ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG

- **A következő években az egészségügyi intézményeknek, a tőzsdéknek, a közlekedési vállalatoknak, az energetikai cégeknek, az internetszolgáltatóknak, valamint a közigazgatási szerveknek is komolyabb előírásoknak kell majd megfelelniük az információbiztonság vonatkozásában.**
- **A kiberbűnözés a legnagyobb gazdasági kárt okozó bűnözési forma, 2011-ben világszerte 400 milliárd dolláros veszteséget okozott.**
- **Egyes becslések szerint naponta mintegy 150 ezer számítógépes vírus kering a világhálón.**
- **Az Európai Unió egységes adatvédelmi szabályozást helyez kilátásba.**
- **A számítástechnikai felhő adat-hozzáférhetőséget biztosít a jogosultak számára a világ bármely pontján.**
- **A számítási felhőre vonatkozó európai szabályok kidolgozása előfeltétele annak az akadálymentes digitális térnek, amelyben valóra válhat az igazi egységes digitális piac.**

A Kormány 2013 márciusában nyújtotta be az Országgyűlésnek „Az állami és önkormányzati szervek elektronikus információbiztonságáról” szóló T/10327. számú törvényjavaslatot, melynek célja, hogy egységes biztonsági követelményeket szabjon az elektronikus információ védelmével kapcsolatban.

A KIBERBŰNÖZÉS

Az egyre inkább tudásalapúvá váló társadalomban és gazdaságban az információ a gazdálkodó szervezet számára érték, ezért annak védelme kiemelt fontosságú. A kiberbűnözés napjainkra a világ legnagyobb gazdasági kárt okozó bűnözési formájává növekedett. 2011-ben 400 milliárd dollárra becsülték az általa okozott kár mértékét, és ez az összeg a netfelhasználók számának folyamatos növekedésével tovább emelkedhet. Egy 2012 év végi adat szerint mintegy 2 milliárd internet-felhasználó van világszerte, s egy információ „ellopásával” átlagosan 130-150 dollár kárt okoznak a bűnelkövetők.

Egyes uniós becslések szerint naponta mintegy 150 ezer számítógépes vírus kering a világhálón, és körülbelül ugyanennyi számítógép meg is fertőződik. A legtöbb támadás az úgynevezett fejlett világ ellen olyan országok szolgáltatóin keresztül érkezik, amelyek nem működnek együtt az információmegosztásban, ezért az informatika fejlettsége miatt ma már “akár egy afrikai sátorból is” érkezhet komoly támadás a különböző védett rendszerek ellen.

Magyarországon is évről évre nő a kibertámadások száma, és már itthon is megjelentek nemzetközi kiberbűnözői csoportok.

SZERVEZETEK INFORMATIKAI- ÉS INFORMÁCIÓBIZTONSÁGA

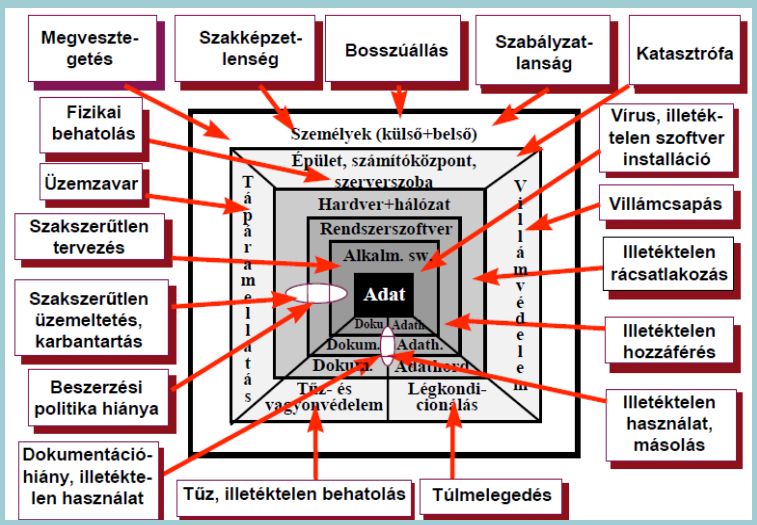
Az információ védelme az információ bizalmasságát, sértetlenségét és rendelkezésre állását jelenti. A védett információ csak az arra felhatalmazottak számára elérhető, teljessége és pontossága pedig garantált. Ez utóbbiakat elsősorban a belső munkatársak, illetve a vállalati adatbázisokhoz interneten, extraneten és elektronikus adatcsere révén hozzáférő stratégiai partnerek gondatlan, esetleg szándékos károkozása veszélyezteti.
Az információbiztonság további jellemzői a hitelesség, számon kérhetőség, letagadhatatlanság és megbízhatóság (ISO/IEC 27001). Az információ-vagyon védelme érdekében legáltalánosabban az információhordozókat és azok kezelését szükséges szabályozni, függetlenül az információ megjelenési formájától.

