Eötvös Loránd Tudományegyetem

Informatikai Kar

Informatikai biztonsági mintaszabályzatok

Berényi Melinda

Témavezető: Kincses Zoltán

Budapest, 2005. június 12.

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani mindenkinek, aki valamilyen módon hozzájárult ahhoz, hogy ez a dolgozat elkészülhessen.

Elsősorban köszönöm témavezetőmnek, Kincses Zoltánnak, hogy érdeklődésemet az informatikai biztonság területe felé fordította. Hálás vagyok a dolgozattal kapcsolatos ötleteiért és útmutatásaiért, melyek nagy segítséget jelentettek a munka folyamán, valamint a végső forma eléréséhez nyújtott szerkesztési tanácsaiért.

Köszönettel tartozom a Biztostű portál készítőinek, informatikai biztonsággal kapcsolatos tananyagaik nemcsak hasznosak voltak a dolgozat készítésekor, hanem azon túl is számos kellemes percet és hasznos időtöltést jelentettek.

Végül, de nem utolsósorban köszönöm a támogatást Gellért Tamásnak, hogy a munka során végig mellettem állt.

Tartalomjegyzék

Bevezetés

Az informatikai biztonságról való gondolkodás manapság megkerülhetetlen tényezővé vált, hiszen biztonsági események tömege veszélyeztet minden informatikai rendszert. Ahhoz, hogy a biztonsági problémák egy nagyobb szervezeten belül jól kezelhetők legyenek, szükség van arra, hogy jól megtervezett, bevezetett, ledokumentált és számon kért intézkedések legyenek meghatározva. Így egyre több helyen mutatkozik igény írott, informatikai biztonságról szóló szabályozás létrehozására.

Összefoglalva dolgozatom célja, hogy átfogó képet nyújtson az informatikai biztonság szabályozásáról, ezen belül pedig áttekintsem az Informatikai Biztonsági Szabályzat elkészítésének módszereit.

Ehhez első részében elméleti áttekintést tartalmaz az informatikai biztonság témaköréről, annak fontosságáról, és az ezzel kapcsolatos szabályozásokról. Bemutatom, hogyan épül fel egy Informatikai Biztonsági Szabályzat, ennek készítésekor milyen problémákra kell odafigyelni. Majd az alkalmazható technikák felsorolása és rövid ismertetése következik, melyek a szabályzat készítése kapcsán szerephez juthatnak.

Dolgozatom második részében egy gyakorlati példa keretében megmutatom, hogy a dolgozat első felében bemutatott elveket milyen módon lehet a való életbe, a gyakorlatba átültetni. Ennek kapcsán az ELTE számára készült el a leendő Informatikai Biztonsági Szabályzatnak több részterület szabályozása, amelyek majdan alapul szolgálhatnak a szabályzat készítéséhez. Ezek nagy része hiánypótló szerepet tölt be, hiszen egységes, mindenre kiterjedő Informatikai Biztonsági Szabályzattal még nem rendelkezik Egyetemünk, és ennek elkészítése a közeljövő feladatai közé tartozik.

I. RÉSZ

1. Az informatikai biztonságról

1.1 Bevezetés

Mai világunkban egyre fontosabb szerepe van a számítógépeknek az azokat hálózatba kötő telekommunikációs rendszereknek. Az élet különböző területein ma már elképzelhetetlen a számítógép és az Internet használata nélkül boldogulni. Az állami, az oktatási és a gazdasági szféra munkavégzése egyaránt a számítógépek használatán alapul, így a számítógépes rendszerektől való függés egyre nagyobb és nagyobb lesz. A termelés, irányítás, oktatás által keletkezett információk, adatok nagy része már nemcsak papír alapon, hanem nagyrészt informatikai rendszerekben tárolódik. A világhálózat, az Internet terjedésével a kommunikáció és a világban való tájékozódás módja is megváltozik. Ebben az új világban az információ valódi értékké vált és annak védelme immáron elengedhetetlen. De nemcsak az adatot, információt, hanem magát a számítógépes rendszert is védeni szükséges, hiszen ezek támogatása nélkül könnyen megbénulhat a számítógépek által át meg átszőtt életünk.

Az informatikai biztonság, mint kedvező állapot elérése érdekében védelmi intézkedéseket kell alkalmaznunk. Ezeknek az intézkedéseknek át kell fogniuk az informatikai rendszer teljes életciklusát (létesítés, használat, változtatás, megszüntetés), és a védelemre fordított összeg arányban kell, hogy álljon az információ vagy a rendszer sérüléséből okozható kárral. Az informatikai rendszer védelme ki kell hogy terjedjen a fizikai, a logikai, a humánpolitikai védelem területére, valamint speciális eszközök és eljárások használatára.

Ezt a védelmet nehezíti, hogy a számítógépes rendszerek bonyolultsági foka egyre nő. Manapság a legjobb szakemberek is nehéz helyzetben vannak, hiszen ebből a bonyolultságból adódóan nem ismerhetik részleteibe menően a pontos működési mechanizmusokat, így rendkívül nehéz arról meggyőződniük, hogy egy rendszer tényleg úgy működik-e, ahogy kellene, valóban biztonságos-e vagy sem. Egy átlagos felhasználó (egy irodai dolgozó, akinek kezében a számítástechnikai rendszer és szoftver nem cél, hanem csak használati eszköz), még ennyire sem ismeri a számítógépet (ugyanúgy ahogy a mikrohullámú sütő vagy televízió működését sem ismeri pontosan, csak használatának módját). Nehezen tudja eldönteni, hogy egy adott rendszert használva mennyire van kiszolgáltatva a számítógépen keresztül rosszindulatú

embertársainak. Az előbbi példában ehhez nyújt segítséget a használati utasítás, amiből megtudhatja mindenki, hogy az elvárt funkcionalitás érdekében mit kell tennie, valamint a saját és környezete biztosságát hogyan tudja megóvni. Ilyen használati utasítás a számítástechnikai rendszerekhez az Informatikai Biztonsági Szabályzat, mely segít a helyes és biztonságos használat elsajátításában.

Ezen felül a rendszer folyamatos működésére nézve az egyes természeti tényezők (tűz, víz, villámcsapás, …) és a hardver meghibásodások is komoly veszélyt jelentenek, az adatok megsemmisülése mindennapos veszély. Ez a bizonytalanság bizalmatlanságot okoz, és a számítógépes rendszerek terjedését tekintve jelentős negatív hatása van.

1.2 Alapfogalmak

Biztonság

A fenti fogalom pontos meghatározása nehéz, különböző helyzetekben különbözően értelmezhetjük, mit jelent a biztonság. A biztonság szoros összefüggésben van az idővel. Általában arról beszélünk, hogy valami biztonságban van, és ezalatt mégis azt értjük, hogy a – közeli vagy távolabbi – jövőben nagy valószínűséggel nem történik vele semmi rossz (a múltban megtett megelőző intézkedéseknek köszönhetően valamint múltbeli tapasztalataink alapján), illetve ha mégis történne, akkor azt valahogyan ki tudjuk küszöbölni, és a jó állapotot rövid időn belül vissza tudjuk állítani. A biztonság megteremtése kapcsán olyan eseményekre kell felkészülni, amelyek eddig esetleg meg se történtek, és ha meg is történtek, az előfordulási gyakoriságuk kicsi. Ebből következik az a szakmai körökben általános nézet, hogy 100%-os biztonság nincs, nem lehet az összes nem kívánt eseményt feltérképezni, számba venni, illetve minden eshetőségre felkészülni, csak vállalni a kockázatát egy esetlegesen bekövetkező biztonsági eseménynek.

A biztonság egyszerre jelenti a rendszer működőképességét, rendelkezésre állását, az információk bizalmasságát, hitelességét és sértetlenségét.

Azt hogy mi a biztonság, sokszor nem is közvetlenül próbáljuk megfogalmazni, hanem éppen az ellentétes fogalmakkal (veszély, kár, kockázat, előre nem látható, nem kívánt esemény) írjuk körbe. Ezek közül több fogalom magyarázata később megtalálható.

Az informatika körében a biztonság különösen összetett, ugyanis itt nem elegendő, hogy egy rendszer jó, működőképes állapotban maradjon, hanem azt is meg kell gátolni, hogy bizalmas információk a rendszeren kívülre jussanak.

Összefoglalva a biztosság az a kedvező állapot, amelynek megváltozása nem valószínű, de nem is lehet kizárni. Vagyis minél kisebb a változás valószínűsége, annál nagyobb a biztonság. A védeni kívánt informatikai rendszer olyan, az adott intézmény számára kielégítő mértékű az állapota, zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg.

Biztonságérzet, veszélyérzet

A biztonság fogalmával szorosan összekapcsolódik, de egyben élesen el is válik tőle a biztonságérzet és a veszélyérzet fogalma. Aki nem törődik a biztonsági kérdésekkel, azt előbb utóbb komoly kár fogja érni. Ennek eredményeképpen nem fog megbízni a számítógépekben, félve, korlátozottan fogja azokat használni, ami így vagy úgy de a munkája hatékonyságának kárára megy majd. Mind a veszélyérzet hiánya, a hamis biztonságérzet, mind a túlzott félelem komoly veszélyt jelent. Ezért rendkívül fontos az informatikai biztonság oktatása, az oktatás és felkészülés révén a valós kockázat megismerése, a tudatos veszélyérzet, a kockázat-arányos védekezés és a megalapozott biztonságérzet kialakítása valamint a maradék kockázat tudatos vállalása

Kockázat

A biztonság fogalma pozitív irányból közelíti meg az elérni kívánt állapotot (Mit szeretnék?), ezzel szemben a kockázat az ellenétes oldalról közelít (Minek a bekövetkezését szeretném megakadályozni? Mi ne történhessen meg?). A kockázat gyakorlatiasabb szemlélettel egy rendszert fenyegető veszélyeket veszi számba, és az általuk okozott károkat próbálja megbecsülni, összegezni. A kockázat matematikai fogalmakkal a rendszert ért váratlan eseményekből keletkező kár várható értéke adott időre vetítve. A kár értéke nagyon sok esetben nem könnyen meghatározható, pénzben nehezen számszerűsíthető, hiszen pl. egy információ elvesztésénél nemcsak az újbóli megszerzésének költsége merül fel, hanem áttételes károk is (illetéktelen kezekbe kerülése, ennek következtében a fogyasztók, felhasználók bizalom vesztése, ebből adódó presztízsveszteségek). Ezért legtöbbször nem is vállalkoznak konkrét becslésekre, inkább csak kockázat elemzésről, a kockázat csökkentéséről, menedzselésről szokás beszélni ezen a területen. Az előzőekből adódóan hazánkban

nagyon kevés biztosító foglalkozik informatikai biztosításokkal, a károk számszerűsítésének nehézségei miatt. Esetleg különböző kockázati kategóriák felállításáról lehet még szó, ahol a károk nem abszolút értékben, hanem egymáshoz viszonyítva jelennek meg.

Adat

Az információ megjelenési formája, jelentéssel bíró szimbólumok összessége.

Adatbiztonság, adatvédelem

Az adatvédelem az adatok jogi értelemben vett (törvényekkel, szabályzatokkal való) védelmét jelenti, míg az adatbiztonság fogalma magát a technikai védelmet fedi.

Adatbiztonságnak nevezzük az adatok jogosulatlan megismerése, megszerzése, módosítása és megsemmisítése elleni logikai (szervezési) és fizikai (műszaki) védelmi megoldások, valamint szervezési intézkedések, eljárások egységes rendszerét.

Szokás még a számítógépes rendszerek és a bennük tárolt információk biztonságát informatikai biztonságnak is nevezni. Az informatikai biztonság két nagy területre osztható: az információvédelem és a megbízható működés. Míg az információvédelem az adatok sértetlenségével, bizalmasságával, hitelességével foglalkozik, addig az utóbbi a rendelkezésre állással és a funkcionalitás biztosításával.

Bizalmasság

Az információkhoz vagy adatokhoz csak az arra jogosultak és csak az előírt módon férhetnek hozzá. A bizalmasság követelményét a megfelelő hozzáférési jogosultságok beállításával lehet elérni.

Sértetlenség

Egy információ vagy rendszer sértetlen, ha csak az arra jogosultak változtathatják meg vagy minden kétséget kizáróan megállapítható az a tény, hogy az előállítás óta változatlan maradt.

Hitelesség

Egy információ akkor tekinthető hitelesnek, ha mind tartalmának, mind létrehozójának (küldőjének) sértetlensége garantálható.

Rendelkezésre állás

A rendelkezésre állás követelménye azt rögzíti, hogy egy adott rendszernek milyen megbízhatósággal kell ellátnia a feladatát. Ez a fogalom körülírható olyan objektív statisztikai jellemzőkkel, mint az üzemidő, a rendelkezésre állási tényező és a sebezhetőségi ablak. Mivel a rendelkezésre állást véletlen események (meghibásodás, tűz, víz, betörés) is fenyegetik, de akár támadók tevékenysége sem zárható ki, a fenti statisztikai jellemzők garantálása érdekében határozott védelmi intézkedéseket kell megtenni.

1.3 Néhány alapvető igazság

Tökéletes biztonság nincs, csak tudatos kockázatvállalás.

Tökéletes biztonság két okból se valósítható meg. Egyrészt a bekövetkezhető váratlan események köre nem behatárolható, így minden eshetőségre nem lehet felkészülni. Másrészt elképzelhetőek olyan események (természeti katasztrófa vagy éppen egy eltérített repülőgép), amelyek olyan kivédhetetlen, elkerülhetetlen veszélyt jelenthetnek, ami ellen nem lehet védekezni.

Továbbá a tökéletes biztonság megvalósulásának lehetőségét akadályozza az is, hogy az emberi és pénzügyi források minden esetben végesek (ez is a normális, hiszen a védekezésnek elég az elszenvedett károkkal arányosnak lennie).

Így mindig kétkedve kell fogadni a tökéletes biztonságú rendszerként aposztrofált termékeket, eljárásokat.

A biztonság nem egy termék, hanem egy eljárás!

Alapvető hiba a biztonságról úgy gondolkodni, mintha az egyszerűen egy termék lenne, amit ha egyszer megvásároltunk, akkor a továbbiakban biztonságban érezhetjük magunkat. A biztonság rendkívül összetett fogalom, különböző helyzetekben más-más eszköz vagy eljárás alkalmazása lehet célravezető. A rendszerek egyre összetettebbek, így nem adhat teljes megoldást egyik vagy másik operációs rendszer, tűzfal, vagy biztonsági beállítás alkalmazása sem, csak ha megfelelő környezetben használjuk. A biztonság alapvetően egy sajátos szemléletmódot követel meg, a biztonságról összefüggéseiben kell gondolkodni. A tűzfal, mint termék önmagában nem old meg

semmit, ha nem megfelelőek a beállításai, és minden hálózati forgalom engedélyezve van.

A biztonság, mint eljárás fogalompárosítás a folyamatosság szempontjából nézve is találó, hiszen legtöbbször nem egyszeri biztonsági intézkedésekről van szó, hanem olyan eljárásokról, amik átfogják a rendszer egész működését.

Addig nem hiszik el az emberek, hogy valami biztonsági esemény érheti őket, amíg meg nem történik velük.

Elkerülendő, hogy csak akkor vegyék komolyan a biztonságot, amikor biztonsági esemény történik, érdemes demonstrálni a fenyegetettséget és a sikeres támadás hatásait. Egy felkészületlenül bekövetkezett biztonsági esemény visszafordíthatatlan és helyrehozhatatlan károkat okozhat.

A legbiztonságosabb hálózat a menedzselt hálózat.

A biztonság eléréséhez elengedhetetlen a folyamatosság, a biztonsági intézkedéseknek a rendszer egész életciklusát át kell fogniuk. Egy vírusirtó telepítése legalább olyan fontos, mint a későbbiekben a rendszeres frissítése. Ugyanígy hiába naplózzuk az eseményeket, ha soha nem nézzük meg, mi került a naplófájlba.

Egy elhanyagolt hálózat az idő teltével egyre nagyobb veszélyt jelent. Sokszor nem is észlelhető a sikeres támadás, mert az elhanyagolt rendszereket ugródeszkának használják a támadók, ezért igyekeznek rejtve maradni a sikeresen támadott rendszerben.

Mindenki célpont az Interneten.

