HAMPEL GYÖRGY*–FABULYA ZOLTÁN**–NAGY ELEMÉRNÉ DR.***

Adatbiztonság a Mérnöki Kar személyi számítógépein

Abstract

It is very important to protect the digitally stored intellectual product in an organization where education and research is the main activity. We have asked our colleagues at the Faculty of Engineering to take part in a survey about data protection. Our findings were:

- Only colleagues, who use computers regularly, sent back the questionnaire via email.
- The most used operating system is Windows XP Pro. Linux and Windows Vista are only used on a few machines.
- The frequency of hardware and software failures (blue screen of death, freezing, virus infection, data loss, etc.) indicate that more frequent maintenance is required.
- The data protection provided by the operating system or other software (firewall, virus scanner, etc.) is more commonly used than hardware based protection (ups, hard disk data protection card, etc.)
- The autoupdate feature is used to update the software, manual update is not typical.
- Nearly all of our colleagues could give a correct estimate of the size of the programmes and documents or other data. So they know how much storage they need to store their files and to make backups.
- Two third thinks that he or she can make backup copies and can also restore them. On the other hand most of them do not know whether there is a backup programme installed on the PC (although Windows XP has one).
- CD, DVD and USB flash drives are used by half of the colleagues to store backup copies. Some use a separate hard disk or a separate partition for the backup. Almost half of them said that they make copies themselves, but the other half thinks that the backup is made automatically by the programmes or they have no clue at all.
- Half of the colleagues think that restoring a complete system from a backup requires more time than installing and setting up all the software. This indicates that the knowledge about backup and restore is mostly theoretic and the computer users at our faculty have no real experience in backing up and restoring.

Bevezetés

A szervezet működése során rengeteg adat keletkezik. Az adatok egyre nagyobb része digitalizált formában jön létre, illetve tárolódik. Az adatok és a belőlük képzett információk jelentős értéket képviselnek; nélkülözhetetlenek a szervezet (törvényes) működése, a szervezet versenyképessége és számos egyéb szempontból is.

Egy olyan szervezetben, ahol az oktatás és a kutatás a fő tevékenység, a digitális formában tárolt szellemi termékek biztonságáról való gondoskodás kiemelt jelentőségű.

* Adjunktus – Szegedi Tudományegyetem, Mérnöki Kar, Ökonómiai és Vidékfejlesztési Intézet.
** Adjunktus – Szegedi Tudományegyetem, Mérnöki Kar, Ökonómiai és Vidékfejlesztési Intézet.
*** Főiskolai Tanár – Szegedi Tudományegyetem, Mérnöki Kar, Ökonómiai és Vidékfejlesztési Intézet.

Az adatvédelem elsősorban jogi kérdés; azt határozza meg, hogy ki, milyen adatokkal és mit tehet. Számos nemzetközi ajánlás, egyezmény született ebben a témakörben és az országok többségében, így Magyarországon is megszülettek a nemzeti jogszabályok (http://europa.eu/scadplus/leg/en/s21012.htm#PROTECTION, http://ppos.hu/index.htm).

„Az adatbiztonság – az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere." (F. Ható, 2001) Az adatbiztonság tehát elsősorban műszaki, szervezési kérdés: segítségével minimálisra kell szorítani a rendszerösszeomlások számát, az adatvesztések mértékét, illetve az ezekből származó anyagi és egyéb károkat.

Az adatbiztonsággal számos nemzetközi és hazai ajánlás foglalkozik. Ezek közül néhány: TCSEC (Trusted Computer System Evaluation Criteria), ITSEC (Information Technology Security Evaluation Criteria), FC (Federal Criteria for Information Technology Security), ISO OSI 7498-2 (X.800) adatbiztonsággal foglalkozó szabvány, vagy Magyarországon az Informatikai Tárcaközi Bizottság biztonsági módszertani ajánlásai. (F. Ható, 2001)

Jelen publikációnkban az adatbiztonság kérdésével foglalkozunk.