A védelem akkor működik helyesen, ha meghatározzuk a védendő információkat, a külső és belső fenyegetéseket és azok kockázatát valamint a védelemhez szükséges szabályozást és eszközrendszert (ISO/IEC 27002).

Az információ hatékony védelme az alábbi tevékenységeket foglalja magába:

- információtechnológiai infrastruktúra (hardver-, szoftver- és hálózat) védelme;
- információkezelés (adatfelvétel, -módosítás, -törlés, informálódás, ill. lekérdezés) védelme;
- ügyviteli folyamatok szabályozása;
- információbiztonsági stratégia, kockázatkezelés.

Informatikai rendszerek fenyegetettségei – Informatikai Tárcaközi Bizottság:



Szabványrendszerek

A ***Közös követelményrendszer az informatikai biztonság minősítéséhez*** (Common Criteria for Information Technology Security Evaluation: CC) az informatikai termékek és rendszerek biztonsági szintjének mérésére és értékelésére készült. Az Egyesült Államokból származik, de Kanada és az Európai Unió is elfogadta annak kritériumait. (www.commoncriteriaportal.org). 1999 óta európai, 2003-tól pedig magyar szabvány változata is elérhető (MSZ ISO/IEC 15408-1, -2, -3).

Az ISO/IEC 2700x egy brit eredetű ***információbiztonsági irányítási rendszer*** (www.iso27001security.com).

Az MSZ ISO/IEC 20000-1, -2 szabvány az ***információs rendszerek üzemeltetési kérdéseivel*** foglalkozik, s szintén brit eredetű (Information Technology Infrastructure Library: ITIL) (www.itsmfi.org).

Informatikai szabályzatok vizsgálata Magyarországon

2011-ben az ***Állami Számvevőszék*** ellenőrizte a központi költségvetési intézmények informatikai szabályzatait, melynek során a belső kontrollrendszer, és annak részeként a belső ellenőrzés értékelését 28 költségvetési szervre, továbbá 11 fejezet esetében a fejezeti kezelésű előirányzatokra vonatkozóan végezte el.

Az ÁSZ ellenőrzés során az ***informatikai szabályzatok*** 46,4%-a (13 intézmény) „megfelelő”, 39,3%-a (11 intézmény) „részben megfelelő”, 14,3%-a pedig „nem megfelelő” minősítést kapott. A fejezeti kezelésű előirányzatokat érintő kérdések vonatkozásában az azokat kezelő intézmények több mint fele (6 intézmény) rendelkezett „megfelelő” informatikai biztonsági szabályzattal.

Az informatikai biztonsági szabályzatok jellemző hiányosságai, hogy azokat nem aktualizálták, a működésfolytonossági tervek nem tartalmaznak egyértelmű és részletes forgatókönyveket a kritikus fontosságú folyamatok és informatikai rendszerelemek visszaállítására vonatkozóan, illetve a számítógépes rendszer mentési eljárásai nem voltak szabályozottak.

AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI STRATÉGIÁJA

A "Nyílt, biztonságos és megbízható kibertér" című uniós stratégia, melyet 2013. február elején ismertettek, az alábbi öt prioritást kiemelve ismerteti a kiberbiztonsággal kapcsolatos jövőképet:

- a kibertámadásokkal szembeni ellenálló képesség megteremtése;
- a számítástechnikai bűnözés drasztikus visszaszorítása;
- a kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát (KBVP) érintő képességek fejlesztése;
- a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
- az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése.

Körvonalazódó irányelvek

Napjainkban elsősorban a banki és a telekommunikációs szektor áll a figyelem középpontjában, a következő években pedig már az egészségügyi szervezeteknek, a tőzsdéknek, a közlekedési vállalatoknak, az energetikai cégeknek, az internetszolgáltatóknak, a közigazgatási szerveknek is komolyabb előírásoknak kell majd megfelelniük az információbiztonság vonatkozásában.

Az Unió hálózati és információbiztonságáról szóló tervezett direktíva célja, hogy az EU tagállamok egységesen kezeljék a kérdést. A tagállamok két legfontosabb feladata:

- hálózat- és információbiztonsági stratégia elfogadása; továbbá
- egy illetékes nemzeti hatóság kijelölése, biztosítva a hálózat- és információbiztonságot érintő kockázatok és események megelőzéséhez, kezeléséhez és elhárításához szükséges pénzügyi és humán erőforrásokat.