Nagyon sokan hajlamosak azt hinni, hogy az ő jelszavuk senkit sem érdekel, vagy az ő rendszerükön nincs semmilyen értékes információ, amiért oda érdemes lenne betörni. A támadók sokszor olyan automatikus eszközökkel keresik a gyenge pontokat, melyek nem foglalkoznak az egyéniségünkkel, csak azzal, hogy egyszerűen kitalálható-e a jelszavunk vagy sem. Egy gyengén védett gép nem kell, hogy értékes adatokat tároljon, elég, ha ugródeszkának használható egy már értékes adatokat tároló gép feltörése felé, és így az eredeti támadó rejtve maradhat a feltört gép álarca mögött.

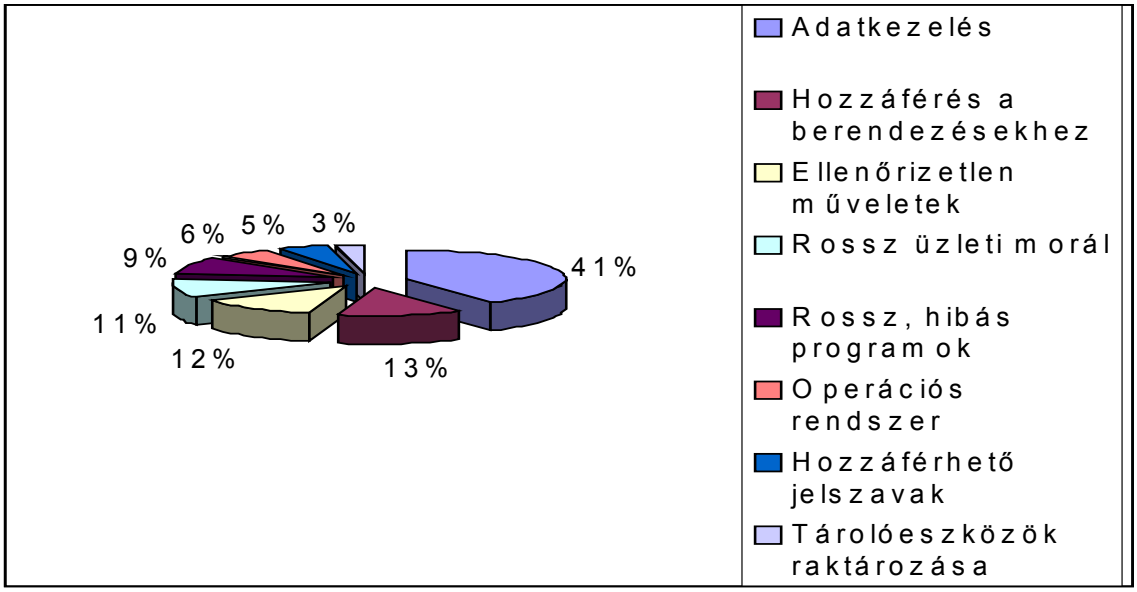
Az Internet forgalmának elemzése azt mutatja, hogy sokan élnek ezzel a lehetőséggel és gyakorlatilag sok-sok számítógép folyamatos üzemben pásztázza az Internetet lehetséges célpontok után vadászva.

A biztonság akkor fog jól működni, ha a biztonságos megoldás egyben az egyszerű megoldás.

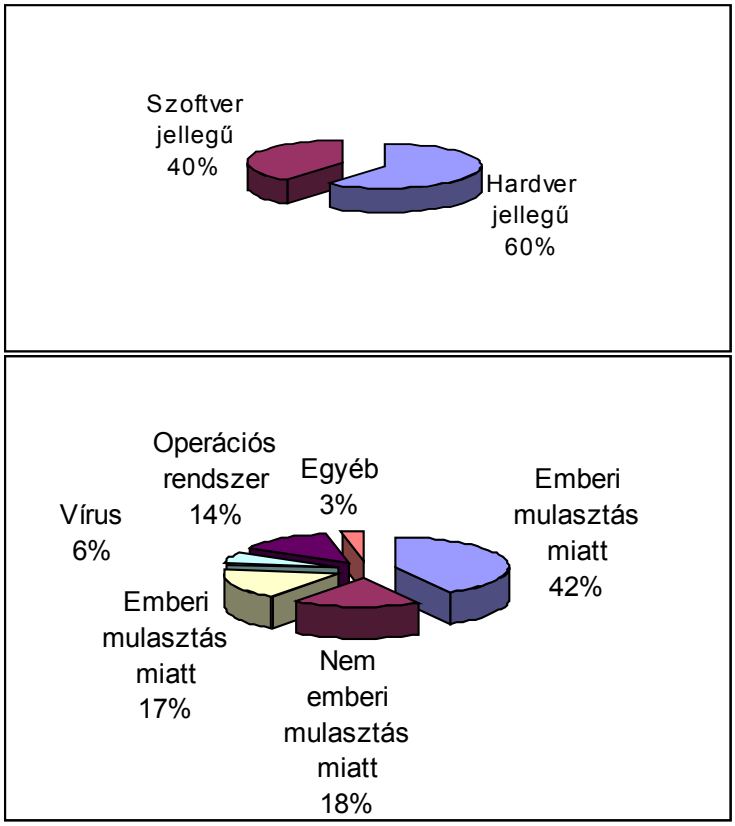
A biztonsági intézkedések sokszor kényelmetlenséggel járnak, ezért az emberek számára terhes lehet, megpróbálják kikerülni, végső esetben szabotálhatják is a rendszert, ami végül rosszabb helyzethez vezet, mint amilyen az intézkedések bevezetését megelőző állapot volt (akkor legalább mindenki tisztában volt vele, hogy nincs megfelelő védelem, így pedig a hamis biztonságérzet illúziójába ringatja magát). Ha például egy rendszerhez gép által generált jelszó használatát teszik kötelezővé, akkor az emberek le fogják írni papírra a jelszavukat, ami adott esetben nagyobb fenyegetettséget jelenthet, mint ha egyszerűbb, de megjegyezhető jelszót választottak volna. A biztonsági megoldásokat mindig lehet fokozni a teljes használhatatlanságig, de többnyire nem ez a cél. Az egyszerű megoldást könnyebb elfogadtatni és a beidegződése is gyorsabb, így sokkal hatásosabb védelem lehet.

1.4 Informatikai biztonság a számok tükrében

Az IT rendszerek gyenge pontjai:



Az IT meghibásodásának okai:



2. Kacsolódó szabványok és ajánlások ismertetése

A következőkben bemutatott szabványok és ajánlások az informatikai biztonság terültét, annak szabályozását járják körbe. Szemléletmódjukban némiképp különböznek egymástól, de mindegyikük széles körben elismertnek és elterjedtnek számít, és rendkívül sok helyen alkalmazzák őket informatikai biztonság megvalósításához iránymutatásnak, és egy részük minőségbiztosítási feladatokra is alkalmas és alkalmazott.

2.1 BS7799 (ISO/IEC17799)

A Brit Szabványügyi Hivatal (British Standard Institute, innen a BS betű pár) által a 90-es évek közepén kiadott, majd 1999-ben átdolgozott szabvány. Eredetileg két részből áll, első része (BS7799-1) lett nemzetközi szabvány (ISO/IEN17799 a nemzetközi szabvány neve, 2000-ben adták ki), ennek magyar nyelvű változata is létezik, címe Az informatikai biztonság menedzsmentje (Code of practice for the Information Security Managment System). A második része (BS7799-2, Information security management System- specifications with guidance for use: Informatikai biztonság menedzsment – útmutatás a használathoz) a gyakorlati elveket helyezi előtérbe, ez a rész nem vált nemzetközi szabvánnyá (jelenleg Nagy-Britannia és néhány európai ország alkalmazza, folyamatban van magyar szabványként történő bevezetése is, jelenleg MSZE 17799-2 néven, „Az információvédelem irányítási rendszerei. Előírás és használati útmutató” címmel magyar előszabványként jelent meg).

Az ISO17799 szabvány az információbiztonságot felülről, a vezetés, menedzsment szintjéről közelíti meg, a szervezet céljaiból és nem pedig az általa előállított termékből indul ki. Mivel nem követelményeket, hanem szabályozási szempontrendszert fogalmaz meg, ezért alkalmas a biztonságmenedzsment tanúsítására is (az ISO9000-es szabványokhoz hasonló szellemben), de alkalmazható a biztonságmenedzsment javítására is. Az ISO17799 szabvány konkrét biztonsági megoldásokkal nem foglalkozik, szándékosan rugalmas szabályrendszert állít fel, ezzel technológiától független tud maradni, képes a technikai fejlődés követésére és nagyon széles spektrumú szervezetek, intézmények számára tud iránymutatást adni. Vizsgálati alanya kiterjed nemcsak a fizikai és technikai, hanem a humán biztonság területére is.

A szabvány által ellenőrzött 10 terület:

1. **Biztonságpolitika**

   A szervezet legmagasabb szintű informatikai biztonsággal foglalkozó dokumentuma, amely útmutatást és tanácsokat ad az informatikai biztonság megtervezéséhez, vezetői szintű döntésekhez és alapelveket határoz meg.

2. **Szervezeti biztonság**

   Javasolja, hogy definiáljanak az informatikai biztonság területén külön feladat- és felelősségi köröket a szervezeten belül, és hogy ezekhez milyen végrehajtási módok tartoznak.

3. **Javak osztályozása és ellenőrzése**

   El kell készíteni egy leltárt a javakról, osztályozni őket, és mindent a fontosságának megfelelő szinten kell védeni.

4. **Személyi biztonság**

   Az emberi hiba, lopás, csalás, szabotázs, hozzá nem értés kockázatának csökkentése a cél. Magában foglalja a dolgozók oktatását, felkészítését, hogy mit várnak el tőlük az informatikai biztonsággal kapcsolatban.

5. **Fizikai és környezeti biztonság**

   A védendő területek meghatározása, és a hozzáférés ellenőrzése a témája.

6. **Kommunikációs és műveleti menedzsment**

   Az információ tárolásának, feldolgozásának és terjesztésének védelméről szól, a hardver, szoftver és hálózati elemek biztonságáról is gondoskodva. Ez magában foglalja mind az információt feldolgozó berendezések helyes működését, mind az információk és egyéb javak sértetlenségének, hitelességének és rendelkezésre állásának biztosítását, a rendszerhibák minimalizálását, a hálózati adatvesztés és adatmódosítás kivédését illetve észlelését is.

7. **Hozzáférési jogok ellenőrzés**

   Emlékeztet arra, hogy az adott intézmény hálózatához, gépeihez illetve információihoz való hozzáférést is ellenőrizni kell (külső és belső visszaélésekre is gondolva).

8. **A rendszer fejlesztése és karbantartása**

   Figyelembe kell venni, hogy a hardver- és szoftverfejlesztések és upgrade-ek milyen hatással vannak a biztonságra, mint a bevezetés, mind a későbbi karbantartás kapcsán.

9. **Üzletmenet folytonossági menedzsment**

   A katasztrófákra való felkészülés fontosságát hangsúlyozza, hogy mindig legyen ilyen esetre terv, ami alapján a nem várt helyzettel is meg lehet birkózni. A katasztrófa itt elsősorban nem természeti csapást jelent, hanem minden olyan eseményt, ami az üzletmenetben helyrehozhatatlan károkat okozhat (a tolerálhatónál nagyobb kiesést akár pénzben, akár időben számítva).

10. **Megfelelőség**

    A fenti előírások összehasonlítását javasolja más jogi szabályokkal.

Az előkészületben levő magyar szabvány a brit szabvány második részéből készült. Célja, hogy a nemzetközi és európai szabványokkal le nem fedett területeken a hazai gyakorlatban is jól használható előírásokat és útmutatásokat adjon az információvédelem irányításához. A szabvány összhangban van az ISO 9001:2000 és az ISO 14001:1996 szabványokkal (a fejezeteik közötti kapcsolat megtalálható az előszabvány mellékletében), így ezekkel együtt a minőségbiztosítás területén is alkalmazható.

2.2 TCSEC

A legrégebbi, az USA Védelmi Minisztériuma által kidolgozott TCSEC szabvány (Trusted Computer System Evaluation Criteria – Kritériumok a számítógéprendszerek megbízhatóságának kiértékeléséhez), amely alapján a számítástechnikai rendszerek biztonsági szempontból minősíthetők. Ennek a szabványnak a használata az USA központi rendszereinél a mai napig is érvényes és kötelező. A TCSEC az informatikai rendszereket biztonsági szempontból négy osztályba sorolja, amelyek különböző erősségű védelmi szinteket jelentenek az alapján, hogy milyen hatékonyan működik az informatikai biztonsági szabályozás. A kategóriákon belül további bontás van, ahol növekvő számozással különböztetik meg az egyre erősebb követelményeket.
A TCSEC alapvető négy biztonsági osztálya:

- D osztály: minimális védelem
- C osztály: szelektív és ellenőrzött védelem
- B osztály: kötelező védelem
- A osztály: bizonyított védelem

A gyakorlati életben elsősorban a B és C osztályok előírásait szokták követendő irányvonalnak tekinteni. A TCSEC a D osztályt érdemtelennek tekinti az informatikai biztonság szempontjából, az A osztály pedig olyan egyedi és eseti előírásokat, tartalmaz (pl. az alkalmazott biztonsági módszerek helyességének matematikai bizonyítása), amelyek a gyakorlatban csak nagyon nagy ráfordításokkal valósíthatók meg.

Az osztályozáshoz a minősítést négy területen kell elvégezni: biztonsági stratégia (security policy), követhetőség (accountability), biztosítékok (assurance), dokumentálás (documentation).

A gyakorlatban használt B és C csoportot a következő módon lehet további osztályokra bontani:

C Csoport

C1 osztály

- korlátozott hozzáférés-védelem
- a hozzáférési jogokat megvonással lehet szűkíteni

C2 osztály

- nem szabályozott, de ellenőrzött hozzáférés-védelem
- a hozzáférési jogok odaítélése egyedre/csoportra szabott

B csoport

B1 osztály

- címkézett és kötelező hozzáférés-védelem
- a hozzáférő alanyokat (felhasználók, programok) és a hozzáférés tárgyait (adatállományok, erőforrások) a hozzáférési mechanizmust szabályozó hozzáférési címkével kell kötelezően ellátni

B2 osztály

- strukturált hozzáférés-védelem,
- az alanyok azonosítása és a hozzáférés ellenőrzése elkülönített referencia-monitor segítségével történik

B3 osztály

- elkülönített védelmi terület
- a biztonsági felügyelő, operátor és a felhasználó biztonsági funkciói és jogai elkülönítve
- már a rendszer tervezése során el kell választani a biztonsági szempontból kritikus részeket

2.3 ITSEC

Az ITSEC (Information Technology Security Evaluation Criteria – Információtechnológia Biztonsági Értékelési Kritériumok) a TCSEC és más nemzeti dokumentumok figyelembevételével az Európai Közösség által kidolgozott ajánlás (1991. június). Első változatának kidolgozásában még csak Anglia, Franciaország, Hollandia és Németország vett részt, továbbfejlesztett változata a fenti dokumentum. Alapvetően megegyezik a TCSEC-kel, főleg elveit és követelményeit tekintve, de bizonyos részekkel ki is bővíti azt (pl. releváns informatikai rendszertípusokra is meghatároz biztonsági osztályokat).

2.4 ISO 9000-3

Az informatikai fejlesztés és karbantartás a szabványosításnak mindig problémás területe volt. Azért van ez így, mert a szoftverfejlesztés és karbantartás folyamata jelentősen eltér az iparban megszokott, és már jól bevált, szabványosított folyamatoktól. Mivel nagyon gyorsan fejlődő technológiai területről van szó, és itt is szükséges valamiféle minőségbiztosítás, ezért szükséges kiegészítő útmutatást adni, amelyben szoftvertermékről is szó van. Ilyen az ISO 9000-hez kiadott 3-as kiegészítés, ami szoftverfejlesztések minőségvizsgálatára szolgál (illetve egy másik, az ISO 12207 szabvány, ami szintén szoftverfejlesztéseknek tanúsítására szolgál).

A szabványosítás sajátossága, hogy a szoftverfejlesztésnél egyes tevékenységek a fejlesztés egyedi fázisaihoz kapcsolódnak csupán, mások pedig a fejlesztés teljes folyamatában alkalmazhatók. Az ISO 9000-3 szabvány követi ezeket a sajátosságokat, és az előírásai tükrözik az előbb említett különbségeket.