Adatbiztonság

Egy számítógépes rendszerrel szemben a főbb biztonsági alapkövetelmények: a rendelkezésre állás (üzemképesség), a működőképesség (elvárt üzemeltetési állapot fenntartása), a sértetlenség (az adatokat csak az arra jogosultak módosíthatják, véletlenül nem változnak), a bizalmasság (nem fordulhat elő jogosulatlan hozzáférés), valamint a hitelesség. (F. Ható, 2001) E követelményeknek megfelelő rendszerek létrehozását és működtetését számos tényező nehezíti: A számítógépes rendszerek adott környezeti feltételek között, adott infrastruktúrával, meghatározott hardverrel és szoftverrel működnek. A számítógépekkel emberek dolgoznak, alkotnak akik – jó esetben – a következetes szempontrendszer szerint mentett dokumentumokat valamilyen adathordozón tárolják. A számítógépek és az adatok már ezen okokból is számos veszélynek vannak kitéve.

Amíg izolált személyi számítógépeken folyik a munka, addig minden felhasználó csak az általa használt rendszer biztonságáért felel. Onnantól kezdve azonban, hogy a számítógépeket számítógép-hálózatba kapcsolják, jelentősen megnő a rendszerek és a tárolt anyagok fenyegetettsége. Egy-egy rosszul védett rendszer vagy egy „tudatlan" felhasználó nem csak saját magát, hanem a vele kapcsolatban álló számítógépeket és adataikat is veszélybe sodorhatja. (F. Ható, 2001)

A számítógép, számítógépes rendszer környezeti infrastruktúrájának lehetséges gyenge pontjai és a fenyegető tényezők: a nem, vagy nem megfelelően védett informatikai berendezések, az illetéktelen személyek felügyelet nélküli jelenléte a számítógép közelében, a védelmi eszközök működési módjának, vagy gyengeségeinek jogosulatlanok által megismerésének lehetősége, előre nem látható környezeti katasztrófák, közműellátási zavarok, az alkalmazott védelmi berendezések zavarai, továbbá a személyek által elkövetett – gépre irányuló – erőszakos cselekmények. Ezek kivédhetők a számítógépek védett elhelyezésével, a védelmi eszközök működőképességének biztosításával és használatával, áram-, tűz-, vízvédelmi eszközökkel, betörés- és behatolásvédelmi eszközökkel; a számítógépeken alkalmazott belépés ellenőrzési, hozzáférés szabályozó jogosultságok alkalmazásával, valamint a rendszer eseményeinek és a felhasználók tevékenységének naplózásával.

A hardver biztonságát veszélyeztető fő gyenge pontok és fenyegető tényezők: a lopás, a külső behatások (hő, víz, elektromágneses sugárzás, mechanikai behatás) miatt meghibásodás, a tartozékok utánpótlásának szervezetlensége; műszaki jellegű hibák, környezeti

hatások (például feszültségingadozás, nedvességtartalom ingadozás, piszkolódás, elektrosztatikus feltöltődés), szoftver által kiváltott hibák a hardverben, személyekkel összefüggő fenyegetés (eszköz károsítása, ellopása. A hardverbiztonságot veszélyeztető tényezők kivédésének módszerei közé tartozik, hogy: az eszközök eltulajdonításának megakadályozása érdekében célszerű a rendszer minden eleméről naprakész nyilvántartást vezetni, az eszközöket és a szolgáltatásaikat csak megfelelő azonosítás után célszerű engedni. A fellépő műszaki hibák gyors megoldása érdekében gondoskodni kell a megfelelő pótalkatrészek beszerzéséről, és ahol lehet hibatűrő konfigurációkat érdemes alkalmazni. A legújabb (még kiforratlan és drága) technológiák alkalmazása általában kerülendő.

Nagyon fontos, hogy tudjuk: a számítógépek általában megbízhatatlan berendezések; mindig fel kell készülnünk a meghibásodásra, adatvesztésre. Különösen igaz ez az adathordozókra. Az adathordozók gyenge pontjai:

- a fizikai instabilitás, vagyis a környezeti hatásokra való érzékenység,
- kikapcsolható írásvédelem,
- könnyű és nehezen ellenőrizhető szállíthatóság,
- az adathordozók tartalma segédeszközök nélkül nem hozzáférhető.

