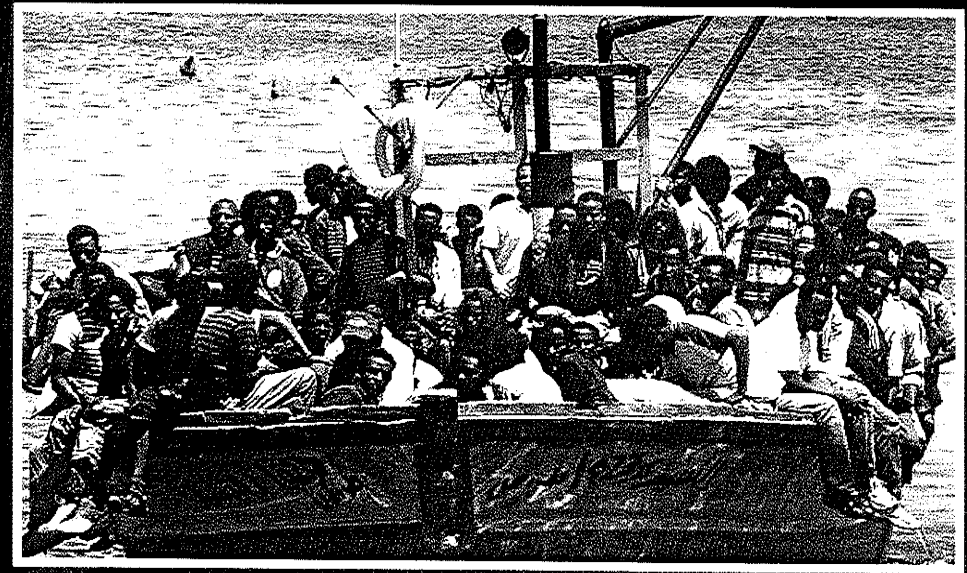
2014
9.

BELÜGYI SZEMLE

A BELÜGYMINISZTÉRIUM SZAKMAI, TUDOMÁNYOS FOLYÓIR



BELÜGYI SZEMLE ■ 2014/9.

SZERKESZTŐSÉG 1051 Budapest, Nádor utca 4.,
levélcím: 1903 Budapest, Postafiók 314,
e-mail: bszemle@bm.gov.hu, telefon: 441-1935

BORÍTÓTERV ÉS NYOMTATÁS
Adyv Grafika Kft.
FELELŐS VEZETŐ Tóth Katalin nyomdavezető

FELELŐS KIADÓ Belügyminisztérium

ISSN 1789–4689

KÖZLÉSI FELTÉTELEK

A szerkesztőség olyan kéziratokat vár közlésre, amelyek a társadalmi devianciák, valamint a közbiztonság és a rendészet kérdéseit kriminológiai, kriminálszociológiai, büntetőjogi, rendészeti szempontból elemzik, értékelik.

A kéziratokon kérjük feltüntetni a szerző nevét, beosztását, telefonszámát, lakcímét.

Kérjük, hogy a cikkek szövegét e-mailben vagy CD-n is küldjék meg.

Felhívjuk tisztelt szerzőink figyelmét, hogy lapunkban nyomdatechnikai okok miatt színes fényképeket és ábrákat nem tudunk megjelentetni, ezért kérjük, hogy azokat fekete-fehérben mellékeljék a cikkhez.

A szerkesztőség a beérkezett kéziratot szakmai szempontból lektoráltatja, és fenntartja a jogot a kéziratok stilizálására, korrigálására, tipografizálására.

El nem fogadott kéziratokat nem áll módunkban visszaküldeni.

A szerkesztőség másodközlést nem vállal.

TARTALOM 2014/9.

KURIS ZOLTÁN

Kommunikációs és információs rendszerek szoftverbiztonságának korszerű megvalósítási eszközei

Korunkat információs társadalomként szokás jellemezni. A társadalom gazdasági, politikai és kulturális működésében meghatározó szerepük van a kommunikációs és információs rendszereknek.

A társadalom működésének szempontjából kiemelt fontosságúak a kritikus infrastruktúrákat működtető kommunikációs és információs rendszerek, feltétlenül szükséges ezek komplex és integrált védelmének megoldása, mivel rendeltetésszerű működésük, a bennük kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának sérülése súlyos biztonsági, politikai, gazdasági károkat, ipari katasztrófákat is előidézhet. A napjainkban kialakítandó elektronikus kommunikációs és információs rendszerek már döntően kereskedelmi forgalomban kapható, így széles körben elterjedt hardvereket és szoftvereket alkalmaznak.

Mértékadó szakemberek szerint a kinetikus energián alapuló hadviselés mellett megjelent a kiberhadviselés, annak elmélete és gyakorlata folyamatosan fejlődik, ez a kritikus infrastruktúrák elleni információs dimenzióban testet öltő hálózati hadviselés informatikai, fizikai és emberi eszközökkel és azok dimenzióiban valósul meg[1]. Az utóbbi időben mind többet lehet hallani – az egyre inkább álcázott és szofisztikáltabb kivitelezésű – kiberbűnözésről, nagyvállalatok és kormányzati szervek elleni online támadásokról, vagy kémkedésről és az ebből eredő károkról.

