Az Infostrázsa

E könyvet munkájával írta:

Bárkányi Gábor, Bíró Tünde, Czikó Attila, Csillag Ferenc, Dakó Balázs, Dávid Zsolt alias Felhő, Dolánszky György, Fabiányi Gábor, Filipszky János, Gangli Éva, Gergácz Lili, Homola Zoltán, Járku Mariann, Kardos András, Kis Andrea, Kiss Lászlóné, Kleisz Anita, Kmetty József, Kóczián Tibor, Kovács Zoltán II Králik János, Kürti János, dr. Kürti Sándor, Mayer Mihály, Megyeri István, Molnár Géza, Nagy Mihály, ifj. Nagy Mihály, Papp Attila, Pécsi Richárd, Pusztai Tamás, Szabó László, Szabó Zsolt, Szokolovszki László, Tán Éva, Varga Krisztián és Zsilinszky Sándor.

Felelős kiadó: a Vikk.net igazgatója

Felelős szerkesztő: Csapó Ida, dr. Kürti Sándor

Lektor: Révbíró Tamás

Műszaki szerkesztő, tipográfia: Perjés László

Vikk.net - VIrtuális KönyvKiadó
1063 Budapest Szondi u. 72.
Tel.szám: (1) 302-02-09, (30) - 9561-566
E-mail cím: vikk.net@lezlisoft.com
Webhely: http://www.vikk.net

© Kürt Rt

ISBN 963 86133 6 X

A Vikk.netnél ingyenesen megjelenő, próbarendelés célját szolgáló könyvek - mint amilyen ez a kötet is - az interneten szabadon terjeszthetőek. A letöltéshez célszerű megkeresni e-könyvkiadónk webhelyét: http://www.vikk.net.

A próbarendelés célját szolgáló kötetekben benne kell maradnia a Vikk.net VIrtuális KönyvKiadó emblémájának és a szerzői copyright jelzésnek.

Vikk.net - VIrtuális KönyvKiadó
1063 Budapest Szondi u. 72.
Tel.szám: (1) 302-02-09, (30) - 9561-566
E-mail cím: vikk.net@lezlisoft.com
Webhely: http://www.vikk.net

Tartalom

Kedves Olvasó!

Az informatikai biztonságról fogsz olvasni vagy 120 oldalon keresztül, ha belevágsz.

Így vesztik el és így lopják el az adatokat. Mások, másoktól.

Ne aggódj, igyekeztünk könnyed stílusban írni.

Dőlj hátra kényelmesen; hidd el, az itt elsütögetett poénok rád nem érvényesek. Ha netán mégis a saját környezetedre ismersz, legalább nyugtasson meg, hogy mások is gondatlanok, felelőtlenek.

Különben is: mire jó az adatok védelme?

Semmire. Sokkal szórakoztatóbb a katasztrófákról mesélni, panaszkodni, szidni a főnököt, a beosztottat, a gyártót és a szállítót, mint megkísérelni megelőzni a bajt, ezzel lemondani a kaland lehetőségéről, és dögunalomban élni.

Lazíts, és merj mosolyogni a mások baján.

Veled ilyen nem történhet. Te kivételezett vagy.

És ha mégis?

Akkor tanulságos is lehet ez az olvasmány.

Kürtölő

Negyvennyolc történet az informatikai biztonságról. Mindegyike két oldal terjedelmű, és mindegyik legalább egy poénnal és egy jó tanáccsal van fűszerezve. E kétperces önálló olvasmányok méltán pályáznak a „Bestseller of WC Library” címre. Kéttucatnyi történetenként a lecsupaszított jó tanácsokat foglaljuk össze. Mi így kövezzük a pokol felé vezető infosztrádát. Ha sikerre vágysz a munkahelyeden, küldj ezekből hetente egyet-egyet az informatikai főnöknek. Nyert ügyed van. Elektronikusan a www.kurt.hu/kurtolo címen találod őket.

Informatikai Biztonsági Technológia IBiT®

Laza körítéssel elővezetett eszmék a rendszerszemléletű informatikai biztonságról. A Kürtölő néhány fejezetében már belekaptunk ebbe a témába; itt kicsit részletesebben tálaljuk.

Történetek

Pillanatképek a KÜRT életéből.

Néhány mosolyt fakasztó helyzet, minden tanulság nélkül.

A Kürt Computernél számítógépek elvesztett értékes adatait állítjuk helyre vagy tíz éve. Évente legalább 2 000 „adatkárosult” kerül a kezeink közé. Ennek megfelelően ránk is igaz az a szállóige, miszerint: „az informatika ma már a világon mindent támogat, de elsősorban az informatikusok megélhetését”.

E könyvecskében olyan érdekes történeteket mesélünk el, amelyek tanulságosak is lehetnek a kedves olvasó számára — függetlenül attól, hogy a számítástechnikai eszközöket önként vagy kényszerből használja.

Egyszerű esetekkel kezdjük, aztán majd belemelegszünk.

1. Féltégla az informatikában

A kilencvenes évek elején egy szigetelőanyagot (üveggyapotot) előállító hazai gyár úgy érezte, megfogta az Isten lábát. Japánok komolyan érdeklődtek iránta, majd egy pillanattal a vásárlás előtt, egy filléres probléma miatt fogták a milliárdjukat, és elmentek.

Mi történt? A gyár teljes adminisztrációja, fejlesztései számítógépen voltak, ahogy az illik. A központi gépben két winchesteren egymástól látszólag függetlenül minden duplikálva volt, szaknyelven szólva a tükrözve voltak az adatok. Az egyik winchester leállt. Sebaj, a másik működött. A hibás eszközt kiszerelték, és elindultak, hogy garanciában kicseréltessék. Ezalatt – pestiesen szólva – a másik winchester is feldobta a talpát.

Így került hozzánk a két winchester, amelyeket kibontva azonnal láthatóvá vált, hogy itt semmi nem maradt az adatokból, a mágneses felületeket a fejek ledarálták. Alaposan megvizsgálva az esetet, az derült ki, hogy a winchesterek pormentes terébe kívülről az üveggyapot finom pora bekerült, és ez okozta a katasztrófát. Tudni kell, hogy a winchester mechanikai része nem légmentesen, hanem pormentesen zárt. Magyarán: a winchester tiszta, pormentes terében lévő levegő – gondolva a hőmérséklet-változás hatására bekövetkező térfogatváltozásra – egy szűrőn keresztül ki tud jutni a szabad térbe, vagy onnan vissza a winchesterbe, a hőfok emelkedésétől vagy csökkenésétől függően.

Megállapítottuk, hogy az üveggyapot a szűrőt átlyukasztva került a winchesterbe.

A helyszíni vizsgálat arra is fényt derített, hogy a szerver a földön állt, alján a két winchesterrel, amelyeket az üveggyapottal fűszerezett por rendesen beborított. A gép kikapcsolásakor a winchesterek lehűltek, levegőt szerettek volna beszívni, de a szűrőn csak tömény por volt, így az jött be – átszakítva a szűrőt.

Ha a szervert két féltéglára helyezték volna, mindez nem következik be.

A féltégla azért lényeges, mert ebben a magasságban a por már a rövidlátó takarító néninek is feltűnhet (kivéve persze, ha a szerver dobozán belül van – mármint a por, és nem a néni).

2. „Akinek a tudás megszerzése drága, nem számol a tudatlanság költségeivel"

Egy privatizálás előtt álló bankunkból érkezett a segélykérés.

Megközelítőleg a következő párbeszéd zajlott le közöttünk:

– A Novell nem indul el – mondták.

– Hozzák be a winchestert, nem nagy ügy – válaszoltuk.

– Már megpróbáltuk beindítani, szereztünk is egy Vrepair-t, de így sem ment.

– Ez már egy kicsit bonyolítja a dolgunkat.

– Ezután még a Norton Disk Doctorral is próbálkoztunk, de az sem segített.

– Ja, így már tényleg katasztrofális a helyzet.

Az ehhez hasonló párbeszédek nálunk gyakoriak. Nekünk a feladat bonyolultságával arányos a tarifánk. Az igazi gond tehát csak akkor jelentkezik, ha a winchester adatai már annyira összekuszálódtak, hogy az adatokat nem lehet helyreállítani, és ez sajnos mindkettőnknek igen rossz.

Hogyan fordulhatnak elő ilyen esetek? Mi a következő, szakmánkat alapvetően érintő problémákat látjuk.

A. Idehaza az információ-technológiában még nem váltak szét határozottan a szakmai területek. Hasonló a helyzet, mint 150 éve az orvoslásban, mikor a fogorvos szülést vezetett le és fordítva. Statisztikáink mutatják, hogy hazánkban szignifikánsan több a szakértelem hiánya miatt bekövetkezett adatvesztések aránya az összes adatmentési feladathoz képest, mint az általános műszaki hagyományokkal rendelkező országokban. Valamilyen oknál fogva egy svájci bankban a rendszergazda, ha Novell problémával találkozik, akkor megnézi, hogy van-e Novell vizsgája, és az érvényes-e, és ha valamelyik kérdésre nemleges választ kap önmagától, akkor szakembert hív.

B. A hardver- és szoftvergyártók harsányan hirdetik, hogy ők óriások, a nekünk szánt termékük csodálatos, nélkülözhetetlen és hibátlan. Ha ezt elhisszük, akkor máris benne vagyunk abban a csapdában, hogy minden jó, és nincs mitől félni. Legyünk óvatosak az óriásokkal (és persze vakon a törpéknek se higgyünk)!

C. Zavaros világunkban még nem igazán kerültek felszínre azok a specializált szakértelemmel rendelkező

vállalkozások, amelyek körül kialakulhatott volna a szakmai bizalom légköre, és amelyek ennek a bizalomnak meg is tudnak felelni. Láthatóan a hályogkovácsok korát éljük, és ha így van, akkor sokan úgy gondolják, hogy az én hályogkovácsom még mindig jobb, mint a másé.

3. „Akinek kalapácsa van, az mindenhol szöget lát."

Adatmentéssel foglalkozunk. Minden olyan probléma érdekel minket, amikor értékes adatok elvesznek vírus, tűzeset, természeti katasztrófa, emberi mulasztás, vagy egyéb ok miatt. A feladatok jelentős része külföldről érkezik hozzánk, ilyenkor az adatvesztéshez tartozó történetet általában nem ismerjük meg, csak magát a műszaki problémát.

Azért vannak kivételek is.

Egy alkalommal az Interpool, rendőri kísérettel, küldött nekünk egy hatalmas ládányi számítástechnikai eszközt – pépes állapotban. A történet szerint valahol Nagy-Britanniában feltételezett értékpapír-hamisítókat lepleztek le (a gépek állapota arra utalt, hogy a leleplezés előtt úthengert alkalmaztak a hardveren). Este hétkor minket mint szakértőket arra kérték, hogy 12 órán belül válaszoljunk a következő kérdésekre:

· Ezek az eszközök alkalmasak voltak-e értékpapír hamisításra?

· Ha alkalmasak voltak, akkor hamisítottak-e velük?

· Ha hamisítottak, akkor mennyit?

A szakmai probléma úgy jelentkezett, hogy a winchester mechanikailag sérült volt, az adatállományok helyreállítása szóba sem jöhetett, de a mágneslemezekről helyenként apró részeket (szektorokat) el tudtunk olvasni. Olyan volt, mint amikor egy könyvet iratmegsemmisítőbe dugnak, és hogy ismét olvasható legyen, a fecnikből kell összeragasztani. De a fecnik egy jó része hiányzott. Reménytelen vállalkozás, pláne mindössze 12 óra alatt.

Azért megpróbáltuk. Hasonló (de nem pépesre vert) gépekkel mi is elkezdtünk értékpapírt gyártani, azaz beszkenneltük az értékpapírokat. Éjjel kettőre sikerült. Ekkor jött az ötlet! Próbáljuk meg a mi számítógépünkben tárolt értékpapír „képre" ráhelyezni az olvasható szektorokat. Mint egy puzzle-játék. Ha a néhány fecninek megtaláljuk a megfelelőjét a mi „képünkön", akkor előbb-utóbb kirajzolódik az értékpapír képe. Ez hajnali négyre olyan mértékben sikerült, hogy a bizonyításhoz elég volt.

A harmadik kérdésre (mennyi értékpapírt hamisítottak?) viszonylag könnyű volt válaszolni. Csak egy patikamérleg kellett. A mi gépünkön gyártottunk 1000 értékpapírt (egész csinosra sikeredtek), és lemértük, mennyi festék fogyott. A ládából előkerült üres festékpatronokból már meg lehetett becsülni, mennyi festéket használtak az úthengerezés előtt. Számításunk szerint hétszámjegyű volt az előállított papírok értéke. Fontban. Később értesítettek, megtalálták a hamis papírokat. Egész jó volt a becslésünk.

Tanulságként e történetből annyit levonhatunk, hogy a mágneses jelek eltüntetésére nem a kalapács a legmegfelelőbb eszköz.

4. Statisztika bikiniben

Az adatvesztés elkerülése érdekében leggyakrabban az alábbi kérdéseket szegezik nekünk:

· Melyek a legmegbízhatóbb adattárolók, winchesterek?

· Milyen jellegű hiba (hardver, szoftver) okozza a legtöbb adatvesztést?

A válasz elől nem kívánunk kitérni, de sajnos általános érvényű választ nem tudunk. A versenyhelyzet olyan mértékű előremenekülésre készteti a hardver/szoftver fejlesztőket és gyártókat, hogy a legjobbak kezei közül is kikerül egy-egy selejtes termék. Ilyenkor a gyártó és a kereskedő fut a pénze után, a végfelhasználó meg az adatait sírja vissza. Azt sem könnyű behatárolni, hogy egy vagy több esemény együttes hatására állt-e elő az adatvesztés. Az igazi katasztrófák nem is kezdetben, hanem a már beüzemelt, biztonságosnak hitt rendszerekben következnek be. Azt sem könnyű meghatározni, hogy egy vagy több esemény együttes hatására állt-e elő az adatvesztés Gyakran mi is rácsodálkozunk egy-egy új problématömegre, amikor nem tudjuk eldönteni, hogy a tányér egyenes-e, vagy a leves görbe.

Kiválasztottuk az 1998-as év több mint ötszáz hazai adatmentéséről készült statisztikát. Közreadjuk. Régebbre visszamenni nem érdemes, a 80 MB-os, vagy DOS-os problémák feltárása ma már nem hoz lázba nagy tömegeket. A külföldi adatmentések bevonása a statisztikai adatokba ugyancsak eltávolítana célunktól, mivel más adattárolók jellemzik – mondjuk – a német piacot, mint a hazait, a műszaki kultúráról, az emberi mulasztás miatt bekövetkezett hibákról már nem is beszélve. Az itt közölt számadatok kerekítettek, és százalékot jelen-tenek.

Az adatmentésre került adattárolók gyártók szerinti megoszlása:

Quantum 25, Seagate 20, WD 15, Conner 7, IBM 5, Maxtor 5, Fujitsu 5, egyéb (<5%) 18.

Az adattárolók kapacitás szerinti megoszlása:

<500 MB 23, 500 MB–1 GB 23, 1–2 GB 22, 2–8 GB 20, >8 GB 6, nem winchesterek 6.

Operációs rendszerek megoszlása:

Microsoft 73, Novell 17, MAC 3, Unix 2, OS 1, egyéb 4.

A felhasználók szerinti megoszlás:

Kereskedelmi 25, számítástechnikai 16, ipari 15, egészségügyi 7, lakossági 6, pénzügyi 6, oktatási 6, állami 5, média 4, mezőgazdasági 3, egyéb 7.

A meghibásodás környezeti oka:

Hardver jellegű 60 (ezen belül emberi mulasztásra visszavezethető 42), Szoftver jellegű 40 (ezen belül emberi mulasztásra visszavezethető 27, vírus 6, operációs rendszer 14, stb.)

Az adatmentés esélye:

Elméletileg lehetséges 78, nincs elméleti esély sem 22

Ezekre a statisztikai adatokra azért úgy kell tekinteni, mint a bikinire! Úgy tűnik, hogy kerek egészet látunk, de tudnunk kell, hogy a lényeg takarva maradt.

Fogalmunk sincs például arról, hogy az egyes adathordozókból mennyi került be az országba, csak arról van adatunk, hogy mennyiről kértek adatmentést.

5. „Három dolog tök biztos: a halál, az adózás és az adatvesztés"

Az élet úgy hozta, hogy a károsult általában egy-egy súlyos adatvesztés után kér fel bennünket adatvédelmi rendszerének felülvizsgálatára. Természetesen utólag mi is nagyon okosnak tudunk látszani. Az igazság az, hogy tudásunk nagy részét a hozzánk került káresetek nagy számából szereztük. Itt azokat a kikristályosodott gondolatainkat szeretnénk közreadni, amelyek általánosan értelmezhetők, függetlenül attól, mekkora rendszere és adatállomány-tömege van a kedves olvasónak. Mindössze három ilyen gondolatunk van, így könnyen megjegyezhetők. Habár ezeket nem is megjegyezni érdemes, hanem folyamatosan alkalmazni.

A. Másolni, másolni, másolni (a lenini gondolatok az informatika nyelvén)

A másolatokat különböző földrajzi helyeken őrizze. Egy épületből egyszerre szokták ellopni az értékeket.

Ha van több másolata, generáljon üzemzavart, majd próbálja meg újból felélesztени a rendszerét (a backupról). Szinte biztos, hogy meglepetések egész sora vár Önre.

B. Óvszerek folyamatos használata

Közvetlenül ne érintkezzék a külvilággal. Legalább egy, de jó, ha több vírusellenőrzőt használ. EXE fájlokat még ekkor se hozzon be kívülről. Az internetes óvszert tűzfalnak hívják. Ne legyen könnyelmű, használja. Viszont akkor is tudnia kell: ez is csak korlátozottan véd!

C. Ne essen pánikba!

Bármilyen rendellenességet észlel, jegyezze fel a történteket, az esetleges hibaüzenetet. Zárja le a rendszert. Gondolja végig, mi történt. Ne próbálkozzék önerőből. Vegye elő a katasztrófatervet (ha van), és aszerint cselekedjék, vagy kiáltson szakemberért.

Ha mégis úgy dönt, hogy önállóan cselekszik, akkor legalább két tanácsot fogadjon meg:

A háttértárolót (winchestert) iktassa ki a rendszerből, és vigyázzon rá, mint a szeme fényére. Tegyen be új tárolót, helyezze üzembe. Készítsen másolatot a backupról. A másolatot töltse be. Ha az 1. pontban leírt lenini eszmét megfogadta, nagy baj nem lehet.

Mielőtt adathelyreállító szoftvert (CheckDisk, Norton, Vrepair...) használna, ismét győződjön meg arról, hogy van másolata, és olvassa el a szoftverhez tartozó legalább 400 oldalas kézikönyvet. Megéri.

A tisztatér kibontása nem ajánlatos, a hibás adatot a mágneslemezen szabad szemmel nem könnyű észrevenni, ugyanis molekuláris méretű, a javítás így „apró" nehézségbe ütközhet.

A kedves olvasó itt úgy érezheti, hogy elvetettük a sulykot. Kérem, ne higgye. 1997-ben 14 darab szétszedett winchestert kaptunk abból a célból, hogy kíséreljük meg róluk az adatmentést. Ezek közül 6 darab számítástechnikai cégtől érkezett, 2 pedig pénzintézettől.

6. RAIDtörténet

Az eset Zürichben történt, az egyik vezető informatikai cég európai központjában. A központ vezetője leendő ügyfeleit kalauzolta, és a többi nagyszerű megoldással együtt bemutatta működés közben a nagy biztonságú adattároló szekrényt (RAID ARRAY) is. A bemutatás annyiból állt, hogy a működő rendszerből kihúzott egy fiókot: tessék, nézzék, nem csalás, nem ámítás, a mi rendszerünk még így is működik!

Sajnos a fiók kihúzása előtt valaki más már kihúzott egy másik fiókot a szekrényből, és ez így már sok volt – a rendszer hibajelzést adott. A központ vezetője ekkor első felindulásában lekapcsolta a hálózatról az adattároló szekrényt, visszadugta a fiókot, majd ismét bekapcsolta a szekrényt.

Ez az adattároló sok mindenre fel volt készítve, de erre az eseménysorozatra nem. Hibajelzéssel végleg leállt, és az európai központ működése megbénult.

Hozzánk 12 órán belül érkezett meg a berendezés. 16 GB adatot lehetett helyreállítani – vagy mindörökre elveszíteni. Elég az hozzá, hogy sok szerencsés körülmény összejátszása folytán az európai központ 80 órás kiesés után ismét működőképessé vált. Dollárban hét számjeggyel volt leírható e 80 óra vesztesége. Az ügy itt nem fejeződött be számunkra, de az esetnek vannak olyan tanulságai, amelyeket minden számítógép-felhasználó megszívlelhet.

Tekintsük katasztrófának azt a helyzetet, amikor a számítógépes rendszer utolsó működőképes állapotát elvárható időn belül a kezelőszemélyzet nem tudja helyreállítani. Az elvárható idő természetesen mást jelent egy banknál, mást egy könyvelő cégnél, és a könyvelő cégen belül is mást jelent a hónap elején, mint a hónap végén.

A lényeg az, hogy katasztrófahelyzetben a felhasználót súlyos veszteség éri.

A kérdés pedig az: Elkerülhető-e a katasztrófa?

Mit kellene tenni, és az mennyibe kerül?

Az adatmentési feladatok megoldásában szerzett tapasztalatunk azt mutatja, hogy a katasztrófahelyzetek legalább fele emberi hibára vezethető vissza.

Távol álljon tőlünk, hogy a szakembereket általános felkészületlenséggel vádoljuk. Nem erről van szó. Sokkal inkább arról, hogy bizonyos, ritkán előforduló helyzetekben, valamely döntéssorozat végrehajtása közben, ha csak egy lépés is hibás, előállhat a katasztrófahelyzet.

Hasonló felelősség terheli az atomreaktor vagy az utasszállító repülőgép irányítóját. Nagy értékű berendezés kezelését bízták rájuk. Csakhogy ők, mielőtt a valós rendszert irányíthatnák, szimulátorban próbálják ki alkalmasságukat. A szimulátor itt nemcsak rutinfeladatok begyakorlására szolgál, hanem arra is, hogy ellenőrizhessék a különleges helyzetekben hozott döntéssorozatok helyességét, és gyakorolják a hibátlan cselekvéssorozat lehető leggyorsabb végrehajtását. Meggyőződésünk, hogy sokszor egy szóló PC is megfelelő lenne egy-egy részprobléma szimulálásához, csak gondolni kellene rá.

Visszatérve a zürichi esetre, a központ vezetője, tanulva a történtekből, felkért bennünket: tartsunk rendszeres felkészítő oktatást neki és kollégáinak a katasztrófahelyzetek elkerülésének és túlélésének gyakorlati tudnivalóiról.

7. Szimulátor

A Szimulátor olyan eszköz, amely a valós rendszer körülményei között (de nem az éles adatokon) lehetőséget biztosít a kezelő számára, hogy vizsgálja a lehetséges zavaró hatásokat, és valós időben begyakorolhassa a szükséges intézkedéseket. A nagy értékű eszközök irányítóinak (pilóták, űrhajósok) felkészítésében ez régóta bevált módszer, de ugyanolyan fontos a számítógépes rendszerek kezelői számára is.