Az adathordozókat fenyegető tényezők:

- gyári hibás adathordozó,
- inkompatibilis formátum, vagy hiányzó kezelő berendezés,
- hiányos jelölés, ami miatt a tartalom esetleg „ránézésre" nem állapítható meg,
- ellenőrizetlen hozzáférés és másolás,
- újrafelhasználás vagy leselejtezés (nem megfelelő) törlés nélkül,
- szervezeti adathordozók magáncélú, illetve magántulajdonú adathordozók szervezeti célú használata.

Sajnos a számítógépek és adathordozóik nem örökéletűek, megsérülhetnek, tönkremehetnek. Szerencsére a mai adattárolók nagyobb mértékben állnak ellen a környezeti hatásoknak (és az embernek), mint korábban, ezért az effajta sérülések száma csökkent. Ugyanakkor az adathordozók méretének jelentős növekedése miatt, sérülés esetén egyszerre nagyobb mennyiségű adat veszhet el.

Az adathordozók sérülése, meghibásodása – és ezzel a rajtuk tárolt adatok elvesztése – elleni védekezés lehetséges módjai:

- az adathordozó óvása környezeti ártalmaktól (hideg, meleg, nedvesség, közvetlen napfény, por),
- az adathordozók átlagos várható élettartamának figyelembe vétele (nem az örökkévalóság, hanem csupán néhány év, esetleg évtized!),
- hibatűrő technológiák (például RAID – Redundant Array of Inexpensive Disks) alkalmazása,
- az állományok szabályos bezárása, a számítógépek szabályos leállítása,
- rendszeres felületellenőrzés segédprogramok segítségével,
- biztonsági másolat rendszeres készítése. (F. Ható, 2000) (Hampel, 2006)

A vizsgálat tárgya, módszer

Egy általunk összeállított kérdőív segítségével azt igyekeztünk megtudni, hogy a Szegedi Tudományegyetem Mérnöki Karán azok az oktató és nem oktató kollégák, akik számítógéppel dolgoznak, miként viszonyulnak az adatbiztonság kérdéséhez.

Az oktatással és kutatással foglalkozó dolgozók szellemi terméket állítanak elő; oktatási anyagokat készítenek, kutatási eredményeikről publikációkat írnak számítógépen; a forrásanyagok összegyűjtéséhez és az egymással való kommunikációhoz használják a belső- és az internethálózatot is. Az egyéb munkakörben foglalkoztatott kari dolgozók jelentős része munkája során szintén használ számítógépet.

A dolgozók és a kar érdeke is, hogy a számítógépes rendszerben, az adathordozókon tárolt szellemi termék hosszabb távon és visszakereshető formában megőrződjön.

A számítógépen kitölthető kérdőívet igyekeztünk úgy megfogalmazni, hogy megértéséhez ne legyen szükség magas szintű számítástechnikai ismeretekre. A könnyebb kitöltés és a feldolgozás egyszerűbbé tétele érdekében mindenhol zárt kérdéseket alkalmaztunk. A kérdőívet elektronikus levélben kapták meg a kari dolgozók, majd szövegszerkesztőben való kitöltés után, ugyanúgy vissza is küldhették.

A kérdőív kérdései:

- Munkakör. Véleményünk szerint azok az alkalmazottak, akik az ügyvitel területén dolgoznak, gyakrabban találkozhatnak olyan előírásokkal, amelyek az adatok biztonságát, védelmét fokozottabban előírják. Így az adatok biztonságát szolgáló tevékenységeik – feltételezéseink szerint – eltérhetnek azokétól a dolgozóktól, akik oktatási, kutatási tevékenységhez használják a számítógépet.
- Számítógép-használat gyakorisága. Azok a felhasználók, akik gyakrabban használják a számítógépet, általában elvárható a nagyobb gondosság. Kérdés, hogy a karon a válaszok alapján valóban kimutatható-e ez a feltevés.
- Hibaesetek, veszélyforrások előfordulási gyakorisága a dolgozók gépein. A felsorolt hibalehetőségek (fagyás, újraindulás, szabálytalan leállás, vírusfertőzés, hálózaton keresztüli támadás, program vagy adatsérülés és adatvesztés) normális esetben nem, vagy csak nagyon ritkán fordulhatnak elő. A kérdésekre adott válaszok a használt számítógépek minőségére, a munkakörülményekre utalnak. A felkínált válaszok minden esetben ugyanazok, de a választási lehetőségek sorrendje minden kérdés esetében más-és más; ennek oka, hogy a válaszoló lehetőleg ne automatikusan, mindig ugyanoda kattintva töltse ki a kérdőívet. (A válaszlehetőségek változtatott sorrendjét más kérdéseknél is alkalmaztuk.) Kérdés, hogy vajon azok a felhasználók, akik gyakrabban találkoznak a felsorolt hibalehetőségekkel, azon túl, hogy tesznek (tesznek-e) ellene, gondosabbak-e az adatbiztonságban?
- A gépre telepített operációs rendszer. Az operációs rendszerek számos beépített biztonsági szolgáltatást tartalmazhatnak (például jelszó, kódolás, vírusvédelem, adatmentés stb.). A korszerű operációs rendszer új és rendszeresen frissített biztonsági elemeket tartalmaz, ami egy elavult, már nem frissített operációs rendszerre nem jellemző. A kérdésre adott válaszokból nem csak azt tudhatjuk meg, hogy mekkora az elavult és már nem biztonságos rendszerek aránya, hanem a következő kérdésekre adott válaszokkal együtt arra is rávilágíthatnak, hogy a felhasználók ismerik-e ezen beépített biztonsági szolgáltatásokat és használják-e azokat.
- Alkalmazott hardveres, szoftveres védelem, illetve az operációs rendszer által biztosított védelem és biztonság. A rendelkezésre álló hardverrel és/vagy szoftverrel megvalósított védelmi szolgáltatások közül melyek azok, amelyeket a felhasználók igénybe vesznek? A megoldás szolgálhatja a rendszerhez, a rendszer elemeihez,

valamint az adatokhoz való hozzáférés korlátozását (védelem), vagy szolgálhatja az adatok megőrzését, sérülésének megakadályozását (biztonság). A válaszokból az is kiderülhet, hogy a felhasználók az operációs rendszeren belül elérhető szolgáltatásokat, vagy inkább külső szállító szolgáltatásait használják-e szívesebben.

- Szoftveres védelem frissítésének gyakorisága. Az alkalmazott védelmi, biztonsági szolgáltatásokat időnként célszerű frissíteni, megújítani; hiszen például egy hónapokkal ezelőtt feltelepített víruskereső a legfrissebb vírusadatbázis nélkül nem ér szinte semmit, csupán hamis biztonságérzetet ad. Kíváncsiak voltunk, hogy a felhasználók gépein a frissítéseket ki és milyen gyakorisággal végzi (már ha végzi egyáltalán).
- A programok és a dolgozó állományai által elfoglalt hely. A programok és a felhasználói adatok, dokumentumok tárolására megfelelő méretű adathordozókra van szükség. Vajon tudják-e a felhasználók, meg tudják-e nézni, vagy ha nem, legalább meg tudják-e becsülni a választ. Az egyszerűség kedvéért itt is zárt kérdéseket alkalmaztunk, a felkínált lehetőségek leszűkítik a választ, de a válaszlehetőségek nem nagyság szerinti sorrendben követik egymást, továbbá irreális választási lehetőséget (irreálisan nagy tárolókapacitás igényt) is megadtunk.
- Adatmentő szoftver van-e telepítve? Vajon tudják-e a felhasználók, hogy a gépükön lévő szoftverek között lehet olyan, ami erre a feladatra képes? Azoktól, akiknek korszerű operációs rendszerük van, azt is kérdezhettük volna, hogy vajon tudják-e hogy a gépükre ilyen program is fel van telepítve. Tapasztalat, hogy bár az operációs rendszer alapfeladatain túl számos egyéb szolgáltatást kínál, a felhasználók jelentős része azokat nem használja – mivel nem tud róla –, hanem helyettük, vagy inkább mellékük más gyártó hasonló termékét telepíti.
- Adatmentés készítése és módja, a mentés visszaállítása. Ha van rá mód, vagy akarat, akkor a felhasználók hányad része képes valamilyen biztonsági másolatot, mentést készíteni az eredeti állományokról? Nem elegendő azonban a biztonsági másolatot elkészíteni, vissza is kell tudni azokat állítani. A programfrissítésekhez hasonlóan itt is kíváncsiak voltunk arra, hogy a felhasználók gépein a biztonsági másolatokat ki és milyen gyakorisággal végzi (feltéve, hogy valaki elvégzi).
- A biztonsági mentés helye. Azok, akik készítenek (biztonsági) mentéseket, hova készítik azt? Melyek a legjellemzőbb adatarchiváló eszközök, adathordozók? Minden – a felsorolásban szereplő – adathordozónak vannak előnyei, hátrányai (például hordozhatóság, sérülékenység, élettartam).
- A programok telepítéséhez, illetve a biztonsági mentés helyreállításához szükséges idő. A programok egyedi telepítése, majd a felhasználó igényeinek megfelelő beállítása sokkal több időt vesz igénybe, mint egy meglévő biztonsági mentés helyreállítása. Az ide kapcsolódó zárt kérdésekkel (és a felkínált választási lehetőségekkel) arra voltunk kíváncsiak, hogy vajon ezzel tisztában vannak-e a felhasználók. A válaszlehetőségek itt sem nagyság szerinti sorrendben követik egymást és – személyi számítógépeket tekintve – szerepelnek a listában irreálisan nagy telepítési és visszaállítási időtartamok.