A kommunikációs és információs rendszerek elleni kibertámadások legnagyobb mértékben a rendszerben alkalmazott szoftverkörnyezet sebezhetőségét próbálják kihasználni. Az információs rendszerek meghibásodásai is legtöbbször szoftverhibákra vezethetők vissza, az incidensek többségének hátterében azonban emberi mulasztás áll. A személyi biztonsági hiányosságokból eredő (a fenyegetések komplexitását is jól szemléltető), az elektronikus rendszerek sebezhetőségét is kihasználó incidenseket jól példázza *Edward Snowden*[2] és *Bradley Manning*[3] nagy nyilvánosság előtt is jól ismert esete. Az úgynevezett „kiberhadviselés" tendenciáit nyomon követhetjük, ha megvizsgáljuk a 2007. április 26–28. között lezajlott észtországi[4] és a grúz eseményeket[5]. Figyelemre méltó, hogy a 2007 tavaszán bekövetkezett észtországi események bírták rá a szövetséget arra, hogy gyökeresen átgondolja a kibervédelmi politika szükségességét, valamint hogy az ellenintézkedéseit új szintre emelje. Ezért aztán a szövetség a fennállása óta először létrehozott és 2008 januárjában bevezetett egy formális kibervédelmi NATO-politikát, amely felállította a szövetség kibertér-politikájának három alappillérét. A fenyegetések területén a tendencia folytatódott, ugyanis 2010 júniusában nyilvánosságra került a *Stuxnet* elnevezésű káros program, amely valami olyasmi, mint egy „digitális bunkerromboló", amely megtámadta az iráni nukleáris programot. Ezzel a szakértők által 2001 óta megfogalmazott figyelmeztetések valósággá váltak, és azt sugallják, hogy a kiberteret előbb vagy utóbb olyan súlyos támadásokra használhatják, amely a fizikai világban halálos következményekhez fog vezetni[6]. Fontos szempont tehát (a személyi és a fizikai biztonsági kockázatokra is figyelemmel) a szoftveres sebezhetőségből eredő biztonsági kockázatokat súlyuknak megfelelően kezelni, és számolni azzal, hogy elektronikus rendszerekben a szoftverbiztonság akkor tekinthető megvalósultnak, ha az abban alkalmazott szoftverekből eredő biztonsági kockázatok technikai megoldásokkal, bevezetett rendszabályokkal annak kritikusságával arányosan kezeltek a rendszer teljes életciklusában (a tervezésétől a rendszerből történő kivonásáig), ez az eljárás a szoftverbiztonság szavatolása. Tekintettel arra, hogy az informatikai rendszerek kutatás-fejlesztése, az úgynevezett „high-tech" gyártás a világban erősen koncentrált, érdekeltségében és szereplőiben szűkülő piac, így eleve biztonsági probléma az alkalmazott megoldások szavatolása, amely során a kizárólagos biztonság nagy valószínűséggel elérhető, de teljes körűen meg nem valósítható.

1 Haig Zsolt – Várhegyi István: A cybertér és a cyberhadviselés értelmezése. http://www.zmne.hu/kulso/mhtt/hadtudomany/2008_e_2.pdf

2 http://www.bbc.com/news/world-us-canada-22837100

3 http://hvg.hu/vilag/20130731_154_ev_az_Wikileakskiszivarogtatonak__i

4 file:///C:/Users/kuriszoltan/Downloads/Hacktivity_Muha_Lajos_2007.pdf

5 Vámosi Gergő – Szedlák Ádám: Az interneten is zajlik az orosz–grúz összecsapás. [origo].hu, 2008. augusztus 11. http://www.origo.hu/techbazis/internet/20080811-az-interneten-is-zajlik-az-oroszgruz-osszecsapas.html

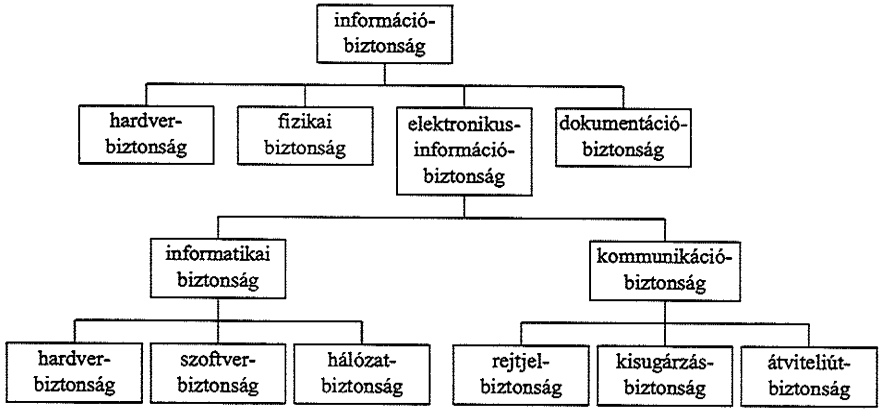
6 http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/HU/index.htm

A szoftverbiztonság szerepe a komplex és integrált védelemben

A kommunikációs és információs rendszerek működésfolytonossága, a bennük kezelt információk bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése komplex és integrált védelem kialakításával valósítható meg. Ennek érdekében összehangolt információbiztonsági rendszabályok megalkotása és bevezetése szükséges a rendszer teljes életciklusára kiterjedően személyi biztonsági, fizikai biztonsági, dokumentumbiztonsági, elhárítási és elektronikus információbiztonsági védelmi intézkedések alkalmazásával. Az *1. számú ábra* mutatja a komplex és integrált védelem fő területeit, azon belül is részletezve az elektronikus információbiztonság területeit, valamint a szoftverbiztonság helyét a komplex információbiztonsági rendszerben.