A Kürt Szimulátora PC alapú számítógéplabor, amelyben megtalálható minden, amire szükség van. Többféle szerver platform és munkaállomások, Token Ring és Ethernet hálózati elemek; szünetmentes áramforrások; Microsoft és Novell rendszerszoftverek; vírusvédő programok; Internet-csatlakozás; rendszerintegrálásban, adatvédelemben jártas szakemberek... Ez így együtt szinte bármilyen PC-s hálózat, rendszer összeállítására, szimulálására lehetőséget ad.

A rendszergazda a Szimulátorba beülve szembesülhet félelmeivel:

· Hardver- szoftverhiba esetén képes-e ismét működővé tenni a rendszerét?

· A backupból feléleszthetőek-e az adatok? Mennyi idő alatt?

· Milyen eszközök, mennyi idő szükséges egyes feltételezett hibák elhárítására?

· A távmenedzselés rendszerbe állítása milyen kockázattal jár?

· Új szoftver üzembe helyezésével milyen problémák jelentkeznek?

· Áramszünet esetén hogyan üzemel a szünetmentes rendszer?

Tény: a rendszergazda saját, élő rendszerét a maga jószántából nem teszi ki zavaró hatásoknak. Sőt többnyire meg van győződve arról, hogy az általa felügyelt eszközök tökéletesek. Amikor nagy ritkán hiba jelentkezik, azt több külső, előre nem látható hatás következményeként értékeli.

A Kürt évente legalább 2000 adatmentéssel kapcsolatos megbízást kap (ebből több mint 400 a hazai). Statisztikáink azt mutatják, hogy az esetek több mint 20 százalékában nincs megoldás. Az adatokat nem lehet helyreállítani, mert az adathordozón lévő mágneses jelek megsérültek, elvesztek.

Erről az oldalról nézve az évente 420 (ebből közel 100 hazai) szerencsétlenül járt, adatait vesztett ügyfél esete már semmiképpen sem tekinthető elszigetelt, egyedi problémának. Ennyi előre nem látható katasztrófa bizony elgondolkodtató. E nagy számok láttán befészkel az ember fejébe a gyanú: vajon az adott területek rendszergazdái rendelkeznek-e megfelelő stratégiával az adatvesztés kockázatának csökkentésére?

Valóban katasztrófa történt-e minden esetben, vagy egyszerűen csak felkészületlenségről van szó?

8. Karakterkáosz

Az értékes adatokat sok mindentől kell védeni, de leginkább az adatok tulajdonosától.

Ritkább eset, de előfordul, hogy a tulajdonos olyan védelmi rendszert épít adatai köré, amelyen már ő maga sem tud áthatolni. Az egyik francia autógyár fejlesztői azzal a kéréssel küldtek hozzánk egy ép adathordozót, hogy az általuk kreált védelmi algoritmust törjük föl. Gyanúsnak találtuk az ügyet, de kérésünkre kétséget kizáróan bizonyították, hogy ők a tulajdonosok, sőt elküldték a kódoló/dekódoló algoritmust is, amelynek segítségével sikerült több éves fejlesztő munkájukat nemcsak az ipari kémek, hanem önmaguk elöl is elrejteni.

Elmondásuk szerint kezdetben évekig kiválóan működött minden, majd időnként megjelent egy-egy ismeretlen karakter a programsorokban. Nem tulajdonítottak neki nagy jelentőséget, a hibákat kijavították, és minden ment tovább. A hibák idővel szaporodtak. Vírusra kezdtek gyanakodni. Valamennyi létező vírusdetektáló programot megvásárolták, kipróbálták. Csak a pénzük fogyott, a problémák száma nem csökkent. Aztán elérkezett az összeomlás. Természetesen mindenről volt másolatuk. A másolatot is megpróbálták visszaolvasni, az is összeomlott. Ekkor kerültünk mi a képbe. Olyan problémával találkoztunk, amelyhez hasonlókkal nap mint nap birkózunk, és amely a nemzeti karakterkészletek számítógépes alkalmazásával kapcsolatos.

A számítástechnika kezdetén egyértelmű volt a megfeleltetés a kijelzett karakterek és az őket leképező, digitálisan tárolt jelek között. Ez volt az ASCII kód – a betűszó az USA Szabványügyi Hivatalát jelzi. Sajnos ez a szabvány nem gondolt az összes létező, nyelvenként különböző karakterekre, ez persze nem is lehetett az USA Szabványügyi Hivatalának a feladata.

Nálunk például a nyelvőrök görcseit először a CWI (Computer World International) ajánlása oldotta fel, mely a magyar nyelvben használatos tizennyolc (9 kis és 9 nagy) ékezetes betűnek meghatározta a számkódját. Ezt a kódot a billentyűzet adott gombjaihoz lehetett rendelni (keyboard driver) és ki lehetett faragni a hozzá tartozó karaktert, például az „Á” betűt, melyet a képernyőn, vagy nyomtatásban látni kívántunk. Sajnos, a CWI-ből nem lett sem hazai, sem nemzetközi szabvány. A szoftverfejlesztő cégek nem vártak, elkészítették a különböző, úgynevezett nemzeti karakterkészleteket, illetve a felhasználóra bízták, hogy a végtelen számú lehetőségből melyiket választja ki

magának, amely természetesen sem az ASCII, sem a CWI készlettel sem került köszönő viszonyba. Sőt önmagával sem, abban az értelemben, hogy mindenki elkészítheti a neki tetsző összeállítást. Ez az oka annak, hogy a régebben vagy más környezetben írt szöveg hieroglifákkal jelenik meg a képernyőn vagy a nyomtatásban.

Visszatérve a franciákra, ők is ebbe a csapdába estek. Ahogy a fejlesztői környezetük, operációs rendszerük, szövegszerkesztőjük változott, úgy változott a kódolásuk, csak erről a gyártók őket nem értesítették. Az összeomlás akkor következett be, amikor a dekódolást a kódolástól eltérő környezetben végezték. És mivel bárki szabadon választhatja meg a neki legjobban tetsző nemzeti karakterkészletet, erre igen nagy esélyük volt. Eddig.

Amint visszakapták értékes állományaikat, szigorú intézkedést hoztak, a legapróbb részletekig kidolgozva, az intézményen belül egységesen használandó szoftverkörnyezetről. Ez a felismerés nekik sokba került.

9. Ékes betűk éktelen problémái

Nagyszerű dolog, hogy a ma legelterjedtebben használt számítástechnikai környezetben valamennyi ékezetes betűnk szinte minden betűtípusban megjeleníthető. Vége annak az időszaknak, amikor a Szárnyaló Bt-nek ékezetes betűk nélkül küldtek levelet, és ezért a címzett vérig sértődött.

Adataink biztonsága szempontjából azonban nagy árat fizetünk azért, mert írásjeleink egy része eltér az angol nyelvterületen használatosaktól. Az ékezetes betűk által okozott problémák részben a kellemetlenség kategóriájába tartoznak, részben viszont súlyos adatvesztéshez vezethetnek.

Szinte mindennapos eset, hogy egy régebben vagy más környezetben megírt szöveg hieroglifákkal teletűzdelve jelenik meg a monitoron vagy a nyomtatón. Ilyenkor a titkárnő infarktust kap. A számítástechnikus meg csak legyint, hókusz-pókusz, klikk ide, meg klikk oda, és lám csodát, minden ismét olvasható.

Az alapproblémát az okozza, hogy a magyar ékezetes betűk számítástechnikai környezetben való használatára született szabványt sem hazai, sem nemzetközi kör-

nyezetben nem vezették be. Ennek következtében ékezetes betűink szabad prédájává váltak a nagy gyártók programfejlesztőinek.

Magyarán: a nagy számban létező és használható betűtípusoknál csak a véletlen műve, ha minden ékezetes betűnket a számítógép következetesen egyazon módon értékeli.

A kesergésen túl e kellemetlenség megszüntetésére egy módszer van, ez pedig a házi szabvány kidolgozása és bevezetése. Egy hozzáértővel meg kell határoztatni azon szoftverek körét (operációs rendszer, szövegszerkesztő, táblázatkezelő, betűkészlet stb.), amelyek önmagukkal az ékezetes betűink szempontjából kompatibilisek, és attól kezdve csak ennek a használatát szabad megengedni a házi környezetben.

Új szoftver vásárlása előtt meg kell vizsgálni, tudja e kezelni a mi ékezeteseinket, és ha nem, milyen módszer van az eddigi ékezetesek átalakítására. Ha ez a környezet nagy, akkor bizony házon belül heves ellenállásra kell számítani az egységesítés miatt. Ilyenkor a titkárnő már elfeledkezik infarktusáról, hiszen alkotmányos jogának érzi a szabad szövegszerkesztő-választást.

Ennél lényegesen komolyabb problémát okoz az ékezetes betűk nem szövegkörnyezetben való használata. Ha például egy dokumentumnak az „árvíztűrő_tükörfúrógép.doc” nevet adjuk, akkor mindenkori operációs rendszerünket komoly nehézségek elé állítjuk.

Be kell látnunk, hogy a számítástechnikában használt betűk társadalmában a mi ékezeteseink csak másodrendűek, ezért nem azonosíthatóak minden esetben egyértelműen. Legjobban akkor járunk, ha az operációs rendszer eleve elutasítja ezt a névadást. Ha nem, akkor nekünk magunknak kell őrizkednünk tőle, különben csapdába kerültünk. Szinte biztosak lehetünk abban, hogy az operációs rendszer egy idő múlva elavul, lecserélik, és az új már vagy másképpen vagy egyáltalán nem fogja értelmezni a mi ékezetes fájlneveinket.

A tanácsunk az, hogy a házi szabványban rögzítve ki kell tiltani az ékezetes betűket a dokumentumok megnevezéséből és a könyvtárnevekből is.

Az is hasznos önkorlátozás, ha dokumentumaink megnevezése 8 karakternél nem hosszabb. Ebben a tartományban ugyanis a jó öreg DOS is értelmezni tud. Nem árt, ha a múlt ismeretében készülünk a jövőre.

10. „Tűzre, vízre vigyázzatok, le ne égjen adatotok!”

· 1993-ban a budapesti vásárváros hatalmas, könnyűszerkezetes B pavilonja kigyulladt és földig égett, benne a kiállítás-szervező vállalat teljes számítástechnikai rendszerével.

· 1995-ben a svájci rádió archívumának helyiségét elöntötte a víz. A hanganyagot több ezer digitális médián, szalagos DAT kazettán és optikai lemezen tárolták. A temérdek úszó kazetta látványa megdöbbentő volt.

· 1997-ben egy nagy német tervező cégnél hétvégén kilyukadt a fűtéscső, két napon át gőzölték a szerverüket és a mellette lévő archív anyagaikat.

· A fenti események közös jellemzője a katasztrófán és a je-lentős anyagi káron túl, hogy csodák csodájára nem történt adatvesztés. A tűzből, vízből és gőzből előkerült eszközök szigorúan meghatározott technológiai folyamaton mentek keresztül, és nem véletlenül. Ezeket az ügyeket ugyanis kü-lönböző biztosítótársaságok menedzselték. Ők futottak a pénzük után, és semmit sem bíztak a véletlenre. Helyzetük-ből adódóan jól ismerték a természeti károk csökkentésére kidolgozott technológiákat és az ezzel foglalkozó vállalkozásokat.

Felsorolunk néhány, ilyen esetben alkalmazott technológiát.

Konzerválás

Az adatok védelme miatt az eszközök szállításának előkészítése különleges gondosságot igényel. Az elázott szalagokat például úgy, ahogy vannak, egyesével, légmentesen csomagolják, hogy megelőzzék a spontán száradást és ezzel a felületek összetapadását, deformálódását. A reménytelennek látszó, összeégett adattárolókat (winchestereket) enyhe vákuumba csomagolják. Az adattároló zárt fémháza jó esélyt ad a benne lévő mágneses felületeknek a megmenekülésre. A vákuum hatására az apróbb égéstermékek a falhoz ragadnak, utazás közben nem karcolják az adathordozó felületeket.

Közömbösítés

Elsősorban a műanyagok égésekor keletkeznek savas kém-hatású gőzök, amelyek a fémeket erősen korrodálják, a forrasztási pontokat sem kímélve. A közömbösítési technológia alkalmazásakor lúgos, majd semleges kém-

hatású vegyszerrel kezelik a szétbontott számítógép minden egyes alkatrészét.

Felületkezelés

Az elázott szalagot egy, a hőfok és a páratartalom szempontjából szabályozott berendezésben, tisztító párnák között csévélik át folyamatosan mindaddig, amíg még nem deformálódik, de már nem is tapad, hogy ebben a pillanatban másolatot készíthessenek róla. A tűzből vagy tűz közeléből előkerült mágneses felületeket meg kell szabadítani a ráolvadt műanyagtól, koromtól, füsttől. Erre a célra kifejlesztettek egy speciális ultrahangos mosógépet, amely szinte molekuláris vastagságú rétegek eltávolítására is képes.

Ezen adatmentő technológiák alkalmazhatóságának legnagyobb ellensége az idő. Néhány napon belül a víz illetve az égés során keletkező maró hatású gázok által okozott korrózió olyan károsodást okoz a mágneses felületen, hogy az az adatmentést lehetetlenné teszi.

11. Adathullás

A magneto-optikai tárolóknál beköszöntött az ősz. Megkezdődött az adathullás. Kilószámra érkeznek hozzánk az olvashatatlan lemezek. Küldi a belga animációs filmstúdió, az olasz gépgyár és a magyar közigazgatás.

A magneto-optikai adattárolókat a 90-es évek elejétől használják tömegesen, elsősorban archiváláshoz. Nagy kapacitású, cserélhető lemezek, viszonylag olcsók. Többször írhatók és olvashatók, és jóval gyorsabbak a floppynál, a szalagos eszközökről nem is beszélve.

Tudtuk, hogy ezek a tárolók nem örökéletűek. A gyártók azonos helyre 1000–3000 hibamentes írást garantálnak, valamint 5–10 év hibamentes tárolást, ha a lemez nincs fényhatásnak kitéve. Mivel utólag egyik paraméter sem ellenőrizhető, csak sejtésünk van arról, hogy az adatvesztések az ígértnél lényegesen korábban következnek be.

Az adattároló lemez egy aránylag vastag műanyag korong, amelyet több, nagyon vékony és speciális tulajdonságokkal rendelkező réteg borít. Az egyik ilyen réteg mágneses tulajdonságú, ez rögzíti az információt. Ugyanennek a rétegnek egy másik fizikai jellemzője, hogy

mágnesezettségével együtt az optikai viselkedése is változik.

A feliratozás lézersugárral történik, oly módon, hogy a sugár felmelegít egy pici területet (cellát), és ezáltal ott a mágnesezettség megváltozik az alaphelyzethez képest. Az adathordozó anyag kettős fizikai tulajdonságát kihasználva, az olvasó egy optikai (foto-elektronikus) eszköz. Az adatok, hasonlóan a winchesterhez, koncentrikus körökön helyezkednek el. Mivel az adathordozó felület fölött védőréteg van, és az író/olvasó eszközök távol vannak a lemeztől, az adatkezelés mechanikailag igen biztonságosnak tűnik (ellentétben a winchesterrel).

Ezzel szemben a viszonylag kevés átírhatóság, a rétegekben elhelyezkedő, speciális anyagok eltérő hőtágulása, öregedése egy sor új hibalehetőséget teremt.

Vizsgálataink szerint az adatvesztést nem a teljes lemez, hanem csak egy-egy cella (bit) állapotának véletlenszerű megváltozása okozza. Ha ez a bit a rendszeradminisztráció területén van, akkor a gép számára a teljes lemez, ha az adatterületen van, akkor csak az adott állomány olvashatatlan. Nos, Murphy törvényei új fejezettel gazdagodnak. Először mindig az értékes bitek vesznek el, hiszen új adat beírásakor a rendszer-adminisztráció területére biztosan bejegyzés kerül, és az azonos helyre történő írások száma, mint említettem, korlátozott.

Az adatvesztés javítási technológiája általában nem okozna nagyon sok fejfájást. Talán hogy ne bízzuk el magunkat, megjelentek a 8, 16, 32 vagy akár 64 lemezt együtt kezelő 10–100 GB-os eszközök (jukebox), és ezeknél már – a nagy adatmennyiség miatt – a bitvadászat rengeteg időt emészt fel.

Tapasztalatunk az, hogy a szalagos tárolók is, noha más fizikai okok miatt, de hasonlóan viselkednek: idővel veszítik adataikat. A világ vezető gazdasági hetilapja, a Business Week 1999 áprilisi számában a CD-ROM-okról szedi le a keresztvizet. A gyártók által garantált 10 év helyett jó, ha 5 évig olvashatók hibátlanul, írja a lap. Ugyanakkor a Ricoh bejelentette: az általa gyártott CD-ROM 200 évig tárol hibátlanul.

Ezt azért ne várjuk meg – úgy félidőben, kb. 100 év múlva erről is készítsünk másolatot!

12. Jobb, ha forog

Zemancsik Béla (zema@drotposta.hu) kérdezte:

„A BIOS-ban a POWER MANAGEMENT SETUP-ban beállítható a winchester leállítása, ha egy bizonyos ideig nem használják. Gondolom, ez kíméli a winchestert, mert nem pörög állandóan. De egy olyan leírást is olvastam valahol, hogy a winchester akkor kopik a legjobban, amikor felpörög, mert akkor még nincs kialakulva a fejek alatt a légpárna, és a fej érintkezik a lemezzel. Vajon mikor kímélem jobban a winchesteremet, ha hagyom időnként (használaton kívül) leállni, vagy akkor, ha állandóan pörgetem?”

Tekintsük át röviden a winchester fizikáját.

Működés közben a fejet a lemeztől egy igen vékony (mikronnál kisebb) légpárna választja el, mely távolság elég nagy ahhoz, hogy a két test ne súrlódjon. Ugyanakkor lényeges, hogy ez a távolság kicsi legyen, abból a szempontból, hogy a mágnesezett forgó lemez mágneses tere a fej által mérhető legyen. Ha a fejben van egy tekercs, akkor olvasáskor ott áram indukálódik (Lenz törvénye), és az indukált áram nagyságát és irányát egyértelműen a forgó mágneses tér, azaz a fej alatt elmozduló mágneses jelek határozzák meg. Íráskor ez a folyamat fordítva játszódik le. A fej tekercsébe áramot vezetve annak mágneses tere átmágnesezi a mágnesezhető felület fej alatt elmozduló részét.

A folyamatos működés a motort és a csapágyat veszi igénybe. A gyártók szerint ezek akár 10 évet is kibírnak. Ha ennek a fele igaz, már az is bőségesen elegendő.

A ki-bekapcsolás általában nem jó a winchesternek. Indításkor, leálláskor a fej és a lemez összeér, súrlódik, kopik, és ez idővel legalább háromféle baj forrásává válik:

· A fejnek, mint a forgó lemez feletti és alatti légpárnán repülő testnek, az alakja megváltozhat, és ezzel a repülése bizonytalan lesz (itt akár a 200 km/h kerületi sebességről is szó lehet, mikronos távolságban a lemeztől, miközben – ugyancsak mikronos pontossággal – oldalirányban is irányt kell tartani).

· A lemezen megsérülhet az adathordozó mágneses réteg.

· A keletkező porszemek a fej és lemez közé kerülhetnek, és ez a Molotov-koktél hatásával egyenértékű.

A fentieknek megfelelően az indítások száma általában korlátozott a winchesterek életében (régi típusoknál 1000–3000, újaknál 30 000–1 000 000).

Mindössze néhány olyan konstrukció van, melynél kiküszöbölték e hibaforrást. Az egyik ilyen megoldásnál a táp kikapcsolásakor egy rugó a fejszerelvényt parkoló helyzetbe húzza, miközben egy fésűszerű szerkezetet betol a fejeket tartó karok közé, és így a fejeket annyira emeli meg, hogy azok a motor leállásakor ne súrlódjanak a felületen. Indításkor a fésű a motor felpörgéséig távol tarja a fejeket a lemeztől, és csak a légpárna kialakulása után engedi le a őket.

Összefoglalva: a winchester lekapcsolását a hordozható gépek akkumulátoros üzemidejének növelésére találták ki, de ez csak az akkumulátornak jó, a winchester szempontjából egészségesebb a folyamatos működés.

13. Nem mi találtuk ki

Buzás Ferenc (franz.max@mail.datanet.hu) Szegedről küldött egy elképesztő történetet. Íme:

„Történt, hogy a barátom, aki régóta szeretne érteni a számítógépekhez, gépet kezdett építeni, természetesen olcsó alkatrészekből. Vett is egy kiselejtezett 200 MB-os winchestert, de azt formázni nem tudta, mivel hogy a 0. track, 0. szektor hibás volt. Emberünk próbálta formázni alacsony szinten is, de a hiba többedszeri próbálkozásra sem szűnt meg.

Intelmem ellenére szétszedte a wincsit, hátha meglát (?!) benne valamit. Mivel látni nem látott semmit, gondolta, mélyebbre nyúl. Imbuszkulcsot ragadott, majd leszedte a lemezeket is, és összeforgatva, átrendezve visszatette azokat az íróasztalán. A nagy matatás után néhány ujjlenyomatot is fölfedezett a lemezek felületén, sőt hamudarabkákat is, mivel idegességében erősen dohányozott, ezért szarvasbőrrel mindent letörölgetett. Gondolván arra, hogy így megbolygatva az eszközt nem lesz minden rendben, a low level format előtt tápot adott, majd egy jókora hangszórómágnessel végigpásztázta a lemez felü-

letét. Ez lehet a „deep level format”, vagy „very low level format”.

Ezek után összekötötte a gépet az eszközzel, és majdnem teljes sikerrel megformázta azt! A formázás közbeni üzenetekből azonban arra következtetett, hogy valamelyik oldal eleje túl sok hibát tartalmaz. Ezért – természetesen az eszközt leállítva – értelemszerűen, csipesszel, a megfelelő oldal fejét beljebb görbítette. Újabb formázás, most már teljesen hibamentesen. Barátom azóta egyszerűen winchesterdoktornak titulláltatja magát, és fontolgatja a szegedi Trombita Kft. megalapítását.”

Első gondolatunk a történethez kapcsolódóan elég földhözragadt volt. Minek építettünk mi csillagászati összegekért a legszigorúbb amerikai szabványoknak is megfelelő, tisztaterű laboratóriumot, miért szereztünk be precíziós eszközöket, amikor elég lett volna egy íróasztal meg egy csipesz?

Komolyra fordítva a szót: a mai winchestergyártók nem adnak esélyt ilyen javítási technológiára. Ennek több oka van. Egyet megemlítünk.

Minden lemezt a gyárban feliratoznak: néhány ezer koncentrikus kört (szervo) mágneses jelek formájában felírnak egy-egy felületre. A winchester úgy működik, hogy a fej a megfelelő két szervo között olvassa, illetve írja az adatot. Ha a szervo felirat megsérül, például úgy, hogy átmágnesezik, a winchester minden hókuszpókusz ellenére is működésképtelen lesz.

14. Redfield és Wodehouse fordítója

Révbíró Tamástól (kilroy@matavnet.hu) kaptunk levelet. Ő író, műfordító, de számítógépes grafikával, animációval is foglalkozik.

„Önök állandóan azzal riogatnak, milyen sokféle módon veszíthetjük el becses adatainkat a magunk hibája vagy a sors kegyetlen szeszélye miatt. Arról azonban még kevés szó esett, hogy mit tegyen az az átlagos magánember, aki a lehető legkésőbb, vagy egyáltalán nem akar adatmentő cég ügyfele lenni."