A Bizottság és a tagállamok között ki kell dolgozni egy együttműködési mechanizmust, amely – rendszeres szakértői vizsgálatok útján – lehetőséget biztosít a kiberbiztonsági kockázatok és események korai előrejelzéseinek megosztására.

EGYSÉGES ADATVÉDELEM AZ EURÓPAI UNIÓBAN

Az Európai Unió 2012 januárjában tette közzé azt a rendelettervezetet, amely egységes, a tagállamokban közvetlenül alkalmazandó adatvédelmi szabályozást helyez kilátásba. A Bizottság az uniós adatvédelmi szabályozás korszerűsítését szorgalmazza, ezért az a változtatások célja, hogy az adatvédelemre Unió-szerte egységes szabályok vonatkozzanak. Ez a rendelettervezetet belátható időn belül a 95/46/EK irányelv helyébe is lépne.

A SZÁMÍTÁSI FELHŐ

A ***számítástechnikai felhő*** (cloud computing). egy internet alapú komplex adattovábbítási-adatszolgáltatási megoldás, amely azonnali adat-hozzáférhetőséget biztosít a jogosultak számára a világ bármely pontján.

Az Európai Bizottságnak az *„Új stratégia az európai vállalkozások termelékenységének és a központi kormányzatok hatékonyságának a számítási felhő révén történő serkentésére”* elnevezésű terve olyan intézkedéseket vázol fel, amelyek 2020-ig 2,5 millió új európai munkahelyet eredményezhetnek és az uniós GDP-t éves szinten nettó 160 milliárd euróval (körülbelül 1%-kal) bővíthetik. A stratégia kapcsolódik az adatvédelmi szabályok naprakésszé tételére vonatkozó 2012-es bizottsági javaslathoz, illetve a kiberbiztonság európai stratégiájához. A számítási felhőre vonatkozó európai szabályok kidolgozása előfeltétele annak az akadálymentes digitális térnek, amelyben valóra válhat az igazi egységes digitális piac.

Források:

- Az EU a magánélet védelméért – Európai Bizottság
- Csak idő kérdése az EU egységes adatvédelmi szabályozása – Origo, 2012. június 16.
- Digitális menetrend: Új stratégia az európai vállalkozások termelékenységének és a központi kormányzatok hatékonyságának a számítási felhő révén történő serkentésére (Brüsszel, 2012. 09.27.)
- Dr. Michelberger Pál - Lábodi Csaba: Vállalati információbiztonság szervezése (In: Vállalkozásfejlesztés a XXI. században, Budapest, 2012.)
- Évről évre nő a számítógépes támadások száma – kormany.hu, 2012. szeptember 17.
- ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management
- Így gondolkodik az EU a kiberbiztonságról – muszakiforum.hu 2013. február 11.
- Jelentés a belső kontrollrendszer és a belső ellenőrzés szabályszerűségének a zárszámadási ellenőrzésbe bevont központi költségvetési intézményeknél lefolytatott ellenőrzéséről ÁSZ jelentés - 2012.09.14.
- Magyarország versenyképes az információbiztonság terén – biztonsagpiac.hu, 2012. november 4.
- Védené az EU a kulcshálózatokat – BruxInfo, 2013. február 7.

Legfontosabb jogszabályok:

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről

2009. évi CLV. törvény a minősített adat védelméről

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

309/2011. (XII. 23.) Kormányrendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokról

5/2011. (II. 3.) Kormányrendelet a Nemzeti Információs Infrastruktúra Fejlesztési Programról

268/2010. (XII. 3.) Kormányrendelet a Kormányzati Informatikai Fejlesztési Ügynökségről

161/2010. (V. 6.) Kormányrendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

242/2007. (IX. 21.) Kormányrendelet az N.SIS informatikai központ feladatait ellátó szerv kijelöléséről, a SIS-be történő adatbevitel elrendelésének és végrehajtásának, valamint az N.SIS Hivatal és a SIRENE Iroda technikai és adminisztratív feladatai ellátásának részletes szabályairól

1035/2012. (II. 21.) Kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról

Készítette: Békési Attila
Képviselői Információs Szolgálat

Országgyűlési Könyvtár

E-mail: infoszolg@parlament.hu
Intranet:http://infoszolg.ogyk.hu
Tel.: (1) 441-4529; (1) 441-6486

Az információs jegyzet belső felhasználásra, az országgyűlési képviselők tájékoztatása céljából készült.
A dokumentum az összeállítás elkészültének időpontjában fennálló aktuális helyzetet mutatja be.
Az információs jegyzet szerzői jogvédelem alatt áll.