1. számú ábra

A komplex információbiztonság rendszere[7]



A kiemelt, kritikus fontosságú kommunikációs és információs rendszerek szolgáltatásainak futtatását, abban adatok kezelését a kor követelményeinek megfelelő szervertermekben üzemelő korszerű hardvert és szoftvert alkalmazó szerverszámítógépekkel lehet leghatékonyabban megoldani, szoftverek tekintetében körültekintően kialakított szoftverbiztonság-szavatolási eljárás alkalmazásával.

7 Kuris Zoltán: A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben. Hadmérnök, 2010/4. http://hadmernok.hu/2010_4_kuris.pdf

A szoftverbiztonság megvalósításához a rendszer szoftverkörnyezetének és az abban alkalmazott szoftvereknek a következő követelményeknek kell megfelelniük[8]:

1. *Megbízható működés:* a szoftver minden körülmények közt végrehajtja feladatát és kiszámíthatóan működik, beleértve az ellenséges körülményeket is, amikor támadás alatt áll.
2. *Megbízhatóan tervezett:* a megbízható szoftver kevés olyan sebezhetőséget, biztonsági rést és gyengeséget tartalmaz, amelyet kihasználva manipulálni vagy szabotálni lehet a szoftver megbízható működését. Akkor megbízhatóan tervezett egy szoftver, ha nem tartalmaz olyan tervezési hiányosságot, amely rosszindulatú módon kihasználható lehet.
3. *Fennmaradóképes (rugalmas):* a szoftver a legtöbb ismert támadásnak ellenáll (védekezik) vagy elviseli őket (továbbra is megbízhatóan működik), amennyire lehetséges, számol a további esetleges támadási formákkal is. Működése a lehető leggyorsabban helyreállítható, alacsony károkkal akkor is, ha a támadást nem tudta elhárítani vagy elviselni.

Az előbbiek megvalósításához fontos, hogy a szoftverkörnyezetben alkalmazott szoftverek közül a kereskedelmi forgalomban kaphatóknak megfelelő működésbiztonsági tanúsítványuk legyen. Ha egyedi fejlesztésű szoftver alkalmazására kerül sor, akkor azt az előbbi elvek szerint tervezzék, működésbiztonságát tanúsító cég vizsgálja. A működésbiztonsági tanúsítványon a szoftverek megbízhatóságát a Common Criteria nemzetközi információbiztonsági szabvány (ISO/IEC-15408) szerinti *Evaluation Assurance Level* megfelelési szint jellemzi. A hétfokozatú skálája az EAL1-től (funkcionálisan tesztelt) a legszigorúbb EAL7-ig (formálisan igazolt módon tervezve és tesztelve) terjed.

Jellemző, hogy gyakorlatilag alig néhány EAL4(+) (tervszerűen tervezett, tesztelt és átnézett) szintűnél magasabb termék létezik a piacon, a szoftvergyártó világcégek szerverre szánt operációs rendszerei (AIX, HP-UX, Solaris, Windows Server 2008 R2, SUSE és Red Hat vállalatoknak szánt Linux disztribúciója) is csak EAL4(+) besorolásúak. Mértékadó szakértői vélemények szerint az EAL4 szint igazából nem túl sok mindent garantál. Az előbbieken túl külön érdemes vizsgálni a szoftverkörnyezet kompatibilitási és interoperabilitási képességét, azaz más-más gyártók termékeinek együtt-

8 https://buildsecurityin.us-cert.gov/introduction-software-security

hatását a kialakított szoftverkörnyezetben (operációs rendszer, adatbázis-kezelő, rendszerközeli alkalmazások, *utilityk*, *toolsok* és a célalkalmazás).

Természetesen önmagában az, hogy biztonságos szoftverek alkalmazására kerül sor, nem garantálja azt, hogy az ezekből felépített szoftverkörnyezet – ami adott esetben fizikailag egymástól több ezer kilométerre lévő szerverparkokban lévő szerverekből kialakított fürtre vagy számítástechnikai felhőre *(cloud computing)* van telepítve – biztonságos legyen. Mindazonáltal a rendszer jelentőségével arányosan megkövetelendő, hogy a szoftverek biztonsági beállításai, interaktivitásuk körültekintően konfigurált legyen, a szoftverkörnyezetben működjön rosszindulatú szoftverek ellen védelmet nyújtó biztonsági szoftver, követelmények szerint naplózás és auditálás, üzemezett mentés és automatizált helyreállítási eljárás.