Ha riogatunk, azzal csak az a célunk, hogy tudatosítsuk a számítógéphez vonzódókban: máig még senki sem találta meg az adatvesztés elkerülésének gyógyszerét. Ha ezt elhiszik, akkor már csak az a kérdés marad, hogy miképp csökkenthető az adatvesztés kockázata. Írásaink közvetve vagy közvetlenül ezzel a kérdéssel foglalkoznak, akár úgy, hogy egy-egy érdekes esetet ismertetünk, vagy ökölszabályokat írunk le, vagy az adatvédelem teljes rendszerét próbáljuk vázolni.

„Helyes gondolat-e például, ha a saját, vésztartalékként létrehozott másolataimat (floppyt, streamerkazettát, CD-t) időnként winchesterre másolom, majd visszaírom? Csökkentem-e ezzel az adatvesztés lehetőségét, vagy éppen ellenkezőleg, növelem?"

Az ön értékes adatai feltehetőleg szöveges és grafikai file-ok. Az ilyen típusú (nagyobb terjedelmű, elkészültük után ritkán változó) dokumentumok biztonságos tárolására ajánlatos, hogy:

· Legalább két másolatot készítsen.

· A másolatok legalább két adathordozón legyenek (például floppy és CD).

· Az adathordozók gyártója különböző legyen.

· A másolatokat legalább két helyen tárolja, távol egymástól.

· Évente olvassa vissza legalább az egyik másolatot, és készítsen újat.

· „Egyes babonák azt tartják, hogy mágneses adathordozót nem szabad a monitor közelében tartani, mert a képcső tekercseinek mágneses térereje tönkreteheti. Van ennek alapja?"

Igen. Nagy mágnes és erős mágneses tér van a monitor belsejében. A mágneses tér árnyékolt, de ennek ellenére nem tanácsolom, hogy közvetlenül a monitor tetejére tegye a floppyt vagy a kazettát.

„Az is érdekelne, hogy a gyárilag írt CD-ken is bekövetkezhet-e adatvesztés, vagy azok más eljárással készülnek, ezért biztonságosak?”

A gyári CD-ROM-ok más, adatvesztés szempontjából biztonságosabb eljárással készülnek, mint az egyedileg égetett lemezek. Ezeket elsősorban a mechanikai sérüléstől és a szennyeződéstől kell óvni. Sajnos az alapanyag öregedésével bekövetkező deformálódás a gyári lemezt is olvashatatlanná teheti. A gyártók 20 éves élettartamot hirdetnek, az adatvédelemmel foglalkozó szakemberek 5-10 évet jósolnak.

15. Okos embernek a nagyapja ültet diófát

Az adatvesztés esettanulmányai kivétel nélkül izgalmas történetek. E történetekben benne van az örök kérdés: Hogyan történhetett ez meg velem?, vagy Mit kellett volna tennem a baj elkerülésére?

Révbíró Tamás levele, melynek lényege: „ne tessék riogatni, inkább azt mondják meg, mitévő legyek!”, késztetett bennünket arra, hogy a teljes körű informatikai biztonsághoz csináljunk étvágygerjesztőt.

E témának a tudományos igényességgel megfogalmazott, teljességre törekvő, szabványban rögzített eljárások adják a keretét. Nem könnyű olvasmány.

Íme a népszerűsítő változat.

Mit jelent az adatok védelme? Mi az, amit védeni kell, mitől, és mindez mennyibe kerül?

· Vannak eszközök (gépek, hálózatok, programok), és vannak ezek segítségével kezelt input/output adatok, adatbázisok. Az értékes, védendő információ ezek terméke. Mondhatjuk: ez az informatikai biztonság tárgya. Ez a

kör elméletileg jól behatárolható, erre a körre megfogalmazhatók az általános védelmi feladatok.

· Az itt körülhatárolt rendszert sok külső és belső hatás éri. Ezek közül az ártalmasak: vírus, tűz, emberi mulasztás, szándékos károkozás, rendszerelem-meghibásodás, stb. Ezek a hatások mérhetők, becsülhetők, rendszerbe foglalhatók, vizsgálhatók, modellezhetők.

· A költségek általában peremfeltételként vagy célfüggvényként jelennek meg. Létezhet egy adott keret, amiből a védelmet meg kell valósítani, de a kérdés úgy is feltehető: mennyibe fog kerülni a kívánatos biztonsági szint elérése?

A korszerű adatvédelmi rendszereket az itt felsorolt három alapelemből gyúrják ki, és a mi szóhasználatunkban Informatikai Biztonsági Technológiának (IBiT®) nevezzük. Az informatikai biztonság azt jelenti, hogy az információtechnológiai (IT) rendszer valamennyi elemét külön-külön is és együtt is folyamatosan ellenőrzik az adatok védelme szempontjából, és a költségkereteken belül korrigálják a rendszert. A teljes vizsgálatot (auditot) általában egy külső, informatikai biztonsági tanácsadásra szakosodott cég végzi. Rávilágít az adatvédelem gyenge pontjaira, az adatvesztés és adatlopás kockázatára, meg még egy sereg kézzelfogható paraméterre. Mindez a felelős vezetők számára világos képet fest a pillanatnyi helyzetről, és kiindulópontot ad a jövő stratégiai döntéseinek meghozatalához.

A hangsúly a rendszeres belső és külső, valamint a részleges és teljes auditáláson és ez alapján az informatikai biztonsági rendszer folyamatos ellenőrzésén, módosításán, felülvizsgálatán van.

A világ olyan irányban halad, hogy a működőképesnek ítélt módszereket, technológiákat egységesíti, szabványosítja. Ez a folyamat játszódik le most az informatikai biztonság háza táján is. Az adatvédelmi rendszerek tartalmi, felülvizsgálatuknak formai követelményei, hasonlóan például az ISO 9000 szabványsorozat alapján kidolgozott minőségbiztosítási rendszerekhez, szabványosítva vannak, illetve a szabványosításuk folyamatban van.

Ahol az adatok komoly értéket jelentenek, ott súlyos gazdasági érdek fűződik az informatikai biztonság megteremtéséhez, legfeljebb ezt ma még nem mindenki ismerte fel.

16. Melyek az adatvesztés leggyakrabban előforduló okai?

Erre a kérdésre már többféle megközelítésből válaszoltunk. Most az eddigiektől eltérő módot választunk, nem hivatkozunk konkrét esetekre, statisztikákra, hanem az ezek ismeretében megfogalmazott általános gondolatainkat engedjük szabadon.

Az adatvesztés számtalan konkrét oka (tűz, víz, vírus, stb.) az adatokkal a következő három dolgot teheti:

A. Az adat nem került rá az adathordozóra, letörlődött, azaz nem létezik

Az adatok ilyenkor megsirathatók, más gyakorlati tennivaló nincs.

B. Az adathordozó eszköz meghibásodott

Az adatmentés szempontjából lényegében csak az adathordozó felület sérülése az, ami érdekes. Ha a felületi kár 1%-nál nem nagyobb, az adatmentő technológia képes a 100%-os helyreállításra, 5%-os felületi hibánál 50%-os a helyreállítás valószínűsége, 10% fölötti felületi hibánál szinte esélytelen az adatmentés. (Az itt leírt összefüggés magyarázatot igényel, erre majd később visszatérünk.) Tapasztalatunk szerint hardverhiba bekövetkezésekor az 1%-nál nagyobb felületi sérülés igen ritka. Ilyenkor a készülék serceg, nyikorog, rezeg, vinnyog. Mindezt normál esetben nem teszi. A nagy méretű felületi károsodást már a felhasználó és környezetének tudatlansága okozza! Csodavárás jogcímén többször bekapcsolják a készüléket, álszakemberek sora vizsgálódik, és az adathordozó felület minden ilyen alkalommal tovább károsodik.

A lábtörésnek futópadon végzett, többszöri diagnosztizálása okozna hasonló, visszafordíthatatlan károsodást. A hozzánk érkező hardveres problémák jelentős részére sajnos ez a jellemző.

C. Szoftveres hiba az adathordozón

Ha a felhasználót esetleg a „brutális” jelzővel illettük volna a hardveres probléma kezelésénél, akkor itt „gyilkost” kéne mondanunk. A nálunk landoló esetek jelentős része már átment a csodadoktorok kezén, használhatatlan adminisztrációs területet (FAT, MFT, könyvtár) hagyva maga után. Orvosi hasonlattal élve az agyat széttrancsírozták. E súlyos szavakhoz rövid magyarázatot fűzünk. Nem szeretnénk azt sugallni, hogy az adatmentő technológia segítségével mindig az első lépésben megtalálható a megoldáshoz vezető út, de ez a technológia előírja,

hogy az eredet állapotot meg kell őrizni. Ha az operáció sikertelen, vissza lehet nyúlni az eredeti állapothoz, és ez akárhányszor megtehető, mert az eredeti állapot nem változik. A helyreállított fájlrendszer pedig CD-re kerül és így a felhasználó ellenőrzésén fennakadó problémák is összevethetők az eredeti állapottal.

A kuruzsló (álszakember, csodadoktor), attól kuruzsló, hogy az eredeti állapotnál rosszabb, esetenként már visszafordíthatatlan helyzetet hagy maga után. A biztonságos gyógyítás a lényeg, nem az iskolai végzettség.

17. Cserebere

A pénz világában a rablások jelentős része a szervezetek belső munkatársainak műve. Ennek megfelelően a banki folyamatokban a szokásos védelmen felül a kezelőszemélyzettől védik leginkább a számítástechnikai rendszert. Ennek a különleges védelemnek egyéb előnye is van: a kezelőszemélyzet tudatlanságából eredően sem tud komoly galibát okozni.

Ahol nincs ilyen különleges védelem, ott megállapítható, hogy az adatvesztések legjelentősebb részéért maga a felhasználó a felelős. Ha már őt nem lehet eltiltani saját számítógépétől, akkor nincs más út, fel kell világosítani.

A közelmúltban történt: egy kisebb vállalkozás szerverében elektromos hiba miatt a winchesteren tönkrement az elektronikai panel. A problémát a helyi „szakember" diagnosztizálta. Ő nagy szerencsének érezte (később kiderült: óriási pech volt), hogy talált egy hasonló winchestert, amelyen hibátlan volt az elektronika. Nagyszerű, gondolta, és kicserélte a paneleket. A winchestert bekapcsolta, működött. Ezután, míg ő a jól végzett munka felett érzett örömét leöblítette egy sörrel, a számítógép a teljes winchester tartalmát, a programokat meg az adatállomá-

nyokat sorra összekevergette és törölgette. Ennél nagyobb bajt szándékosan is nehéz lett volna előidézni.

Mi történt valójában?

A winchester adattárolója nem más, mint néhány mágnesezhető felületű tárcsa. Ezekre a felületekre az író-olvasó fej, mint koncentrikus körökre (sáv) lát rá.

Felületenként akár 2-3 ezer ilyen körpálya is lehet. A winchester egy olvasási/írási ciklusban nem a teljes körpályát, csak annak egy részét (szektor) látja. Sávonként a szektorszám százas nagyságrendű, így egy winchesterben a szektorok számát legalább hét számjegy írja le.

A gyártás során a mai technológiákkal lehetetlen elérni, hogy mágnesezhetőség szempontjából a teljes tárcsafelület hibátlan legyen. Ennek megfelelően a gyártók, miután a winchestert összeszerelték, tesztelik a tárcsákat, és a hibásnak talált szektorokat kitiltják a használatból. Ez a kitiltás azt jelenti, hogy a hibás szektorok címét feljegyzik egy programocskába (firmware), amely állandóan felügyel arra, hogy ezeket a helyeket írásra vagy olvasásra ne használhassa a gép.

A gyártók ezt a firmware-t nagy előszeretettel helyezik el az elektronikai panelen. Ez a programocska természetesen csak egy bizonyos winchesterre jellemző, mint emberre az ujjlenyomat, hiszen a hibák helyéből adódóan minden winchesterre más és más működést ír elő.

A „szakember” azzal, hogy felcserélte a paneleket, összekeverte a használható illetve nem használható területeket. Azt sajnos senki sem garantálhatja, hogy minden tárcsa azonos helyen legyen gyártáshibás.

Az ötös lottót sokkal könnyebb eltalálni, ott nem kell milliónyi számmal bíbelődni.

18. Milyen a spájz?

Se szeri, se száma azoknak az eseteknek, amelyekben az adatvesztést a felhasználó tudatlansága okozza. Ezek közül jó néhány elkerülhető lenne, ha legalább azok tisztában lennének az adattárolás elméletével, akik a gyakorlatával foglalkoznak. Anekdotázás helyett most a PC világában alapvetőnek számító adattárolási ismeretek közreadására teszünk kísérletet.

Az adattároló eszköz (winchester, floppy, optikai tároló...) véges számú, egyértelműen meghatározható helyű és hosszúságú adattároló szakaszból (szektor) áll. Egy floppy lemezen ezernyi, egy winchesteren milliónyi ilyen szektor van. A szektor hossza általában 512 byte, vagy ennek egész számú többszöröse (kettő, négy vagy nyolcszorosa). A szektor hosszából látható: kicsi az esélye annak, hogy egy adatcsomag (fájl) egyetlen szektorba begyömöszölhető legyen.

Az első nekifutásra logikusnak tűnő elképzelés, hogy egy fájlt az egymás után következő szektorokon tároljunk, a szalagos tárolókat (streamereket) kivéve nem valósult meg. Ennek szervezési oka van. Óriási időveszteséget jelentene, ha minden egyes fájl módosításakor az adattároló tartalmának jó részét át kellene helyezni új helyre, annak függvényében, hogy a módosítástól rövidebb vagy hosszabb lett az adott fájl.

Ha nem ilyen egyszerű logika szerint történik az adattárolás, akkor hogyan?

Az adattárolás szervezéséért az operációs rendszer (DOS, Windows...) a felelős. Általánosságban elmondható, hogy minden operációs rendszer a saját adminisztrációs táblázatain (FAT, inode...) keresztül oldja meg a szervezést. Lényegében e táblázatok tartalmazzák azt az információt, hogy mely szektorokon és azok milyen sorrendjében tárolódik egy adott fájl. Ugyanezek a táblázatok adnak felvilágosítást arról, hogy hol vannak üres szektorok, amelyeket újabb fájlok tárolására lehet felhasználni.

Az adatvesztés elkerülése érdekében lényeges, hogy ezek az adminisztrációs táblázatok épek maradjanak. Ha megsérülnek, hasonló helyzet áll elő, mint amikor egy könyvtár anyagát iratmegsemmisítőbe dugják. Az egyes sorok (esetünkben: szektorok) olvashatóak, de annak kibogozása, hogy ezek mi-lyen sorrendben következtek egymás után, hogyan álltak össze fejezetekké és könyvekké (fájlokká), valamint katalogizált könyvtári rendszerré (directory), önsanyargató szerzeteseknek való, szinte remény-

telen feladat. A Holt tengeri tekercsek töredékeit összerakosgató tudósok jó ötven éve fáradoznak hasonlóval.

19. Matatás a spájzban

Az előző részben az adattárolásról írtunk. Ennek lényege az volt, hogy egy adatcsomag (fájl) az adattároló rekeszekbe (szektor) az „ahogy esik, úgy puffan” elv alapján kerül bele.

Az operációs rendszer (DOS, Windows...) által kezelt adminisztrációs táblázatok (FAT, inode...) tárolják azt az információt, amely megmondja a fájlkezelőnek, hogy hol vannak üres szektorok, ahol új fájlokat lehet tárolni, illetve a lefoglalt szektorokból milyen logika szerint lehet összeállítani az egyes meglévő fájlokat, hogy azok, mint programok vagy adatbázisok, használhatók legyenek.

Emberi segédlet szükséges ahhoz, hogy az újonnan üzembe helyezett adattárolót az adott operációs rendszer a sajátjának érezze. Programok segítségével lehet eljutni addig, hogy az üres adminisztrációs táblázatok az operációs rendszer részére rendelkezésre álljanak.

Particionálás (FDISK)

Ennek az eljárásnak a végrehajtása után az adattároló már alkalmas arra, hogy a számítógép őt felismerje, saját-

jának tekintse. Az eljárás alapvető mozzanata az adattárolónak a bemutatkozásra való felkészítése, az úgynevezett partíciós tábla elkészítése. Amikor a számítógép egy adattárolóhoz fordul, és az be tud neki mutatkozni, mert van partíciós táblája, akkor a gép ezzel a tárolóval a továbbiakban hajlandó együttműködni.

Formázás (FORMAT)

Formázással készülnek el az adott operációs rendszer adminisztrációs táblázatai (boot sector, FAT, inode...). Kijelölésre kerül a táblázatok helye, mérete és kezdő értékei, pont abban a formában, ahogy az adott operációs rendszer ezt megköveteli.

A formázás speciális esete az ún. alacsony szintű (low level) formázás, amelynek során a formázó program minden egyes szektort felülír valamilyen tesztkóddal. A formázásnak ez a módja igen időigényes, és utána biztos, hogy az adattároló előző életéből semmilyen adat helyreállítása nem valósítható meg. Egyes adattárolókat a low level formázás végérvényesen tönkretesz. Azokról a winchesterekről van szó, amelyek gyártója a gyárilag hibás szektorok kijelölését az operációs rendszer elől elzárt, de a formázó program számára hozzáférhető helyen tárolja.

Az eddig leírtak ismeretében világosan látható, milyen létfontosságú az adminisztrációs táblázatok épségének megőrzése az adatbiztonság szempontjából. A szándékos károkozók ezt pontosan tudják. A vírusok nagy része például itt fejti ki tevékenységét, mert itt kis beavatkozással is totális káosz érhető el.

Sajnos a rendszerterületek tönkretételére jó szándékkal is egyre több lehetőség kínálkozik.

Nem lehet törölni! Törölj néhány fájlt, hogy törölhess!

20. Még mindig a spájz

Az előző két részben körbejártuk az adattárolók szoftveresen legérzékenyebb területét, a rendszeradminisztráció táblázatait (FAT, inode...). Ezek a táblázatok biztosítják, hogy a pici darabokra tördelve tárolt adatcsomag részletei egységes egésszé álljanak össze, amikor a kedves felhasználó dolgozni szeretne velük. Az operációs rendszer kezeli ezeket a táblázatokat, általában hibátlanul.

És mi van akkor, ha...

A. Jön a szokásos lefagyás

Az operációs rendszer önmaga generálja a hibát, minek következtében lefagy a gép. Az első alkalommal hideg futkároz az ember hátán, aztán megszokja. Kikapcs-bekapcs, és újból lehet dolgozni, legfeljebb egy-két., a lefagyás előtt szerkesztett állomány odavész. Természetesen léteznek operációs rendszerek, amelyeknél ilyen jellegű hiba nem fordul elő, de nem ezek lettek a legelterjedtebbek.

B. Magunk keressük a bajt

A szokásos koreográfia: váltani kívánjuk az operációs rendszert, vagy módosítani szeretnénk az operációs rendszerek háttértároló (winchester) felosztását. Természetesen egy lépésben. Mivel az operációs rendszer egyedi rendszeradminisztrációs táblázatokkal rendelkezik, a változtatásnál ezek a táblázatok az új operációs rendszernek megfelelően átírásra kerülnek, és a régi táblázatok törlődnek. A gyakorlat azt mutatja, hogy az átírásba rendszeresen hiba csúszik, az új táblázat még nem, a régi táblázat már nem elérhető és minden odavész. Az egyik ilyen slágertermék a „Partition Magic" nevű program – áldozatainak se szeri, se száma.

C. Károkozás történt

A rendszeradminisztráció területei váltak a vírusoknak kedvenc terepévé. Itt ugyanis kis munkával jó nagy kárt lehet okozni. Persze nem kell nagy képzelőerő egyéb károkozási formák kivitelezéséhez sem.

Meggyőződésünk, hogy az átlagos felhasználó számára önállóan egyetlen lehetőség van: az értékes állományok rendszeres másolása, mentése, amíg lehet. Ha bekövetkezett a baj, azaz a rendszeradminisztráció terü-

letei megsérültek, akkor szakemberért kell kiáltani, mert véleményünk szerint ma nincs forgalomban olyan univerzális szoftvereszköz, amely szakmai ismeretek nélkül használható lenne az ilyen típusú problémák gyógyítására.

21. A két fantom

Nagyszerű cikk olvasható a PC World 1998. novemberi számában „Mentsük, ami menthető" címmel Makk Attila (makk.attila@idg.hu) tollából. A szerző nyolc pontban foglalja össze az adatvédelem tennivalóit:

1. Olvassuk el a kézikönyvet.
2. Mindennek járjunk a végére.
3. Titkosítsunk.
4. Rendszeresen mentsük az adatokat.
5. Használjunk víruskeresőt.
6. Alakítsunk ki kényelmes, biztonságos munkahelyet.
7. Személyesen is ügyeljünk az adatbiztonságra.
8. Tartsuk naprakészen ismereteinket.

A 6. ponthoz („Alakítsunk ki kényelmes, biztonságos munkahelyet") tartozó gondolatébresztő anekdotát itt is közreadjuk:

Egy nagy bank fiókjában esett meg, hogy az ügyintéző, egy csinos, formás hölgy panaszkodott: gépe rendszeresen zagyvaságokkal írja tele a képernyőt, a félig rögzített adatokat időnként „magától", önhatalmúlag eltárol-

ja, és olykor mindenfajta hibát jelez. A szakemberek mindent ellenőriztek. A gép rendben volt, a program is, kerestek vírust, szabotőrt, másik gépet állítottak be... Mindhiába.

Végül megnézték, hogyan folyik a munka, amikor a hiba előáll. Kiderült, hogy a hölgy az előtte felhalmozott papírokból vette el a lapokat a kódoláshoz. Ehhez kissé kényelmetlen mozdulattal előre kellett nyúlnia. Miközben előrehajolt a papírjaiért, keblével a billentyűzetre nehezedett, és ily módon gépelődtek a rejtélyes üzenetek.

Ez persze így mulatságosan hangzik, de képzeljük el, hány álmatlan éjszakát okozott a két „fantom" a biztonságért felelősöknek!

Lehet, hogy biztonságosabb lenne ezen a munkahelyen férfiembert alkalmazni?

22. Adatmentéshez repülőgép

Az adatmentési feladatok megoldásaira általában az a jellemző, hogy műszakilag bonyolultak, speciális és méregdrága eszközöket igényelnek. Ezenfelül a sikeres problémamegoldáshoz az is szükséges, hogy több szakmai terület különlegesen képzett szakemberei képesek legyenek együttműködni akkor, amikor a feladat elvégzésére viszonylag rövid idő áll rendelkezésre.

Közreadunk egy három éve megtörtént esetet, amelynek megoldásához a fentiekre nem igazán volt szükségünk.

Egy afrikai országból megkerestek minket, és sürgős segítséget kértek. Az adatok szigorúan titkosak, fizetik az utunkat és minden elképzelhető költségünket, a vízummal a repülőtéren várnak, azonnal induljunk. Kint megállapítottuk, hogy a nagygépes (mainframe) rendszerbe épített adattároló mechanikai hibás, a motor nem pörgeti föl a lemezeket. Az ilyen jellegű probléma megoldásához tiszta terű laboratórium szükséges. Abban az országban ilyen nem létezett. Az adattárolót, amely volt vagy húsz kiló, kiszereltük a gépből, és indulás Budapestre. Egy helybéli kétméteres biztonsági őr személypoggyászként hozta a

csomagot. A Ferihegyen baleset történt. Leszálláskor nagy huppanás, az adattároló eldőlt, és teljes súlyával a biztonsági őr lábfejére esett, átalakítva a csontok és izmok egymáshoz való, jól megszokott viszonyát. A követség kérésére rendőri kíséretet rendeltek volt ki, de az események után már mentőre is szükség lett. Két szirénával érkeztünk a városba.