A szabvány Magyarországon is elfogadott, irányelvnek tekinthető az ISO 9001 alkalmazására szoftverfejlesztés és karbantartás területén. A szabvány gyakorlatilag a szoftverfejlesztésnek a teljes folyamatát végigköveti, illetve a szoftvernek az alkalmazását is. 10 lépésben összefoglalva a következőket vizsgálja:

1. Általános feltételek meghatározása
2. A szerződés átvizsgálása
3. A megrendelő követelményeinek előírása
4. A fejlesztés tervezése

5. Minőségtervezés
6. Programszerkesztés és programírás
7. Tesztelés és bevizsgálás (érvényesítés)
8. Átvétel
9. Másolatkészítés, szállítás és üzembe helyezés
10. Karbantartás

2.5 COBIT

Az ISACA (Information Systems Audit and Control Association – Információs Rendszer Ellenőrzési és Kontroll Egyesület) által kidolgozott szabvány a COBIT (Control Objectives for Information and Related Technology), amely segítséget nyújt az információ technológia irányításához, kontrolljához és ellenőrzéséhez.

A COBIT olyan általánosan elfogadott informatikai kontroll célok és irányelvek gyűjteménye, amelyek széles körben alkalmazhatóak és elfogadottak az IT biztonság ellenőrzésének és szabályozásának területén mind a vezetők, mind a felhasználók, mind az auditorok körében.

A COBIT rendszer alapján vizsgákat is szerveznek, itt a CISA (Certified Information System Auditor) minősítést lehet megszerezni, ami hazánkban is elfogadott és elismert vizsga informatikai biztonsági szakemberek számára.

A rendszer kézikönyveinek (3. kiadásának) létezik magyar nyelvű változata is, ez „Irányelvek az információ-technológia irányításához, kontrolljához és ellenőrzéséhez” címmel 2000 évben készült el a COBIT Irányító Bizottsága és az IT Governance InstituteTM gondozásában.

A keretrendszer 34 általános kontroll irányelvet tartalmaz. Ezek négy csoportba sorolhatók:

- tervezés és szervezet;
- beszerzés és üzembe állítás;
- informatikai szolgáltatás és támogatás;
- felügyelet.

A COBIT küldetése: „Mértékadó, naprakész és nemzetközi érvényű, általánosan elfogadott informatikai kontroll irányelvek kutatása, kidolgozása, publikálása és

támogatása, amelyeket napi munkájuk során tudnak használni az üzletemberek, ellenőrök és könyvvizsgálók.”

2.6 Common Criteria (ISO15408)

A Common Criteria, azaz Közös Követelményrendszer az Egyesült Államok, Kanada és az EU támogatásával jött létre 1996-ban (az érvényben levő szabványokat akarták egységesíteni), majd 1998-ben megjelent a 2.0-s változat, ami a következő évben ISO15408 néven nemzetközi szabványnak lett elfogadva. Jelenleg a 2.1-es változat van érvényben. Magyar változata az Informatikai Tárcaközi Bizottság 16. számú ajánlásaként lett kiadva.

Egységes, a megvalósítástól független biztonsági szinteket definiál, szám szerint hetet (EAL1-EAL7, Evaluation Assurance Level). Egy védelmi profil (szint) funkcionális és garancia követelmények összességét tartalmazza. A szintek egyértelműen meghatározott tulajdonságokkal rendelkeznek, adott fenyegetettségek ellen védettek, és a vizsgált rendszer védelmi intézkedéseinek bizonyíthatóan elégségesnek kell lennie ahhoz, hogy ezeket a fenyegetéseket kivédje.

2.7 ITIL

Az ITIL (Information Technology Infrastructure Library) a brit kormányzati szervek közreműködésével kialakított, hazájában BS 15000 néven szabvánnyá vált módszertan gyűjtemény. Az informatikai infrastruktúrának az üzemeltetési (tervezés, bevezetés, működtetés) kérdésit tekinti át. Az általános elveken túl tartalmaz kifejezetten gyakorlati kérdésekkel foglalkozó részeket is. Több mint 40 kötete látott napvilágot, ebből a 10 legfontosabb lett maga az ITIL ajánlás. Magyar nyelven az Informatikai Tárcaközi Bizottság 15. számú ajánlása tartalmazza (itt is csak első tíz kötetének témáit), valamint az „ITIL – az informatikaszolgáltatás módszertana” címmel 2002-ben készült munka.

2.8 ITB ajánlások

Az Informatikai Tárcaközi Bizottság (ITB) által kiadott ajánlások mára idejét múlttá váltak (közel tíz éve. 1994-96-ban láttak napvilágot), de történelmi szempontból mindenképpen lényeges megemlíteni őket, hiszen informatikai biztonság témakörében állami szinten ezek az első kezdeményezések hazánkban.

Az ajánlások közül a 8-as, 12-es és 16-os kapcsolódik szorosabban az informatikai biztonság témaköréhez.

A 8. számú ajánlás „Informatikai biztonsági módszertani kézikönyv" címmel jelent meg. A dokumentum az informatikai biztonság jelentőségéről, alapjairól, és az elvégzendő feladatokról szól (főleg informatikai vezetőknek, és főleg az államigazgatás területén), az informatikai biztonság európai ajánlásokhoz igazodó megteremtéséről.

A 12. számú ajánlás (Informatikai rendszerek biztonsági követelményei) első részében biztonságpolitikával és biztonsági stratégiával foglalkozik, másodikban biztonsági követelményekkel (itt különböző biztonsági osztályok és azok követelményeinek leírása található), a harmadik rész pedig egy Informatikai Biztonsági Szabályzat tervezetét tartalmazza. A dokumentum az informatikai biztonságot két nagy területre osztja, ezek az információvédelem és a megbízható működés. Míg az elsőbe a bizalmasság, sértetlenség és hitelesség követelménye tartozik, addig a másodikba a rendelkezésre állás és funkcionalitás.

A 16. számú ajánlás a korábban már említett Common Criteria magyar nyelvű megfelelője.

Teljes átdolgozásuk és korszerűsítésük folyamatban van IBiT (Informatikai Biztonsági Technológia) címmel.

3. Törvényi háttér

A szabványok és ajánlások az informatika rendszereket alkalmazó és működtető egyének és szervezetek munkáját segíti elő. De mindig akadnak, akik ki akarják használni a hiányosságokat, jogosulatlan előnyökre szeretnének szert tenni, ezért mára az informatikai biztonság is megköveteli a törvényi szabályozást. A visszaéléseket nehéz lenne megakadályozni, ha nem lennének büntetőjogi következményei a szabálytalanságoknak. Ugyanakkor a törvényhozók sincsenek könnyű helyzetben, hiszen olyan törvényeket kell alkotniuk, amik a lehető legnagyobb mértékben függetlenek a technológiától, így a technikai fejlődés ellenére is hosszú távon alkalmazhatók maradnak. Ezért tapasztalhatjuk az alább felsorolt törvények esetében is azt, hogy a technológiához kötődő elnevezések helyett igyekeznek általánosabb, inkább a funkcionalitást meghatározó fogalmakat használni. Ezen kívül a törvényeknek nem szabad gátolniuk a technikai és gazdasági fejlődést, és szabályozást csak ott kell létrehozni, ahol erre valóban szükség van.

2001. évi CXXI. törvény

A törvény a Büntető Törvénykönyv 2002. április 1-től hatályos módosítását tartalmazza. A Büntető Törvénykönyvbe új vétségek és bűncselekmények kerültek be, mégpedig a következők:

- „*Számítástechnikai rendszer és adatok elleni bűncselekmény*” és
- „*Számítástechnikai rendszer védelmet biztosító technikai intézkedések kijátszása*”.

A fenti kategóriák a Btk. 300/C illetve 300/E paragrafusában találhatók.

A 300/C passzus szerint a törvény bünteti, ha valaki „*számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad*”. Ezen kívül büntetendő az is, aki „*számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz*” illetve „*adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza*”. A büntetés lehet szabadságvesztés, pénzbüntetés vagy közérdekű munka. Ugyanennek súlyosbított változata, ha mindezt jogtalan haszonszerzés miatt követi el valaki.

A 300/E paragrafus szerint büntetendő, aki „*a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot*

a) készít,

b) megszerez,

c) *forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz*”,

illetve ha ilyen ismeretet más rendelkezésére bocsátja. A büntetés alól felmentést jelent, ha valaki tevékenységét a hatóságok előtt felfedi.

A törvény a fenti esetekre igen szigorú büntetéseket szab ki, egyes esetekben a büntetés mértéke megegyezik az emberölés alapesetének büntetésével.

A 300/F paragrafus értelmező rendelkezéseket tartalmaz, melyben definiálja a számítástechnikai rendszer fogalmát:

„*A 300/C. § és a 300/E. § alkalmazásában számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége.*”

1992. évi LXIII. törvény

Az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szól. Alapszabályként említendő, hogy személyes adataival mindenki maga rendelkezhet (kivéve, ha az adatkezelést törvény rendeli el), és a közérdekű adatokat mindenki megismerheti. Az adatkezelőnek illetve adatfeldolgozónak nemcsak jól felfogott érdeke, hanem törvényes kötelessége is a birtokában levő adatok biztonságáról gondoskodni:

„*10. § (1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.*

(2) Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.”

A törvényt a 2003. évi XLVIII. törvény módosította európai uniós jogharmonizációs kötelességek miatt.

2001. évi XXXV. törvény

A 2001-ben elfogadott, majd 2004-ben módosított törvény az elektronikus aláírás jogi szabályozásának alapjait teremti meg. A törvény más fejlett országokhoz képest későn jelent meg (az Európai Unióban 1999-ben jelent meg a 99/93/EC jelű direktíva, de ekkorra már több tagállam is rendelkezett elektronikus aláírási törvénnyel). Azonban így hatalmas a jelentősége, hiszen elektronikus aláírás nélkül nincs hiteles elektronikus ügyintézés, és így a MITS (Magyar Információs Társadalom Stratégia) alappillére. A törvény nagyon sok területen lehetővé teszi a papír alapú dokumentumok helyett elektronikus aláírás, illetve dokumentum használatát, de azért még koránt sem az élet minden területén (például az anyakönyvvezetés hivatalos, papír alapú formáját továbbra se váltja ki csak elektronikus dokumentum).

2001. évi CVIII. törvény

A törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szól, a 2003. évi XCVII. törvény módosította rendelkezéseit. A törvény összhangban van az Európai Unió 2000/13/EC jelű, azonos témájú irányelvével. A törvény célja ez elektronikus kereskedelem és más elektronikus szolgáltatások feltételeinek megteremtése, ezáltal a magyar gazdaság versenyképességének javítása, valamint a fogyasztók jogainak védelmének szabályozása. A törvény hatálya nem terjed ki a magánjellegű kommunikációra.

Az informatikai biztonsággal kapcsolatban meg lehetne említeni még egyéb speciális területekre vonatkozó rendelkezéseket (az államtitokról és a szolgálati titokról, az üzleti titokról vagy banktitokról szóló törvényeket), melyek mind fokozott biztonsági előírások betartását vonhatják maguk után.

4. Útmutató az Informatikai Biztonsági Szabályzat (IBSz) elkészítéséhez

4.1 Bevezetés

Az Informatikai Biztonsági Szabályzat minden esetben meglehetősen intézmény specifikus, az adott intézmény szerkezetét, adottságait messzemenően figyelembe kell venni, a tények és körülmények ismerte nélkül nem képzelhető el megfelelő szabályozás. Nem is célom, hogy konkrétumokkal foglalkozzam ebben a részben, de bizonyos irányelveket, alapvető, széles körben alkalmazható technikákat érdemes lehet bemutatni.

Mint minden szabályzat elkészítését, az IBSz elkészítését is gondos tervezés kell, hogy megelőzze. Fel kell mérni mind az intézmény igényeit és kötelezettségeit, mind a rendelkezésre álló lehetőségeit. Ilyen és ehhez hasonló kérdéseket kell feltenni:

- Milyen tevékenységet folytat az intézmény?
- Mely szervezetek használnak informatikai támogatást?
- Hol és hány személy használja az informatikai rendszert (külső és belső felhasználók)?
- Milyen informatikai eszközökkel rendelkezik az intézmény?
- Milyen meglévő szabályzatai vannak már?
- A szervezet által kezelt adatok milyen biztonsági osztályba tartoznak?
- Milyen kockázatokkal kell számolni, ezek bekövetkezése milyen hatással lehet az intézményre?

Az IBSz elkészítésekor törekedni kell a kockázatokkal arányos védelem kialakítására, és figyelembe kell venni az egyenszilárdság elvét. Eszerint a rendszernek mindenhol azonos erősségű védelemmel kell rendelkeznie, nem érdemes egyes elemekre nagyobb összeget/energiát ráfordítani, hiszen úgyis a gyenge pontokon várható a támadás, és inkább ezeket kell „szintbe hozni”.

Az Informatikai Biztonsági Szabályzatnak nem szabad a levegőben lógnia, szervesen illeszkednie kell a többi, már meglévő belső szabályzathoz (pl. Szervezetei és Működési Szabályzat, Iratkezelési Szabályzat, Leltározási Szabályzat, Tűzvédelmi Szabályzat, stb.), az átfedéseket kerülni kell, mindent a megfelelő helyen kell leírni (pl. a rendszergazda feladatkörét nem itt, hanem az ügyrendnél kell meghatározni). A

szabályzatnak természetesen figyelembe kell vennie az aktuálisan érvényes jogszabályi előírásokat, és jó, ha létező informatikai szabványon alapul.

A szabályzatnak a vezetés legfelső szintjéről támogatást kell élveznie, az abban foglaltaknak mindig vezetői döntésen kell alapulnia, hiszen érvényre juttatásuk csak így lehetséges. De a szabályokat nemcsak betartatni kell, hanem meg is kell ismertetni azokkal, akiknek használniuk, alkalmazniuk kell. Alapvető elvárás, hogy a szabályzatot minden érintetthez el kell juttatni, és szükség esetén gondoskodni kell a megfelelő oktatásról is (gondolok itt elsősorban a szakemberek felkészítésére).

Egy szabályzatot nemcsak létrehozni kell, hanem azt karban is kell tartani a megváltozott igényeknek, követelményeknek, technikai fejlődésnek megfelelően. Legjobb, ha maga a szabályzat egy kellően rugalmasan megszövegezett dokumentum, és a konkrét intézkedéseket mellékletek tartalmazzák, így azok egyszerűbben frissíthetők. Hasznos, ha a változásokat verziószámozással követjük nyomon. Alapkövetelmény, hogy az IBSz újabb verziói maradéktalanul váltsák fel a régieket, ne fordulhasson elő, hogy új verzió létezésekor még egyes helyeken a régit alkalmazzák.

4.2 A szabályzat részei

4.2.1 A szabályzat tárgya

Az Informatikai Biztonsági Szabályzat egy olyan intézkedés együttes, amelynek egy adott szervezet informatikai rendszerével kapcsolatos biztonsági intézkedéseit, előírásait kell tartalmaznia. A szabályzatnak a szervezet (lehetőleg ugyancsak írásba foglalt) Biztonságpolitikájában jelzett irányelveket kell követnie és a gyakorlatban megvalósítania. Míg a Biztonságpolitika egy magasabb szintű, főleg vezetői döntéseket és alapelveket tartalmazó dokumentum, addig az Informatikai Biztonsági Szabályzat alacsonyabb szintű, jobban a gyakorlati kérdéseket helyezi előtérbe, amik konkrét cselekvési mintákat határoznak meg, éppen ezért mellőzendő is a magasabb szintű elvek megismétlése ebben a dokumentumban. Itt lehet említést tenni azokról a célokról, amiknek elérése érdekében a szabályzat létre lett hozva, és ami miatt az intézménynél az informatikai biztonsággal foglalkozni kell.

4.2.2 A szabályzat minősítése

Az Informatikai Biztonsági Szabályzat általában az adott intézmény belső használatára szolgáló dokumentuma. Itt a minősítésnél kell meghatározni, hogy az adott intézmény az általa kezelt adatok biztonsági osztályba sorolása alapján milyen globális biztonsági besorolásba tartozik.

4.2.3 A szabályzat hatálya

A szabályzat személyi, tárgyi és szervezeti hatállyal is rendelkezik. Ezek megállapításánál ügyelni kell arra, hogy az informatikai biztonság szempontjából ne maradjanak szabályozatlan terültek, és ne is legyenek átfedések más szabályzatok által kezelt területekkel.

A személyi hatályt érdemes minden, az informatikai rendszert használó személyre kiterjeszteni, a tárgyi hatályba beletartozik a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes köre is.