Kiemelten fontos, hogy kockázatértékelési eljárásban meghatározott időszakonként a rendszer biztonsága felülvizsgálatának részeként kellő hangsúlyt fordítsanak a szoftverbiztonság felülvizsgálatára, mert világszerte a szoftverbiztonsági kockázatok növekedése veszélyezteti legnagyobb mértékben a kommunikációs és információs rendszereket. Azt, hogy a szoftverbiztonsági kockázatok miként növekednek, a következő gondolatokkal lehet szemléltetni.

A szoftverbiztonság növekvő jelentősége

Napjaink trendje, hogy a köz- és a magánszféra nagyobb (domináns) szereplői is egyre nagyobb mértékben veszik igénybe külső szolgáltatók informatikai szolgáltatásait. Pár évvel ezelőtt ennek jellemző formája még az outsourcing volt, a szervezetek internettől szeparált belső hálózatán, telephelyein üzemelő informatikai eszközöket egy külső cég üzemeltette, a szervezeteknek csupán saját bérelt vonalaik voltak. Megállíthatatlanul terjed a *cloud computing,* amelynek lényege, hogy külső szolgáltató a telephelyein működtetett hardverinfrastruktúrán virtualizációs technológiák korszerű alkalmazásával kínál a vevő igényeihez igazodó szolgáltatásokat, akár virtualizált szervert is. A virtualizált szolgáltatások, szerverek nagy előnye, hogy az erőforrásai dinamikusan skálázhatók, így például megvalósítható az, hogy egy virtualizált szerveren futó számlázórendszer a havi egyszeri számla-feldolgozási időszakban például tízszer több processzorteljesítményt és memóriát alkalmazzon. A távoli telephelyen futó szerver és a felhasználó által működtetett végponti eszköz (például asztali vagy notebook számítógép, táblagép, okostelefon) közötti adatkommunikációs csatorna a védett kommunikáció érdekében jellemzően az internet biztonságos hálózati protokollja (például https), vagy virtuális magánhálózat (VPN). A saját szerverparkot üzemeltető szervezetek is gyakran lehetővé teszik egyes dolgozóiknak zárt hálózataik távoli elérését VPN-en keresztül.

Mindazonáltal bebizonyosodott, hogy még a legbiztonságosabbnak tartott VPN megoldások is támadhatók. Ezt példázza az is, hogy 2011. május 21-én kanadai hadititkok megszerzése céljából megkísérelték feltörni egy amerikai hadiipari nagyvállalat, a Lockhead Martin informatikai rendszerét, a cég állítása szerint a támadás sikertelen volt ugyan, de erre reagálva azonnal leállították a VPN-es távoli elérést, amelyhez az RSA SecurID hardverkulcson alapuló megoldást alkalmazták[9]. Az eset kapcsán informatikai szakértők azon véleményüknek adtak hangot, hogy a területen piacvezető RSA megoldását többé nem lehet biztonságosnak tartani. Válaszul az RSA felajánlotta ügyfeleinek a hardverkulcsok cseréjét (negyvenmilliót alkalmaznak világszerte), ami részben beismerésnek is tekinthető. De a tendencia sajnálatos módon nyomon követhető napjainkban is, sőt egyre szofisztikáltabbak a támadások. Friss hírek szerint 1,2 milliárd jelszó, és a hozzájuk tartozó felhasználói név került orosz hackerek kezébe.[10]

A Gartner piackutató egyik sajtóközleménye[11] szerint a mobil-előfizetések száma 2011-ben elérte az 5,6 milliárdot, 2015-re 7,4 milliárd mobil-előfizetést prognosztizálnak. A Nemzetközi Távközlési Egyesület adatai szerint[12] a világ lakosságának harmincöt százaléka használ internetet, míg a fejlett országokban a lakosság hetvennégy százaléka. A világ pénzforgalma (amely nagyjából százszorosa a tényleges áruforgalomnak) döntően elektronikus tranzakciók keretében zajlik, 2010-ben az Egyesült Államokban a papíralapú pénz már csak mindössze tíz százaléka volt az összes forgalomban lévő pénznek[13].

Az infokommunikációs technológiák fejlődésével és elterjedésével együtt mind több eszköz és szolgáltatás lesz online elérhető, ezzel egyidejűleg dinamikus nő a kibertámadások száma. A Symantec biztonsági cég 2011. évi internetes biztonsági fenyegetettségekről készített beszámolójában[14] kiemelt következő néhány adat jól szemlélteti a fenyegetések dinamikus növekedését:

a) nyolcvan százalékkal több támadást detektáltak, mint az előző évben (5,5 milliárd támadás);