A biztonsági őrt a János Kórház, a winchestert mi vettük kezelésbe. Szakembereink előkészültek az operációra, de a vizsgálatok néhány apró felületi sérülésen kívül semmilyen lényeges hibát nem jeleztek, a motor felpörgött, és minden működött. Egy óra alatt elkészültek a hibátlan másolatok az adattárolóról.

Mi történt?

Az adattároló tárcsák felülete teljesen sík, a felettük tizedmikronnyi távolságban repülő író/olvasó fejek felülete ugyancsak. Amikor a winchester kikapcsolt állapotban volt, ezek a felületek összeértek, és egymáshoz tapadtak. Ugyanúgy, mint két nedves üveglap. Az adott winchesterbe húsz író/olvasó fej volt beépítve; ezek letapadása miatt a motor nem tudott felpörögni, nem tudta a fejeket eltávolítani a tárcsákról. A gépből való kiszerelés, a szállítás vagy a poggyásztartóból való lepottyanás hatására a fejek elváltak a tárcsafelületektől, így már semmi szükség sem volt a szakértelmünkre.

A letapadás jelensége a gyártók számára is ismert, ezért a tárcsa felületének kialakításánál a legfelső réteget „érdesítik". Normál üzemben a tárcsa forgásakor kialakuló légpárna tartja távol a tárcsa felületétől a fejeket. Ki-be kapcsolásnál nincs légpárna, a fejek súrlódnak a tárcsán, és idővel elkoptatják az érdesített réteget. Ekkor következhet be a letapadás. Párás környezetben (például Afrikában) ennek nagyobb az esélye.

23. Ruha teszi az árut?

Manapság, ha egy kétdekás csokibogyót nem csomagolnak 10 dekányi négyszínnyomású sztaniolba, ellátva szlovén nyelvű használati utasítással és lengyel termékismertetővel, akkor a kereskedő roggyant dekoritlemezzel borított, soha nem tisztított pultjára az a csokibogyó nem kerülhet. Ezzel szemben a számítástechnikai csúcstechnikát árusító üzletekben, a króm és márvány portálok mögött a 30 000 forintos winchestert egy feltépett oldalú PVC zacskóban adják át a kedves vevőnek.

Mi az oka ennek a furcsa állapotnak?

Talán az, hogy a csokibogyó bejárja a számára előírt gyártási, értékesítési utat (gyártó, nagykereskedő, kiskereskedő, vevő), míg az idehaza vásárolt winchester még véletlenül sem. Ezt vakon állíthatjuk. A hazánkban eladásra kerülő winchestereket általában nem közvetlenül a végfelhasználónak, hanem a számítógépgyártóknak szánják, ennek megfelelően húszasával-ötvenesével ömlesztve csomagolják. A csomagolás így biztonságos; a baj akkor van, ha a kedves vevő nem a teljes rekesznyi árut veszi meg.

Mielőtt túlzottan belebonyolódnánk az ügybe, és a kereskedők felháborodva írnának, hogy hitelt rontunk, szeretnénk elhitetni, hogy ez az írás az ő érdekükben (is) született. Magyarán: rengeteg pénzt spórolhatnának, ha a winchestereket átcsomagolnák antisztatikus zacskóba, és szivacsos kartondobozba – természetesen egyenként. A garanciális gondok jó része elkerülhető lenne. Persze az igazi megoldás az lenne, ha végfelhasználóknak készített winchestereket árusítanának. Ilyen is létezik, csak drágább beszerezni.

A fenti csomagoláskultúrának (vagy kulturálatlanságnak) egyéb veszélye is van. A kedves vevő úgy érezheti, hogy a winchester az egyetlen termék, amelyet nem kell védeni, hiszen így látta annál a kereskedőnél, akiben ő megbízik.

Egy ügyfelünk a napokban két winchesterét hozta adatmentésre. Nagy csokor virággal állított be, az ügyfélszolgálaton dolgozó hölgyek nem kis örömére. A virág kézben, gondosan papírba csomagolva, míg a két winchester egy reklámszatyorban, pucéran, folyamatosan egymáshoz koccanva utazott.

„Minek vigyázni rá, úgyis rossz” – gondolhatta, és nagyot tévedett. Gondatlan kezelés, hiányos, nem szakszerű csomagolás esetén vagy az elektronikai panel, vagy a

mechanika, vagy mindkettő szinte biztosan tönkremegy. Egyszerűbb esetben a winchester ára, legalább 30 000 forint van kidobva az ablakon. Ha különleges típusról van szó, és ezért nem szerezhető be már ilyen, akkor az ára az adatmentés szempontjából végtelen.

És mindez azért, mert a kereskedő a történet elején ömlesztve vásárolta az árut, és megspórolta egy fél szál rózsa árát.

24. A csodálatos particionáló

Történeteinket általános alannyal és általános tárggyal írjuk, ilyesformán: valaki valamit valahol elkövetett. Ezt önvédelemből tesszük. Tudjuk, hasznos lenne, ha egy-egy konkrét termék adatvesztési képességét alaposan kitárgyalhatnánk. Lenne miről írni. Mindössze kétszer szegtük meg érintőlegesen e szabályt. Egy hardver-meghibásodás kapcsán írtunk a Novell 3.11 összeomlásáról. Írhattunk volna bármi másról, de az adott esetben a Novell volt ott, az adott esetben teljesen vétlenül. A Novellt hivatalosan védők és érte önként áldozók le is szedték rólunk a keresztvizet. És felhívtuk a figyelmet egy kiváló termék, a Partition Magic nem szakszerű, nem elővigyázatos használata esetén bekövetkező rengeteg adatvesztési lehetőségre is. Ez a program nem egy agyoncsicsázott termék, de gyors és kényelmes abban az esetben, ha a használatos operációs rendszereink adattároló felosztását változtatni akarjuk.

Közreadunk egy részletet Horváth László leveléből (stuba@freemail.c3), aki arról ír, hogyan kell a Partition Magic programot használni anélkül, hogy adatvesztés bekövetkezne:

„...Otthoni gépemen most 4 operációs rendszer van feltelepítve a 6.2 Gb-os winchesteremre, és a Linux kivételével a területeket a PM segítségével hoztam létre.

Természetesen a fontos dolgaimat rendszeresen lementem, és sokszor telepítem ismételten a rendszereket. Eddig semmi problémát nem okozott a winchester feldarabolása, és csak ezzel a módszerrel tudom kipróbálni az állandóan megújuló dolgokat. Kipróbáltam már több partícionáló programot, de kezelhetőség, sebesség, méret, sőt biztonság tekintetében ez volt a legjobb.

Még egy kiegészítés: meg kell jegyeznem, hogy csak az alapvető funkciókat használom, így például még sosem konvertáltam úgy partíciót, hogy azon adatok lettek volna. Inkább töröltem és ismét létrehoztam...”

Ja, ha valaki érti a szakmáját, annak nem tudunk újat mondani.

25. Töményen, poén nélkül

Az eddigi történetek esszenciáit csokorba gyűjtöttük.

Íme:

1. Védd a portól eszközeidet. Ne tedd a padlóra a gépet. A monitort, billentyűzetet takard le, ha nem használod. A printert is.

2. Szakmailag felkészült, vizsgázott szakembereket alkalmazz.

3. A mágneses jeleket mágnessel lehet eltüntetni.

4. A hazai adatmentések 78%-ban sikeresek. Az esetek 22 százalékában nincs megoldás.

5. Legyen sok másolatod. Védekezz (több módszerrel is) a vírus ellen.

6. A RAID rendszer a szokásosnál nagyobb biztonságot nyújt, de ez sem 100%-os. Jó, ha van mögötte backup.

7. A személyzetnek legyen lehetősége a különleges helyzetek gyakorlására, a megmérettetésre. De ne az élesben működő rendszeren!

8. Titkosítsd értékes adataidat.

9. Az ékezetes betűk használatához készíts házi szabványt. Csak szövegkörnyezetben használj ékezetes karaktereket. A fájl- és könyvtárneveknél nagy veszélyt jelentenek. Tartózkodj a 8 karakternél hosszabb fájlnevektől.

10. Különleges gondossággal vigyázz a sérült adattárolóra. Ne szedd szét.

11. Optikai tárolók, CD lemezek használhatóságának időtartama jó, ha fele a gyártók által ajánlottnak.

12. A winchester élettartamát a ki- és bekapcsolások általában csökkentik.

13. A mai winchestereknél a tisztatéren belüli javításnak szokványos szerviz környezetben nincs esélye.

14. Az archivált adatokat is érdemes időnként (pl. évente) újból másolni.

15. Létezik tudományos igényességgel kidolgozott, úgynevezett Informatikai Biztonsági Technológia.

16. Csak akkor próbálkozz adatok helyreállításával, ha az eredeti, (hibás) állapotot meg tudod őrizni. A legsúlyosabb, esetenként végzetes állapotokat nem a számítástechnikai eszközök hibái, hanem a javítási próbálkozások idézik elő.

17. Winchestert elektronikai panel cseréjével javítani – az adatokra nézve életveszélyes lehet.

18. A rendszer-adminisztrációs táblázatok épségének megőrzése mindennél fontosabb.

19. Alsó szintű (low level) formázással esetenként a winchester örökre tönkretehető.

20. A rendszeradminisztrációs táblázatokat átíró segédprogramok használata csak komoly szakértelemmel és szigorú védelmi intézkedések betartásával járhat sikerrel.

21. Alakíts ki kényelmes munkahelyet.

22. Párás környezet jelentősen csökkenti az adattároló élettartamát. Legalább évente cseréld le (vagy a környezetet, vagy az adattárolót).

23. Az adattárolót gondosan csomagolva szállítsd, még akkor is, ha rossz.

24. Meglévő rendszer átparticionálása előtt készíts másolatot a teljes rendszerről.

26. Dátum okozta meglepetések

A 2000. év problémáját boncolgatjuk utólag, az adatvédelem szempontjából. Kétségesnek tűnhet, hogy érdemes erről beszélni, hiszen 2000. január 1. már elmúlt. De hát számítógépben tárolt dátumok továbbra is lesznek, és még évek múlva is léteznek majd olyan állományok, amelyek rögzítési időpontja 1999. december 31. előtti.

Három esetet mesélünk el, adatmentési szempontból ezek mindegyike sikerrel zárult.

A. Egy könyvelést is tartalmazó számítógépes rendszeren valaki 1998-ban kipróbálta, mi lesz, ha 2000 lesz. Átállította a gép óráját. Pechjére a rendszer helyesen kezelte a dátumot: tudta, hogy a 2000 nagyobb, mint az 1999. A könyvelőprogram szétnézett a gépben, és észrevette, hogy a könyvelési tételek egy évnél régebbiek – ugyanis 1998-ból származtak –, ezekre a 2000. év könyveléséhez semmi szükség. Ennek megfelelően automatikusan, egyesével törölte mindet. Másolat nem készült, a könyvelőprogram egyedi készítésű volt, a programozót nem lehetett fellelni. Matt. Pedig a 2000. év még el sem kezdődött.

B. Egy pénzintézetben olyan szoftvert vásároltak, amely a 2000. év problémáját diagnosztizálja különböző szempontokból. A szoftvert lemásolták, az eredetit biztonságos helyre elrakták, és a másolattal elkezdték a diagnosztizálást, ami teljes káoszt okozott a rendszeradminisztrációs területekben. Ez ráadásul a szoftvergyártó szándékai szerint történt: így védekezett az illegális használat ellen. A pórul járt felhasználó utóbb elolvasta a szoftverhez tartozó leírást, és megtalálta benne a virágnyelven megfogalmazott közlést, mely szerint „másolat használata esetén esetleges problémák jelentkezhetnek”.

C. Egy jól képzett egyetemista diplomamunkája írása közben letöltötte az Internetről az egyik operációs rendszer gyártójának a 2000. év problémáját javító szoftverét. Igen ám, de az ő gépén ezen felül még két másik operációs rendszer is tartózkodott, erről azonban a javító szoftver nem vett tudomást. A következő bekapcsoláskor a gép rendszerhibát jelzett, és nem indult el. A fiatalember elment a számítógépe szakszervizébe, ahol a rendszerhibát konstatálva újratelepítették a javított operációs rendszert. Ez volt a legbiztosabb módszer arra, hogy a diplomamunka minden adata szétzilálódjon.

Tanácsunk a dátumproblémával kapcsolatos vizsgálatoknál is ugyanaz, mint minden más esetben, ha gépün-

kön új helyzetet állítunk elő: a régi állapotról másolatot kell készíteni! Az, hogy egy szoftvert ellenőrzésre, javításra fejlesztettek, nem jelenti azt, hogy ellenőrizetlenül ráengedhetjük a működő rendszerre.

A Windows észlelte, hogy az Ön számítógépe 12 hónaposnál öregebb. A megfelelő működéshez a Windows 98-nak újabb gépre van szüksége. Kérjük, frissítse a konfigurációt.

27. Hasonló jókat kívánunk

Vírus. Undorító szörnyeteg. A készítője is, ha belegondolunk a lelkivilágába. Elkészíti gyalázatos alkotását, majd szétküldi, és röhög a markába. Aztán lerohan vásárolni, és a boltban kilométeres sor áll, mert a vírusa feldúlta a raktárnyilvántartást. Ne adj' Isten, meglátogatja anyukáját a kórházban, ahol teljes a káosz, mert a gyógyszerkészlet nyilvántartása is fejreállt. És ezt a sort a végtelenségig lehetne folytatni.

Április 26-án rendszeresen végigvonul a világon a CIH vagy Csernobil nevű vírus, amely a legelterjedtebb operációs rendszerekbe (Win95, Win98...) fészkeli be magát. A legjelentősebb vírusellenőrző programok legújabb verziói fel vannak készülve rá, mégis felmérhetetlen károkat okoz. A CIH tevékenysége abból állt, hogy az adattároló elejéről – 1-től 100 MB méretű területet – véletlenszerűen letöröl.

A megtámadott operációs rendszereknél minden esetben a letörölt területre kerül az a táblázat, amely nyilvántartja az adatállományok darabjainak az adattárolón való elhelyezkedését. Úgy működik ez, mint – teszem azt – egy számítógéppel irányított gyógyszerraktár, ahol a jobb

helykihasználás miatt bármelyik áru bárhova kerülhet, de az „agyközpontnak” pontos információja van minden áruról és az üres helyekről is. Ha az agyközpont – esetünkben az operációs rendszer – megsérül, csak a teljes és pontos leltár képes az eredeti helyzet visszaállítására.

Az apró problémát az jelenti, hogy egy ilyen winchesteren tárolt „raktárban” akár 18 milliárd (nem tévedés, a 18-at kilenc darab nulla követi) áru is lehet, amelyek ráadásul nem viselnek feliratot, így a hashajtót az aszpirintől nem egyszerű megkülönböztetni. Az adatmentő laboratórium felkészültségén, tapasztalatán múlik, hogy a hashajtó és az aszpirin szétválasztása csak nagy valószínűséggel vagy pontosan végrehajtható-e. És ez nem mindegy.

Kulcskérdés még az is, hogy a szétválogatás mennyi idő alatt hajtható végre. Ha a válogatás teljesen automatikus (kidolgozott technológiája van például a „súly, szín, méret” szerinti válogatásnak), tehát a legkorszerűbb eszközök alkalmazását feltételezve, ilyen bődületes mennyiség átvizsgálása akkor is legalább három napig tart. És erre az időre a fent említett kórház jószerivel működésképtelen. Ha a válogatás nem automatizálható, (mert a hashajtó és az aszpirin színe, súlya és mérete azonos), akkor az idők végezetéig tarthat a vizuális (vagy ízleléses) eljárás.

Amit ajánlani szeretnénk az értékes adatok használóinak: vásároljanak vírusellenőrzőt, akár több fajtát is, és rendszeresen frissítsék. Ezzel együtt használjanak hosszabb időtartamot átölelő mentő (backup) rendszert. Így jelentősen csökkenthető a károkozás kockázata.

A vírus készítője pedig naponta látogassa anyukáját a kórházban. Vagy – még inkább – fordítva.

28. Lopni is csak tiszta forrásból

Az illegális szoftverhasználat is vezethet adatvesztéshez. A történteken még az sem segít, ha a felhasználó nincs tudatában annak, hogy az általa használt szoftver nem jogtiszta. Megtörtént eseteket sorolunk fel.

Szoftver upgrade – azaz frissítés, korszerűsítés. Hurrá, újabb verziójú, kényelmesebben használható operációs rendszerem lesz, gondolta a felhasználó, és megkezdte a telepítést. Ahogy az a nagy könyvben meg volt írva, lépésről lépésre mindent precízen végrehajtott. A telepítő szoftver is tette a dolgát, a régi részeket törölte, és az új részekkel felülírta. Mindez az utolsó lépésig nagyszerűen ment. Ekkor ugyanis a szoftver megkérdezte a felhasználó azonosító számát („user identification number"), amelyet az eredeti szoftverrel együtt kellett volna megkapnia. Csak hát ilyet a kalózpéldányhoz nem mellékelt senki. Így az új operációs rendszer nem került működőképes állapotba, a régit meg az új már részben letörölte. Passz.

A másik történet szokásosan indult. Az adattároló meghibásodott. Elsőre idegesítőnek tűnt a helyzet, de ott állt a drága hardvereszközökkel telepített archiváló rendszer, hogy a több éves fejlesztések adatait és a cég pénzügyeit gondosan tárolja. Sajnos nem elég gondosan. Az archiválást végrehajtó szoftvert ugyanis időkorlátozással vették (kapták) – azzal a megkötéssel, hogy csak egy bizonyos határnapig működik. Ha úgy ítélik, hogy bevált, kifizethetik a használatba vételért járó összeget, és megkapják az időkorlátot feloldó kódot. Ez az apróság elkerülte az érdekeltek figyelmét, az archiváló szoftver pedig a határidő lejárta után az értékes adatok helyett hexadecimális nullákat rakott el több gigabájtnyi mennyiségben.

Ja, kérem, a mai világban ilyen olcsón és áfamentesen ennyi hexadecimális nullát kapni, az azért nem semmi.

Az igazsághoz tartozik, hogy ilyen, időkorlátozással vagy mennyiségi korlátozással védett szoftverek az Internetről vagy reklám CD-kről szabadon leszedhetők, csak a fizetésről, a regisztrációról nem szabad megfeledkezni. A „shareware" és a „freeware" közötti különbség olykor jól érzékelhető – egy idő után például hexadecimális nullákban manifesztálódhat.

29. Y2K

Ezt írtuk 1999-ben:

A 2000. év dátumproblémája lerágott csont. Mármint a sajtóban, nem a valóságban. Fel kell kötnie a gatyáját annak, aki újat akar mondani róla. Felkötöttük.

Itt és most csak az adatvesztés kockázatának csökkentéséről szólunk. Azon belül is csak arra a problémára koncentrálunk, amelyet a számítógépekben a hibás dátumszámoló algoritmusok generálnak majd – és nemcsak január elsején, hanem attól kezdve folyamatosan. Minden nap éppen annyiszor, ahányszor megkérik őket, hogy számoljanak. Ezek az algoritmusok úgy fognak működni, mint megannyi vírus: hibás, a valóságnak nem megfelelő számokat fognak előállítani.

A vírus-analógia azért is helyénvaló, mert ezek a hibás, dátum típusú számok aktivizálódni fognak. Mikor? Amikor a programok ezekkel a téves – akár negatív! – számokkal dolgozni kezdenek, olyan adatbázist hagyva maguk után, amelyből már nem lehet kibogozni, hogy mi, mikor és hogyan okozta a problémát. A megelőzésnek egy ésszerű, ma leggyakrabban alkalmazott módját ismertetjük, amely a dátumszámoló algoritmus helyének felderítésére koncentrál.

Hardver

Több ezer diagnosztizáló program jelent meg, egy részük ingyen letölthető. Minimálisan arra adnak választ, hogy a gép órája 2000-ben is megfelelően fog e működni, vagy sem. Az intelligensebbek nemcsak a vizsgálat idején jeleznek, hanem beülnek a rendszerbe, és folyamatosan figyelnek. Ez nagyobb biztonságot (kisebb kockázatot) jelent, mert arra senki sem vehet mérget, hogy az egyszeri vizsgálatnál a dátumszámoló algoritmus minden ága kipróbálásra kerül. Persze ezek a rezidens szoftverek már fizetősek. Gépenként akár 5-10 ezer forint is lehet az áruk. Egyes gépeknél, ahol flash BIOS van, a gyártók támogatást adnak a gyógyításhoz, a hibás rész lecseréléséhez. Jó, ha ezt a műveletet szakember végzi, mert nem nehéz az alaplapot örökre tönkretenni.

Operációs rendszer (OR)

Az OR gyártói készítették vagy fogják készíteni a javító szoftverecskéket. Sajnos van olyan, aki még – például a

magyar nyelvű változatához – nem készítette el. Ennél rosszabb az, aki kijelentette, hogy nem is fogja. A szegény Win3.x magyar változata is erre a sorsra jutott. Ha több OR van egy gépen, előfordulhat, hogy a javító programocskák egyikben-másikban elkavarnak valamit, amire már volt is példa. Ajánlatos tehát elmenteni a teljes rendszert, mielőtt a javítóprogramot ráeresztjük.

Felhasználói szoftverek

Ez a leginkább szerteágazó, tehát legzavarosabb terület. A legnagyobb gyártók elkészítették (vagy ígérik, hogy elkészítik) a javítókészletet. Nagy számban vannak forráskódú programokat ellenőrző programok. Különböző tesztelő, szimulációs rendszerek is ismertek a diagnosztizálásra. Ennek ellenére a probléma megoldásának az lehet a legkézenfekvőbb formája, ha lecseréljük a felhasználói szoftvert.

30. Y2K egy év múlva

Ezt írtuk 2000-ben:

Szeretnénk most azt sugallni, hogy az Y2K probléma megoldásával foglalkozni még ma sem késő, illetve soha nem lesz késő, csak az idő múlásával egyre több kellemetlenséggel kell majd szembenézni.

Mire gondolunk?

Az egyik legnagyobb banknál – abban az alrendszerben, amely az ügyfelek számítógépes kapcsolaton keresztüli tranzakcióit kezelte – káosz keletkezett. Az utóbbi napokban az ügyfelek a szokásosnál lényegesen több érvénytelen (nem banki napra vonatkozó) tranzakciót próbáltak lebonyolítani. Az ügyfél oldalán a szoftver jelezte, hogy 1999 után 1900 következik, de ennek ellenére továbbította a kért dátumra előírt tranzakciót. Na bumm, akkor mi van? – mondhatnánk. Csakhogy 1900-ban a hétköznapok más dátumhoz kapcsolódtak, mint 2000-ben. A bank oldalán a probléma úgy jelentkezett, hogy seregével kapta a szoftvere által szombatinak és vasárnapi-

nak értelmezett átutalási megbízásokat, amelyeket természetesen nem teljesített, hiszen az ő számítógépe is 1900 dátumaihoz kapcsolta a napokat. Néhány nap alatt több tízezer tranzakció futott ebbe a zsákutcába.

Magát a problémát felismerni nem volt nehéz. Kijavítani sem. Pénz- és presztízsveszteséget jelentett viszont az elmaradt tranzakciók végrehajtása és az ügyfelek meggyőzése arról, hogy a történtek ellenére a bank biztonságosan működik.