Eredmények és következtetések

A kérdőívek kitöltésére 10 nap állt rendelkezésre; 64% a küldés napján, 20% a 6-9 napon, 8-8% pedig az utolsó napon, illetve határidő után érkezett vissza kitöltve. Az összesen 25 kitöltött kérdőív között volt egy hibásan visszaküldött, feldolgozhatatlan is.

A kitöltésben létszámuknál nagyobb arányban vettek részt az oktatók (79%), az ügyviteli alkalmazottak aránya 13% és az egyéb munkakörben foglalkoztatottak aránya 8% volt. Bár volt mód arra, hogy a kitöltők nem beazonosítható módon küldjék vissza a levelet, ezzel a lehetőséggel senki sem élt.

Többen jelezték, hogy ugyan kitöltenék a kérdőívet, de nem értenek hozzá (azaz nem tudják önállóan elvégezni az ehhez szükséges műveletsort: elektronikus levélből űrlap megnyitása; válaszlehetőségekből választás; űrlap mentése; új levél létrehozása; űrlap csatolása a levélhez; levél elküldése). Bizonyára voltak olyanok is, akik nem szívesen adták volna a nevüket a válaszokhoz, azonban mivel nem volt elegendő ismeretük ahhoz, hogy beazonosíthatatlan levélcímet használjanak, inkább nem töltöttek ki kérdőívet. Volt olyan is, aki jelezte, hogy azért nem válaszol, mert attól tart, hogy a válaszaiból kiderülhet a személyazonossága.

Bár igyekeztünk egyszerű kérdéseket feltenni, mégis voltak olyanok, akik – visszajelzésük alapján – azért nem válaszoltak, mert nem értettek meg minden kérdést, vagy egyes fogalmak jelentésével nem voltak teljesen tisztában. A kérdőívben szándékosan nem magyaráztunk meg fogalmakat (pl. RAID1) – a biztonsági mentés értelmezése kivételével – abból a megfontolásból, hogy ha egy, a vizsgált témakörhöz tartozó fogalom nem ismerős, vagy nem érthető a válaszoló számára, akkor azt a gyakorlatban – nagy valószínűséggel – nem is használja. Mindenesetre lehetséges, hogy a kérdések egy részének nem értése is visszatartó erővel bírt a kérdőív címzettjei számára.

Munkakör: A kevés számú ügyviteli alkalmazott válaszai alapján nem volt kimutatható eltérés a kérdésekre adott válaszokban és nem igazolódott az a feltevés, mely szerint az ügyviteli alkalmazottak jobban vigyáznak a saját (és mások) adataira, mint az oktatók.

A számítógép-használat gyakorisága: A kitöltött kérdőívet kizárólag olyanok küldték vissza, akik rendszeresen, szinte minden munkanapon használnak számítógépet a munkájukhoz. Ez alapján feltételezhetjük, hogy a Mérnöki Karon egyrészt ők azok, akik valamennyire érdeklődnek a téma iránt, fontosnak tartják a témát, továbbá megvan a tudásuk és képességük is egy elektronikus dokumentum fogadására, módosítására és továbbítására.