9 Bodnár Ádám: Az RSA kicseréli az összes SecuriD tokent. HWSW.hu, 2011. június 7. http://www.hwsw.hu/hirek/46832/rsa-securid-token-lockheed-martin-biztonsag.html
10 http://www.holdsecurity.com/news/cybervor-breach/
11 http://www.gartner.com/it/page.jsp?id=1759714
12 http://en.wikipedia.org/wiki/Global_Internet_usage
13 http://www.federalreserve.gov/releases/h6/20110127/
14 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

b) a spamek száma az előző évhez képest ötven százalékkal emelkedett (napi 62 milliárdra becsülik), ez a teljes e-mail forgalom hetvenöt százaléka;
c) minden kétszázkilencvenkilencedik e-mail adathalász, minden kétszázharminckilencedik vírusos;
d) a kétezer-ötszáz fő feletti vállalatok ötven százaléka volt célpontja célzott támadásnak;
e) a vállalati vezetők, középvezetők és kutatás-fejlesztési területen dolgozók 42 százalékának támadták az elektronikus postafiókját;
f) száznyolcvanhétmillió embernek lopták el személyes adatát;
g) az előző évhez képest negyven százalékkal, 403 millióra emelkedett a különböző rosszindulatúszoftver- *(malware)* variánsok száma;
h) az év folyamán 4989 új szoftversebezhetőséget derítettek fel, átlagosan napi nyolc sebezhetőség felfedésére kerül sor, ezek különösen veszélyesek (javítócsomagok hiányában nehéz ellenük védekezni, mindazonáltal a sebezhetőség ténye széles körben gyorsan ismertté válik).

Egyre inkább számolni kell azzal is, hogy a rendszerben használt szoftverek fejlesztésének, működtetésének, jogosult alkalmazásának rendszerében rosszindulatú személy is pozícióba kerülhet, a szoftverbiztonsági rendszert tehát úgy kell kialakítani, hogy ezek a fenyegetések is a lehető legalacsonyabb kockázattal járjanak.

A 2011. novemberi londoni kibertér-konferencián mondott beszédében *David Cameron* brit miniszterelnök évi ezermilliárd dollárra becsülte a kiberbűnözésből eredő globális károkat[15]. Ugyanekkora károkat becsült *Jamie Shea,* a NATO felmerülő biztonsági nehézségekért felelős helyettes főtitkára is. 2011. december 7-én egy romániai tárgyalás utáni sajtótájékoztatón a következőket mondta: *„Szinte minden héten van olyan incidens, amely arra emlékeztet bennünket, hogy a kiberbiztonság kapcsolódik életünk szinte valamennyi aspektusához. Ezermilliárd dollár tűnik el évente a globális gazdaságból a kiberbűnözés miatt. Az ipari titkokat, szerzői jogokat, szellemi tulajdont, államtitkot egyre nehezebb megvédeni. A gazdaságok e komplex rendszereken működnek, amelyek könnyen megsemmisíthetők."*[16] A kormányzatok egyre súlyosabb fenyegetésként tekintenek a kiberterrorizmusra.

15 http://webarchive.nationalarchives.gov.uk/20130217073211/http://ukinmontserrat.fco.gov.uk/en/news/?view=Speech&id=685398482

16 http://www.infosecisland.com/blogview/18577-NATO-Cybercrime-Drains-One-Trillion-Dollars-from-Economy-Yearly.html

Sokszor még a legkorszerűbb adatközpontok működését is megbénítja szoftverhiba. Ezek közül 2012-ben az egyik legnagyobb nyilvánosságot kapó eset volt, amikor a szökőévkezelés szoftverhibája miatt 2012. február 29-én egy teljes napra leállt a világon a Microsoft Azure számítástechnikai felhőszolgáltatás, amelyet a világ számos nagyvállalata alkalmaz üzletileg kritikus rendszereihez.

Megalapozott az a megállapítás, hogy a kibertér biztonságának fontosságát ma már az államok vezetése is súlyának megfelelően kezeli. *Obama* amerikai elnök szavai szerint *„a kiberfenyegetettség az egyik legsúlyosabb gazdasági és nemzetbiztonsági kihívás nemzetünk számára",* a 2011. évi londoni kibertér-konferencián a brit miniszterelnök, az amerikai alelnök, számos miniszter, nagyvállalat és nemzetközi szervezet vezetője képviseltette magát. E konferenciasorozat 2012. évi rendezvénye Budapesten volt. Hazánk először 2011-ben vett részt a NATO kibervédelmi gyakorlatán. A 2012-ben hazánkban megrendezett gyakorlaton a Nemzeti Biztonsági Felügyelet szervezetében létrehozott kibervédelmi központ eredményesen koordinálta a feladatokat.[17]

A szoftverbiztonság szabályozottsága, támogató dokumentumai

A hazai jogszabályi környezetben a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) kormányrendelet meghatározza a szoftverbiztonság követelményeit a minősített adatok elektronikus kezelésének szempontjából. Megállapítható azonban, hogy csak a legfőbb követelményeket határozza meg, végrehajtásának módját nemzeti minősített adatok vonatkozásában további normatívák nem szabályozzák.