A kedves olvasó gondolhat arra, hogy badarság ez az egész, hiszen a média csak arról beszél, hogy semmilyen lényeges Y2K probléma nem jelentkezett. Ezt a kérdést szeretnénk gyorsan elintézni azzal, hogy ma senkinek sem érdeke feltárni, milyen veszteségei voltak vagy lesznek a nem megfelelő Y2K felkészülés miatt. Illetve – ahogy az lenni szokott – a jelentkező veszteségeket nem az Y2K rovatban fogják elszámolni.

31. Hiszti

Jó sok levelet kaptunk a dátumváltási probléma (Y2K) kapcsán. E levelek egy részének a mondanivalója az, hogy a hisztériakeltés jó üzleti fogás volt, semmi több. Néhány idézet:

„Az a tény, hogy a világban semmi jelentős esemény nem történt, azt bizonyítja, hogy az Y2K csak egy felfújt léggömb volt." – „Ez az egész cirkusz csak az embereknek örökös félelemben való tartására és a valódi változások elrejtésére alkalmas taktika." – „Sajnos ti is, ismeretlen barátaim [értsd: a Kürt dolgozói], ti is beálltatok a sorba, és szítottátok a tüzet. Lehet, hogy sokat kerestetek vele, de elgondolkoztatok-e valaha is azon, hogy mi volt az értelme?"

Valóban elég sokat kerestünk, és el is gondolkodtunk. Ezekből a gondolatokból egy csokorra valót közreadunk. Azt persze nem állítjuk, hogy a tömegtájékoztatás ezektől a gondolatoktól lenne hangos.

A. Az Y2K probléma valóságos volt, és ma is az, csak éppen előre senki nem tudta és most sem tudja felmérni a hatását. Melyik felelős vezető vállalta volna annak a koc-

kázatát, hogy semmilyen intézkedést sem tesz ebben a helyzetben?

B. Az Y2K probléma nem felmérhető hatása miatt a világ legjelentősebb rendszereit (így a magyarországi szolgáltatási rendszereket is) átvizsgálták. Ezeknek a vizsgálatoknak az eredménye óriási jelentőségű:

– egy sereg rendszerhibára fény derült,

– elavult rendszerelemeket lecseréltek,

– lehetőség volt fejlesztésekre (amelyek az Y2K kényszere nélkül elmaradtak volna).

C. A Gartner Group egy 1998-as jelentésében azt írta, hogy a legfejlettebb országokban a rendszerek (egészségügyi, szolgáltatói, adminisztratív...) működési hibái miatt az állampolgárokat évi 2–3 atrocitás éri. A közepesen fejlett országokban (a miénk ide sorolható) ez évi 200–300. Csak az Y2K probléma miatt várhatóan évi 2–3 újabb rendszerhibát fog észlelni a polgár. Ez a fejlett országokban a lakosságot alapvetően érinti majd, hiszen még egyszer annyi hibával fognak találkozni, mint eddig. A közepesen fejlett országok népét alig észrevehetően, és természetesen az elmaradottakét szinte egyáltalán nem (például Albániát, vagy Bangladest valószínűleg senki nem irigyli, mert az Y2K probléma megoldására igen keveset kellett áldozniuk).

D. Ha hosszabb időn keresztül nem rabolnak ki, nem lopják el a kocsimat, és nem kergetik meg a lányomat, attól még nem biztos, hogy hiba volt létre hozni, és el kell sorvasztani a rendőrséget. Előfordulhat az is, hogy jól végzi a dolgát.

E. A magyarországi viszonyokkal kapcsolatban sajnálatosnak tartjuk, hogy nagy államigazgatási, egészségügyi, stb. rendszereink állapota olyan, amilyen. És még sajnálatosabb, hogy még az Y2K „hisztéria" sem volt elég ezeknek a rendszereknek a tisztességes, alapos felülvizsgálatához. Ennek következményei hétköznapi kellemetlenségeinkbe lesznek beépítve. Az ezzel járó óriási idő-, pénz- és energiapocsékolás pedig mindannyiunk számláján jelentkezni fog.

32. Magyarázzuk a bizonyítványt

Ez ideig vagy harminc esettanulmány-féleségen rágta át magát a kedves olvasó, és szívta magába a hasznosnak szánt tanácsokat. Például ilyeneket, hogy „ne tartsd a földön a számítógépedet”, vagy „takard le egy ronggyal, amikor nem használod”. Persze időnként elragadtattuk magunkat, és a fentieknél bonyolultabb összefüggésekre is felhívtuk a figyelmet: „a fájl vagy a mappa megnevezésénél ne használj ékezetes betűket”, vagy „jó, ha ezen megnevezések hossza nyolc karakternél nem több”.

Most irányt váltunk, és az elkövetkező néhány alkalommal az informatikai biztonság elméleti kérdéseivel foglalkozunk. A katekizmust az alapkérdésekkel kezdjük, nem túl tudományosan.

1. Mi az informatikai biztonság tárgya?
Az adat.

2. Melyik adatot kell védeni?
Az értékeset.

3. Melyik az értékes adat?
Az, amelyiket annak tartunk.

Ezek eddig maguktól értődő meghatározások, a gyakorlatban idáig mégis ritkán szoktak eljutni. Sajnos, ha a harmadik kérdésre nincs pontos válasz, nincs tovább miről beszélni.

Rembrandt a gyermekkori rajzaiból valószínűleg egy csomót összetépett, mégpedig azért, mert nem tartotta őket értékesnek. Ma minden egyes ákombákoma vagyont érne. Szüleink korában Sztálin összes műveit gyűjtötték. Az sem volt sikeres értékmeghatározás.

Természetesen könnyedén ki lehet jelenteni, hogy minden, ami a számítógépemben van, értékes adat. E kijelentés következményeivel azonban majd a „mennyibe kerül egy egységnyi adat védelme?” kérdésre adandó válasznál kell szembenézni.

4. Hol található az értékes adat?
Az adatnak, így az értékes adatnak is, két állapota van. Vagy az adattárolóban csücsül, vagy éppen utazik az adattárolók között.

5. Mitől kell védeni az értékes adatot?
Mindössze két veszéllyel kell szembenézni. Ez a megsemmisülés, illetve annak veszélye, hogy illetéktelenek kezébe kerül.

A helyzet pikantériája, hogy minél jobban védem az adatot a megsemmisüléstől, azaz minél több másolatot készítek a világ különböző pontjain, annál nagyobb lesz a kockázata annak, hogy ellopják. Ez az állítás persze fordítva is igaz.

- Alighanem rajta vagyunk egy levelezési listán.

33. Magyarázzuk a bizonyítványt (folytatás)

Az előző oldalakon az informatikai biztonság elméleti kérdéseivel gyötörtük Önt, Kedves Olvasó. Az alábbi kérdéseket tettük fel, és válaszoltunk is rá: Hogy ne kelljen visszalapozni, hanem lendületből haladhassunk tovább, még egyszer ideírjuk az eddigieket.

1. Mi az informatikai biztonság tárgya? – Az adat.

2. Melyik adatot kell védeni? – Az értékeset.

3. Melyik az értékes adat? – Az, amelyiket annak tartok.

4. Hol található az értékes adat? – Vagy az adattárolóban csücsül, vagy éppen utazik az adattárolók között.

5. Mitől kell védeni az értékes adatot? – A megsemmisüléstől, illetve az illetéktelen hozzáféréstől.

Az 5. kérdést részleteiben is megkapargatjuk. Kezdjük az adat megsemmisülésének lehetőségével.

6. Mitől semmisülhet meg az értékes adat?

Természeti katasztrófa: „Hát ki tudhatta ezt előre?" kér-

déssel és széttárt karokkal meg lehet úszni. Lásd: Budapest Sportcsarnok.

Adattárolási hiba: „A gyártó a hibás, meg a szállító. Azt ígérték, hogy örökké hibátlan lesz! Az adatokra miért nem vonatkozik a garancia?"

Nem szándékos károkozás: „Hogy tudom adattárolási hibaként feltüntetni azt, hogy elszúrtam valamit?"

Szándékos károkozás: „Minden rendben volt, csak éppen erre az egy vírusra nem voltunk felkészülve!"

7. Milyen statisztikai adatok állnak rendelkezésünkre az adattárolási hibák megoszlásáról?

(Valamennyi meghibásodási okot együtt 100%-nak véve.)

Hardver jellegű meghibásodás 60%, ezen belül emberi mulasztás (pl. „leesett arról a hülye asztalról") 42%; nem közvetlen emberi mulasztás 18%.

Szoftverhiba 40%, ezen belül emberi mulasztás 17%, az operációs rendszer hibája 14%, vírus 6%, egyéb 3%.

8. Melyek az illetéktelen hozzáférés (adatlopás) fő okai? Az angol nyelvben kerestek hét „E" betűvel kezdődő szót, és ezekből definíció lett.

Hiúság (Ego)
Sikkasztás (Embezzlement)
Lehallgatás (Eavesdropping)
Ellenségeskedés (Enmity)
Kémkedés (Espionage)
Zsarolás (Extortion)
Hibás döntés (Error)

9. Milyen statisztikai adatok állnak rendelkezésünkre az illetéktelen hozzáférés (lopás) célpontjairól?

(Valamennyi okot együtt 100%-nak véve). Belső adattárolás gyengeségeinek kihasználása 41%, szabad hozzáférés a berendezésekhez 13%, ellenőrizetlen belső folyamatok 12%, belsők morális gyengeségének kihasználása 11%, gyengén védett programokon keresztül való bejutás 9%, operációs rendszeren végrehajtott betörés 6%, jelszavak ismertté válása 5%, az adatraktározás gyengeségének kihasználása 3%.

A fenti statisztikából, ha semmi mást, csak azt a következtetést vonjuk le, hogy a lopott adatok legjelentősebb része (77%) a belső munkatársak kezén át vándorol célja felé, akkor már érlelődhet is a gondolat, hogy hol kell kezdeni a védekezést.

34. Itt a tárcsa, hol a tárcsa

A számítástechnikát alkalmazó cégek csillagászati összeget költenek adatvédelemre, az adatvesztések száma mégis évről évre növekszik.

Érdemes egy pillantást vetni az FBI adataira. Az 500 PC-nél többet használó USA-beli cégeknél 1996-ban 36%, 97-ben 47%, míg 98-ban 54% esélye volt annak, hogy adatvesztés következik be rendszerükben.

A KÜRT 1999-ben összesen 3119 adatmentést hajtott végre. Izgalmas statisztikát készítettünk ezekből. Hardverjellegű meghibásodás: 60%, ezen belül emberi mulasztás miatti meghibásodás 42% (például az adathordozót leejtették). A nem hardverjellegű (pl. szoftveres) hibák közül az emberi mulasztásra visszavezethető 17%. Az emberi tényező tehát összesen 59%, szép arány.

Technológiánk alkalmas arra, hogy minden mágnesesen rögzített adatot visszanyerjünk. Tavaly az adatmentésre kerülő esetek valamivel több mint 22%-a mégis menthetetlen volt – például azért, mert a felületek teljesen tönkrementek, vagy az adatokat szándékosan felülírták, stb.

A 22% az 681 adattárolót jelent, azaz legalább ennyi céget, amely végleg elveszítette értékes adatát. Itt összesen 2 276 GB-nyi adat elvesztéséről van szó. Statisztikánk szerint ebből a nem menthető 681 esetből 403-ban emberi mulasztás miatt semmisültek meg az adatok mindörökre. Tehát nem vesztek volna el, ha a rendszergazda tudja, mi a teendő – de nem tudta, vagy rosszul tudta. A 403 esetben összesen 1 286 GB adat veszett el. Ha 1 GB adatmentése ezer dollárba kerül, akkor összesen több mint egymillió dollárt fizettek volna ki a károsultak örömmel, hogy adataikat visszakapják.

E statisztikák készítése közben kollégáink nem savanyodtak meg, sőt időnként igen jól szórakoztak. Íme egy mosolyfakasztó eset:

A hazai „Top 100”-ban lévő cégtől érkezett az adathordozó. Megvizsgáltuk, majd szakvéleményt írtunk, mint minden esetben. A szakvélemény megírását nálunk számítógép segíti: a vizsgálati eredmény kódjaiból képzett kulcskifejezések kerülnek bele az előre megírt sablonba. Az említett esetet az alábbi szakvélemény rögzítette:

Az eszköz állapota: a mechanika sérült / megbontás nyomai láthatóak (ez két kódból előállított két kulcskifejezés).

Részletes szakvélemény: a mechanikai rész üres / nincs adathordozó tárcsa / nincs fejszerelvény (újabb három kód).

Adatmentésre vonatkozó megállapítások: az adatmentés nagy valószínűséggel nem oldható meg.

Ezt a kulcskifejezést azért fogalmaztuk meg ilyen árnyaltan, hogy menekülő utunk legyen az esetleges tévedésünknél. A fenti adatlapból egyértelműen az derül ki, hogy az adathordozónak éppen az adathordozó része nem állt rendelkezésünkre.

Ilyen esetre nem gondoltunk előre – nemhogy kulcskifejezésünk, de még díjszabásunk sincs rá.

35. Vagy a tányér egyenes, vagy a leves görbe

Újsághír 1: A rendőrség az Egyesült Királyságban letartóztatott egy fiatalkorút, aki kedvére törögette fel a bombabiztosnak hirdetett internetes bankfiókokat.

Újsághír 2: A banki szoftvert készítő cég szóvivője a fenti hír kapcsán kijelentette, hogy terméke teljes adatvédelmet nyújt.

A fenti hírek kapcsán született gondolataink:

Az informatikai forradalomnak sok haszna és haszonélvezője van. A haszonélvezők között az informatikai tömegterméket gyártók foglalják el a dobogós helyeket. Ők voltak a forradalom kirobbantói is.

Mi volt az informatikai forradalom előtt?

Volt egy világméretű, konszenzuson alapuló termelési rendszer, melynek főbb elemei: 1 Tudományos kutatás. 2 Ipari termelés. 3. Folyamatos minőségellenőrzés. 4. Jogi szabályozás. Gondoljunk csak a gyógyszerek vagy a gépkocsik gyártási folyamatára. Ezekben az esetekben mindenki tudomásul veszi, sőt elvárja, hogy egy új gyógyszer

vagy autótípus gyártásba vételét komoly tudományos kutatás előzze meg. E termékek átalakítása általában nem engedélyezett, nem lehet „csak úgy" belepiszkálni. Az autójukat tuningolgató lelkes amatőröknek rendszeresen meggyűlik a bajuk a műszaki vizsgán.

Azt is mindenki elfogadja – sőt elvárja –, hogy ha egy gyógyszer vagy egy autótípus valamilyen szempontból hibásnak bizonyul, akkor a gyártó ezt a terméket mindaddig kivonja a forgalomból, amíg a hibát ki nem küszöböli. A termék felhasználóját a jog széles körűen védi.

Mit hozott ezzel szemben az informatikai forradalom?

A sok-sok jótétemény mellett, melyeket e helyen nem kell külön ismertetni, az értékesítés lett az isten: teljesen maga alá gyűrte a tudományos kutatást és a jogi szabályozást. Elsősorban ennek következménye, hogy a tömegesen használt informatikai termékek nem mindig felelnek meg az egyéb ipari termékekkel kapcsolatban kialakult természetes elvárásainknak.

De hát hogy is felelhetnének meg? Éppen ez a forradalmi ezen a területen: hogy minden olcsó, minden mindennel összedugható, stb. De vajon miért lehet „olcsó"? Például azért, mert a biztonságot illető tudományos kutatásokat nem finanszírozza. Sok esetben nem is tudná, mert „a mindent mindennel összedugni" elvet nem lehet tudományosan megközelíteni. Mármost gondoljunk csak bele, milyen jogi procedúra elé nézne az, aki két – vagy akár több – gyógyszergyártó termékét összekeverve az így előállított zagyvalékot értékesítené?

Ma az átlagos számítógép-felhasználónak az az érzése támadhat, hogy a gépkocsi-hasonlatnál maradva, a mi összerakott eszközeink időnként nem kormányozhatók, időnként nem fékezhetők, időnként minden ésszerű magyarázat nélkül szét kell szedni és ismét össze kell rakni őket, hogy működjenek – de azért nagyszerű, hogy vannak, még ezekkel a hiányosságokkal együtt is. Sőt, nem is tudnánk már meglenni nélkülük.

Visszatérve az újsághírekre, az informatikai forradalom rengeteg áldása mellett hozzá kell szoknunk legalább két kellemetlenséghez:

A. Az informatikai biztonság kérdése még nincs megoldva.

B. A szóvivők hülyének néznek minket.

36. Hová lesz a magyaros virtus?

Léteznek nagy biztonságú informatikai rendszerek, ezeket azonban nem a ma tömegesen használt szoftver- és hardvereszközök területén kell keresni. Ezzel nem azt akarjuk mondani, hogy e tömegesen használt eszközök felhasználóinak nem érdemes adatbiztonsággal foglalkozniuk, csak tudniuk kell, hogy lyukas hálót foltozgatnak.

Az informatikai rendszerek biztonságát nemzetközi előírások alapján minősítik. Sajnos ezek még nem szabványok. Az Amerikai Védelmi Minisztérium skálája szerint a nem katonai alkalmazásoknál a legmagasabb minőségi fokozatot B1-gyel jelölik. E rendszerek biztonságos működésének szinte egyetlen veszélyforrása maradt, és ez a kezelőszemélyzet. Ide értendők mindazok, akik egy cégen belül adatokhoz hozzáférhetnek, függetlenül attól, hogy van-e erre jogosultságuk, vagy sem.

Hogy ez a kezelőszemélyzet mekkora kockázatot jelent az adatlopásoknál, arról időnként felröppen egy-egy hír.

· Fejlesztési adatok átadása a vetélytársnak (VW – GM)

· Üzleti stratégiák kiadása a konkurensnek (Rover – BMW)

Az adatvesztés területét vizsgálva, minden veszélyforrást figyelembe véve a legkülönbözőbb helyről származó statisztikai adatok mind egybecsengenek abban a tekintetben, hogy az emberi mulasztás viszi a pálmát, legyen az véletlen vagy szándékos károkozás. Számszerűsítve: az emberi mulasztás okozta adatvesztések a teljes adatvesztési portfolió 60–70 százalékát teszik ki. Ugyanakkor a vírusok által okozott adatvesztés „csak” 6–7 százalékos értéken van.

Szinte biztosak vagyunk abban, hogy a fenti statisztikai adatok ellenére a cégek ma sokkal nagyobb erőforrásokat mozgósítanak a vírusvédelemre, mint a kezelőszemélyzet tevékenységének szabályozására, ellenőrzésére.

Az Informatikai Biztonsági Technológia két szinten foglalkozik a kezelőszemélyzet tevékenységével:

Alapfolyamatok (adatvédelem és adatbiztonság)

Az ide vonatkozó szabályzatok egyértelműen rögzítik a kezelőszemélyzet tevékenységi körét, jogosultságait, felelősségét, ellenőrzési rendszerét.

Rendszerfolyamatok (IT rendszer és IT szervezeti folyamatok)

Az adatvédelem és az adatbiztonság szempontjából optimalizálják az informatikai (IT) rendszerben végbe menő folyamatokat és az IT szervezet felépítését, működését. Magyarán: a kezelőszemélyzetből a legkevesebben, és ők is a lehető legritkábban jussanak az adatok közelébe. Csak akkor és csak úgy, amikor ez előírt tevékenység a számukra.

Mindezeknek a szabályozásoknak az a célja, hogy a kezelőszemélyzet a lehető legjobban körbe legyen kerítve, és tevékenységének szabadsági foka a lehető legkisebb legyen.

A kedves olvasó, ha megértette, miről van szó, bizonyára elhúzza a száját. Ez bizony már nem a magyaros virtus kibontakozásának a terepe. Sőt, ha hozzávesszük, hogy ma már a kezelőszemélyzet minden informatikai tevékenysége automatikusan (szoftver segítségével) ellenőrizhető, akkor látnivaló, hogy a kör bezárult, vagy bezárható.

37. Szerverek és egyéb ínyencségek

Az informatikai biztonsággal foglalkozni kívánók igen sokat meríthetnek Srágli Attila (stragli@choraii.com) és Bedő Sándor (bsanyi@valerie.inf.elte.hu) „Linux szerverek biztonságos üzemeltetése” című munkájából. A következő néhány oldalon gondolatébresztő részeket adunk közre e tanulmányból.

Mi az, hogy security?

A közhiedelemmel ellentétben a security nem egy kínai étel neve. A security latin gyökérből eredő angol szó, és biztonságot jelent. Az alábbiakban annak a tényezőnek megállapításához használjuk, hogy egy-egy szerver mennyire áll ellen az őt érő szándékos vagy természetes eredetű rongálásoknak. Gyakran ezt a két dolgot külön szokták választani; mi itt nem tesszük, hiszen mindkettő ellen lehet és kell védekezni.

A szándékos rongálások ellen akkor tudjuk felvenni a harcot, ha számítógépünk operációs rendszere képes valamilyen szintű jogosultságok vagy privilégiumok kiosztására. Egyfelhasználós rendszereknél (pl. DOS, Windows vagy OS/2) ennek persze nincs értelme, tehát ne hagyjuk magunkat megtéveszteni akkor, amikor a Windows95

felhasználói azonosítót és jelszót kér tőlünk! A DOS és a Windows95 valójában egyfelhasználós rendszer. Ezeknek a rendszereknek a szintjén a security nem értelmes fogalom, pontosabban nem foglalkozunk vele. Ha a rendszerünk többfelhasználós operációs rendszer (pl. UNIX, VMS vagy NT), akkor a security ilyen vonatkozása a felhasználók jogosultságait, a fájlok, erőforrások hozzáférési jogosultságait jelenti.

Az üzembiztonságot is a security címszava alá soroljuk, és annak megállapítására használjuk, hogy számítógépünk vagy szoftvereink mennyire stabilak, azaz kissé közönségesebben: milyen gyakran romlanak el. Ha például a számítógépünket floppylemez segítségével indítjuk el, akkor az hosszú távon kevésbé biztonságos, mintha belső, külön erre a célra tervezett diszkeket használnánk, mert a floppy rendszeres használat esetén hamar „elkopik", tehát használhatatlan lesz a rendszer.

Létezik a securitynek hivatalos megközelítése is, amely 7 osztályba sorolja a számítógépeket. Az osztályozás az USA Védelmi Minisztériumától származik, és ORANGE BOOK néven vált híressé. Ez a dokumentum nem „feltörési nehézségeket'" definiál, hanem a rendszer egyes szintjeinek elkülönítettségét, a jogosultságok skálázhatóságának finomságait figyelembe véve állít fel csoportokat. Fontos tudnivaló az is, hogy az ORANGE BOOK nem ismeri a hálózat fogalmát. A hardver és a szoftver együtt kapja a minősítést.

38. Szerverek és egyéb ínyencségek (folytatás)

A biztonság (security) kategóriái az USA Védelmi Minisztériumában megfogalmazott „ORANGE BOOK" szerint:

D: Nincs semmi security. Tipikus példája egy DOS–os PC. Az nem töri fel a rendszert, aki nem akarja.

C1: A rendszer egyes részei, egyes erőforrások védetté tehetők.

C2: Ezt a szintet szokták elfogadható security osztálynak nevezni. A rendszerhez csak jogosultsággal lehet hozzáférni, és a rendszeren belül is léteznek védett erőforrások. Ebbe a kategóriába sorolhatók az IBM gépei, a VMS rendszert használó számítógépek, néhány UNIX-változat, és újabban a Windows NT 4.0 is megkapta ezt a minősítést.

B1: A rendszer minden erőforrása védve van, csak jogosultságokkal rendelkezők számára hozzáférhetők.

B2: Ez az osztály a B1 szigorítása úgy, hogy az események naplózhatók, ill. elég finoman hangolható felhasználói csoportok (adminisztrátor, rendszerprogramozó, felhasználó) hozhatók létre.