4.2.4 Kapcsolódó törvények, szabályzatok, ajánlások

A szabályzatnak hivatkozni kell a figyelembe vett törvényi előírásokra és ajánlásokra, azokkal összhangban kell lenni. Az Informatikai Biztonsági Szabályzatot az intézmény egyéb, már létező szabályzataival együttesen kell alkalmazni, és itt lehet ezekre hivatkozni, felsorolni őket. Továbbá itt lehet említést tenni azokról a műszaki szabványokról és ajánlásokról, amelyek előírásainak az intézmény informatikai rendszere eleget tesz.

4.2.5 Feladat és felelősségi körök az informatikai biztonság területén

Az informatikai biztonság területén jól körvonalazott feladatköröket kell meghatározni, és az ezekhez tartozó felelősségeket is meg kell jelölni. Mellékletként csatolni lehet egy listát, ami az adott feladatkörökhöz rendelt személyeket és elérhetőségeiket tartalmazzák. Ezt a listát naprakészen kell tartani.

4.2.6 Intézkedések

A szabályzat legnagyobb hányadát kitevő rész, megtervezéséről és az alkalmazható technikákról a következő fejezetben lehet részletesen olvasni.

4.2.7 Szankciók

A szabályzat egyik legfontosabb része, hiszen e nélkül nehezen képzelhető el a szabályzat betartathatósága. A szankcióknak arányban kell állniuk az elkövetett vagy elmulasztott cselekedetekkel, és adott esetben elrettentő jelleggel is kell bírniuk, de a törvényi előírásokkal, elvekkel mindenképpen összhangban kel állniuk. A szankcionálás lehet az intézmény saját jogkörében, kivéve ha az elkövetett tett törvényben megfogalmazott következményekkel is jár, ilyenkor eszerint kell eljárni.

4.3 A szabályzat bevezetése

A szabályzat bevezetését a legfelsőbb vezetői szintről kell kezdeményezni, hiszen a benne foglaltak így lesznek mindenki számára elfogadhatók. A szabályzatot a szervezet összes tagjához el kell juttatni, és nekik aláírásukkal kell igazolniuk, hogy a szabályzatot megismerték, és a benne foglaltakat elfogadták. A későbbiekben az új felhasználókkal is minden esetben hasonló módon kell eljárni.

A szabályzat bevezetését szükség esetén oktatásnak, felkészítésnek kell megelőznie, hiszen egyrészt a szükséges ismeretek hiányában nem várható el a helyes alkalmazás, másrészt a szabályzatban foglaltak elfogadtatása jóval egyszerűbb, ha az alkalmazó tisztában van annak hátterével, jelentőségével.

4.4 A szabályzat karbantartása

A szabályzat elkészülte és bevezetése után gondoskodni kell annak folyamatos, a változásokat követő fejlesztéséről. Legalább évente felül kell vizsgálni, hogy a benne foglaltak időszerűek, érvényesek-e, és a felmerülő új kihívásokra új válaszokat kell adni a szabályzatban.

5. Alapvető biztonsági technikák

A legfontosabb biztonsági technikák bemutatása előtt érdemes pár szót szentelni arra, hogyan is érdemes kiválasztani a megfelelő intézkedéseket, és ezeket az intézkedéseket hogyan csoportosíthatjuk. Minden intézkedésnek egy lehetséges biztonsági eseményhez kell kapcsolódnia, így először a védendő területeket kell számba venni, és meghatározni azok gyenge pontjait, hogy ehhez rendelhessünk a megfelelő védelmi intézkedéseket.

A következők alapján elemezhetjük a védendő terület és a biztonsági intézkedés kapcsolatát:

1) Milyen problémát old meg a védelmi intézkedés?
   Nagyon fontos, hogy a biztonsági intézkedés kapcsolódjon a problémához, és ne legyen öncélú.
2) Mennyire jól oldja meg az adott problémát?
   A hatékonyság alapvető szempont a védelmi intézkedés kiválasztásánál.
3) Milyen újabb problémákat vet fel az adott védelmi megoldás?
   Egy informatikai rendszerben minden újabb elem újabb kockázatok forrása lehet, ezért fontos ezt a kérdést is megvizsgálni.
4) Mennyibe kerül a szóban forgó biztonsági intézkedés?
   Ez a másik, nem elhanyagolható szempont egy adott intézkedés kiválasztásánál. Itt nem csak gazdasági költségekre (pénzügyi, humán erőforrásokra) kell gondolni, hanem az intézkedés bevezetésének szociális problémáira is.
5) A fenti szempontok alapján megéri-e biztonsági intézkedés alkalmazása.
   Ha egy biztonsági intézkedés bevezetése nagyobb megterhelést jelent, mint az általa elért előnyök, akkor ez nem elfogadható megoldás. De az is előfordulhat, hogy egyszerűen nem állnak rendelkezésre a szükséges erőforrások, és ekkor a biztonsági esemény bekövetkezésének kockázatát kell felvállalni.

Az első alfejezetben ezen a védelmi intézkedéseknek egy csoportosítását mutatom be, majd a fejezet többi részében olyan általánosan alkalmazott biztonsági technikák következnek, amelyek megismerése és alkalmazása nemcsak egy Informatikai Biztonsági Szabályzat elkészítésekor kerülhetnek előtérbe, hanem hasznosak lehetnek minden, informatikai rendszert használó egyén számára.

5.1 Védelmi intézkedések csoportosítása

A védelmi intézkedések megtervezésénél széles körben elfogadott és a gyakorlatban is alkalmazott elv az ún. PreDeCo védelem-tervezési módszer. Ez a módszertan a biztonsági intézkedéseket három egymásra épülő és egymást kiegészítő részre bontja:

- megelőző (preventive),
- észlelő (detective) és
- javító (corrective)

kontrollokra. A kontroll szó itt az a szemléletmódot tükrözi, hogy a veszélyeket nem feltétlenül megszüntetjük, vagy teljesen kizárjuk azok bekövetkezését – hiszen ez legtöbbször nem is lehetséges –, hanem megpróbáljuk őket kontroll alatt tartani. Legjobb megelőzni a bajt, de ha ez nem sikerül, legalább fel kell ismerni annak bekövetkezését, és ha felismertük, akkor jó, ha van mód elhárítani a veszélyhelyzetet.

A megelőző kontrollok közé tartoznak azok a technikák, amivel megpróbáljuk elkerülni egy adott veszélyhelyzet bekövetkezését. Nagyrészt ide tartoznak a szabályozások is, hiszen alapvetően ezek is megelőző rendelkezéseket tartalmaznak.

Az észlelő kontrollok lényege, hogy minél előbb felismerjék a nem kívánt esemény bekövetkezését, és így korlátozható legyen a káros hatás. De ez csak úgy valósulhat meg, ha a veszély felismerését cselekvés is követi.

A javító, elhárító kontrollok ezt a cselekvést jelentik, amik megakadályozzák a nem kívánt esemény folytatását, magukban foglalják a káros hatások megszüntetését és a normál állapot visszaállítását. Ekkor gyakran szerephez jutnak a felkészülő intézkedések is (biztonsági mentések készítése), és különösen nagy károkat okozó veszélyhelyzet esetén a Katasztrófaterv.

Az informatikai biztonság három alapvető fenyegetettsége, a bizalmasság (confidentiality), sértetlenség (integrity), és a rendelkezésre állás (availability) elvesztésének megakadályozása érdekében mindhárom féle védelmi intézkedést alkalmazni tanácsos. Ennek a két oldalnak a kombinálásából származik a PreDeCo/CIA mátrix, ami egy adott védendő terület esetén egy helyen rögzíti a fenyegetettségek típusát, és a hozzájuk tartozó három féle védelmi intézkedést a következő formában:

	C	I	A
Pre			
De			
Co			

A táblázat alkalmazásának haszna abban mutatkozik meg, hogy a tervezést szisztematikussá teszi, hiszen a tervező rá van kényszerítve, hogy az összes lehetőséget végiggondolja, és ne maradhasson ki olyan megoldás, ami az adott helyzetben szükséges lett volna.

5.2 Felhasználó azonosítás

A felhasználó azonosítás – más szóval autentikáció – minden informatikai rendszer biztonságának alapja. A felhasználók kellő megbízhatósággal történő azonosítása egy gép számára nem egyszerű feladat, a visszaélések ezért ezen a területen gyakoriak, így a megvalósításnál nagy figyelmet kell tanúsítani.

A felhasználó azonosításnak alapvetően három fajtáját ismerjük: tudás, birtok és biometria alapú eljárások. Mivel egyik módszer sem tökéletes, mindegyiknek vannak gyenge pontjai, így egy igazán biztonságos rendszer esetén a megbízható azonosításhoz legalább két módszer együttes és független alkalmazása szükséges.

A tudás alapú azonosítás esetén a felhasználót az alapján azonosítjuk, hogy mit tud, azt ellenőrizzük, hogy birtokában van-e a megfelelő (többnyire titkos) információnak. Ebbe a csoportba tartoznak a jelszavak és PIN kódok. Nagy előnyük, hogy olcsón és egyszerűen alkalmazhatóak, hátrányuk, hogy észrevétlenül eltulajdoníthatók (lehallgathatók, kitalálhatók), és az átlagos jelszavak nem biztosítanak igazán erős védelmet. Erre egy nagyon szép szemléltetés található a `www.biztostu.hu` weboldalon, ahol egy tanulságos játék keretében ki lehet próbálni, hogy adott jelszó mennyire jelent erős védelmet. (Pl. az egyszerű „zebra” jelszót egy másodperc körüli idő alatt megtalálja a gép a szótárban lineáris kereséssel, ellenben a „kiBhf4mr” jelmondat alapú betűszót csak kimerítő kereséssel lenne képes megtalálni kb. 10,3 év alatt, és ha ezt kiegészítem még egy betűvel, akkor már 1000 évnél is több időt venne igénybe a megfejtés.)

Mivel a jelszavak jelentik a felhasználó azonosítás legelterjedtebb módját, így érdemes odafigyelni a megfelelő jelszó kiválasztására, és az Informatikai Biztonsági Szabályzatban segítséget kell nyújtani az erős jelszó választásához. A mellékletben található egy írás a helyes jelszóválasztásról.

A birtok avagy kulcs alapú azonosítás arra épül, hogy az adott felhasználónak mije van, tulajdonában van-e valamilyen tárgy, ami elég egyedi ahhoz, hogy őt egyértelműen azonosítsa (pl. bankkártya, diákigazolvány). Ide tartoznak a különböző mágneskártyák, chipkártyák és intelligens kártyák (smartcard-ok). Használhatóság, másolhatóság és ár szempontjából megtalálhatók a legkülönbözőbb megoldások.

Biometrián alapuló azonosítás esetén közvetlenül azt vizsgáljuk, hogy az adott személy fizikai-biológia voltában kicsoda (pl. ujjlenyomat, retina, hang alapján történő azonosítás). Itt az egyszerű megoldások általában könnyen kijátszhatók, a nagy megbízhatóságúak pedig drágák, bizonyos esetekben pedig még adatvédelmi problémákat is felvethetnek ezeknek a személyes adatoknak a tárolása.

5.3 Logikai hozzáférés védelem

A felhasználó azonosítást, autentikációt követi az autorizáció, a jogosultságok felhasználóhoz történő rendelése. A megfelelő védelem biztosítása érdekében az információkhoz való hozzáférést korlátozni kell, és ellenőrizni kell, hogy valóban csak az arra felhatalmazottak férhetnek hozzá az érzékeny adatokhoz. A jogosultság kezelésnek két elméleti megközelítése van.

A DAC (Discretionary Access Control), azaz önkényes (belátáson alapuló) hozzáférés védelmi mód esetén az objektum, dokumentum tulajdonosa határozza meg, hogy ki milyen módon férhet az adathoz. Ebben az esetben nagy a felhasználó felelőssége, és hozzá nem értése esetén ez komoly veszélyeket rejt magában.

A MAC (Mandatory Access Control), azaz előre meghatározott, kötelező hozzáférés védelem esetén a jogosultságok beállítását nem a tulajdonos végzi, hanem az központilag történik. Ezt az elvet alkalmazzák intézmények, vállalatok rendszerei esetén.

Ez a fajta jogosultság kezelés egyrészt megakadályozza a jogosulatlan hozzáférést, másrészt segít abban, hogy egy hozzá nem értő ne okozhasson károkat, hiszen egyszerűen nem fér hozzá az adatokhoz.

5.4 Javítások, frissítések

Ahogy egyre bonyolultabbá válnak a programok, egyre több hiba fordulhat, és fordul is elő bennük. A támadók ezeknek a hibáknak, biztonsági réseknek a kihasználására törekszenek. A szoftverfejlesztő cégek többnyire igyekeznek a felmerült hibákat kijavítani, és ezeket a javításokat közzé is teszik, viszont óhatatlanul lépéshátrányban vannak a támadókhoz képest. Ha a felhasználó nem követi a javítások, frissítések megjelenését, akkor még ezek ellen az ismert hibák ellen sem lesz védve a számítógépe, és ezt a gondatlanságot senki sem engedheti meg magának, aki egy kicsit is ad az informatikai biztonságra.

5.5 Vírusvédelem

A vírusok, férgek, trójai programok a számítógépek kártevői. Ma, a hálózatba kötött gépek világában terjedésük olyan gyors, hogy megelőző védelem nélkül esélyünk sincs ellenük. Megismerésük és felismerésük nagyon fontos, ezért álljon itt néhány mondatban rövid meghatározásuk.

A vírusok olyan programrészletek, amik önmagukat képesek reprodukálni, és más programokat megfertőzni.

A férgek önálló programok, amik ugyancsak képesek magukat másolni, és eljuttatni más rendszerekbe.

A trójai programok általában valami hasznos funkció álcája mögött végzik romboló tevékenységüket.

Terjedésük történhet fertőzött állományok másolásakor, letöltésekor, fertőzött makrókat tartalmazó dokumentumokkal, és e-mail-ben csatolt fájlként is.

Az ellenük irányuló védekezés legelterjedtebb módszere vírusvédelmi szoftver alkalmazása, ám ezek csak akkor nyújtanak megfelelő védelmet, ha memóriarezidensen futtatjuk őket, és rendszeresen frissítjük az adatbázisukat. A vírusvédelmi szoftverek nemcsak jelezni tudják, ha vírust észlelnek, hanem megoldást is kínálnak (megjavítják, törlik, vagy karanténba zárják a fertőzött programot). Mivel a mai vírusok legnagyobb része e-mail-ben vagy Internetről történő letöltés alkalmával terjed, ezért olyan programot kell használni, ami képes a hálózati forgalom és a levelezés szűrésére. A víruskereső programok legtöbbször rendelkeznek olyan heurisztikus keresési

funkcióval, amelynek segítségével nemcsak a már ismert vírusok, hanem bizonyos esetekben az újak ellen is védelmet jelenthetnek, ezzel azonban óvatosan kell bánni, mert könnyen téves diagnózist adhatnak.

A vírusok elleni védelem másik fontos, de kevésbé gyakran alkalmazott eszközei a blokkolók. Ezek a programok rátelepednek a kritikus rendszerfunkciókra, és jeleznek, ha valamely program ezeket igénybe akarja venni. Használatuk gyakorlott felhasználót igényel, mert a vírusok mellett gyakran más segédprogramok is alkalmaznak kritikus rendszerfunkciókat, és ezzel téves riasztásokat is adnak.

Végül érdemes még megemlíteni az integritásellenőrző programokat. Ezek minden fontosabb objektum adatait feljegyzik, és ha valamelyik megváltozik, akkor jeleznek. Az előzőhöz hasonlóan ezt a tünetet sem csak vírusok okozhatják.

A vírusvédelmi szoftverek használatáról a mellékletben található hasznos leírás.

5.6 Tűzfalak

A fogalomtárban található definíció szerint a „*hálózati tűzfal hardver- és szoftvereszközök, valamint óvintézkedések együttese, amely - fizikai és logikai elválasztás segítségével - egy (belső) hálózatot a (külső) hálózati támadásoktól megvéd*”. A meghatározás nem teljesen pontos, hiszen a tűzfal nem csak minket véd meg a külvilágtól, hanem adott esetben a külvilágot is tőlünk, hiszen mindkét irányú forgalom ellenőrzésére képes.

Egy hálózatra kötött számítógép sohasem lehet teljes biztonságban, hiszen bármikor akadhatnak rosszindulatú egyének, akik a kellő védelem hiányában megtámadhatják a gépet, ezért jó, ha tudjuk, hogy mikor mi történik épp a számítógéppel. A tűzfalak képesek a hálózati forgalom ellenőrzésére, naplózására, valamint előre beállított szabályok szerint bizonyos csomagok áthaladásának blokkolására is. A tűzfalaknak létezik szoftveres és hardveres változata is.