A közelmúltban fontos mérföldkő volt az állami és önkormányzati szervek elektronikus információbiztonságáról szóló, 2013. július 1-jén hatályba lépő 2013. évi L. törvény (a továbbiakban: információbiztonsági törvény) megalkotása, amely a szoftverbiztonságot kiemelt hangsúllyal kezeli. Megalkotása azért is volt mielőbb szükséges, mert az elektronikus közszolgáltatást nyújtó rendszerekre vonatkozó szoftverbiztonsági követelményeket részletesen szabályozó korábbi, az elektronikus közszolgáltatás biztonságáról szóló

17 Szűcs László: Sikeres volt a kibervédelmi gyakorlat. Honvedelem.hu, 2011. december 16. http://www.honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat

223/2009. (X. 14.) kormányrendeletet 2012. április 22-vel hatályon kívül helyezték. Ennek következtében a létesülő rendszerek szoftverbiztonsági követelményeinek érvényesítésére (a használatbavételi eljárások során) nem adtak megfelelő normatív támogatást.

A hazai normatív szabályozás folyamatban van, amely a szabványok és ajánlások közül kiemelten az információbiztonsági irányítási rendszerekkel kapcsolatos ISO/IEC 27000-es szabványcsoporton, az ISO/IEC 15408 Common Criteria és az irányadó NATO- és EU-szabályozásokon alapul. A KIB 25. számú ajánlásaként kiadott magyar informatikai biztonsági ajánlás, amely az informatikai biztonság irányítás és értékelés teljes folyamatát lefedi, köztük a szoftverbiztonságot is kiemelten kezeli.

A NATO-rendszerek esetén a szoftverbiztonsági követelmények (elvek, módszerek, eszközök) a rendszer teljes életciklusára vonatkozóan a NATO biztonságpolitikájának támogató direktíváiban pontosan meghatározottak. Ezek közül a szoftverbiztonságot részletesebben szabályzók minősítettek, illetve nem nyilvánosak, ezért nyílt publikációban nem elemezhetők. Viszont „kiemelten figyelemre méltó", hogy mindenki számára elérhető a NATO információbiztonsági weblapja (http://www.infosec.nato.int/). A weblap egyik leghasznosabb szolgáltatása a NATO minősített adatok kezelésére tanúsított hardverek és szoftverek katalógusa, amelyek többsége normál kereskedelmi forgalomban kapható. Tekintettel arra, hogy az itt szereplő termékeket alapos bevizsgálás után engedélyezték NATO minősített adatokat kezelő rendszerekben történő alkalmazásra, más termékhez képest kisebb kockázatúak, tehát ismeretük mindenképpen ajánlott a hazai információbiztonsági szakemberek számára. A termékekhez, köztük szoftverekhez biztonságos műszaki kivitelezési útmutatók tölthetők le (STIG).

Az amerikai Nemzetbiztonsági Hivatal és az amerikai Nemzeti Szabványügyi és Tecnhológiai Intézet információbiztonsággal foglalkozó weblapjain (http://www.nsa.gov/ia/ia_at_nsa/ ; http://csrc.nist.gov/) is mindenki által elérhetően részletes biztonságos konfigurálási útmutatók vannak az elterjedtebb szervereken és végpontokon alkalmazott szoftverekre vonatkozóan. Egy-egy ilyen útmutató, például egy szerver operációs rendszer vagy adatbázis-kezelő szoftver esetén jellemzően több száz oldalas, és a szoftverbiztonság összes aspektusára kiterjed.

Az útmutatók első fejezete általánosan meghatározza, hogy az abban leírt eljárások közül melyek mikor követelmények, és mely esetben csak ajánlottak. Jellemzően közös alapelvük, hogy az alkalmazott szoftvereknek csak a rendszer rendeltetéséhez szükséges moduljait telepítsék, minden felesleges szolgáltatás legyen letiltva. Ez után az installálásuk, rendszerspecifikus beállításaik, frissítésük, a jogosultságok, monitorozások, naplózások, auditálások, a hibadetektálásuk, mentés-helyreállítás menedzsmentjének megvalósítását tárgyalják.

Majd joggal és értelemszerűen vetődik fel a kérdés, hogyan valósítható meg egy a kor követelményeinek megfelelő rendszerbiztonságos szoftverarchitektúra, amely szavatolja szolgáltatásainak működésfolytonosságát, a benne kezelt információk bizalmasságát, sértetlenségét és rendelkezésre állását.

A szoftverbiztonság korszerű megvalósítása

A gyakorlati tapasztalatok azt mutatják, hogy gyakorta olyan kommunikációs és információs rendszerek vannak alkalmazásban világszerte (és hazánkban is) kritikus fontosságú feladatok ellátására, amelyek megalkotásakor nem kalkulálták megfelelően a biztonsági kockázatok növekedését, illetve a felhasználásuk iránti növekvő igényt, tervezésükkor a biztonsági elvek nem kellő mértékben érvényesültek, architektúrájuk hibatűrés, skálázhatóság szempontjából alulméretezett, ezáltal működésbiztonságuk, támadásoknak történő ellenállásuk már nem felel meg a kor követelményeinek. Ebből levezethető a kritikus infrastruktúrák sebezhetőségének növekedése is.