B3: A B1, B2 és B3 osztályok között igazán lényegi különbség a skálázhatóság. Egy B2–es rendszer üzemeltethető úgy, ahogy egy B3–as, a különbség abban van, hogy a B3–at nem lehet lebutítani. Röviden szólva a B3 nem más, mint az a B2, ahol a fent említett lehetőségek nem lehetőségek, hanem alapszolgáltatások.

A1: Ez a csúcs. A1–es rendszer nagyon kevés van a világon, mindössze tizen–egynéhány működő rendszer. Az A1 minősítés azt jelenti, hogy bizonyított tény, miszerint a B3 osztály beállításai nem törhetőek fel.

Mivel az itt ismertetett tanulmány [Srágli Attila és Bedő Sándor „Linux szerverek biztonságos üzemeltetése"] a Linuxszal foglalkozik, érdemes átgondolni, hogy a UNIX–ok az egyéb, biztonságosnak vélt rendszerekhez képest hol állnak security tekintetében.

Kezdjük az összehasonlítást a VMS-sel. A UNIX–okban általában a fájlok hozzáférési jogait a +rwxrwxrwx karaktersor jellemzi. r az olvasási (read) jogot, w az írási (write) jogot, és x a futtatás (execute) jogát jelenti, a háromszori ismétlés pedig a tulajdonos–csoport–mindenki más (user–group–other) hármashoz tartozik. A + helyén

lehetnek egyéb beállítások, de ezek néha csak rontanak a helyzeten.

A VMS ennél többet tud: (RWED; RWED; RWED; RWED) a jellemző security karaktersor, ahol a R az olvasás, W az írás, E a futtatás és D a törlés (delete) jele. A négyes osztás a rendszergazda–tulajdonos–csoport–mindenki más felosztásból származik. A UNIX–ok 3x3 security bitjével szemben a VMS–nek 4x4 ilyen bitje van.

A különbség már a fentiekből is könnyen érzékeltethető. Jogosultságok tekintetében a VMS sokkal finomabban skálázható, mint egy UNIX.

39. Szerverek és egyéb ínyencségek (további folytatás)

Az itt közölt intelmek szélesebb körben, a Linux szervereken túl is értelmezhetők.

Milyen hardvert vásároljunk?

Ha komoly szolgáltatást szeretnénk nyújtani, és fontos a folyamatos működés, akkor már a hardver vásárlásánál gondolnunk kell a minőségre. Vegyünk ipari házat, amely alkalmas több hónapon (esetleg éven) keresztül megszakítás nélküli üzemelésre, és esetleg fizikai védelmet is nyújt a betörés ellen. Ezek a házak általában speciális tápegységet tartalmaznak, szétszerelésükhöz vagy kezelőfelületükhöz kulccsal vagy mágneskártyával lehet hozzáférni. A közönséges PC házak (5 000–10 000 Ft–os kategória) tápegységei nem több éves üzemre, hanem napi kb. 12 órás használatra tervezettek, a keylock pedig egy közönséges csavarhúzóval átállítható, illetve egy jumper lehúzásával hatástalanítható. Ezek a házak néhány csavar eltávolításával szétszerelhetők, ami a gépen tárolt adatok fizikai lopását könnyíti meg. (Sok helyen persze nincs szük-

ség ilyen intézkedésekre, de ha fegyveres őr nem vigyázhat a konzolra, akkor ezek a dolgok is megnehezíthetik a cracker életét.)

A folyamatos üzemhez elkerülhetetlen egy szünetmentes tápegység beszerzése. Ebből is érdemes a legolcsóbbak helyett valami komolyabbat beszerezni. Figyeljünk arra, hogy a szünetmentesnek akkor van értelme, ha az áramkimaradásról a Linux is értesül. Létezik olyan megoldás, ahol az UPS és a PC a soros porton kommunikál. Ez az olcsóbb és butább megoldás. (Ha szükség van a soros portokra, ez nem használható.) Az intelligensebb megoldás, amikor az UPS-hez egy bővítőkártyát adnak, amelyen keresztül az áramszolgáltatás leállását, újraindulását, illetve sok egyéb mást is közölni tud a Linuxszal.

Sok kellemetlenséget okozhat, ha a processzorunk hűtőventillátora menet közben felmondja a szolgálatot. Ez nehezen észrevehető probléma, mert ha a CPU nincs komolyabb terhelés alatt, akkor a rendszer hibátlanul képes működni. Ne sajnáljuk a pénzt komolyabb hűtőbordákra vagy golyóscsapágyas hűtőventillátorra, mert annak élettartama sokszorosa pár száz forintos társainak.

Biztonsági szempontból meggondolandó, hogy a gépben legyen-e a telepítés után is floppy- vagy CD-meghajtó, ugyanis egy rendszerlemezről bootolt kontrollprogrammal vagy operációs rendszerrel (pl. Linux rescue disk) root jogokkal mountolhatóvá válnak a számítógép diszkjei. Ez ellen jó megoldás a floppy kiszerelése vagy a boot sequence átírása a BIOS–ban, hogy bootoláskor a rendszer ne próbáljon floppyról vagy CD–ről bármit is elindítani. Ha a gép könnyen szétszerelhető, vagy a BIOS nincs jelszóval védve, akkor ez persze semmit nem ér. A BIOS jelszó sem igazi megoldás, mivel a legtöbb BIOS–nak van default passwordje, amit nem nehéz megszerezni...

40. Adatvédelem kicsiben

Részlet egy levélből:

„Ez úton szeretnék köszönetet mondani a sok jó és hasznos tanácsért, amit hétről-hétre olvashatunk a Computer Technika hasábjain. Kezdettől fogva olvasom ezeket az értékes sorokat. Az 'egyszerű' felhasználói státustól eljutottam odáig, hogy a cégemnél is hallgatnak rám a biztonság terén. Az én tevékenységem a közúti szállítás szervezése, végrehajtása. Az Ön írásai nyomán kezdtem el az otthoni gépemen az adatok mentését, CD-re írását... Körülnéztem a cégemnél is, és megdöbbentem, hogy egy kb. 20 gépből álló rendszeren nem végeznek adatmentést. Például nincsen állandó víruskereső program, és mindenki olyan floppyt hoz be otthonról, amilyet csak akar. Otthoni referenciáim alapján a főnökeim megfogadták a tanácsaimat, és útmutatásaim alapján pótolták a hiányokat. Az első víruskeresési akciónál majdnem kiment a biztosíték, annyi vírust talált a program..."

Jól esik a dicséret, ám a levélíró egy jellemző problémát is feltárt, és mindjárt megvalósítható megoldást ajánlott rá.

A kis és közepes méretű cégek informatikai biztonságáról van szó. Ezek a cégek komoly védelmi rendszereket nem tudnak megfizetni, önálló, csak ezzel a témával foglalkozó szakember sem fér bele a cég költségvetésébe. Az ilyen méretű cégek vezetői nem vesznek tudomást az adatvesztési kockázatról, de legalábbis megpróbálják homokba dugni a fejüket. Itt kétféle kockázatról van szó: elvész a cég fontos adatállománya és nem lehet helyreállítani (adathordozó-meghibásodás, vírus, szándékos károkozás...) illetve illetéktelenek kezébe kerülnek a cég fontos, titkos adatai (jogtalan másolás, lopás...).

Pedig az ilyen kis és közepes méretű cégek részére is létezik a pénztárcájukhoz méretezett informatikai biztonsági stratégia.

Az itt csokorba gyűjtött írásokban, a Kürtölőkben, amelyekre levélírónk is hivatkozik, főleg olyan informatikai biztonsági rendszerszemléleti megoldásokat közöltünk, amelyeket házon belül el lehet határozni, meg lehet tervezni, végre lehet hajtani, és ha mindez megtörtént, akkor rendszeresen ellenőrizni kell. E tevékenységsorozat pedig nem igazán pénztárcafüggő.

A legnehezebb helyzetben a cég vezetője van, mert hasonló típusú probléma megoldására külső cégeknek szokott megbízást adni. Ha elromlik a szállítójárműve, szer-

vizbe viteti; ha fél, hogy ellopják, biztosítást köt rá. Ha elromlik a számítógépe, szakembert hív, az adataira viszont nem tud biztosítást kötni. Az adatvesztés kockázatvállalását nem bízhatja külső cégre. Ilyen esetben a számítástechnikai szolgáltató is csak széttárja a kezét, ahogy az autószervizben tennék, ha azzal keresné fel őket, hogy kocsiját ellopták.

Tapasztalatunk szerint a cégvezetők nem foglalkoznak e problémával – mindaddig, amíg egy súlyos adatvesztésbe bele nem rohannak. És ennek az esélye a statisztikai adatok tanulsága szerint is egyre nagyobb.

Boldog lehet az a cégvezető, akinek olyan munkatársa van, mint levélírónk, aki alulról építkezve, lépésről-lépésre csökkenti az adatvesztés bekövetkezésének kockázatát. Ez a tevékenység előre tervezetten és felülről indítva is végrehajtható, és nemcsak katasztrofális adatvesztés után. Akkor nagy valószínűséggel végrehajtják, de előtte – ezt könnyű belátni – sokkal gazdaságosabb.

41. Drót nélküli tápegység

Az elmúlt év végén egy közepes méretű hazai vállalatnál (300 PC, 8 szerver) az egyik szerver szünetmentes tápja felmondta a szolgálatot. Megjavították, és visszaszállították a helyére, de a szerverrel nem kapcsolták össze, mert a szervert ehhez le kellett volna állítani. Aztán később sem kapcsolták össze, mert elfeledkeztek róla. Év végén, a legnagyobb hajtásban (talán éppen annak következtében) a hálózat túlterheltsége miatt kiment a biztosíték, a delej elszállt, és vele együtt a szerver is. Teljes harci díszben ott állt ugyan mellette a szünetmentes táp, „cordless” üzemmódra azonban nem volt felkészítve. Az áramszolgáltatás helyreálltával a termelés nem tudott beindulni, most már a szerver adatvesztése és a backup rendszer (szoftver- és adatmásolatokat tartalmazó biztonsági archívum) elemi hibái miatt. Katasztrófaterv nem volt, csak fejetlenség és kapkodás. A veszteségeket 8 számjegyűre becsülték forintban.

A cégvezetésnek kézenfekvő és azonnali intézkedése volt az informatikai rendszer biztonságtechnikai felülvizsgálata, és a kívánt biztonsági szint megvalósítása. Ez 3 hetes procedúrát jelentett a cégvezetés és az informatikai

dolgozók számára. Az informatikai biztonságtechnikai rendszer az alábbi strukturális lépéseken esett át:

· a kívánatos biztonsági állapot meghatározása,

· jelenlegi adatvédelmi/adatbiztonsági állapot felmérése,

· az informatikai rendszer felülvizsgálata, kockázatelemzés,

· a biztonságot veszélyeztető „rések" feltárása,

· megoldási javaslatok kidolgozása és azok végrehajtása,

· tesztelés, üzembe helyezés, oktatás.

Az itt felsoroltak az Informatikai Biztonsági Technológia (IBiT®) nemzetközileg elfogadott rendszerében az alapmodulokon belüli tevékenységek. Ezek a modulok egységes szabályozási rendszert alkotnak, amelynek keretét maguk a szabályzatok adják. A szabályzatrendszer strukturált szerkezetű, lefedi a teljes adatvédelmi rendszert (Mentési Szabályzat, Vírusvédelmi Szabályzat...) és a teljes adatbiztonsági rendszert (Titkosítási Szabályzat, Hozzáférési jogosultságok...). Ezek a szabályzatok mind-mind az informatikai rendszer hatékonyabb működését, az adatvesztés és az adatlopás megelőzését szolgálják. Az előre elkészített Informatikai Katasztrófaterv pedig a már bekövetkezett esemény okozta kár minimalizálását célozza meg, és olyan esetekre nyújt megoldást, ha a felmerülő informatikai problémát a rendelkezésre álló erőforrásokkal nem lehet megoldani.

A tapasztalatok – az egészségügyhöz hasonlóan – azt mutatják, hogy a megelőzés (prevenció) lényegesen olcsóbb, mint a gyógyítás, vagyis az eredeti, kívánt állapot helyreállítása. Ráadásul, aki nincs felkészülve a megelőzésre, az szinte biztosan teljesen felkészületlenül áll a katasztrófahelyzetben.

A fent idézett történet eddig szokványosnak tűnhet. Talán be sem került volna ebbe a sorozatba, ha nem lenne csattanója. Az informatikai biztonságtechnológiai rendszer üzembe helyezésekor rendszeresen azt észleltük, hogy illetéktelen kezek igyekeznek hozzáférni a raktárkészlet adatbázisához. A következmény rendőrségi ügy lett, megírták a lapok is.

Mi nem következik egy szünetmentes tápegység hibájából...?

42. Gazdátlanul

Azoknál a kisebb, nagyobb és legnagyobb állami szervezeteknél, amelyekkel munkánk során kapcsolatba kerülünk, az adatbiztonság leginkább a brekegő kétéltű hátsó fele által szimbolizált színvonallal jellemezhető.

Lehet, hogy az előző mondat túl általánosra sikeredett, de valószínűleg még így sem fejezi ki a valós helyzet elképzelhetetlen mélységeit.

Szívszorongatónak következzék itt néhány egy közepes méretű költségvetési szervezet informatikai biztonsági rendszerében feltárt kockázati tényezők közül:

A vállalati szint:

· A feladatkörök és a felelősségek nincsenek definiálva.

· Egyik irányban sincs megfelelően szabályozott belső kommunikáció az IT szervezet és a felhasználók között.

Az IT szervezet:

· Az IT szervezeten belüli feladatok, felelőségek csak szóban vannak meghatározva, dokumentációjuk hiányos.

· Az informatikáért felelős osztályvezetőnek az informatikai feladatok menedzselésére nincs elég ideje.

Az Informatikai Stratégia:

· Nem létezik Informatikai Stratégia.

· Továbbképzés és oktatás sem a felhasználók, sem a rendszergazdák részére nincs tervezve.

Az informatikai rendszer:

· A működés folyamatos fenntartásához szükséges tartalékrendszerek nem állnak rendelkezésre.

· A munkák naplózása hiányos, a hibák kezelése nincs kiemelve.

· A jogosultságok, hozzáférések szabályozását a szerverek oldalán csak részben oldották meg, a felhasználói gépeken egyáltalán nem.

A vállalati adatstruktúra:

· A felhasználók saját asztali számítógépeiken is tárolnak fontos, bizalmas adatokat, melyek védelme és titkosítása nincs megoldva. Ez a probléma különösen fontos a vezetők által használt hordozható számítógépek esetében, mivel a Társaságnál évente egy-két laptop el is tűnik.

A vállalat mentési rendszere:

· A backup rendszerre nincs megfelelő szabályozás, ezért azt kizárólag csak a rendszergazda tudja üzemeltetni.

· A mentésekhez nincsenek megfelelő hardver- és szoftvereszközök.

· A mentett adatokat tartalmazó médiák azonosítása és tárolása elégtelen.

Az informatikai vészhelyzet kezelése:

· Nincsen semmilyen katasztrófaterv. (Sem általános, sem az IT-re vonatkozó.)

És ezen kockázati tényezők (magyarán hiányosságok) felsorolásának jegyzőkönyve még 14 sűrűn teleírt oldalon keresztül folytatódik.

Megnyugtató viszont az, hogy van már néhány állami szervezet, ahol komolyan veszik az értékek védelmét. Ezért kezdődött meg a fenti szervezetnél is az Informatikai Biztonsági Technológia (IBiT®) tervezése és bevezetése.

43 Pici, mozog és értékes

Az újsághírekből tudjuk, hogy 2000. augusztusában az USA-ban néhány napig nem találtak egy fontos nemzetvédelmi adatokat tartalmazó notebookot. Később előkerült, de a nemzetbiztonság felelősei aggódnak, hogy ezalatt a winchester tartalmát lemásolták-e, vagy sem. Ha pedig aggódnak, az azt jelenti, hogy a winchester adatai nem voltak védettek.

A notebook ellopása olyan kockázati tényező, amellyel mindenki találkozik, aki rendelkezik ilyen eszközzel. Ha ilyen esetről hall az ember, először alkalmasint az anyagi kárra gondol, holott a számítógépeken tárolt adatok, információk értéke lényegesen meghaladhatja magának a hardvernek és a szoftvernek az értékét. Ezért még legalább két problémával számolnunk kell:

· Van-e olyan másolat az adatokról, amelyet nem loptak el?

· Az értékes adatok titkosítva voltak-e, hogy illetéktelen ne férhessen hozzájuk?

Ha egyáltalán foglalkoznak valahol a notebookokkal kapcsolatos biztonsági kérdésekkel (vállalati IT stratégia,

biztonsági szabályzatok...), az akkor is legfeljebb a lopással összefüggő kockázatokig terjed.

Az Informatikai Biztonsági Technológia (IBiT®) nemzetközileg elfogadott rendszerében a notebookhoz kapcsolódó adatbiztonsággal önálló fejezet foglalkozik. Néhány lényeges elem ezekből:

Vírusvédelem

A Vírusvédelmi Szabályzatban, éppen a notebook mobilitása miatt, külön kell foglalkozni ezekkel az eszközökkel. A telepítések, frissítések központi végrehajtása csak az éppen a hálózatra kapcsolt eszközöknél működik. Mivel a notebookoknál ez nem biztosítható, sőt a notebookok általában a vállalatvezetők kezében vannak, igen macerás a havi vagy ennél is gyakoribb frissítések végrehajtása.

Szoftver-legalizáció, szoftverkövetés

A probléma ugyanarról a tőről fakad, mint a vírusvédelemé. Bonyolítja a helyzetet, ha az IT szervezetben más felelős a vírusvédelemért és más a szoftverkövetésért, mert a notebookot használó főnököt ilyenkor már többen ostromolják rendszeresen.

Felhasználói jogosultságok

Mivel a notebook jellegéből fakad, hogy változtatja helyét, és feltehetően nemcsak a vállalaton belül, ezért ezek a számítógépek fokozottan ki vannak téve az illetéktelen hozzáférések veszélyének. Így kiemelten fontos a megbízható beléptető rendszer és a számítógépen tárolt anyagok titkosítása. A szokásos problémán felül megjelenhet még az „egy gép, több felhasználó” esete is. A jogosult hozzáférések szabályozására mind a notebookon, mind a hálózaton belül egyedi rendszergazdai tevékenységek szükségesek.

Az Informatikai Biztonsági Technológia szabályzatrendszere kitér még egy sor szükséges, notebookhoz kapcsolódó biztonsági intézkedésre, amelyek felsorolása azonban már meghaladná e könyvecske terjedelmét.

Étvágygerjesztőnek (vagy elrettentőnek) remélhetőleg ennyi is elég.

44. Az iparág hazugsága

A Byte 2000. júliusi számában „Az iparág hazugsága, avagy Buffer Overrun" címmel jelent meg Fóti Marcell (marcellf@netacademia.net) írása a sorozatos rendszerfeltörésekről és az ezzel kapcsolatos biztonsági problémákról. Rövidítve közreadjuk. Izgalmas.

„Nemrégiben egy külhoni szaklapban olvastam egy hackerrel készített interjút. Idézném a párbeszéd utolsó, csattanónak szánt két sorát:

(Riporter) – Why? (Miért? Mármint: miért teszitek, amit tesztek?)

(Hacker) – Because we can. (Mert képesek vagyunk rá.)

Pont. Cikk vége. S bennem a döbbenet: hát ilyen ostoba a riporter kolléga? Itt fejezi be a riportot, miközben üvöltve kínálkozik a következő kérdés: – Why? – Miért vagytok képesek rá? Miért nincs végleges megoldás a problémára? Mi a fenét tudtok Ti, tizenévesek, amit a Pentagon nem tud?

Valahogy úgy érzem: vagy senki sem látja, vagy – hogy ne higgyem magam minden tudás letéteményesének – senki sem meri kimondani a sorozatos rendszerfeltörések mögött álló valódi okot: azt, hogy a jelenlegi számítógépes architektúra pocsék.

Szerintem a számítógépek elvi alapja, a Neumann-architektúra az oka mindennek, mert rossz, elavult őslény, 50 éves technológia.

A Neumann-elv lényege, hogy adva van egy adattároló egység, amelyen egy feldolgozó egység dolgozik. Az adattárolóban az adatok és a programkódok is szépen megférnek egymás mellett, hiszen pusztán kódolás, azaz értelmezés kérdése, hogy ami az adattárolóban található, az programkód-e (winword.exe), vagy adat (fontos.doc). Zseniális elgondolás, olyannyira, hogy egyesek szerint számítógép nélkül, papírral és ceruzával a kézben ki sem lehet találni.

Ám csúnyán fest, ha programkódot szeretnénk adatként értelmezni (próbáljuk ki: Norton Commanderben nyomjunk F3-at a winword.exe-n), és azonnal borul a masina, ha adatot programkódként kezelünk (Pentium-hiba 1998-ból: nem létező processzorutasítás hívásakor a proci elszáll).

Ebben az architektúrában a gyenge pont a stack, avagy verem – ahol a programkód és az adat fertelmesen egymásba mosódik. A klasszikus Buffer Overrun hacker-

technika azt használja ki, hogy minden szoftver garantáltan hibás, ráadásul az alatta dolgozó hardver is tervezési hibás. Ha például egy egymillió kódsoros Linuxban csak egy ezreléknyi a kihasználható hiba, akkor is van 1000 dobásunk! Ha a verem felülírását megfelelően irányítja a hacker (például beküld távolról egy embertelen hosszú URL-t egy webkiszolgálónak, amely ezt lenyeli), akkor saját programját helyezheti el a veremben, s erre ráugrathatja a vezérlést, amellyel API hívásokat kezdeményezhet.

Nyissátok már ki a szemeteket, emberek! Mit tud a tizenéves hacker? Látni! Közismert tényeket megfelelően csoportosítva kreatív megoldásokat kiagyalni! Egyszóval a hazug világ orcájába röhögni: „Because we can."

45. Az iparág hazugsága (folytatás)

A hacker-technológiák a Neumann-elvet használják ki. Ebből a témából merítettünk, amikor közreadtuk Fóti Marcell gondolatainak rövidített változatát. Csirmaz László fűzött (csirmaz@ceu.hu) értékes megjegyzést e témához:

„...sajnálatos, hogy a Neumann-elvvel kapcsolatban – szerintem – félretájékoztatja olvasóit, mondván: ‚...a Neumann-architektúra rossz, elavult őslény.' Hivatkozási alapja az, hogy a tárban a program és az adat békésen megfér egymással, és adatokat programként, programot adatként lehet kezelni.

Míg ez utóbbit főleg előnyként szoktak emlegetni (önmódosító programok), és a Neumann-elv is ezt szorgalmazta, addig adatokat programkent csak ritkán használunk (például az overlay-es programok esetében ez történik). Az, hogy adatok programok összekeveredhetnek, kizárólag az operációs rendszerek hibája. A Microsoft termékeinek belső felépítését nem ismerem, de a Linuxról írt szurkapiszka sajnos nem állja meg a helyét. Az idézett ‚Buffer Overrun' hackertechnika az operációs rendszer hibáit használja ki, ezek a lehetőségek az újabb (két évnél nem régebbi) rendszerprogramokban már nincsenek meg.