A tűzfalaknál szabályokat állíthatunk fel, ami alapján blokkolódik, vagy tovább engedésre kerül egy csomag. A szabályok vonatkozhatnak a csomag típusára, tartalmára, de származási helye alapján is hozhatunk döntést. Nagyon sok tűzfal program nemcsak a hálózati forgalom analízisére képes, hanem egy gépen belüli aktivitásokat is figyelheti.

A tűzfal akkor képvisel hatásos védelmet, ha a szabályok, ami alapján egy csomag sorsáról dönt, jól vannak beállítva. Túlságosan engedékeny beállításokkal támadások veszélyének tesszük ki magunkat, a túl szigorú szabályozás pedig a hálózati kapcsolat használhatatlanságához vezethet.

A személyes tűzfalak használatáról a mellékletben található hasznos leírás.

5.7 Titkosítás

A titkosítás az informatikai biztonság egészét érintő technika. Az információ értéke manapság nagyon megnőtt, és nemcsak a katonai és államigazgatási terülten, hanem a kereskedelem és a magánszféra esetében is egyre fontosabb az adatok védelme, elrejtésük a kíváncsi tekintetek elől. Kriptográfiai technikákat alkalmazhatunk az adatok és a kommunikációs csatorna titkosítására is.

A titkosítás története az ókorra visszavezethető. Először magának az üzenetküldésnek a tényét próbálták elrejteni (szteganográfia), majd az üzenetet próbálták kódolni átrendezéses, vagy behelyettesítéses kódolással (ez utóbbira példa a Caesar-kódolás, ahol az abc betűit három pozícióval arrébb toljuk). A behelyettesítéses kódolás nagyon sok variációt rejt magában, ennek ellenére könnyen törhető gyakoriság analízis segítségével.

A titkosítás alapelve, hogy egy módszer megbízhatósága nem függhet a kriptográfiai algoritmustól, hanem csak az alkalmazott kulcs titkosságától. Tehát nem jó módszer az, ha az algoritmust titokban tartjuk, helyette a kulcs titkosságáról kell gondoskodni.

Shannon, amerikai matematikus bebizonyította, hogy létezik tökételes rejtjelező, de ez a gyakorlatban használhatatlan, ugyanis a titkosításra szánt üzenet hosszával megegyező hosszúságú, véletlen számsorozatra lenne szükség kulcsként, és ennek biztonságos célba juttatása ugyanolyan nehéz feladatot jelent, mint magának az üzenetnek a titkos továbbítása. A gyakorlatban viszont léteznek olyan rejtjelezők, amik ha nem is tökéletesek, de megfelelően erős kulcs alkalmazása esetén visszafejtésükhöz elfogadhatatlanul sok időre van szükség.

A rejtjelező módszereknek két nagy típusát különböztethetjük meg, a szimmetrikus és az aszimmetrikus kulcsú kódoló eljárásokat.

Szimmetrikus kulcsú rejtjelezőknél a kódoló és a dekódoló kulcs ugyanaz, vagy valami egyszerű szabály alapján számíthatjuk őket egymásból. Ide tartozik a 20. század második feléig megalkotott kódoló eljárások mindegyike, az utóbbi évtizedekből pedig a leghíresebb, és leggyakrabban használtakat említeném meg: DES, 3DES, AES. Ezeket az eljárásokat többnyire titkosításra alkalmazzuk, de több protokollban is szerepet játszanak, pl. az üzenetek sértetlenségének biztosításában és a távoli partnerazonosításban, és az üzenetek titkosságán kívül azok hitelességének bizonyítására is alkalmasak.

Az 1970-es évek második felétől jelentek meg az első aszimmetrikus kulcsú kriptográfiai eljárások. Ezeknél a kódoláshoz és a dekódoláshoz használt kulcsok egy kulcspárt alkotnak, amik szorosan egymáshoz tartoznak, de egymásból nem számíthatók ki, csak nagyon nehezen. Az algoritmusok alapja egy nehéz matematikai probléma, amely segítségével speciális „rejtekajtós" egyirányú függvények készíthetők. Ilyen matematikai problémák pl. az egészek faktorizációs problémája (ezen alapul az RSA kódolás), a diszkrét logaritmus probléma (pl. Diffie-Hellman kulcsegyeztető protokoll), vagy az elliptikus görbék pontjain értelmezett diszkrét logaritmus probléma. Az aszimmetrikus (vagy nyilvános) kulcsú eljárásokat alkalmasak titkosításra is, de nem ajánlott, és nem is szokták erre használni, mert egyrészt nagyon számításigényesek, másrészt az értelmes szövegek kódolása növeli a törés veszélyét. Elterjedtebb alkalmazásuk a kulcsegyeztető protokollok és a partnerazonosítás, digitális aláírás területén van.

5.8 Egyéb

A teljesség kedvéért nem szabad elfeledkezni az informatikai biztonság terültén alkalmazható más technikákról sem, amelyek részletesebb kifejtése már nem fért a dolgozat keretei közé, azonban említésük mindenképp szükséges:

- Behatolás érzékelő eszközök
- Biztonságos szoftverfuttatási környezetek
- Spam szűrők
- Digitális aláírás
- Tokenek, intelligens kártyák, jelszógenerátorok
- Hálózati architektúra megválasztása

II. RÉSZ

6. Mintaszabályzatok az ELTE részére

6.1 Hálózathasználati szabályzat

Bevezetés

Az ELTE hálózata az akadémiai (NIIF) hálózat részét képezi, így annak Felhasználói Szabályzata érvényes rá (`http://www.iif.hu/aup/` – a teljes szabályzatot lásd a Mellékletben). Jelen szabályzat az előbbi szabályzattal összhangban, annak iránymutatásait figyelembe véve készült.

A szabályzat az ELTE Informatikai Biztonsági Szabályzatának többi rendelkezésével együttesen alkalmazandó, a szabályzat által nem tárgyalt kérdésekben a Magyar Köztársaság hatályos törvényei az irányadók.

A szabályzat hatálya

Jelen utasítás mindenkire nézve kötelező, aki használja az ELTE számítógép-hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed az ELTE összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz az ELTE számítógép-hálózatát használja. Ha az intézmény harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

A hálózat használatának szabályai

Az ELTE hálózata nem használható az alábbi tevékenységekre (a NIIF Felhasználói Szabályzata szerint, kiemelve a legfontosabb részeket, a teljes lista megtalálható a korábban hivatkozott web címen és a Mellékletben):

- a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszer terjesztése);

- profitszerzést célzó, direkt üzleti célú tevékenység és reklám;
- a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
- a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, hálózati játékok, kéretlen reklámok);
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan);
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
- másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok közzététele);
- hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

Felelősök

Felelősöket kell kinevezni, akik kontrollálják a hálózat egyes részeinek, szolgáltatásainak működését, rendeltetésszerű és szabályos használatát, valamint felelnek a biztonsági előírások betartásáért és betartatásáért. A felelősöket az Információtechnológiai Központnál be kell jelenteni, róluk elérhetőségükkel együtt nyilvántartást kell vezetni, ezeket a listákat naprakészen tartani, és rendszeres időközönként (legalább félévente) ellenőrizni.

A felhasználók kötelességei

- A felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködni a hálózat üzemeltetőivel a szabályzat betartatása érdekében.

- A felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználó azonosítóval kerül végrehajtásra.

A felhasználók jogai

- Minden egyetemi polgárnak joga van saját felhasználói fiókhoz és levelezéshez (e-mail címhez), web és news szolgáltatáshoz. Az egyetem a „ludens" illetve „caesar" nevű gépen biztosít felhasználói fiókot (`<felhasznalo_nev>@elte.hu` illetve `<felhasznalo_nev>@caesar.elte.hu` formájú e-mail címekkel). A karok és tanszékek további hálózati szolgáltatásokat biztosíthatnak.
- A felhasználónak joga van a felhasználói fiókhoz való hozzáféréshez. Az Egyetem ezt központi, kari illetve tanszéki számítógép-termeiben illetve laborjaiban teszi lehetővé.
- A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetői tiszteletben tartják, ettől eltérni csak a törvény által meghatározott esetekben lehet.
- A rendszer technikai problémáiról (tervezett vagy rendkívüli eseményekről) tájékoztatni kell a felhasználókat.
- A felhasználók számára elérhető módon közzé kell tenni a felhasználókra vonatkozó szabályok érvényes változatát.

Szankciók

A Szabályzat megsértésének gyanúja esetén az esetet ki kell vizsgálni, és a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket, amelyre a következők az irányadók:

- A Szabályzat előírásainak nem ismerete nem mentesít a következmények vállalásának kötelességétől.
- A Szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.
- A Szabályzatnak egy figyelmeztetést követő ismételt megsértése szándékos elkövetésnek minősül.

- A Szabályzat szándékos megsértése esetén az elkövető a hálózat használatából ideiglenesen vagy véglegesen kizárható, és az eset súlyosságától függően fegyelmi eljárás folytatható le ellene.
- A szándékos elkövető köteles megtéríteni az általa okozott károkat a Polgári Törvénykönyv előírásai szerint.
- Ha az elkövetett cselekedet kimeríti valamely hatályos magyar törvény tényállását, akkor a felelősnek kötelessége megtenni a megfelelő törvényi lépéseket.
- A felelősnek kötelessége tájékozatni az Információtechnológiai Központot és az adott szervezeti egység vezetőjét a Szabályzat súlyos megszegéséről.

6.2 Jelszókezelési szabályzat

Bevezetés

A jelszó a hozzáférés kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszó fontosságával és a nem megfelelő jelszókezelés következményeivel, mert egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a jelszó tulajdonosára, hanem az Egyetem informatikai rendszerére is negatív következményekkel járhat.

A jelszavaknak két nagy csoportját különböztethetjük meg a következők alapján: adminisztrátori vagy egyszerű felhasználói jogú azonosítót véd a jelszó, a szabályozás ennek függvényében eltérhet, az adminisztrátori jelszavakhoz mindig a szigorúbb szabályok érvényesek.

A szabályzat hatálya

Jelen szabályzat mindenkire érvényes, aki az ELTE hálózatának bármely részéhez jelszó használatát igénylő hozzáféréssel rendelkezik.

Alapelvek

- Nem szabad könnyen kitalálható jelszavakat választani! (A helyes jelszóválasztáshoz a következő bekezdés ad segítséget.)
- A jelszavakat mindenképp titokban kell tartani! (A jelszavak védelméről a későbbiekben található útmutató.)
- Az induló jelszót az első bejelentkezéskor meg kell változtatni.
- A jelszavakat rendszeres időközönként cserélni kell (adminisztrátori jelszó esetén 3 havonta ajánlott, egyéb esetben félévente).
- Új jelszónak nem szabad az utolsó 5 régi közül egyiket sem megadni.
- Ha a felhasználónak gyanúja támad, hogy jelszava kompromittálódhatott, azonnal meg kell változtatnia.
- 5 sikertelen próbálkozás után a felhasználói fiók zárolandó.
- A jelszavakat nem szabad kódolatlanul tárolni.

- Azon személyek, akik különböző rendszerekhez, illetve több felhasználói azonosítóval is rendelkeznek, a különböző rendszerekhez, azonosítókhoz különböző jelszavakat kell használniuk.
- Ahol lehetséges, a jelszavakra vonatkozó alapszabályokat (jelszóhossz, jelszócsere, előző jelszavak megadásának tilalma) az adott informatikai rendszer segítségével ki kell kényszeríteni.

Helyes jelszóválasztás

- Nem szabad könnyen kitalálható, személyre jellemző jelszavakat használni (pl. személyes adatok, családtagok, barátok neve, házi kedvenc neve…).
- A jelszónak legalább 7 karakter hosszúnak kell lennie.
- Nem szabad sorozatokat használni (pl. abcdefg, 7654321, asdfghj).
- Kerülni kell a szótári szavak használatát (ezek egy számjeggyel kiegészített változatai sem biztonságosak).
- A jelszó tartalmazzon kis- és nagybetűket, lehetőleg számokat és speciális karaktereket is.
- A nemzeti billentyűzet állíthatósága miatt nem javasolt az ékezetes karakterek, az Y, a Z és a 0 (nulla) használata.
- A jelszónak könnyen megjegyezhetőnek kell lennie. Könnyen megjegyezhető erős jelszavak például a jelmondat alapú betűszavak. Választunk egy kedvenc mondatot (szólást vagy idézetet akár), pl.: „**K**i **i**tt **b**elépsz, **h**agyj **f**el **m**inden **r**eménnyel!”, majd ennek kezdőbetűiből összeállítunk egy betűszót: „kibhfmr”. Ezt utána variálhatjuk nagybetűkkel, számokkal, jelekkel, pl.: „kiB3hfmR-”, és kész az erős jelszó, amit később mégse lesz nehéz felidézni.
- Végül pedig: Ne használjuk a példákban felsorolt jelszavakat!

Jelszóvédelem

A jelszót titokban kell tartani, másokkal azt nem szabad megosztani (családtagokkal, barátokkal sem). A legerősebb jelszó sem ér semmit, ha azt könnyen elérhető helyen tartjuk, vagy könnyen megszerezhető. Különösképpen figyelni kell az alábbiakra:

- A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
- A jelszót se a feljebbvalóknak, se a rendszergazdáknak, adminisztrátoroknak nem szabad elárulni, ha kifejezetten kérik ezt, akkor sem.
- Tilos közös jelszavakat használni (még családtagokkal, barátokkal sem szabad).
- A jelszót nem szabad leírni, és elérhető helyen tárolni (irodában, táskában…).
- A jelszót nem szabad semmilyen számítógépes rendszeren titkosítás nélkül (pl. egyszerű szövegfájlban) tárolni.
- A jelszót nem szabad telefonon vagy e-mail-ben továbbítani.
- Ne utaljunk a jelszó tartalmára (pl. „a kedvenc együttesem neve”).
- Ne használjuk a programok jelszó megjegyző funkcióját.
- A jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
- Ha a jelszó kompromittálódott, vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni a jelszót, és értesíteni kell az adott rendszer operátorát.
- Cseréljük jelszavunkat legalább félévente (adminisztrátori jelszavaknál az ajánlott periódus 3 hónap). A jelszavak véletlen támadásoknak is áldozatul eshetnek, ezért fontos a rendszeres jelszócsere.

6.3 Levelezési szabályzat

Bevezetés

A szabályzat célja, hogy biztosítsa az elektronikus levelezés zavartalanságát, valamint védje az Egyetem hírnevét. Minden egyetemi polgárnak lehetősége van `<felhasznalo_nev>@elte.hu` formájú postafiókot igényelni, és ezt magáncélokra is használni, az Egyetem nem monitorozza a hálózatából küldött, illetve ide érkező levelek tartalmát.

Az Egyetem hálózatán átmenő leveleken központilag vírusellenőrzés történik, ami különböző védelmi és szűrési funkciókkal egészül ki.

A szabályzat hatálya

A szabályzat érvényes minden levélre, amit az `elte.hu` tartományba eső e-mail címről küldtek.

Alapelvek

- A levelek nem képviselhetnek a hatályos magyar jogszabályokba ütköző magatartásformát.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelek tartalma nem sérthet meg szerzői és szomszédos jogokat.
- A levelek nem ronthatják az Egyetem hírnevét, megítélését, nem terjeszthetnek róla szándékosan valótlan információkat.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.

Szabályok

- Tilos kéretlen leveleket, hirdetéseket küldeni.
- Tilos a levélbombák, levelezési láncok küldése illetve továbbküldése.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.

- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről az egyetemi levelező rendszert e-mail szeméttel (spam) terhelhetik meg.
- Az Egyetem hálózatán maximum 5 Mb méretű levelek küldhetők, ez a korlát az egyes helyi (kari, tanszéki) szerverek levelező rendszerei esetében negatív irányban módosulhat.

Tanácsok

- A hálózaton történő (titkosítás nélküli) levelezés nem biztonságos, könnyen megfigyelhető (akárcsak egy levelezőlap tartalma), ezért érzékeny információkat titkosítás nélkül soha ne küldjünk e-mailben.
- Ismeretlen feladótól érkezet, különös témájú, csatolt fájlt tartalmazó levelekkel legyünk nagyon óvatosak, a jelek vírusfertőzésre utalhatnak, töröljük a levelet.
- Nagyméretű fájlokat ne küldjünk sok címzettnek, mert ez túlzott mértékben terheli a hálózat forgalmát, helyette tegyük elérhetővé egy publikus helyen (weben vagy FTP szerveren), és a levélben csak az elérési helyét küldjük el.

