost) hoztak nyilvánosságára hackerek az interneten. Igaz, hogy a jelszavak hash függvényét tárolta csak az Adobe, de a jelszó emlékeztetőt tisztán olvashatóak voltak, és a jelszavak hosszát is ki lehetett találni mindenfajta próbálkozási kísérlet nélkül. http://xkcd.com/1286/

[38] Lásd https://en.wikipedia.org/wiki/Comparison_of_password_managers, bár nem a legfrissebb a lista.

kialakítása miatt is jóval biztonságosabb, mintha magunk tároltuk volna a jelszólistát egy Word dokumentumban – amit ugyanúgy megszerezhetnek, ahogy a papír alapú listát is elveszíthetjük.[39]

A más irodai felhasználó által használandó jelszavakról is ejtsünk néhány szót. Hasonlóan az internet használati szabályzathoz, a jelszavak esetén is biztosítsuk szabályzatban azt, hogy a jelszavakat titokban tartsák, és azt is, hogy a jelszó használati követelmények megsértése esetén megfelelő jogkövetkezményeket alkalmazhassunk.

Kényszerítsük ki a megfelelő informatikai beállításokkal, hogy a felhasználónak kiosztott jelszót köteles legyen első alkalommal megváltoztatni, és azt is, hogy a rendszergazdák ne ismerhessék meg a felhasználók jelszavait.[40]

13.1.1. – Hálózati intézkedések és 10.1.1. – A kriptográfiai intézkedés alkalmazásának szabályzata

Bár e két intézkedés nagyon széles témakört ölel fel, itt alapvetően csak a kommunikáció bizalmasságáról gondoskodó intézkedésekről szeretnék írni. A hálózati védelmi intézkedések egyéb vonatkozásairól a 6.2.1. és 6.2.2. számú intézkedések is kellő részletességgel szólnak.

Ma már az ügyfelünkkel sokféle módon kapcsolatot tarthatunk, emailben, különféle alkalmazásokkal, webes vagy internetes szolgáltatások biztosította funkciókkal, mint a fájlmegosztások, közösségi oldalak funkciói, azonnali üzenetküldés, vagy akár ügyfélkapus üzenetküldés stb.

Egyáltalán nem a terrorizmus vagy általánosságban bűnelkövetők érdekében, de tudatában kell lennünk annak, hogy előfordultak már (természetesen csak külföldön!) olyan jogszabályellenes titkos információgyűjtések, ahol az ügyvédet védői minőségében figyelték meg.[41] Külföldi kommunikáció esetén jogellenes megfigyelésre sor kerülhet a fogadó országban is, meg útközben is.

Hacsak nem a hivatalos szervek jogellenes hozzáférésétől tartunk, a hagyományos telefonos kommunikációs formák előnye, hogy nagy általánosságban a két kommunikáló felet nagyobb biztonsággal tudják védeni, mint a három-öt éve működő webes szolgáltatások működtetői, és annak is nagyobb az esélye, hogy az ügyvéd-ügyfél kommunikációt védő hagyományos garanciákat legalább e körben betartják.

A hivatalos szervek ugyanúgy hozzáférhetnek a legnépszerűbb új kommunikációs alkalmazásokhoz is – a gyakorlati kérdés inkább az, hogy a kommunikációs alkalmazást működtető szervezet mely országban honos, és ha az nem Magyarország, akkor milyen az ott honos szervek és a hazai szervek közötti együttműködés.

A hagyományos telefonálást tekintve ma a fő kockázati tényező az, hogy számítógépszerűbbé és sokoldalúbbá (bonyolultabbá) váltak a telefonjaink. Így egyre nagyobb a valószínűsége, hogy az ilyen sokoldalú végberendezéseken is vannak olyan sérülékenységek, amelyek eddig csak a számítógépeinket jellemezték (lásd a 12.2.1. számú intézkedést). Ezeket a sérülékenységeket kihasználhatják a rosszindulatú szoftverek és hackerek. Könnyen hozzáférhetnek hívásadatokhoz, sőt, kellő mobil internetes sávszélesség esetén a telefonhívás lehallgatása is reális veszély lehet.

---

[39] Lásd a LastPass esetén 2015-ben egy ilyen betörés, https://blog.lastpass.com/en/2015/06/lastpass-security-notice.html/, de olyan adatot nem szereztek meg, amely az „osztott fiókokhoz" hasonlóan hozzáférést engedhetne más jelszavakhoz.

[40] Ezeket a modern operációs rendszerek alapértelmezett beállításként biztosítják.

[41] Lásd az 5. lábjegyzetben említett ügyet.

Az ügyvédi titokra nézve a legnagyobb veszély ma is a titkosítás nélkül küldött email üzenet. Fejlődés, hogy a levelezőprogram és levelezőszerver közötti kapcsolat ma jóval nagyobb valószínűséggel titkosított, mint tíz éve. A saját, ügyvédi oldalunkat illetően mindenképpen gondoskodjunk arról, hogy a mi levelezőszerverünk és a levelező alkalmazások közötti kapcsolat ilyen, titkosított legyen. Éppen elég kockázat az, ha a levelezőszerverek közötti kapcsolat például nem titkosított, de erre úgysincs ráhatásunk.

Célszerű a levelezőprogramok által biztosított titkosítást használnunk. Minden hazai ügyvédnek, aki rendelkezik ügyvédi elektronikus aláírással, lehetősége van a titkosító tanúsítvány használatára is. Így ha egy kollégának van ilyen tanúsítványa, csak keressük ki az illető nyilvános titkosító kulcsát a megfelelő tanúsítványtárban,[42] töltsük le, és azt telepítve már küldhetjük is neki a titkosított emailt.[43] Remélhetőleg a jövőben lesz majd olyan nyilvános LDAP szolgáltatás, aminek segítségével az ügyvédek a szakmán belül (országokon átnyúlóan) is egyszerűbben tudnak titkosított emailt küldeni.[44]

Ha ez nem megy, mert pl. ügyfélnek kell emailt küldeni, érzékenyebb információk esetén még mindig jobb, ha magát a csatolmányt titkosítjuk, például a minden gépen elérhető tömörítőprogramok útján, az egyszeri jelszót pedig más csatornán (pl. SMS-ben vagy telefonon, azaz ne emailben) adjuk meg.

16.1.2./13.1.1 – Információbiztonsági események jelentése

Szükséges, hogy írott szabályozási eszközökkel is biztosítsuk, hogy a munkavállalók és irodai tagok is egyértelműen kötelesek legyenek bármilyen információbiztonsági eseményről (így rosszindulatú kód futásáról, vagy hálózati támadás észleléséről, adatvesztésről, eszköz kieséséről) a megfelelő személyt értesíteni.

---

[42] https://srv.e-szigno.hu/index.php?lap=tanusitvanytar#, https://www.netlock.hu/index.cgi?lang=HU&tem=ANONYMOUS/kereses/tanusitban.tem

[43] Ennek mikéntjéről Outlook esetén pl. itt olvashatunk: https://support.office.com/en-ca/article/Encrypt-email-messages-8d6bf544-ec91-41ea-9e65-2c362f6a3f7f

[44] Erre vonatkozóan a CCBE-ben bizonyos projekttervek már készültek, de még bizonytalan, hogy megvalósul-e, és ha igen, mikor.