Hibaesetek, veszélyforrások előfordulási gyakorisága a dolgozók gépein: A válaszok alapján a gépek hardver- és szoftver tekintetében karbantartásra szorulnak (szorulnának). A szabálytalan leállás/leállítás, újraindulás/újraindítás a válaszolók körülbelül felénél fordult elő az elmúlt egy évben háromnál több alkalommal. A választ adók közel 40%-a találkozott számítógépes kártevővel (arra, nem tért ki a kérdőív, hogy a kártevőnek volt-e ideje megfertőzni a gépet, vagy időben közbelépett a víruskereső). Több, mint harmaduknak nincs tudomása arról, hogy érte-e a gépét hálózaton keresztüli támadás és a kitöltők közel fele válaszolt úgy, hogy adatsérülés, vagy vesztés történt a gépén. Azoknak a válaszaiban, akiknél a felsorolt jelenségek gyakrabban fordultak elő, nem volt kimutatható eltérés az adatbiztonsággal kapcsolatos hozzáállásukban, tevékenységükben.

A gépre telepített operációs rendszer: szinte a Windows XP Pro és Home az egyeduralkodó, 1–2 gépen Linux és Windows Vista is előfordul. Ez azt jelenti, hogy mindenki korszerű, a gyártó által gyakran frissített rendszerrel rendelkezik, amelyek saját biztonsági szolgáltatásokkal is rendelkeznek.

Alkalmazott hardveres, szoftveres védelem, illetve az operációs rendszer által biztosított védelem és biztonság: A válaszokból kiderül, hogy a hardver által biztosított védelem használata kevésbé jellemző; a számítógép bekapcsolásakor kért jelszó használata a leggyakoribb (38%). A szünetmentes tápegység, valamint túlfeszültség elleni védelmet biztosító eszközök használata csak néhány felhasználónál fordul elő. Az operációs rendszer által biztosított szoftveres védelmet a felhasználók többsége használja (tűzfal 63%, automatikus frissítés 75%, jelszó 46%), de kiegészíti egyéb szoftveres védelemmel is (tűzfal 64%, ví-

rusvédelem 83%). A kérdéscsoportra leadott válaszok összesítése alapján a hardveres védelem alkalmazása 13%, az operációs rendszer szoftveres védelmének alkalmazása 45%, az egyéb szoftveres védelem alkalmazása 44%-ban jellemző.

Szoftveres védelem frissítésének gyakorisága: A válaszok szerint a telepített szoftverek automatikus frissítése a felhasználók 96%-ánál be van kapcsolva. Néhány esetben a felhasználó, illetve egyéb segítség gondoskodik rendszeresen, vagy alkalmanként a frissítésről. Olyan nem fordul elő, hogy valakinél ne legyen valamilyen módon megoldva a szoftverek frissítése.

A programok és a dolgozó állományai által elfoglalt hely: A válaszolók többsége reális adatokat adott meg mind a programok mérete (5–20 gigabájt 61%), mind pedig az adatok által elfoglalt tárhely tekintetében (0–10 gigabájt 54%). Születtek azonban olyan válaszok, amelyekből valószínűsíthető, hogy a felhasználó vagy nincs tisztában azzal, hogy valójában mekkora tárhelyet foglalnak el a programja és az adatai, vagy másik lehetőségként: mindenféle programot feltelepít a gépére majd csak jó lesz valamire alapon (ami tovább növeli a telepített szoftverkörnyezet komplexitását és ezzel a lehetséges rendszerösszeomlás valószínűségét), illetve olyan korábbi adatokat, dokumentumokat is tárol a gépén, amiket már nem használ.

Telepített adatmentő szoftver: Mindössze 38% válaszolt úgy, hogy a gépén van kifejezetten az adatok biztonsági mentésére szolgáló szoftver, 37% szerint nincs és 25% nem tudja. Tekintettel arra, hogy a többség gépén Windows XP van telepítve, nyilvánvalóan arról van szó, hogy a felhasználók többsége nem ismeri az operációs rendszer ezen szolgáltatását. (A kérdőív nem tért ki arra, hogy vajon az adatmentő szoftver az operációs rendszer sajátja, vagy egyéb szoftver.)