6.4 Vírusvédelmi szabályzat

Bevezetés

A számítógépes vírusok a számítógépen tárolt adatok és programok kártevői. A vírus a megfertőzött program futása közben másolja, többszörözi önmagát. Rendszerbe kerülésük történhet fertőzött lemeztől történő rendszerindítási kísérlet (bootvírusok), egy fertőzött program elindítása (fájlvírusok), egy vírusos makrókat tartalmazó dokumentum megnyitása (makróvírusok), vagy e-mail-ben csatolt állományként terjedő makró- illetve script vírusok, férgek megnyitásának eredményeként. A vírusok gépről gépre terjednek, többnyire észrevehetetlenek, amíg nem aktivizálódnak. Ekkor azonban nagy kárt okozhatnak pótolhatatlan adatok megsemmisítésével, a rendszer bénításával, bizonyos esetekben hardveres károkozással. A víruskeresők, vírusirtók használata elengedhetetlen, de ezek is csak a már ismert vírusok ellen jelentenek igazi védelmet. Ez a szabályzat az előbbiekben felsorolt káros hatások megelőzésére, és a vírusfertőzés esetén elvégzendő teendők leírására szolgál.

A szabályzat hatálya

A vírusvédelmi szabályzat minden az Egyetem hálózatába kötött személyi számítógépre és szerverre vonatkozik.

Vírusfertőzés gyanús helyzetek

Sok jele lehet vírus jelenlétének, azonban ezek nagy része normál tevékenység eredményeként is előállhat. Mivel a vírusok írói általában igyekeznek elkerülni a feltűnő viselkedést, a felhasználó nem feltétlenül találkozik az alább felsorolt – vírusfertőzésre utaló – jelenségekkel:

- A víruskereső program névvel azonosított vírust jelez. A lehető legerősebb vírusjegy.
- Fájl másolása esetén az újonnan keletkezett és az eredeti példány hossza eltérő. Nagyon erős vírusjegy.

- Szokatlan és váratlan képernyő tevékenység (szokatlan üzenetek, ablakok megjelenése). Erős vírusjegy.
- Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak). Általánosan erős vírusjegy. Ha az operációs rendszer újraindítása után is fennáll, erős vírusjegynek tekinthető.
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál. Átlagosan erős vírusjegy. Helytelen rendszerkonfiguráció is okozhatja.

Vírusvédelmi teendők

Az alábbi utasítások betartása erősen ajánlott a vírusfertőzések megelőzése, illetve azok kockázatának csökkentése érdekében:

- Vírusvédelmi szoftvert kell használni. Biztosítani kell a szerverek és a munkaállomások vírusvédelmét. Ehhez az Egyetem korlátlan felhasználói licencet vásárolt az ALBACOMP Rt.-től, amely VirusBuster és Sibary Antigen termékeket tartalmaz. Ezek szabadon felhasználhatók minden ELTE dolgozó és hallgató személyi számítógépének védelmére, valamint a levelező szerverek vírusvédelmére. A szolgáltatás részleteiről, a telepítő csomag megszerzésének lehetőségeiről részletesen a következő helyen találhatók információk:
  `http://itk.elte.hu/szolgaltatasok/felhasznalo/szoftver/antivirus.html`
- A vírusvédelmi programnak rezidens módban kell futnia, így az minden egyes rendszerindításkor aktivizálódik, és állandó háttérvédelmet biztosít. A felhasználóknak nem szabad kikapcsolni ezt a védelmet.
- Ne fusson egyszerre két vírusölő program.
- Kéthetente minden gépen teljes vírusellenőrzést kell végrehajtani (a vírusvédelmi szoftver támogatja az időzített keresési funkciót).
- A vírusvédelmi program vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell. Ha erre lehetőség van, az automatikus frissítést kell választani, így az új elemek rögtön megjelenésük után felkerülhetnek a rendszerre.
- Idegen helyről származó adattárolókon (floppy, HDD) használat előtt vírusellenőrzést kell végezni.
- Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.

- Az Office csomag programjainál, ahol lehet, be kell állítani a makrók jelenlétének kijelzése funkciót. Idegen állományokat csak makrók futtatása nélkül opcióval szabad megnyitni.
- Ismeretlen, megbízhatatlan forrásból származó furcsa, gyakran vicces e-mail-ek csatolt fájljait nem szabad megnyitni, azonnal törölni kell őket. Az e-mail-ben küldött vírusok, férgek rendszeresen operálnak valamilyen különös megjegyzéssel a levelek tárgy bejegyzésében.
- A fontos adatokról és a rendszerkonfigurációról készüljön archiválás.

Teendők vírusfertőzés esetén

- Tájékoztatni kell a vírusvédelemért felelős személyt (operátort, rendszergazdát) a fertőzésről vagy annak gyanújáról.
- A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó lemezről. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal (lehetőleg hálózati kapcsolat nélkül).
- A vírusvédelmi szoftvert elindítjuk, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.
- A víruskeresést addig kell végezni, amíg el nem éri a rendszerfelelős, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál.
- Ezek után a rendszer újraindítható a szokott módon.

6.5 Távoli elérés szabályzata

Bevezetés

A szabályzat célja, hogy irányt mutasson az Egyetem belső hálózatához távoli gépről történő csatlakozáshoz. A szabályzat betartásával megakadályozható, hogy az Egyetem hálózatát, informatikai rendszerét a nem jogosult felhasználásból eredő károk érjék. A károk magukban foglalják az érzékeny adatok elvesztését, az Egyetem hírnevének károsodását, illetve az Egyetem belső rendszerének sérülését.

A szabályzat hatálya

Az Egyetem hálózatának távoli elérésére az egyes egyetemi szerverek távoli elérésének keretében van lehetőség (terminál kapcsolat, fájlcsere szolgáltatás), valamint a behívó szerver szolgáltatás keretében (PPP, amely minden oktató számára ingyenesen, hallgatók számára pedig egy minimális költségtérítéssel érhető el). A szabályzat mindkét típusú kapcsolatra vonatkozik, valamint kiegészül a szolgáltatások igénybevételénél elfogadott rendelkezésekkel.

Szabályok

- A bejelentkezés időtartamára a felhasználóra érvényes az ELTE Hálózathasználati Szabályzata.
- A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító / jelszó megadása).
- A belépési azonosítókat másra átruházni, illetve más azonosítóját használni nem szabad.
- A belépési adatokat senkinek sem szabad elárulni.
- A bejelentkezéseket ellenőrizni és naplózni kell.
- Távoli bejelentkezés adminisztrátori jogokkal csak biztonságos, birtokláson és jelszón alapuló felhasználói azonosítással lehetséges.

- A távoli elérésnek biztonságos kapcsolaton keresztül kell megvalósulnia (telnet helyet SSH, FTP helyett SFTP vagy SCP, vagy valamilyen biztonsági protokollon keresztül).
- A bejelentkezett végpontot nem szabad felügyelet nélkül hagyni, még rövid időre sem.
- 5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani.
- Behívó szerveres kapcsolat esetén, ha a végpont az Internetre másik csatornán keresztül is csatlakozik, tűzfal használata kötelező.

6.6 Szerver biztonsági szabályzat

Bevezetés

A szabályzat célja, hogy az Egyetem szervereire olyan követelményeket és alapbeállításokat határozzon meg, amik a biztonságos használatot elősegítik. Jelen szabályzat alapelveket határoz meg, mivel konkrét utasítások megfogalmazása a különböző szerverek különböző operációs rendszerei és szolgáltatásai miatt nehézségekbe ütközne.

A szabályzat hatálya

A szabályzat vonatkozik minden az Egyetem tulajdonában, illetve felügyelete alatt levő szerverre, valamint az `elte.hu` tartomány alatt található összes szerverre.

Alapelvek

- A Egyetem hálózatába kapcsolt szervereket az Információtechnológiai Központhoz tartozó Számítógéphálózati Központnál (továbbiakban SZHK) be kell jelenteni, ezekről az SZHK nyilvántartást vezet. Bejegyzetlen szerver nem működhet az Egyetem hálózatán.
- A szerverekről minimálisan a következő információkat nyilván kell tartani:
  - A szerver fizikai helye
  - A szerver melyik szervezeti egységhez tartozik, ki a felelőse (elérhetőségével együtt)
  - Hardver konfigurációja és operációs rendszere
  - Főbb funkciói és szolgáltatásai

  Ezeket az információkat naprakészen kell tartani.
- A szervereket számítógépközpontban vagy legalább zárt helyiségben kell elhelyezni. A szerverekhez való hozzáférést fizikailag is korlátozni kell.
- A szervereknek illetéktelen behatolástól jól védettnek kell lennie (megfelelő alapbeállítások használata, majd upgrade-k, biztonsági javítások mielőbbi telepítése).

- A szerverek konzoljairól az adminisztrációs tevékenység befejeztével ki kell lépni, nem szabad felügyelet nélkül bejelentkezve hagyni.
- Hacsak nem szükséges feltétlenül, nem szabad adminisztrátori jogosultságokkal használni a szervert.
- A szervereken le kell tiltani minden nem használt szolgáltatást.
- Ha adottak a technikai lehetőségek, a biztonságos kapcsolatfelvételt kell preferálni, adott esetben csak az ilyen típusú hozzáférést szabad engedélyezni (telnet helyett SSH, FTP helyett SFTP, SCP használata).
- A szerverhez illetve szolgáltatásaihoz történő hozzáférési kísérleteket naplózni kell, és ezeket a naplókat rendszeresen ellenőrizni.
- A biztonsági mentéseket minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.
- A biztonsági eseménynaplókat … időre visszamenőleg, a mentéseket pedig … ideig meg kell őrizni.[1]
- A jelentős biztonsági eseményeket be kell jelenteni az Információtechnológiai Központnak.

[1] A helyi vagy törvényi szabályzattól függően (pl. pénzügyi adatokra, tanulmányi eredményekre stb. vonatkozhatnak ezek a szabályok vagy törvények).

6.7 Felhasználó kezelési szabályzat

Bevezetés

Az informatikai rendszer használatával való visszaélés kizárása érdekében minden felhasználónak egyedi felhasználó azonosítóval és az ahhoz tartozó jelszóval kell azonosítania magát. Felhasználó az Egyetem dolgozója vagy hallgatója lehet, egyéni elbírálás alapján külső személy is kaphat felhasználó azonosítót.

Mivel sok és sokféle rendszerre lehet felhasználó azonosítót létrehozni, ezeket más-más szervezeti egységek felügyelik, ezért az alábbiakban csak általános vezérelvek lesznek felsorolva.

A szabályzat hatálya

A szabályzat érvényre juttatási körébe tartoznak mind az operációs rendszerhez, mind egyes alkalmazásokhoz hozzáférési jogot biztosító felhasználói azonosítók az Egyetemi hálózat bármely részére vonatkozólag.

Alapelvek

- A felhasználó azonosítók kiadása központilag történik minden rendszer esetében.
- Felhasználó azonosítót írásban kell igényelni.
- Azonosító igénylésekor egyértelműen meg kell határozni a jogosultságot birtokló, azért felelősséggel tartozó személyt. Ellenőrizni kell, hogy az igénylő jogosult-e a felhasználó azonosítóra (hallgatók esetében érvényes diákigazolvány, vagy a Tanulmányi Osztály igazolása, dolgozók esetében a munkáltatói jogú felettes igazolása).
- A felhasználónak aláírásával kell igazolnia, hogy a használat feltételeit és szabályait megismerte, és azokat magára nézve kötelezőnek tekinti.
- Adminisztrátori feladatokat ellátó személyek részére a normál felhasználói feladatok ellátására és adminisztrációs célokra külön azonosítót kell létrehozni.
- A különböző hozzáférési jogosultságok a felhasználó azonosítóhoz kapcsolódnak.

- Az azonosításnak (és ha szükséges hitelesítés) meg kell előznie az informatikai rendszernek a felhasználóval kapcsolatos valamennyi más kölcsönhatását.
- A felhasználó azonosítót le kell tiltani, ha azzal visszaélés történt, és az esetet ki kell vizsgálni.
- A felhasználó azonosítókat a rendszerből törölni kell, ha a felhasználó már nem az Egyetem polgára, illetve már nincs az adott rendszer használatához joga.

6.8 Mentési és archiválási szabályzat

Bevezetés

Az elektronikusan tárolt adatok folyamatosan ki vannak téve a hardver meghibásodásának lehetőségének, ezért a biztonság növelése és a károk csökkentése érdekében szükség van rendszeres mentésekre. Míg a mentések fő feladata a biztonsághoz kapcsolódik, addig az archiválás egy korábbi állapot eltárolását szolgálja. Ez utóbbinak biztonsági incidensek bekövetkezése esetén lehet fontos szerepe, a napló és log fájlokban, valamint egyéb adatok között értékes információkat, nyomokat lehet találni a biztonsági esemény bekövetkezésével kapcsolatban. Technikai megvalósításuk hasonlósága miatt kerülnek egy helyen tárgyalásra.

A szabályzat hatálya

A szabályzat érvényes minden az Egyetem tulajdonában, illetve felügyelete alatt levő szerverre, valamint az `elte.hu` tartomány alatt található összes szerverre.

Feladatok

- Ki kell jelölni azokat a személyeket, akiknek a biztonsági mentéseket illetve archiválásokat el kell végezniük. Ezt dokumentálni is kell.
- Hetente teljes biztonsági mentést kell végezni a rendszerről, a köztes időben pedig naponta inkrementális mentés készítése szükséges. Az ehhez szükséges adathordozókat rotálni lehet (7 kazetta a napi mentésekhez, 4 a hetihez).
- Havonta, évente teljes rendszerarchiválást kell készíteni, és ezeket megőrizni. Ehhez biztosítani kell a megfelelő számú adathordozó egységet.
- A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák.
- On-line rendszerek esetén hideg mentést kell alkalmazni.
- A biztonsági mentéseket és archiválásokat tartalmazó adathordozókat minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.

- A mentéseket tartalmazó adathordozókon jól láthatóan fel kell tüntetni a mentett rendszer nevét, a mentés típusát és idejét.
- A biztonsági eseménynaplókat 1 évre visszamenőleg, a teljes mentéseket pedig a törvényben foglalt ideig meg kell őrizni.
- Legalább évente visszatöltési kísérletet kell végezni a technika megfelelőségének ellenőrzése érdekében.

6.9 Katasztrófakezelési terv (vázlat)

Bevezetés

Informatikában katasztrófáról nemcsak a hétköznapi értelemben vett természeti katasztrófák esetén beszélünk, hanem egy kisebb meghibásodás, áramkimaradás is vezethet informatikai katasztrófához, hiszen itt katasztrófát az informatikai rendszer helyrehozhatatlan, elviselhetetlen károsodása jelenti. Az ilyen veszélyeket, úgynevezett katasztrófa-okokat nem lehet teljesen kivédeni, de hatásukat csökkenteni lehet. Az ilyen megelőző és elhárító tevékenységeket nevezzük katasztrófakezelésnek.

Jelen szabályzat nem tartalmazza az egyes rendszerek speciális igényeinek megfelelő katasztrófa elhárítási tervet, hanem általános alapelveket fogalmaz meg, amit minden konkrét rendszer esetén ki kell egészíteni a gyakorlatban végrehajtandó feladatokkal.

A szabályzat hatálya

A szabályzatot alkalmazni kell az Egyetem minden kritikus fontosságú rendszere esetén.

Alapelvek

- A katasztrófák megelőzése érdekében megfelelő hibatűrő rendszereket kell alkalmazni (szünetmentes tápegységek, RAID rendszerek alkalmazása), és rendelkezni kell tartalék eszközökkel.
- Rendszeresen biztonsági mentéseket kell készíteni.
- Létre kell hozni egy listát, ami tartalmazza a katasztrófa helyzet esetén értesítendő személyeket és elérhetőségeiket. A lista lehetőség szerint egy sorrendet is tartalmazzon, így úgynevezett riadóztatási láncot alkotva. A listát naprakészen kell tartani, és rendszeres időközönként ellenőrizni szükséges.
- Felelősségi és döntési jogköröket kell meghatározni az adott rendszer esetén. (Pl.: Ki rendelheti el a katasztrófa helyzetet? Kinek milyen feladatot kell végrehajtania?)