A veremben NINCS program, hanem ott az eljáráshívás visszatérési címe tálalható. A hardver lehetővé teszi, hogy programként csak megadott tárterületek legyenek használhatók, aminek tartalmát viszont a program nem változtathatja meg. A ‚Buffer Overrun' egy tervezési hiányosságot és (legalább egy) programozási hibát használ ki: nincs ellenőrizve egy memóriatömb túlírása (programozási hiba), illetve az operációs rendszer nem tiltja le a verembeli adatok végrehajthatóságát (tervezési hiba). Ezek semmi esetre sem a Neumann-architektúra hibái, mint ahogyan VMS alatt ilyen trükkök nem is alkalmazhatók."

Megérkezett Fóti Marcell válasza is:

„Már ennek előtte is kaptam a fejemre, hogy nem a Neumann-elv a hibás, hanem a felhasználása nem elég körültekintő. Az akkori érvelők ezt azzal a példával támasztottak alá, hogy nem a kés műszaki elve hibás azért, ha elvágom vele az ujjam. Ez igaz. Ugyanakkor kedvenc mondásom a mai szoftveriparra, hogy körömreszelővel nem lehet űrhajót gyártani. A mai fejlesztések elképesztően primitív módszertanon alapulnak ahhoz képest, hogy zsinórban gyártanak több tízmillió soros szoftvereket. Hibás az egész, az első sor leírásától kezdve!

Viszont nem igaz, hogy a két évnél fiatalabb operációs rendszerek nem szenvednek ettől a bajtól. Elég csak feliratkozni a MS Security Bulletinekre: Átlagosan havi két esetet regisztrálnak. A Linuxnál is, bár azokat a listákat nem követem naprakészen. A VMS zárt világában nem csoda, hogy nem volt vírus és nem volt klasszikus hackertámadás. Szegény Kevin Mitnick is kénytelen volt ‚hagyományos' módon ellopni a VMS forráskódját: besétált, és elvitte."

46. A kényelem veszélye

Az itt következő esetet több újság is megírta. Nem követünk el indiszkréciót, nem sértünk banktitkot, ha az incidenst a magunk sajátos szempontjából ismertetjük.

A világ egyik vezető bankja értesítette ügyfeleit, hogy az internetes tranzakciók során, a bank által az ügyfeleknek kiadott szoftverecskén keresztül vírus érkezik a bank rendszerébe, ezért kérve kérik ügyfeleiket, hogy a továbbiakban ne használják ezt a szoftvert, de különben is mindent megtesznek azért, hogy bla-bla-bla-bla.

Mi történt?

A bank, mint minden rendes bank, ügyfeleit több azonosítóval látja el: felhasználói név, jelszó, ugró kód (scratch list). Az ugrókód egy csomó három-, négy- esetleg ötjegyű egyedi jelsorozat. Ezeket a kódsorozatokat a bank állítja elő, egyedi módon minden ügyfelének. A bank az ugrókód listáját nem elektronikus úton juttatja el az ügyfélhez, hanem papíron – postán, borítékban, talán faxon is. Az ugrókódok rendeltetése az, hogy az ügyfélnek minden tranzakcióhoz a listából soron következő kódot is használnia kell önmaga személyazonosságának igazolására.

Ez a rendszer első pillantásra biztonságosnak látszik. Csakhogy a bank egy lépéssel elébe ment a baj bekövetkeztének. Felismerte: ügyfelei számára kényelmetlenséget jelent az ugrókódok listájára vigyázni, mindig elérhető, mégis biztonságos helyen tartani. Kényelmi szolgáltatásként küldött tehát egy kis programocskát, amely a felhasználói gépeken ülve nyilvántartja az ugrókódok listáját (egyszer, legelőször természetesen be kell pötyögni az egészet), és valahányszor a banki rendszer a következő kódot kéri, e programocska adja azt át a banki szoftvernek.

Az ismeretlen szerző ebbe a programocskába ültette bele a vírust, és a tranzakciók során nemcsak az ugrókód, hanem a vírus is átkerült a banki rendszerbe.

Milyen következményekkel lehetett számolni?

Két dolog történhetett, és ez kizárólag a vírus készítőjének akaratától, felkészültségétől függött:

· Adatvesztés. A vírus a banki rendszeren belül adatokat törölhet. A bank speciális nehézsége az, hogy rendszerében percenként több tízezer tranzakció zajlik le. A probléma észlelése és a helyreállítás közötti időben nem tudja fogadni a tranzakciókat, hacsak erre az időszakra egy – nagy kockázattal működő – puffer-rendszert be nem indít.

· Adatlopás. Ugyanezzel az erővel a vírusba épített utasítások hatására az ugrókódok illetéktelenek kezébe kerülhetnek, ami minden bank rémálma. Valamennyi ügy-

fél valamennyi ugrókódjának visszahívása a bank működését hosszú időre megbéníthatja.

Az újsághírekből az derült ki, hogy az adott bankban példásan működött a katasztrófaelhárítás. Megállapították, hogy a vírus adatlopásra nem volt felkészítve. A vírus észlelésétől az informatikai rendszer átállításáig alig pár óra telt el.

Szinte biztos, hogy az eset kapcsán a bank továbbfejlesztette vírusvédelmi rendszerét, vírusvédelmi szabályzatát pedig új fejezettel bővítette.

Ennek az esettanulmánynak mindenki számára szóló üzenete az lehet, hogy a biztonsági szempontok és a kényelmi szempontok hatásai alapvetően ellentétesek.

47. Az információ uralma

Intellektuális élmény, ha az ember fésületlen gondolatai egyszer csak egységes rendszerbe foglalva jönnek szembe. Ezt az élményt okozhatja Carl Shapiro és Hal R. Varian könyve, amely a 2000. esztendőben jelent meg magyarul „Az információ uralma, a digitális világ gazdaságtana" címmel.

Az informatikai forradalom szennyesének feltárása, az ökölszabályok kialakulásának bemutatása, az új gazdaság szükséges és elvárható szabályainak, szabványainak felvázolása a legjobbkor jött.

Néhány részlet arról, hogy miként gondolkodnak a szerzők az informatikai biztonság növelésének lehetőségéről, nem kispályás körülmények fennforgása esetén:

„A szabványok mérséklik a fogyasztók technológiai kockázatát, ugyanakkor a szabványok meggyorsítják az új technológia elfogadását. A sok támogatóval rendelkező szabvány rendkívül sokat tehet a technológia hitelének megteremtésében, amely azután önmagát igazolja. Ezzel szemben az inkompatibilis termékeknél a vásárlók zavarodottak lesznek, és félnek, hogy a termékkel nem tudnak majd mit kezdeni. Nemrég az 56 Kbps-os modemek pia-

cának bővülését késleltette az a tény, hogy a gyártók nem tudtak megegyezni egy közös szabványban."

„A szabványháború egyik kockázata az, hogy a piaci részesedésért vívott csata aláássa a fogyasztók valamelyik technológia felülkerekedésébe vetett bizalmát, aminek eredménye egy győztes nélküli háború. E háború áldozatává válhat az a magányos új technológia is, amelyet nem támogat elég vállalat a piacon ahhoz, hogy szabvánnyá válhasson."

„Ha a szabvány valóban nyitott, a fogyasztók kevésbé aggódnak amiatt, hogy kiszolgáltatottak. Ekkor ugyanis számíthatnak a valódi versenyre a későbbiekben. Így van ez a CD piacon, ahol a Sony, a Philips és a DiscoVision Associates csak igen szerény jogdíjra tart igényt. Ugyanez történt az IBM nyitottsága miatt a PC piacon. És be is indult a verseny. Az operációs rendszerek viszont sajnos a Microsoft uralma alá kerültek. Elsősorban a Netscape nyomására azonban a Microsoft is rákényszerült arra, hogy az olyan nyitott szabványok felé mozduljon el, mint az XML, egyszerűen azért, hogy ügyfélkörének lehetősége legyen a többi felhasználóval való biztonságos hálózati kommunikációra."

„A fogyasztók számára az egyik legrosszabb végeredmény, ha olyan szabvány mellé állnak, amelytől széles körben azt várják, hogy nyitott lesz, ám később, amikor már tömegesen lekötötték magukat, rájönnek, hogy a szabványt lezárták. A Motorolát vádolták azzal, hogy éppen ezt a taktikát alkalmazta a modemek szabványának támogatásakor."

„Az információs korszak jelenlegi legnagyobb szabványháborúja a mobil telefonok piacán alakult ki, megosztva az európai, amerikai és japán fogyasztókat a GSM, a TDMA és a CDMA rendszerek között."

Mi, az informatikai rendszerek kiszolgáltatottjai, továbbra is álmodozhatunk a gyártóktól független jogi és etikai szabályozottságról, amelyet a klasszikus iparágakban már réges-régen kitaláltak.

48. Mazsolák

A hard disk mint szennyvíztisztító

Egy budai pincét néhány napra elöntött a csatorna vize. A pincében állt a szerver, volt szivattyú is, de ez utóbbi csak a vizet tudta továbbítani, a zagyot nem. A szennyvíz megtette hatását, a winchesterek elektronikája szétmarva, a dobozon belül a tisztatérben állt a víz. De milyen víz? Kristálytiszta!

A winchestergyártás mai technikai színvonalát jellemzi, hogy a fedélbe épített mikroszűrő nemcsak a levegőben lévő porszemektől óvja a fejet és a tárcsákat: zagyszűrésre is kiváló. Mivel a mágneses felületek, hála a mikroszűrőnek, nem korrodálódtak, a megfelelő technológiai lépések alkalmazásával az adatmentés, a megrendelő legnagyobb csodálkozására, maradéktalanul végrehajtható volt. Levelet is írt köszönetképpen, amelyben ékesszólóan megfogalmazta, hogy miből csináltunk aranyat – neki.

Csodadoktorok

Mire hozzánk került a winchester, már többen erőszakot követtek el rajta. A tisztatér kibontva, a tárcsák kiszedve. A buheráló magánszorgalomból még diagnózist is mellékelt a merevlemez teteméhez: a motor rossz, csak azt kell kicserélnünk, a többi már gyerekjáték.

Itt üzenjük a csodadoktoroknak, hogy tucatnyi szabadalmazott eljárás létezik arra vonatkozóan, hogy a tér legalább három pontjában meghatározott helyről kiemelve egy közepén lyukas tárcsát, hogyan kell azt ezred mikron pontossággal ugyanoda visszatenni. Kérjük, ezeket a koordinátákat legközelebb legalább collstokkal mérjék le, hogy a mi dolgunk már tényleg gyerekjáték legyen.

Persze van más, ennél sokkal kézenfekvőbb megoldás is. A tisztatér szüzességét egy, a fedelet lezáró csavarra ragasztott matrica védi. Amíg ez érintetlen, addig tényleg gyerekjáték a motorcsere. Legalábbis azok számára, akiknek van collstokjuk.

Interaktív adatmentés

Valahol valakik ötvenkétezer .DBF fájlt töröltek a lemezről. Majd feleszméltek, hogy nem ezeket kellett volna.

Elküldték hozzánk a tárolót, mi formailag helyreállítottuk a file-okat, és visszaküldtük.

Teljes csőd, mindössze harminckettő lett használható. Itt megállt a tudományunk, mondtuk, de a megrendelő nem hagyta annyiban. Küldött a tartalomra jellemző mintát. Újabb 120 fájl vált használhatóvá. „Na, ennyi" – mondtuk. „Nem addig a'" – replikázott a megrendelő, és újabb mintákat küldött. Végül is beláttuk: ha a kliens jobban fut a pénzünk után, mint mi saját magunk, azt meg kell hálálni. Ezután vagy harminc, a fentiekhez hasonló tili-tolival feltakarítottuk a szennyest, és helyreállítottuk mind az ötvenkétezer DBF-et.

Nonstop drive

Nagy a baj, mondta az ügyfél. A winchester fölpörög, majd leáll, aztán ismét fölpörög, majd ismét leáll, és így megy ez napestig. Mindeközben pedig nem lehet hozzáférni, úgy el van foglalva önmagával, mint egy hiú nő.

Szakemberünk, mielőtt nekikezdett volna az adatlapok kitöltésének, megkérdezte: miért van a számítógép RESET gombja rágógumival leragasztva? „Az az átok gyerek" csapott homlokára az ügyfél, majd saját kezűleg elvégezte a cég történetének eddigi legolcsóbb adatmentési műveletét.

49. Melléfogások változó kimenetellel

A. Egy nemzetközi szervezet menekültekkel foglalkozó itthoni képviseletén a szerverről naponta készítettek mentést. Ez a gép tárolta a legfontosabb adatokat. Egy szép napon a szerver winchestere tönkrement. A mentett anyag helyreállításakor derült ki, hogy csak a programfájlokat mentették, az adatfájlokat nem.

Kétségbeesve hívtak minket. Több napnyi tisztaszobás munka után sikerült az adatokat helyreállítani. Mindez hét éve történt. Ekkor lett e nemzetközi szervezet hosszú távra ügyfelünk. Azóta mi tartjuk karban a rendszerüket. Géphiba több is történt ez idő alatt, de adatvesztés soha!

B. Nagy cég, bőven van pénz az adatvédelemre: 24 órás portaszolgálat, kamerarendszer, drága szerver, DAT (szalagos mentőegység), RAID (redundáns adattárolási rendszer). Az egyik reggel a felhasználók nem tudtak bejelentkezni a szerverre. A rendszergazda észlelte, hogy a RAID rendszerből több winchester is hiányzik. Éjjel valaki a működő szerverből kivette ezeket, és elvitte. Rendőrségi nyomozás derítette ki jóval később, hogy éppen a védelemmel megbízott portaszolgálatból huncutkodott valaki.

Semmi gond – gondolta a rendszergazda, és elővette a tartalék szervert, mert az is volt a raktárban. A rendszer elindult, már csak az adatokat kellet visszatölteni a szalagos mentőegységről. Mindez néhány perc alatt lezajlott. A rendszergazdának itt kezdett gyanús lenni az ügy. Kiderült, hogy a szalagokon nem volt semmilyen adat. Bár minden nap lefutott a mentés, a log fájlt ellenőrizték is, és ezt rendben lévőnek találták, de soha nem ellenőrizte senki, hogy van-e adat, és az visszatölthető-e. Noha a winchestertolvajt nyakon csípték, a winchesterek és vele együtt a pótolhatatlan adatok soha nem kerültek elő. Ennek az esetnek a kapcsán vezettük be az adott cégnél az Informatikai Biztonsági Technológiát, amely a tolvaj kezét lefogni nem tudja, de e veszéllyel képes számolni egy távoli backup rendszer üzembe helyezésével.

C. A saját házunk táján történt. A szerverszobánk kicsi. Van benne hét szerver és két telefonközpont, egy sereg kiegészítő eszközzel, amelyek rendesen termelik a hőt. Kapott is a szoba egy hőfokszabályozós ventillátort a hő elvezetésére. Egy alkalommal a telefonszerelő, míg a szobában matatott, zajosnak ítélte a ventillátort, és kikapcsolta. Munkája végeztével azonban elmulasztotta visszakapcsolni, és egyik szerverünk winchestere a nagy melegben tönkrement. Volt mentésünk, katasztrófatervünk és szakemberünk is, de akkor is dühösek voltunk. A ventillátor kapcsolójába épített 100 forintos időkapcsolóval mindezt megspórolhattuk volna. Ez az időkapcsoló 30 percnyi állás után visszakapcsolja az áramot.

Most már.

50. Töményen, poén nélkül

Az előző két tucatnyi történet esszenciája csokorba gyűjtve:

26. A dátumprobléma az Y2K problémától függetlenül is jelentkezhet, sőt!

27. Nem lehetsz elégedett a vírusvédelmeddel.

28. Az illegális szoftver használatát időnként a gyártók is megnehezítik. Csakhogy ez később szokott kiderülni: amikor már komoly a baj.

29. A DOS és a Windows 3.X operációs rendszert nem fejlesztik tovább.

30. A dátumprobléma a munkanap – hétvége meghatározásánál is jelentkezik.

31. Aki nem égette meg magát, az műbalhénak véli az Y2K körüli hajcihőt.

32. Értékes adat az, amit annak tartok. Minél több adatot tartok értékesnek, annál drágább a védelem megszervezése és fenntartása.

33. Utólag mindenki talál magyarázatot az adatvesztés okára.

34. Nem a winchester doboza, hanem a benne lévő tárcsa az adathordozó.

35. Adatlopáshoz elsősorban az operációs rendszerek hibáit használják ki.

36. A kezelőszemélyzet tevékenységének szabályozása elsőrendű érdek.

37. A korszerű operációs rendszerekbe beépítettek bizonyos fokú védelmet (security). Használjuk ki!

38. A VMS nagyobb biztonságot nyújt a jogosultságok tekintetében, mint a Unix.

39. Ne sajnáljuk a pénzt a szerver tápegységére. Meg a szünetmentes tápra se.

40. Az Informatikai Biztonsági Technológia a kisvállalatok számára is szükséges.

41. Nem elég a szünetmentes tápegységet megvenni, be is kell kapcsolni.

42. Az állami szervezetek az informatikai védelemre sajnos nem sokat fordítanak, noha a támadásoknak egyre inkább ki vannak téve.

43. A notebook informatikai védelme, a mobilitása miatt, igen macerás, de nem megoldhatatlan.

44. A hálózati rendszerekbe való behatoláshoz nem kell különleges szakértelem.

45. A hardver meglévő tervezési hibái, az operációs rendszer programozási hibái és a Neumann-elv együttesen felelős a könnyű hálózati behatolásokért.

46. A biztonság és a kényelem szempontjai hatásukat tekintve alapvetően ellentétesek.

47. A szabványosítás az informatikai biztonság kulcskérdése.

48. A legolcsóbb adatmentés a rágógumi eltávolítása a RESET gombról.

49. A ventillátorba épített filléres időkapcsoló milliós károktól óvhat meg.

AZ INFORMATIKAI BIZTONSÁGRÓL

1. Murphy: Ami elromolhat, az el is romlik

Mindenkit megdöbbent, ha repülőgép lezuhanásának hírét hallja. Az ilyen katasztrófa a TV-híradók első képsorain, az újságok „horror" oldalain szerepel. Füstölgő roncsok, túlélésre halvány remény...

A repülés technikája elméletileg tökéletesen ki van dolgozva, és mégis, műszaki hiba, emberi mulasztás vagy szándékos cselekmények miatt bekövetkezik egy-egy tragédia.

A repülés biztonságát minden érintett területre kiterjedő rendszer védi. E rendszer előírásainak maradéktalan betartása elméletileg biztosítja, hogy a légi utasok minden esetben eljussanak a célállomásra. Ha nagyritkán a biztonsági rendszeren akár alkatrészhiba, akár bomba formájában áttör egy-egy „zavaró hatás", beindul egy katasztrófa-elhárítási cselekvéssorozat.

Van, amikor ez sem vezet eredményre, és bekövetkezik a tragédia. Ilyenkor átfogó vizsgálatot tartanak a katasztrófa okának megállapítására. A vizsgálat célja az, hogy megtalálják és kiküszöböljék a rendszer hibáját, amely a

bajt okozta vagy lehetővé tette annak bekövetkeztét. Az itt vázolt rendszer működési zavara hatalmas anyagi kárt okoz és rendszerint emberáldozattal is jár. A minket körülvevő rendszerek általában (és szerencsére) nem ilyen kiélezett helyzetben működnek. Amit tapasztalatból viszont már tudunk, nincs 100%-os biztonsággal működő rendszer.

Az informatikai rendszerek (és a továbbiakban ezekkel foglalkozunk) mára teljesen átszőtték életünket, és többnyire megbízhatóan működnek. A „többnyire megbízható működés" csak akkor kerül górcső alá, ha az alkalmazási terület jelentős, esetleg pótolhatatlan értéket képvisel.

A repüléstechnikában ezek a fogalmak magától értetődőek, de mondjuk az államigazgatási rendszereknél már felmerülhet a kérdés, hogy mennyit érdemes áldozni egy közepesen biztonságos rendszerre, vagy hogy a biztonság egy-két százalékos növelése megéri-e a ráfordításokat?

Aki e témával foglalkozik, az tudja, hogy ilyen esetekben elsősorban a válaszadó pozíciója (vevő/eladó, főnök/beosztott) határozza meg a válasz tartalmát, mert objektív kapaszkodót nem könnyű találni.

E tanulmánnyal az a célunk, hogy megmutassunk néhány objektív kapaszkodót.

2. Ha nincs 100%-os biztonság, mekkora az elfogadható?

„A hűtőkamránkkal úgy kétévente történik valami. Áramkimaradás, vagy a kompresszor hibája miatt leolvad. Ilyenkor kb. 30 ezer forint értékű mélyhűtött áru megy tönkre. Amikor mérlegeltem, hogy vegyek-e 300 ezer forintért saját áramfejlesztőt és 200 ezerért kétkompresszoros hűtőgépet, elvetettem a gondolatot, mert a költség nem lett volna arányban a veszteséggel.

· Ha gyakrabban lenne áramkimaradás, vagy egymillió forint értékű kaviárt tárolnék a hűtőkamrában, másként döntenék.

· Ha pótolhatatlan laboratóriumi kutatási eredményeim hűtött tárolást igényelnének, változtatnék a hűtési rendszer biztonságán.

A fenti gondolatkísérlet következtetései:

· Kívánatos, hogy a rendszer működési biztonságáról legyen információm.

· Jó, ha ismerem a védendő „eszköz" értékét.

· Lényeges, hogy tudjam a biztonság növelésének a költségeit.

3. Mindent vagy semmit – volna esetleg középút?

„A légi utasforgalomban a biztonság általában teljes körű, de a katasztrófaterv végrehajtásakor a repülőgép biztonságával már csak annyira foglalkoznak, amennyire ez elősegíti az emberek védelmét. Az emberek között is a pilótáknak fokozottabb védelme van (pl. katapult), és az első osztályon utazók a statisztikák szerint védettebbek, mint a gép végében helyet foglalók."

Ha nem lennének költségkorlátok, a teljes rendszer egységes, minden szintre kiterjedő, azonos minőségű védelme jelentené a legnagyobb biztonságot. A gyakorlat azt mutatja, még a fenti, szándékosan kiélezett példában is, hogy az optimális biztonság szelektív. Ami értékesebb, az fokozottabb védelmet igényel. Szinte biztos, hogy minden környezetben, így az informatikában is, kialakulnak a biztonságra törekvés ösztönös, logikus formái. A nagy és bonyolult rendszereknél azonban az ösztönösség nem mindig tűnik elegendőnek.

Egy banki rendszernél feltételezhetően az adatok biztonsága a meghatározó jelentőségű, és a számítástechnikai eszközök biztonsága lényegében csak az eszközök piaci értéke szempontjából érdekes.

4. Hogyan védekezzek?

„Az autómat akkor törték fel, mikor egy pillanatra benne hagytam a táskámat."

„Éppen akkor törtek be hozzánk, amikor elfelejtettem bekapcsolni a riasztót."

„A winchesterem akkor ment tönkre, amikor a backup sem működött."

A védekezésben az a legnehezebb, hogy folyamatos készenlétet és cselekvést igényel.

Téved az, aki úgy hiszi, hogy a biztonság áru vagy szolgáltatás formájában megvásárolható.

A biztonság folyamatos fenntartásához természetesen szükségesek az áruként és szolgáltatásként megvásárolható elemek, de a biztonság ennél lényegesen több: a szervezet életébe beépülő, folyamatosan ellenőrzött, karbantartott technológia.

5. Milyen az átfogó informatikai biztonság?

A mi megközelítésünkben az informatikai biztonság egy technológia, amelynek keretrendszerét az ide vonatkozó szabványok szerint kidolgozott eljárások gyűjteménye adja.