Adatmentés készítése és módja, a mentés visszaállítása: A válaszok szerint a felhasználók 67%-a képes biztonsági mentés létrehozására, ugyanakkor – saját állításuk szerint – ennél többen, 75%-nyian tudnak biztonsági mentésből programokat és adatokat visszaállítani. Ez az eredmény jól tükrözi az általános vélekedést, mely szerint a visszaállítás könnyebb, mint a biztonsági mentés elkészítése, ugyanakkor ellentmond a gyakorlati tapasztalatoknak: a felhasználók általában csak azt tanulják meg, hogy hogyan kell menteni, de abban – gyakorlás során – nem szereznek tapasztalatot, hogy hogyan kell visszaállítani és csupán az éles helyzetben szembesülnek a visszaállítás problémáival. A válaszok szerint 8% képes biztonsági mentés készítésére, de ugyanakkor nem tud visszaállítani. A válaszolók negyede nem tud sem biztonsági mentést készíteni, sem visszaállítani. Legtöbben saját maguk készítenek anyagaikról és programjaikról másolatot – alkalmanként (46%), rendszeresen (38%) –, 25% véli úgy, hogy erről programok gondoskodnak automatikusan és 8-8% válaszolt úgy, hogy a másolatot más készíti, nem készül, vagy nem tudja, hogy készül-e.

A biztonsági mentés helye: A többség többféle médiát is használ a mentések tárolására. Legtöbben írható cd-t, vagy dvd-t használnak (63%, várható élettartam kb. 5 év). Sokan használnak pendrive-ot vagy memóriakártyát (42%, könnyen elveszhet, ellophatják, élettartamára gyakorlati tapasztalatok még nem állnak rendelkezésre). 38% használ kifejezetten erre a célra fenntartott merevlemezt, ami biztonságosabb megoldás, mintha ugyanarra az adathordozóra történne a mentés, mint ami az eredeti állományokat is tartalmazza (25% ment így). Bár ez esetben felmerül, hogy ez a „külön merevlemez" nem csak egy másik merevlemez lehet, hanem az eredeti állományokat tartalmazó lemeznek egy másik partíciója is, amit az operációs rendszer másik háttértárnak „lát". (A merevlemezek élettartamára gyakorlatban a jótállás idejéből lehet következtetni: néhány év.)

A programok telepítéséhez, illetve a biztonsági mentés helyreállításához szükséges idő: A felhasználók nagy része tisztában van azzal, hogy az egyedi telepítés, majd beállítás sok időt vesz igénybe. A többség (67%) szerint 4–8 óra szükséges a telepítéshez, ami figye-

lembe véve a használt rendszereket, reális válasz. Ugyanakkor annak megítélésében, hogy mennyi idő szükséges a biztonsági másolatból történő visszaállításhoz, helyreállításhoz, már jobban szóródnak a vélemények, a többség (57%) 3-nál több órát jelölt meg. A használt rendszereket és az adatok mennyiségét figyelembe véve viszont 1, legfeljebb 2 óra elegendő kell legyen. A felhasználók háromtizedének véleménye szerint a rendszer visszaállítása biztonsági mentésből hosszabb ideig tart, mint a telepítés és beállítás, további 21% szerint pedig azonos ideig tart. A kérdésekre adott válaszokból levonhatjuk azt a következtetést, hogy a Mérnöki Karon a számítástechnikában járatosabb felhasználóknak sincs elegendő tapasztalatuk az adatmentés és -visszaállítás terén.

Publikációnk az eredményeket tartalmazó diagramokat terjedelmi korlátok miatt nem tartalmazza. Kérjük, hogy azok, akik részletesebben is érdeklődnek a felmérés eredményei iránt, küldjenek elektronikus levelet a hampel@mk.u-szeged.hu címre.

Irodalom

F. Ható Katalin (2000): Adatbiztonság, adatvédelem. Számalk Kiadó. Budapest.

Hampel György (2006): Bevezetés a mérnökinformatikai eszközök használatába. Oktatási segédlet. Szeged.