- A visszaállításra ütemtervet kell készíteni, amely pontosan és részletesen tartalmazza az elvégzendő feladatokat, a hozzájuk kapcsolódó hardver és szoftver eszközök elérhetőségével együtt.
- Listát kell készíteni a legszükségesebb funkciókról és szolgáltatásokról, és elsődlegesen ezeket kell visszaállítani.
- Ellenőrző lista szükséges annak eldöntéséhez, hogy minden előírt feladat végre lett-e hajtva, és így a rendszer újraindítható-e.
- A katasztrófa tervben foglaltakat oktatni, és legalább évente tesztelni kell katasztrófa helyzet szimulálásával.
- A katasztrófa tervet legalább évente, és minden jelentősebb változás bekövetkezésekor felül kell vizsgálni, és az abban foglaltakat a megváltozott körülményekhez igazítani.

Összegzés

Dolgozatomban a következő eredményeket értem el:

- A bevezető rész segíti az olvasót, hogy a biztonságról a helyes fogalmai alakuljanak ki, és átérezze az informatikai biztonság problémájának jelentőségét.
- Az informatikai rendszerek biztonságos üzemeltetéséhez szükséges előírások és módszerek átfogó ismertetése, az informatikai biztonsági szabályzatok felépítésének bemutatása, és a biztonsági problémákat megoldani hivatott technikák felsorolása segítséget ad azoknak, akik valaha Informatikai Biztonsági Szabályzat készítésével valami módon kapcsolatba kerülnek.
- Elkészült kilenc mintaszabályzat az Egyetem részére, amelyek jó kiindulási alapot nyújthatnak a továbbiakhoz.
- A mellékletben található leírások hasznos segítséget nyújthatnak bárkinek, aki akár csak saját számítógépet üzemeltet, és a dolgozat hatására jobban odafigyelne annak biztonságos működtetésére.

A dolgozat készítése során nagyon sok hasznos ismeretre tettem szert, és megismerkedhettem azokkal a fórumokkal, ahol az informatikai biztonsággal kapcsolatos ismereteimet tovább bővíthetem.

Az Egyetem részére készült szabályzatok valós igényeket tükröznek, pontosításukkal, bővítésükkel, rendszergazdákkal és vezetőkkel történt egyeztetés után akár a közeljövőben az Egyetem Informatikai Biztonsági Szabályzatának részévé válhatnak.

Irodalomjegyzék

- ELTE-BME konzorciumban ITEM K+F pályázat keretében készített informatikai biztonsággal foglalkozó internetes oktatóanyag.
  http://www.biztostu.hu (2005. 06. 12.)

- A mellékletben idézett informatikai biztonsági technikák bemutatásának, valamint a dolgozatban idézett törvények forráshelye.
  http://www.cert.hu (2005. 06. 12.)

- A BS7799 szabványról szóló információforrás.
  http://www.bs7799.hu (2005. 06. 12.)

- MSZE 17799-2, Az információvédelem irányítási rendszerei. Előírás és használati útmutató.
  Magyar Szabványügyi Testület, 2004

- Az Informatikai Tárcaközi Bizottság weboldala, ajánlásainak lelőhelye.
  http://www.itb.hu (2005. 06. 12.)

- Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai (IHM-MTA tanulmány)
  http://www.cert.hu/ismert/00tanulmany/MTAsec_w1.pdf (2005. 06. 12.)

- Informatikai biztonsági szabályzat minták.
  http://www.sans.org/resources/policies/ (2005. 06. 12.)

- NIIF hálózat Felhasználói Szabályzata
  http://www.iif.hu/aup (2005. 06. 12.)

Mellékletek

A. Informatikai biztonsággal kapcsolatos ismertetők a Hun-CERT weblapjáról

1. Hogyan válasszunk magunknak jelszavakat?

Egyre több jelszó és PIN kód áraszt el bennünket a bankkártyától a számítógépes rendszereken át a mobiltelefonig. Sokaknak ehhez kell hozzávenni a háztartási eszközök, beléptetőrendszerek és riasztók vagy a gépjármű különböző kódjait. Hogyan kezelhető biztonsági szempontból optimálisan ez a része a mindennapi életünknek?

Az egyszerű kódok könnyen megjegyezhetők, így nagy a kísértés, hogy minél egyszerűbb kódot válasszunk. Ez addig jó, amíg az egyszerű kóddal más nem él vissza. A biztonságban a megelőzés jobb, mint a kezelés, így következzen néhány megelőzést segítő tanács a jelszóválasztáshoz és kezeléshez. (Jelszóerősség-teszt elérhető a *Biztostű* portálon)

Milyen a rossz jelszó?

Előbb nézzük, milyen a **nem megfelelő jelszó**. Alaptanács, hogy ne válasszunk olyan jelszót, ami:

- ránk jellemző (becenév, családtag vagy háziállat neve, kedvenc focicsapat, és hasonlók)
- könnyen tippelhető (számsorozat, mint az 1234 vagy karaktersorozat, mint a qwerty)
- túl rövid (2-5 karakter hosszú), ha egyáltalán van hossza („elég enter-t ütni és belépsz!")
- tartalmaz olyan karaktereket, melyek nem biztos, hogy minden esetben elérhetők (pl. ékezetes betűk)
- szótári vagy ismert szó bármilyen nyelv szótárában vagy nyelvében

Ez utóbbi esetben idegen nyelvkörnyezetben sem nyerő ötlet valami ízes magyar kifejezés alkalmazása, ami szerintünk nem szerepel egy akadémiai kiadó szótárában. Volt rá példa, hogy kutatók Internet oldalakról és hírcsoportokból gyűjtött cikkek alapján állítottak fel szótárakat úgy, hogy az adott nyelvet nem is ismerték. Az egyes szavak gyakoriságát vették alapul, így az obszcén szavak és a szleng kifejezések is bekerültek a jelszókitaláló alkalmazás számára gyűjtött szótárba. Az okosabb jelszó-kitaláló programok még azt is kipróbálják, hogy a szótári szó elején vagy végén van-e szám, tehát az 'alma' helyett az 'alma2' jelszó választása csak nekünk macerásabb, mert hosszabb, de egy jelszókitaláló programnak nem nagy feladat erre rájönni.

A másik véglet a minél véletlenebb és összefüggéstelenebb jelszó választása, mert kísérletek is igazolják, hogy ezeket könnyen elfelejtik a felhasználók, és az elfelejtett jelszó cseréjével járó kellemetlenségek a rendszergazdákat is feleslegesen terhelik

Milyen a jó jelszó?

Az előzőek alapján azt a következtetést vonhatjuk le, hogy **a jó jelszó**:

- nem szótári szó,
- van benne vegyesen betű, szám és speciális karakter is, így
- megfelelő hosszúságú
- nem köthető az egyénhez, és
- könnyű megjegyezni, hogy
- ne írjuk fel, mert nem tudjuk megjegyezni,
- és nem tartalmaz speciális ékezetes betűket

Amíg nem terjednek el az intelligens kártyás biometrikus azonosítással működő rendszerek vagy az egyszerhasználatos jelszavak (azért emlékezünk az 5 M-re: Mit old meg, Mennyire jól, Mik az új problémák, Mennyiért, Megéri-e?), addig a statikus jelszavak és PIN kódok világát kell optimális módon alkalmaznunk. Jelenleg a célra legalkalmasabb jelszótípus a kódmondaton alapuló jelszó.

Mielőtt kiválasztjuk a megfelelő kódmondatot, ismernünk kell a korlátokat. Ha az adott rendszerben a jelszavak bármilyen hosszúak lehetnek, mert úgyis csak az első néhány karaktert veszik figyelembe, vagy a kis- és nagybetűket nem különbözteti meg a rendszer (érdeklődjünk a rendszergazdánál!), akkor felesleges hosszabb és vegyes kis/nagybetűs jelszót használnunk.

Optimális megoldás

A következő lépés a kódmondat alapjának kiválasztása. Ez lehet egy kedvenc mű részlete („Mily becsben áll a rossz, ha kiderül, hogy van még rosszabb?" mondja Shakespeare Lear királya). Az első rész rövid változata ékezetek nélkül minden páros karaktert nagy betűvel írva: 'mBaR', és ebbe csempészhető számjegy is, mondjuk a közepére '42', az élet értelme (ld. Douglas Adams: Galaxis Útikalauz). Egy kis speciális karakterrel fűszerezve előáll az 'mB_42aR' sorozat, amit a kitaláló könnyen megjegyez, és az általános követelményeket is teljesíti. Az adott rendszer specifikumát is be lehet csempészni az algoritmusba (pl. az adott szerver nevének első betűje), így már csak a levezetésre kell emlékeznünk.

A felhasználó válassza a kódmondaton és algoritmuson alapuló jelszót, mivel ugyanolyan könnyen emlékezetbe véshetők, mint a naivul kiválasztottak, de elég nehéz kitalálni, mint a

véletlenszerűen generált jelszavakat. Az algoritmusos változat több rendszer esetén is jól használható (ha több szerveren van azonosítónk, nem tanácsos mindenütt ugyanazt a jelszót alkalmazni) és véd az ellen is, ha az egyik helyen felfedik a jelszavunkat. Emlékezzünk, a biztonság nem termék, hanem eljárás, tehát nem ér sokat az optimális választás sem, ha a vonal lehallgatható, és így a mintaszerűen megalkotott jelszavunkat megszerzi a támadó, de ez ellen is lehet védekezni (ld. a Kódolt kommunikáció című anyagot).

Ezek után már a megfelelő humorérzékkel tudjuk kezelni az ilyen szólásokat: „A jelszavam a kedvenc papagájom neve, és mivel hetente jelszót kell cserélnem, most úgy hívom a papagájomat, hogy *fgxZC2&!0_oéoK"*.

2. *Amit a vírusirtásnál tudni kell...*

Ha észrevesszük, hogy valamilyen úton-módon vírus került a gépünkre, azonnal meg akarunk szabadulni tőle. De ilyenkor is be kell tartanunk néhány szabályt, különben váratlan dolgokkal találkozhatunk: például ott marad a vírus a gépünkön, vagy irtás után visszakerül. De az is lehet, hogy a rendszerünk nem fog jól működni. Az ilyen hibák elkerülése végett figyeljünk a következő szabályokra.

A vírusölés szabályai:

1. Ne fusson két vírusölő program!
2. Kapcsoljuk ki a Windows rendszer „system restore" funkcióját!
3. Frissítsük a vírusölő adatbázisát!
4. „Safe" módban indítsuk el a gépet!
5. Vigyázzunk a vírusirtás közben a felkínált lehetőségek kiválasztásánál!

1. Ne fusson két vírusölő program!

Két vírusölő program egyáltalán nem nyújt nagyobb biztonságot, mint egy. Ilyenkor szokott előfordulni, hogy az egyik vírusölő észrevesz egy vírust, és abban a pillanatban a másikhoz tartozó ablak is megjelenik, és mindkét vírusölő ki szeretné irtani a vírust, de ez nem sikerül, mert kölcsönösen akadályozzák egymást. Ha nem bízunk meg teljesen egyik programban sem, akkor külön-külön futtassuk le, a futtatás alatt pedig állítsuk le a másikat!

2.Kapcsoljuk ki a Windows rendszer „system restore" funkcióját!

A Windows XP/ME operációs rendszerek alatt javasoljuk a „system restore" funkció ideiglenes kikapcsolását. Ez tulajdonképpen arra szolgál, hogy rendszerhiba esetén visszaállítsa a megsérült fájlokat. Sajnos, ha valamilyen vírus, féreg vagy trójai volt az állományban, azt is visszaállítja.

Windows XP esetén a „system restore" funkció kikapcsolása:

Start -> jobb egérrel: My Computer -> Properties -> System Restore -> Turn off System Restore

3. Frissítsük a vírusölő adatbázisát!

Gyakori hiba, hogy a vírusölő adatbázisát elfelejtik frissíteni. Hetente, de van amikor naponta jelennek meg új vírusok. Csak friss adatbázissal érdemes az vírusirtást megkezdeni, különben lehet, hogy néhány vírus eltűnik a gépünkről, de ott maradhat még egy-kettő!

4. „Safe” módban indítsuk el a gépet!

A vírusirtás megkezdése előtt az úgynevezett „safe” módban indítsuk újra a gépet.A „safe” mód a Windows rendszerek diagnosztikai üzemmódja, ilyenkor az operációs rendszernek csak a legszükségesebb elemei indulnak el. A Windows 3.1 és az NT kivételével minden Windows rendszer indítható ilyen üzemmódban.

Windows XP esetén:

Start -> Run msconfig -> BOOT.INI -> SAFEBOOT utána bootolás.

5. Vigyázzunk a vírusirtás közben a felkínált lehetőségek kiválasztásánál!

A vírustalálatnál a vírusölők nagy többsége három lehetőséget kínál fel: javítsa ki (vagy más kifejezéssel gyógyítsa meg) a vírusos állományt, zárja karanténba vagy törölje. Ne essünk pánikba, és ne a törlést válasszuk elsőre! Ugyanis ha éppen egy rendszerállományt törlünk, akkor abból bajok származhatnak. Tehát a kijavítással próbálkozzunk! Ha ez valami miatt nem lehetséges, akkor megpróbálkozhatunk egy másik vírusölővel. (Ne felejtsük el az elsőt leállítani!). A karanténba zárás is jobb megoldás a törlésnél, mert onnan visszahozható az állomány.

3. Személyes tűzfalak használata

1. Miért használjunk tűzfalat?

Az Internet révén ma már a világ túlsó felén lévő számítógéppel is kapcsolatot tudunk létesíteni, információkat tudunk lekérni, küldeni. Ugyanakkor a hálózatok kiépülése nemcsak előnyt jelent, hanem a gépünkre leselkedő veszélyek is megszaporodtak. Naponta hallunk vírusokról, férgekről, trójaiakról, számítógépekbe történő betörésekről. A veszélyeket nem tudjuk teljesen kiiktatni, de némi előrelátással sok bosszúságtól megkímélhetjük magunkat.
Az elektronikus levelezés kapcsán a vírusokról már szinte mindenki hallott, s egyre többen használnak vírusölő programokat. A vírusölők valóban nyújtanak egyfajta védelmet. Azonban számos más nyitott kapu is van a számítógépünkön. Ha ezeket mind becsuknánk, elvágnánk magunkat a világhálótól.

A tűzfalat éppen azért találták ki, hogy legyen egy olyan eszköz, ami a számítógépünkről kimenő illetve a beérkező forgalmat ellenőrizze és szabályozza. A szabályozás módjának gépenként változnia kell, hiszen minden gép gazdája más-más szolgáltatást vesz igénybe az Internetről és más-más szolgáltatást nyújt az Internet felé, s ráadásul szolgáltatásonként a célközönség is eltérő lehet. Tehát e forgalmak zavartalan átengedésekhez néhány kaput nyitva kell hagynunk, de a többi nyitva felejtett kapu csak a besurranók - a hackerek, crackerek - dolgát könnyíti.

A tűzfal tulajdonképpen egy olyan eszköz, amely a számítógép(ek) és az Internet közé 'falat' állítva a be- és kimenő forgalmat ellenőrzi és szabályozza. Az eszköz lehet egy fizikai valóságban létező, akár egy teljes intézményi hálózat védelmére szolgáló eszköz, de lehet egy személyi számítógépen futó program is.

Hangsúlyoznunk kell, hogy a tűzfal sem nyújt teljes biztonságot! Általában nem véd meg a spyware-től, a trójai falótól, bár bizonyos fokú védelmet nyújthat.

A tűzfal által nyújtott biztonság mértéke függ a szabályok felállításától. Ahhoz, hogy ezeket a szabályokat optimálisan határozzuk meg, néhány fogalmat értenünk kell. A továbbiakban ezek tisztázására is kitérünk.

Ebben a leírásban a tűzfalak legegyszerűbb változatáról, a csak egy-egy Windows operációs rendszerrel ellátott számítógépet védő tűzfalról, az ún. **személyes tűzfal-ról** (personal firewall) esik szó. A 'személyes' szót elhagyjuk, de mindenütt értelemszerűen oda kell gondolni.

2. Kinek lehet szüksége tűzfalra?

Sokakban felmerül a kérdés: miért pont az én gépemen lévő információkra lenne valakinek szüksége? Valóban, a támadóknak csak egy része választja ki tudatosan a célgépet, a többiek inkább 'alkalmi tolvajok'. Azonban a gépünkön - még ha jelszavakat, hitelkártya

információt, pénzügyi információkat, személyes leveleket nem is tárolunk - lehetnek olyan adatállományok, amelyek eltűnése, megváltozása ellehetetleníti a gép használatát. A támadók egy részét csak a puszta rosszindulat vezérli, mások szórakozásképpen lépnek be idegen gépekbe, van, aki a tudását akarja fitogtatni, vagy - s ez egyre gyakoribb - a feltört számítógépet egy harmadik fél elleni támadásra használja fel, így elfedve a valódi tettes nyomát.