Hibatűrés szempontjából alulméretezett egy rendszer, ha az elvárt rendelkezésre állást nem tudja teljesíteni, ha például az energiaellátása, az adatkommunikációs csatornái, a hardverei, a szoftverekkel megvalósított szolgáltatásai nem megfelelő mértékben redundáns kialakításúak, egy elemnek a meghibásodása a rendszer teljes szolgáltatáskiesését okozhatja (például ha 99,99 százalékos rendelkezésre állás az elvárt, hetente egy percet állhat a rendszer). Skálázhatóság szempontjából akkor alulméretezett egy rendszer, ha a kapacitása és a funkcionalitása nem bővíthető dinamikusan az új és megnövekedett felhasználási igényeknek megfelelően.

A szervezetnek gyakran nincsenek meg az informatikaiinfrastruktúra-fejlesztések időszakos szervezeten belüli megvalósításához szükséges erőforrásai, illetve gyakorta költséghatékonyabb havidíjas konstrukcióban külső szolgáltatók adatkommunikációs szolgáltatásainak, szerverszolgáltatásainak igénybevétele. Ezért mind több szervezet választja azt, hogy a működése szempontjából kritikus informatikai szolgáltatások és bizalmas információk kezelését is külső szolgáltatók által működtetett informatikai infrastruktúrán valósítsa meg. Elősegíti ezt az is, hogy a távközlési szolgáltatók ma már ha-

zánkban is a legkorszerűbb technológiájú adatkommunikációs szolgáltatásokat kínálják (FlexCom bérelt vonal, fényszálas vezetékes, 4GL mobilinternet) megfizethető áron. A szervezetek egyre komplexebb szerverszolgáltatásokat vesznek igénybe külső szolgáltatóktól, napjaink számítástechnikaifelhő-szolgáltatásainak egyik nagy előnye, hogy kiválóan skálázhatók, a számos szolgáltatónak köszönhetően áraik versenyképesek a saját üzemeltetéshez képest, ráadásul biztonságosságuk működtetőik üzleti létérdeke is.

Figyelemre méltó azonban az is, hogy nagyobb szervezetek sokszor a központosítás irányába haladva sem bízzák szervereik kiszolgálását külső szolgáltató informatikai infrastruktúrájára, gyakran saját szervertermeikben létesítenek úgynevezett privát felhőket *(private cloud)*.

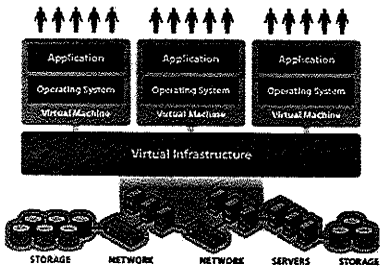
Összefoglalva, az irodai munkakörnyezetben alkalmazott informatikai szolgáltatások mobil elérése növekvő igény. A korszerű szoftverbiztonság megvalósítását azonban egy rendszerben, annak teljes életciklusára a piaci trendekből prognosztizálható fejlődésre, biztonsági nehézségekre tekintettel kell megalkotni.

Ha a szervezet számára lehetséges korábbi informatikai szolgáltatásaik migrálása, új szolgáltatásainak bevezetése saját informatikai infrastruktúrájának fejlesztésével, akkor célszerű, hogy a hibatűrés és skálázhatóság érdekében a szervereket, aktív hálózati eszközöket, adattároló egységeket *(storage)* hardvervirtualizációs technológiák alkalmazásával privát felhőbe szervezze. Ennek megvalósításában napjaink egyik piacvezető szoftvermegoldása a VMware Virtual Infrastructure, miközben a Microsoft Hyper-V megoldásának is dinamikusan nő a piaci részesedése. A *2. számú ábra* szemlélteti a leírtak megvalósítását.

A virtualizált infrastruktúrán menedzsmentkonzol szoftveralkalmazással pillanatok alatt hozhatók létre virtualizált szerverek és munkaállomások, erő-

2. számú ábra

A VMware Virtual Infrastructure logikai vázlata



Forrás: http://www.vmware.com/virtualization/virtual-infrastructure.html

rásaik az igényeknek megfelelően dinamikusan változtathatók, az alkotóelemeik állapota, változásuk, üzemeltetésükben végrehajtott műveletek egységes felületen naplózódnak, lehetővé téve azt is, hogy az üzemeltető szerepkörben csak a feladatai mértékében tudja ezeket az erőforrásokat vezérelni. A virtualizált számítógépekről könnyen készíthetők mentések, tükörmásolatok a fejlesztési folyamatokhoz vagy kockázatértékelési tesztekhez, amelyek az éles szoftverkörnyezet funkcionalitásának bővülését és biztonságának növelését célozzák úgy, hogy azok működését nem veszélyeztetik. Hiba esetén könnyen visszaállíthatók korábbi állapotba.