Az Informatikai Biztonsági Technológia elemei az informatika (IT) rendszeréhez illeszkednek, ott válnak előírásokká, végrehajtható utasításokká. Ennek megfelelően,

az IT szervezeti egységének, az ott dolgozóknak a tevékenysége bővül, de új szervezet létrehozását, vagy szervezeti átalakítást az Informatikai Biztonsági Technológia alkalmazása nem igényel.

Az Informatikai Biztonsági Technológia alapgondolata a többszintű, visszacsatolásos folyamat-szabályozás.

A több szint az IT elemeket, az ezekből épülő logikai/fizikai egységeket alkotó alrendszereket és a teljes rendszert jelenti.

6. Mit jelent az informatikai biztonság?
Mit kell védeni, mitől, és mindez mennyibe kerül?

· Vannak eszközök (gépek, hálózatok, programok) és ezek segítségével kezelt input/output adatok és adatbázisok. Az értékes, védendő információ ennek a rendszernek a terméke. Jó közelítéssel ez az informatikai biztonság tárgya. A fenti kör elméletileg jól behatárolható és erre a körre megfogalmazhatók az általános informatikai biztonsági feladatok.

· Az itt körülhatárolt rendszert egy sor külső és belső hatás éri vagy érheti. Vírus, tűz, emberi mulasztás, szándékos károkozás, rendszerelem meghibásodás, stb. Ezek a hatások mérhetők, becsülhetők, rendszerbe foglalhatók, vizsgálhatók, modellezhetők.

· Általában a költségek peremfeltételként, vagy célfüggvényként jelennek meg.

A korszerű informatikai biztonsági rendszert, az itt felsorolt három alapelemből gyúrják ki, és a mi szóhasználatunkban Informatikai Biztonsági Technológia a neve. E technológia alapja az információtechnológiai (IT) rendszer valamennyi elemének folyamatosan vizsgálata az informatikai biztonsági eljárások szempontjából. A vizsgálatok eredményétől függően, a legjelentősebb veszélyforrásoknál, a költségkereteken belül, korrigálják a rendszert.

Az itt leírt folyamat az IT rendszer üzemeltetésének része, vagy részévé kell, hogy váljon. E vizsgálatokkal párhuzamosan, általában évente, a teljes vizsgálatot egy informatikai biztonságra szakosodott, külső (auditáló) cégnek is szükségszerűen el kell végeznie, aki a független vizsgáló szemszögéből összehasonlítja a megfogalmazott biztonsági eljárásokat a szabványelemekkel és a gyakorlati alkalmazással. Mindezen vizsgálatok célja az, hogy rávilágítsanak az informatikai biztonság gyenge pontjaira, az adatvesztés kockázatára és még egy sereg kézzelfogható paraméterre, mely a felelős vezetők számára világos képet fest a pillanatnyi helyzetről, és kiindulópontot ad a jövő stratégiai döntéseinek meghozatalához.

A hangsúly a rendszeres (belső/külső, valamint a részleges/teljes) vizsgálaton és ez alapján az informatikai biztonsági rendszer folyamatos módosításán, javításán van.

A világ olyan irányba halad, hogy a működőképesnek ítélt módszereket, technológiákat egységesíti, szabványosítja. Ez a folyamat játszódik most le az informatikai biztonság háza táján. Az informatikai rendszerek tartalmi, és felülvizsgálatuk formai követelményei szabványosak, illetve a szabványosításuk folyamatban van, hasonlóan például az ISO 9000 szabványsorozat alapján kidolgozott minőségbiztosítási rendszerekhez.

Ahol az adatok komoly, esetenként pótolhatatlan értéket jelentenek, ott alapvető gazdasági érdek az Informatikai Biztonsági Technológia bevezetése.

7. Milyen út vezet az Informatikai Biztonsági Technológia bevezetéséhez?

7.1 Az elhatározás:

Az informatikai biztonság megvalósításának feltétele a felső vezetés elkötelezettsége. A felső vezetés felel a rábízott értékekért, ő képes eldönteni az adatvesztés, az adatlopás okozta károk mértékét és ennek megfelelően az informatikai biztonságra fordítandó (vagy fordítható) erőforrások nagyságát.

7.2 Az elmélet:

Ma az a tendencia figyelhető meg a világban, hogy minden nagy horderejű műszaki eljárás szabványosítási folyamaton megy keresztül. Így van ez az informatikai biztonsággal is. Az informatikai biztonság szabványosításának célja: az informatikai biztonság eljárásainak egységes keretbe foglalása, annak érdekében, hogy az dokumentált, visszakereshető, elemezhető, módosítható és a megelőző tevékenységet támogató legyen. Ez a mondat a maga bonyolultságában azt fejezi ki, hogy az informatikai biztonság egy visszacsatolt önjavító folyamat (vagy legalábbis annak kellene lennie).

Az informatikai biztonság eljárásai szabványosak, illetve szabványosításuk folyamatban van.

7.3 A gyakorlat:

*7.*3.1 A felső vezetés által kidolgozott (vagy kidolgoztatott) informatikai stratégiai célok megfogalmazása, lényegében egy kézikönyv megalkotása a szabvánnyal és a helyi adottságokkal összhangban.

7.3.2 Adott körülmények között az informatikai biztonság minősítő vizsgálata. A minősítő vizsgálat a rendszer elemeinek, az alrendszereknek és a teljes rendszernek a működését vizsgálja megfelelőség vagy nem megfelelőség szempontjából.

7.3.3 A minősítő vizsgálat eredményeinek értékelése és intézkedési terv kidolgozása. Visszacsatolás a 7.3.1 ponthoz.

8. Tapasztalásaink

Tapasztalatból tudjuk, hogy az informatikai biztonság több irányból is megközelíthető.

Azon az oldalon, ahol már tíz éve állunk (adatmentés, katasztrófa-elhárítás), naponta találkozunk a negatív példák tucatjaival. Évente 2.000 adatmentés kerül hozzánk. Ezeknek közel egynegyedére (évente legalább 400 esetben) nincs megoldás, pótolhatatlan értékek vesznek el.

Több éves kutatási eredmények, műszaki alkotások dokumentációi, közintézmények, kórházak adatbázisai az áldozatok. Utólag szinte minden esetben levonhatók a következtetések, és a „Mit kellett volna tenni?" kérdésre egyértelmű válasz adható.

1996-ban indultunk el az informatikai biztonságot a megelőzés oldaláról megközelítő úton. Szakmai ismereteinkhez közelálló kis részfeladat kidolgozására kaptunk megbízást egy, a svájci biztosító társaságok és a velük kapcsolatban álló bankok részére kidolgozandó informatikai biztonsági projektben.

Ekkor találkoztunk először a szabványosított eljárásokra épülő informatikai biztonsági technológiával.

Az Informatikai Biztonsági Technológia tervezése, bevezetése, alkalmazása során szerzett eddigi tapasztalatainkat csokorba gyűjtöttük.

· Logikusan felépített, folyamatosan fejlődő, szabványokra épített technológia.

· Szabadon elérhető, megfelelő szakmai felkészültséggel könnyen testre szabható.

· Alkalmazásához komoly elhatározás és a résztvevők elkötelezett együttműködése szükséges, hiszen az IT rendszer teljes egészét érinti.

· A folyamatos üzemeltetés, karbantartás az IT szakembereire hárul, külső segítséget ez a tevékenység nem igényel.

· Az EU országaiban a kiemelt rendszereket (állami kézben lévő, biztosító társaság által felügyelt, stb.) időszakonként külső, független auditor kötelezően felülvizsgálja. Az állami támogatás, illetve a biztosítás fenntartásának

feltétele az informatikai biztonsági audit megléte. A külső, független audit természetesen akkor is elvégezhető, ha az nem kötelező.

· A bevezetés, alkalmazás egy sor, az informatikai biztonságon túlmutató eredménnyel jár, vagy járhat. Például a költségelemzés, a kockázatelemzés eredményeinek további felhasználása, racionalizálási ötletek, a hatékonyság növekedése, stb.

9. Összefoglaló

Az informatikai biztonság mérhető és meghatározható fogalom. Az informatikai biztonság célja az informatikai rendszer azon állapotának elérése, amelyben a kockázatok elfogadható intézkedésekkel elviselhető mértékűre csökkenthetők. Ez az állapot olyan nemzetközi szabványokon alapuló előírások és megelőző biztonsági intézkedések betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és megbízhatóságát érintik.

Az itt megfogalmazottakat ülteti át a gyakorlatba a nemzetközileg elfogadott szabványokra és a KÜRT Computer Rendszerház Rt. 12 éves adatmentési, adatvédelmi tapasztalatára épülő integrált adatvédelmi, adatbiztonsági rendszer, az Informatikai Biztonsági Technológia (IBiT®).

A KÜRT Rt. által fejlesztett IBiT® rendszer nyílt, amelynek alapját képezik:

· a British Standards (BS) 7799 szabványai;

· az ISACA (Information Systems Audit and Control Association) által kidolgozott COBiT (Control Objectives for Information and Related Technology) ajánlásai;

· a Common Criteria irányelvei;

· az Informatikai Tárcaközi Bizottság ajánlásai.

A KÜRT Rt. szakemberei rendelkeznek CISA (Certified Information System Auditor) nemzetközi minősítésű auditori vizsgával.

Az Informatikai Biztonsági Technológia (IBiT®) alapkövetelményei és alapelemei:

· A felső vezetés elkötelezettsége;

· Az informatikai rendszer elemeinek, valamint a köztük lévő kapcsolatoknak a rögzítése;

· Az informatikai rendszer működésének dokumentált szabályozása;

· Az informatikai rendszer folyamatos működésének és működtethetőségének biztosítása;

· A védendő rendszerek, alrendszerek körének és prioritásának tisztázása;

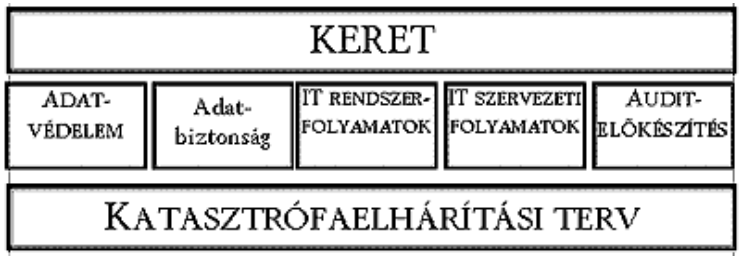
· A felelősségi körök tisztázása;

· Az informatikai rendszer működésének folyamatos korrigálása;

· Az informatikai rendszer és az informatikai biztonsági rendszer működtetését és irányítását végző személyek megfelelő felkészültségének és folyamatos képzésének biztosítása.

Az Informatikai Biztonsági Technológiához (IBiT®) kapcsolódó szabályzatok a vállalat szabályzati rendszerének integráns részei.

Az IBiT® szerkezete:



Kedves Olvasó!

Gratulálunk, hogy idáig eljutottál.

Nekünk 12 év kellett ahhoz, hogy idáig jussunk.

Ha az adataid védelméhez sikerült néhány ötletet adnunk, az külön öröm.

A továbbiakban nem fárasztunk szakmai zsargonnal, és nem is ijesztgetünk féltve őrzött adataid elvesztésével.

A következő lapokon 12 éves történelmünkből találsz néhány mosolyt fakasztó történetet.

E történetek elolvasása után talán lesz erőd ahhoz, hogy az előzőekre visszalapozz, és az adatvédelmi ötleteket saját környezetedben alkalmazd.

E szép és felelősségteljes, de keserves feladathoz sok sikert kívánnak a KÜRT munkatársai.

Történet 1

A történészek megírják majd, hogy a KÜRT már 1989 legelején, egy Fehérvári úti Patyolat fiókban kísérletet tett a monolitikus állam szétzúzására. A monolitikus állam és a Fehérvári úti Patyolat meghatározó volt kezdeti életünkben.

Ez utóbbinál, két bejárati ajtó lévén, egyiken a hibás adattárolót (winchestert) hozták be, a másikon a mosnivalót. Az utóbbit, ha nem volt a kosztól csontkemény, szoftvernek neveztük. Igaz, hogy két ajtón jöttek be az ügyfelek, de odabenn ugyanaz a kollégánk foglalkozott mind a hardver, mind a szoftver átvételével.

Látható: mi már ekkor megpróbálkoztunk a rendszerintegrációval: szoftver-hardver egy kézben! Sőt gondoltunk a bónrendszer bevezetésére is. Tíz winchesterjavítás után járt volna egy ingyen gatyamosás. Vagy fordítva.

Sajnos, mire e projektet beindítottuk volna, már akkora rés keletkezett az államszocialista rendszeren és a Patyolat vállalaton, hogy ott maradtunk gatya nélkül. Ezzel szemben dőlt hozzánk a sok rossz winchester. Így utólag már nem is bánjuk.

Történet 2

Gyönyörű nyári nap, verőfény. Fehérvári út, a KÜRT központja 80 négyzetméteren. Itt volt az igazgatóság, a könyvelés, az ügyfélszolgálat, a szerviz egy része, a kereskedés, a raktár meg a patyolat, sőt egy-egy WC, mosdó, konyha meg ebédlő is.

Egy alkalommal újságíró jött látogatóba. Égtem a vágytól, hogy elmondhassam, a KÜRT így, meg úgy, szabadalom, csúcstechnológia, high-tech, meg minden. Bent az igazgatói irodában 50 fok és 5 munkatársam 13 négyzetméteren. Ajánlottam: menjünk ki az utcára, ott kellemesebb, legalább 20 fokkal kevesebb és legalább 20 négyzetméterrel tágasabb. Felettünk ott virított a cégtábla: KÜRT WINCHESTER CENTRUM. Éppen belekezdtem, hogy a KÜRT így, meg úgy, amikor egy járókelő megszólít: „Uram, a Winchesteremen az irányzék elromlott, vállalják a javítását?" Mondom: „Nem, azokon a winchestereken, amelyeket mi javítunk, nincs irányzék."

Mire belekezdenék, hogy a KÜRT high-tech, így meg úgy, megszólít egy másik hozzánk látogató: „Önöknél a 0.6-os sörétet ezres, százas vagy tízes csomagban lehet kapni? Esetleg súlyra megy?" Mondom: „Nem, a mi winchesterünkbe nem lehet sörétet tölteni."

Mire belevágnék, hogy KÜRT, high-tech, meg így, meg úgy, az újságíró megjegyzi: „Nézze, az elmúlt öt percben már a második ügyfelét hajtotta el. Tulajdonképpen miből élnek maguk?”

Mire én: „A pucerájból.”

Történet 3

Kürti Sándor:

Ez a történet a testvéremről, Kürti Jánosról szól, pontosabban a testvérem és a zongora kapcsolatáról.

Nekünk egy Blüthner versenyzongoránk volt. Nagymamától maradt, aki nagy tehetségnek indult, majd zongoratanár lett. János Beatlest meg Omegát játszott volna szívesen a Blüthneren, amit anyukánk, finoman fogalmazva, szentségtörésnek tartott. Ez a konfliktus Jánosunknak is elvette a kedvét a nagy fekete behemóttól. A Blűthner ezután hosszú időn keresztül ott terpeszkedett a lakás közepén kihasználatlanul. Annyi feladata maradt, hogy karácsonykor az ajándékokat alá dugdostuk. Hason csúszva izgalmasabb volt a felfedezés.

És akkor eljött a nagy nap. Jánosnak, a mágneslemezt összeszerelő szerszámhoz nagy, sík felületre volt szüksége. A Blűthner teteje adta magát. Ennyi időt soha nem tartózkodott a zongoránál.

A zongora teteje fokozatosan életre kelt, vasdarabok, drótok, optikák, mechanikák, elektronikák lepték el. 1944-ben a volokolamszki országút látképe lehetett hasonló.

Amikor testvérem a mágneslemez-szerelés technológiáját szabadal-maztatta, a rajzokon a nagy síklapnak a Blüthner intarziás tetejét vázolta fel.

Senki sem értette, miért kell a tartólemeznek ilyen bonyolultnak lennie.

Történet 4

Kiss Eta, a főkönyvelőnk elhitette velünk, hogy egy fontos dolog van a világon (a szexen kívül), és ez a pénzügyi fegyelem. Tűzzel-vassal irtotta a kockázatos ügyleteket, noha volt belőlük elég.

1993-ban történt, hogy az Ipari Minisztérium ajánlatára beszállítottunk egy „korunk hőse" típusú vállalkozó beruházásába 30 milliónyit. Ez volt akkor minden mozdíthatónk. Ipari Minisztérium, gondoltuk, ennél jobb ajánlólevél nem kell. Mikor elmúlt a határidő, de a pénzünk nem jött meg, Eta utánanézett. Nem az Ipari Minisztériumnak, hanem korunk hősének. Éppen kétmilliárd hiánya volt akkor, és ezzel szemben mindössze egy szakadt téglagyárat tudott felmutatni Hajdúszoboszlón.

Első felindultságunkban másnap, az Őrmester fegyvereseivel megerősödve nekiindultunk, és elfoglaltuk fél Hajdúszoboszlót, agyagbányástul, csilléstül, vasútvonalastul.

Ha már ott voltunk, két horgásztavat, egy melegvizű forrást, meg a téglagyárat is magunkévá tettük.

A helybéliek még tátották a szájukat, mikor mi már gyártottuk a téglát. Ez így ment öt éven keresztül, mígnem eladtuk az utolsó téglát is, és vele együtt az egész gyárat.

Történet 5

Kürti Sándor:

Első cégautónk egy Zsuk típusú, 1 tonnás szállító jármű volt. 15 évesen került hozzánk, 15 000 forintért. Évenként ezer forint nem is rossz ár, pláne, hogy a tankja is tele volt. A járműhöz 3 sebességi fokozat járt alapkiépítésben.

Raktárt és szereldét a kezdetekkor a Svábhegyen, lánykori nevén a Szabadsághegyen béreltünk, szemben az amerikaiak golfpályájával. Akkoriban még nagy raktárra volt szükségünk, mert egy átlagos adathordozó akkora volt, mint egy konyhaszekrény, és mi évente vagy ezret javítottunk. A Zsukba éppen 20 konyhaszekrény fért bele, és benne is volt ennyi, amikor egy szép szeptemberi napon mindezt a raktárbázis felé próbáltam terelgetni.

Erre az időpontra esett a golfpálya közepébe épített új amerikai iskola ünnepélyes évnyitója is. Már majdnem célhoz értem a Zsukkal, amikor az hirtelen hátramenetbe váltott, majd kisvártatva lyukat ütve a kerítésen és a tornateremen, az ünneplők közé engedte a konyhaszekrényeket és a fékfolyadékot. Az ünnepi beszédet tartó kulturális attasé elsőre csak ennyit tudott kinyögni: Holy shit, what the hell? Lie down! A tolmács, jó érzéssel, csak az utolsó szavakat

fordította: mindenki hasra! Szó mi szó, én még életemben ennyi gyönyörű nőt nem fektettem le. Ruhástól! Az adattárolók és a fékfolyadék 1:1 arányú keverékébe!

Ez volt az első eset, hogy külföldi területre merészkedtünk szolgáltatásunkkal. Azóta ezt már többször megtettük.

Igaz, a Zsuk nélkül.

Történet 6

A tisztaszoba a KFKI területén áll: hatalmas építmény, külön férfi és női öltözőkkel. Mindkét nemnek két-két öltözője van, egyikben az utcai öltözet le, a másikban az űrhajós öltözet fel. A tisztatérbe tizenkét ajtón át lehet bejutni.

Dolánszky Gyuri első munkahelye e tisztaszoba volt, ahol Magdikával és Bandival dolgozott együtt. Magdi mindig korán jött és korán ment, Bandi ezzel szemben későn járó típus volt. Gyuri találkozott mind a kettejükkel, de csak munka közben, az űrhajós ruha és a fejfedő diszkrét takarásában.

E sci-fibe illő ruházatra azért van szükség, nehogy a haj, a szemfesték meg a hasonló matériák belepotyogjanak a csúcstechnológiába. Ez kétségkívül előnyös, de van hátránya is: uniformizál. Viselőjéből szinte semmi nem látszik.

Elég az hozzá, hogy három kollégánk már jó ideje együtt dolgozott, amikor egyszer a Fehérvári úti főhadiszálláson általános KÜRT értekezletet tartottunk. Itt mindenki jelen volt. Gyuri barátunk, miután észrevett a tömegben egy igen csinos hölgyet, igazi gentlemanként megkö-

zelítette, és annak rendje-módja szerint udvariasan bemutatkozott. A hölgy megriadt, és aggódó tekintettel érdeklődni kezdett Gyuri egészségi állapota iránt. Gyurink ekkora már teljesen összezavarodott.

Aztán, amikor ismét az ismeretlen hölgyre vetette tekintetét, és megpróbált mélyen a szemébe nézni, kezdett derengeni valami emlék, hogy ezeket a szemeket ő már látta valahol. Sőt akkor már hónapok óta együtt dolgozott e szép szempár tulajdonosával, Magdikával.

Lépcsőházi gondolat

Miután végigküzdötted magad e könyvecskén, Kedves Olvasó, kényelmesen hátradőlhetsz. Az adatvédelemről, az informatikai biztonságról lehullott a lepel. Mindent tudsz immár. Talán nem zavar meg e jóleső érzésedben még egy gondolatom:

A legjobb szabályozó- és védelmi rendszer, amellyel valaha találkoztam: a vegetatív idegrendszerem által menedzselt jómagam. Például a májam, amióta az eszemet tudom, teszi a dolgát, a szívem ugyanígy. A szimpatikus (nem vegetatív) idegrendszeremmel szabályozott tudatom, vélt felsőbb-rendűségével, folyamatosan támadja a számomra legértékesebb rendszert, szerény személyemet. Pia, cigi, stressz, stb.

No jó, nem közvetlenül támad, de nem is védekezik tisztességesen, csak úgy ímmel-ámmal. A tervek már rég megszülettek, ám folyamatos végrehajtásukról, ellenőrzésükről szó sincs. Jó, ha évente egyszer, úgy szilveszter táján születik egy utasítás. És az év többi napján, órájában, percében?

Isten óvjon attól, hogy a vegetatív idegrendszerem egyszer kikérje szabadságát, és ez időre átadja feladatait a

szimpatikusnak, a legapróbb részletességű végrehajtási utasításokkal együtt. Ahogy magamat ismerem, egy órába se telne, és elszúrnék valamit, még akkor is, ha tudatom tisztában van vele, hogy ettől feldobom a talpam.

Ezek után milyen esélye van a tudatomnak, hogy egy számára nem létfontosságú rendszert sikerrel menedzseljen?

Köszönetet mondunk mindenkinek. Szponzorainknak, akik már vesztettek adatot; és jövendő szponzorainknak, akik majd ezután fognak...

KÜRT Computer Rendszerház Rt.
1112 Budapest, Péterhegyi út 98.
Tel.: 228-5410 – Fax 228-5414
E-mail: kurt@kurt.hu
Honlap: www.kurt.hu

Tárhelybérlés világszínvonalon!

10, 350 és 500MB tárhely előre telepített szerveroldali megoldásokkal.
Vendégkönyv, form-mailer, apróhirdetések, linkgyűjtemények, képeslapküldő, web-áruházak hitelkártyaelfogadási lehetőséggel...

Ha nálunk bérel tárhelyet, csatlakozhat mini-Portal projectünkhöz, amelynek keretein belül számos előre telepített szolgáltatást helyezhet üzembe saját célra, ingyenesen.

LezliSoft - az első magyar virtuális könyvkiadó, a Vikk.net tárhelyszolgáltatója és fejlesztője.

http://www.lezlisoft.com - http://www.miniportal.hu