A virtuális szervereken kiszolgált komplex üzleti alkalmazásokat (például vállalatirányítási rendszerek, szervezeti portálok) háromrétegű architektúrába szokás szervezni, amelyben az adatok tárolását és hozzáférését tipikusan egy relációs adatbázis-kezelő rendszer (például Oracle Database Microsoft SQL Server szoftverrel), a dinamikus tartalmak előállítását alkalmazásszerver, a felhasználói felületet jellemzően webszerver szolgáltatja. Ez esetben a végponti eszközökön a szolgáltatások igénybevétele mindössze webböngészőt igényel, így a végponti eszköz lehet akár egy táblagép vagy okostelefon is. Ma már általános biztonsági követelmény, hogy a szerverek közti és a szerver–kliens közti kommunikációk titkosított adatcsatornán keresztül történjenek, az adatok védelme érdekében az adatbázisszintű titkosítás, a nyilvános kulcsú infrastruktúra (PKI) alkalmazása, amely hitelesítő tanúsítványokat szolgáltat a rendszerben alkalmazott szolgáltatásoknak, eszközöknek és felhasználóknak. Az ilyen rendszer a komplex üzleti alkalmazás szolgáltatásai és az abban kezelt információvagyonhoz történő hozzáférés feletti teljes kontrollt teszi lehetővé, biztosítva ezáltal, hogy azokat csak a jogosult eszközökről a jogosult felhasználók érjék el.

A szoftverbiztonság lényeges tényezője a komplex végpontvédelem hardveres és szoftveres megoldásokkal, alkalmazása alapvető követelmény. Az integrált védelmi szoftverek vírusvédelmet, kémprogramok elleni védelmet, hálózati fenyegetések elleni védelmet (tűzfal, behatolásvédelem) nyújtanak. Követelmény, hogy proaktív fenyegetésérzékelésük is legyen, azaz észleljék az új és gyorsan módosuló rosszindulatú programokat, felfedjék az ismeretlen fenyegetéseket is, aktívan blokkolják a támadásokat. A területen a két piacvezető a Symantec és a McAfee. Az üzleti felhasználásra szánt termékek a végpontokra (szerverek, asztali és notebook számítógépek, táblagépek, okostelefon) központi menedzsmentalkalmazásukból telepíthetők, ebből irányítható és felügyelhető az összes végpont.

Nagyobb informatikai infrastruktúrát alkalmazó szervezetek nem nélkülözhetik a szoftverekkel megvalósított automatizált rendszerfelügyeletet, amely magában foglalja a működésfelügyeletet, a változás-, a konfiguráció-, a verzió-, az eszközállomány-, a hiba-, a kapacitás- és az eseménykezelést, ezek megvalósítását. Ilyen szoftverek például a Microsoft System Center (fő elemei Configuration Manager és Operation Manager), az IBM Tivoli és Rational termékcsaládja. A külső szolgáltatók számítástechnikai felhőjén (például Amazon EC2, Microsoft Azure) megvalósított informatikai architektúrák automatizált rendszerfelügyelete is megoldható ezek alkalmazásával.

Összegzés, következtetések

Megállapítható, hogy a kommunikációs és információs rendszereknek mind komplexebb szolgáltatásokat kell nyújtaniuk, ezért informatikai infrastruktúrájuk egyre összetettebb. Szolgáltatásaik működésfolytonossága, a bennük kezelt adatok bizalmasságának, sértetlenségének, rendelkezésre állásának sérülése súlyos károkhoz vezethet, a kritikus infrastruktúrákat működtető és a minősített adatokat kezelő rendszerek esetén ez még hatványozottabban értelmezhető. E rendszerek komplex és integrált védelmén belül egyre fokozottabban kell ügyelni a szoftverbiztonságra, mivel a rendszerek működését gyakran a nem megfelelően kialakított és üzemeltetett szoftverarchitektúra veszélyezteti. Az ellenük irányuló dinamikusan növekvő támadások döntően a szoftverkörnyezet sebezhetőségét próbálják kihasználni. Ezért fontos, hogy a rendszerben megfelelő működésbiztonsági tanúsítványú, bevizsgált szoftvereket alkalmazzanak. A kritikusabb alkalmazások fejlesztésekor ezért kiemelten fontos tényező az egyedi szoftverfejlesztések biztonsági auditja, a kialakított szoftverkörnyezet működtetésének, változásmenedzsmentjének szabályozottsága, felügyelete, védelme, amelyek automatizálását szoftveres megoldások is segítik.

A szabályozott működéshez fontos, hogy a jogalkotók jogszabályokban, normatív utasításokban meghatározzák a rendszerek működtetésére vonatkozó követelményeket a társadalom szempontjából kritikus fontosságú kommunikációs és információs rendszerek tekintetében, hazánkban ennek érdekében került sor az információbiztonsági törvény megalkotására. Az előbbiekben kifejtettekből is következik, hogy a szoftverbiztonság megvalósításában fontosak és alapvetően szükségesek az információbiztonsági szabványok, ajánlások, az információbiztonsággal foglalkozó szervezetek és a gyártók biztonságos kivitelezést támogató útmutatói. A korszerű szoftverbiztonság megteremtéséhez a szoftvergyártó cégek a kor követelményeinek megfelelő korszerű szoftvereket kínálnak, amelyek centralizált kontrollt gyakorolnak az üzemeltetett rendszer felett. A külső szolgáltatók által kínált számítástechnikai felhő-szolgáltatások egyre inkább költséghatékony lehetőségek a saját informatikai infrastruktúra fenntartásával szemben, mind több rendszer válik így elérhetővé, így a szoftverbiztonság területén belül a proaktív fenyegetések elleni védelemre különösen nagy súlyt kell fektetni.