Ezek után arra a kérdésre, hogy kinek lehet szüksége tűzfalra, a válasz az, hogy mindenkinek, aki:

- az adatállományait vagy nyomtatóját másokkal meg kívánja osztani,
- aki valamilyen Internet szolgáltatás működtet (pl. Web szervert üzemeltet),
- aki megengedi, hogy a számítógépébe távolról is belépjenek (remote access),
- aki szeretné a számítógépét távolról is vezérelni
- aki figyelni szeretné az Internet forgalmát, főleg azért, hogy az ellene irányuló támadási kísérleteket idejében észrevegye,
- és aki nem akar tudtán kívül egy harmadik fél elleni támadás részesévé válni.

3. Mit kell tudnia egy tűzfalnak?

A TruSecure Corporation által működtetett ICSA Labs a kereskedelmi forgalomban lévő tűzfalak minősítésével foglalkozik. Egy termék csak akkor kaphatja meg a minősítés, ha

- Microsoft hálózati környezetben képes a végpontok védelmére,
- kétféle (helyi hálózati és kapcsolt vonalas (dialup), egyidejű hálózati kapcsolat esetén is képes a védelemre,
- több, egymás után történő dialup kapcsolat esetén is folyamatosan képes a védelmet biztosítani,
- a hálózatról érkező, közönséges támadásokat képes blokkolni,
- képes a kifelé menő hálózati forgalmat korlátozni,
- az eseményekről konzisztens és jól használható feljegyzéseket képes készíteni.

A kritériumok pontos megfogalmazását lásd ezen a lapon. A minősítés feltételei időről-időre változnak, a jelenleg a 4.0 -s változat van érvényben.

4. Hogyan működnek a tűzfalak?

A tűzfalak működésének megértéséhez néhány fogalom tisztázására szükség van: a következő rész a legfontosabb protokollokat és a portokat ismerteti.

4.1 Néhány fontosabb protokoll

Az Internet kommunikációs protokollja a **TCP/IP** (Transmission Control Protocol/Internet Protocol). Nemcsak a nagyterületű hálózatok használják, hanem a legtöbb lokális hálózat is evvel működik. Kétszintű protokoll, a TCP-ből és az IP-ből áll.

A **TCP** a magasabb szint, feladata az Interneten továbbítandó üzenetek, adatállományok kisebb csomagokká (packet) való szétdarabolása, és a csomagokhoz információ hozzáfűzése (TCP header - például tartalmazza a csomagok sorszámát.). Szintén a TCP szint feladata a célgépen a csomagok összefűzése. A TCP kétirányú protokoll, ami azt jelenti, hogy a feladó a csomagok megérkezéséről nyugtát vár. Ilyen protokollon alapszik pl. az FTP, HTTP, SMTP, POP3.

Az alsóbb szintű protokoll, az **IP** a csomagok címzési adatokkal való ellátását végzi (mintha egy borítékot készítene, ráírva a címzett és a feladó adatait). Ez a protokoll használja a jól ismert IP címeket.

További protokollokról is szót kell ejtenünk:

ICMP (Internet Control Message Protocol): mint a neve is mutatja, üzenetkezelésre, vezérlésre szolgáló protokoll. Az ICMP protokollal leginkább a ’ping’ parancs forrt össze, amellyel egy IP cím elérhetőségét vizsgáljuk. A válasz szintén egy ICMP üzenet, az ’Echo’.

UDP (User Datagram Protocol): A TCP-ez hasonlóan az IP feletti protokoll, de annál jóval egyszerűbb. Az UDP az üzenetet nem darabolja fel, ahogy a TCP teszi. Ez a protokoll egyirányú, ami azt jelenti, hogy az UDP csomag (azaz a datagram) megérkezéséről a feladó nem vár nyugtát. Legismertebb alkalmazása a domain név feloldása IP címmé.

PPTP (Point-to-Point Tunneling Protocol): lehetővé teszi, hogy a nyilvános hálózaton egy saját kommunikációs csatorna (az ún. tunnel) létrehozásával két magánhálózat biztonságosan összeköthető legyen. (Ez a fajta összeköttetés a VPN).

4.2 A portokról

A portok egy hálózati kommunikációs csatorna végpontjai. A portok használata teszi lehetővé, hogy egy adott számítógépen futó alkalmazások, ugyanazt a hálózati erőforrást használva, a beérkező csomagokból csak a nekik szóló csomagokat kapják meg.
(Például az egyik gépen lévő browser (Netscape vagy Internet Explorer) lekér egy másik gépen futó web szerverről egy html lapot, akkor a két gép között létrejövő kommunikációs csatornát az egyes gépek IP címei, valamint a browserhez illetve a web szerverhez tartozó port szám határozza meg.)

A fent említett protokollok közül a TCP és az UDP alkalmazza a portokat.

A portokat számokkal (is) azonosítjuk, értékük 0-65535 között lehet. A portok és a hozzájuk tartozó protokollok/szolgáltatások azonosításával a IANA (Internet Assigned Numbers Authority) foglalkozik, az erről szóló dokumentumot ld. itt.
A portszámokat három csoportba osztják:

- jól ismert portok (well known ports),
- regisztrált portok,
- dinamikus vagy privát portok.

A jól ismert portok a 0-1023-as sávban lévő portok, amelyeket általában csak rendszerprocesszek vagy rendszerprogramok használnak, és ezek szorosan kötődnek valamilyen szolgáltatáshoz: a 20 és 21-es port az FTP-hez, 22-es az SSH-hoz, 25 az SMTP-hez, 32 a telnet-hez, a 80-as a HTTP-hez stb.

A regisztrált portok (1024-49151) sokkal kevésbé kötődnek egy-egy szolgáltatáshoz, ilyen portszám többféle célra is felhasználható.

A privát portokhoz (49152-65535) nem kapcsolódik semmilyen szolgáltatás.

4.3 A tűzfalak működése

Nagyon sokféle tűzfalat szerezhetünk be a piacról, de a következő alapfunkciók rendszerint mindegyikben megvannak:

- Csomagszűrés

  A tűzfalon belül egy szabályrendszer állítható fel. A szabályoknak megfelelő csomagokat a tűzfal továbbengedi vagy eldobja. A szabályok által meghatározott kritériumok lehetnek: a csomagok iránya (be- vagy kifelé menő), a forrás- illetve a célgép IP címe, portszámok stb.
- Nem szabványos csomagok kiszűrése

  Néhányan nem szabványos csomag küldésével próbálnak egy gépre bejutni. A tűzfalnak az ilyen csomagok szűrésére is fel kell készülni.
- Portok nyomkövetése, blokkolása

  A tűzfalnak figyelnie kell az egyes portokon folyó forgalomra. Ezt azt jelenti, hogy érzékelnie kell, ha valaki végigpásztázza a nyitott portokat (ún. port scanning), képesnek kell lennie az egyes portok lezárására, valamint fel kell tudni figyelnie az egyes portokon jelentkező 'gyanús' forgalomra is.
- Alkalmazások védelme

  Egyes tűzfalak nemcsak a portok, hanem az Internet alkalmazások védelmét is képesek ellátni. Vagyis az egyes alkalmazásokhoz tartozó be- és kifelé menő hálózati forgalmát külön elemzi.
- Riasztás

Hasznos tulajdonság, ha a tűzfal gyanús hálózati forgalomnál automatikusan riasztja a rendszergazdát, így azonnal lehetőség nyílik a beavatkozásra.

- Nyomkövetés

  A hálózati forgalomról készült feljegyzések (ún. log file-ok), az ezekből készíthető riportok segíthetnek a felállított szabályok tökéletesítésében, a gyanús forgalom kiszűrésében.

- MD5 védelem

  Ha egy alkalmazáshoz tartozó forgalmat engedélyezünk, akkor feltételezzük, hogy a forgalom ártalmatlan. Ezt használják ki bizonyos trójai falovak úgy, hogy ugyanazon a néven egy más - legtöbbször ártalmas - funkcióval is rendelkező alkalmazásra cserélik le az eredeti programot. Mivel az alkalmazás neve, portja nem változott meg, a tűzfal kiengedi a forgalmat, mellékesen kiengedve a számítógépünkről összeszedett információkat is. Ezt megelőzendő találták ki az MD5 védelmet. Lényege: minden alkalmazásról készül egy 'ujjlenyomat', azaz egy, csak az adott állományra jellemző 128 hosszú bitsorozatot. Ha az alkalmazást átírják, az ujjlenyomat is megváltozik, s ezt a tűzfal észreveszi és figyelmezteti a rendszergazdát.

- Egyéb funkciók

  A tűzfalak többsége nem egy szabályrendszerrel érkezik. Ilyenkor kiválaszthatjuk a számunkra legmegfelelőbb szintet, anélkül, hogy a szabályok mélyebb ismeretére szükségünk lenne.

5. Internetről letölthető tűzfalak

Ha olyan szerencsések vagyunk, hogy kereskedelmi forgalomban lévő tűzfal vásárlására van lehetőségünk, akkor az ICSA Labs által minősített termékek közül válasszunk

De nagyon jó termékek találhatók az otthoni használatra szabadon letölthető tűzfalak között is. Ezek nemegyszer a kereskedelmi forgalomban lévő termék kissé lebutított változata. Néhány otthoni felhasználásra szabadon letölthető tűzfal:

Név	Verzió	Op. rendszer	Tárigény
ZoneAlarm	3.7.098	Windows 98/Me/NT/2000/XP	3 MB
Sygate Personal Firewall	5.0	Windows 95/98/ME/NT/2000/XP	5 MB
Tiny Personal Firewall	2.0.15	Windows 98/Me/NT/2000/XP	1.4 MB
Outpost Personal Firewall	1.0.18	Windows 95/98/98SE/ME/NT4/2000/XP	2.71 MB
Kerio Personal Firewall	2.1.4	Windows 98/NT/ME/2000/XP	2 MB

A Windows XP már tartalmazza a Internet Connection Firewall (ICF) nevű tűzfalat. Hátránya, hogy a számítógépünkről kimenő forgalmat nem szűri, azt feltételezve, hogy kifelé csak engedélyezett adat megy (ld. MD5 védelem).

B. Az akadémiai (NIIF) hálózat Felhasználói Szabályzata

Az informatikai és hírközlési miniszter
20 /2004. (VI.21.) IHM rendelete
a Nemzeti Információs Infrastruktúra Fejlesztési Program
Felhasználói Szabályzatának
közzétételéről

A Nemzeti Információs Infrastruktúra Fejlesztési Program működtetéséről szóló 95/1999. (VI. 23.) Korm. rendelet (a továbbiakban: Kormányrendelet) 9. §-ának (4) bekezdésében foglalt felhatalmazás alapján az alábbiakat rendelem el:

1. §

(1) A Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzatát (a továbbiakban: Szabályzat) e rendelet *melléklete* tartalmazza. E rendelet mellékletét képező Szabályzat szövegét az Informatikai és Hírközlési Közlönyben kell közzétenni.
(2) A Szabályzatot az Informatikai és Hírközlési Minisztérium és a Nemzeti Információs Infrastruktúra Fejlesztési Iroda (a továbbiakban: NIIF Iroda) internetes honlapján is közzé kell tenni.

2. §

A Szabályzat a NIIF Iroda és tagintézményei között - a Kormányrendelet 9. § (3) bekezdése alapján - kötendő csatlakozási és szolgáltatási megállapodás vagy szerződés mellékletét képezi.

3. §

Ez a rendelet a kihirdetését követő 15. napon lép hatályba.

Kovács Kálmán

Melléklet a 20/2004. (VI.21.) IHM rendelethez

A Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzata

Bevezetés

1. §

A jelen dokumentum (a továbbiakban: Szabályzat) a Nemzeti Információs Infrastruktúra Fejlesztési Program működtetéséről szóló 95/1999. (VI. 23.) Korm. rendeletben (a továbbiakban: Kormányrendelet) meghatározott, a Nemzeti Információs Infrastruktúra Fejlesztési Program (a továbbiakban: NIIF Program) keretében működtetett számítógép-hálózat (a továbbiakban: NIIF hálózat) használatát szabályozza a NIIF tagintézmények és a NIIF felhasználók számára.

Értelmező rendelkezések

2. §

Jelen Szabályzat alkalmazásában:

a) „*NIIF felhasználók”*: a NIIF tagintézményekben a NIIF hálózat használói.

b) „*NIIF Iroda”*: a Kormányrendelet 2. §-ának (3) bekezdése alapján a NIIF Program végrehajtására alapított teljes jogkörrel rendelkező önállóan gazdálkodó központi költségvetési szerv.

c) „*NIIF szolgáltatások”*: a Kormányrendelet 9. §-ának (3) bekezdése alapján a NIIF Iroda illetve a NIIF tagintézmények között létrejött csatlakozási és szolgáltatási szerződés vagy megállapodás keretében meghatározott, a NIIF tagintézményeknek nyújtott hálózati csatlakozás, hálózati és információs szolgáltatások, valamint a szolgáltatásokhoz a NIIF Iroda vagy szerződéses partnerei által biztosított infrastruktúra.

d) „*NIIF tagintézmények”*: felső- és közoktatási intézmények, kutató-fejlesztő helyek, közgyűjtemények és egyéb oktatási, tudományos és kulturális szervezetek, amelyek a Kormányrendelet 9. §-ában meghatározott módon NIIF tagintézményekké váltak.

A NIIF hálózat célja

3. §

A NIIF hálózat célja a Kormányrendelet 1. §-ának megfelelően országos és nemzetközi számítógépes hálózati kapcsolatok és információs szolgáltatások nyújtása felső- és közoktatási, kutatás-fejlesztési, közgyűjteményi, oktatási, tudományos és kulturális célokra.

4. §

A NIIF hálózatot a NIIF tagintézmények a 3. §-ban meghatározott célokra használhatják. Ebbe beleértendő a hálózatnak a tagintézmények tevékenységéhez kapcsolódó adminisztratív és információs feladataival összefüggő használata is.

5. §

Azon intézmények, amelyek nem tagintézményei a NIIF Programnak, azonban valamely NIIF tagintézménnyel oktatási, kutatás-fejlesztési, közgyűjteményi, tudományos vagy kulturális tevékenységre irányuló szerződéses munkakapcsolatban (projektben) együttműködnek, a NIIF hálózat szolgáltatásait használhatják ezen szerződés fennállásának tartama alatt, kizárólag ezen szerződéses munkakapcsolat céljaira. Ilyen együttműködési szerződést NIIF tagintézmény csak meghatározott időtartamra köthet. A NIIF tagintézmény az ilyen szerződés megkötéséhez köteles a NIIF Iroda jóváhagyását kérni, és köteles a munkakapcsolat befejezését a NIIF Irodának bejelenteni. Amennyiben a NIIF Iroda úgy találja, hogy a szerződés nem a fenti tevékenységre irányul, indokolt esetben megtilthatja a nem NIIF tagintézmény számára a NIIF hálózat használatát.

6. §

A NIIF hálózat a 4. és 5. §-ban meghatározott kereteken belül minden tevékenységre használható, amely nem ütközik a 7. §-ban foglalt rendelkezésekbe.

A NIIF hálózat használata

7. §

A NIIF hálózat nem használható az alábbi tevékenységekre, illetve ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszer terjesztése);

b) nem NIIF tagintézmények egymás közötti forgalmának bonyolítása, kivéve ha azt az 5. §-ban meghatározott szerződéses munkakapcsolat indokolja;

c) a NIIF szolgáltatásoknak nem NIIF tagintézmények számára való továbbítása, beleértve a jóhiszemű ą továbbadást is, kivéve az 5. §-ban meghatározott szerződéses munkakapcsolatokat; a NIIF hálózatba kapcsolt rendszereket a működtetőknek a lehetőségek szerint úgy kell konfigurálniuk, hogy az ilyen használatot megakadályozzák (pl. nyílt levelezési átjáró stb.);

d) profitszerzést célzó, direkt üzleti célú tevékenység és reklám;

e) a NIIF hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;

f) a NIIF hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, hálózati játékok, kéretlen reklámok);

g) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan);

h) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;

i) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok közzététele);

j) mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek, hirdetések);

k) a hálózati erőforrások magáncélra való túlzott mértékű használata;

l) a hálózati erőforrások, szolgáltatások olyan célra való használata, amely az erőforrás/szolgáltatás eredeti céljától idegen (pl. hírcsoportokba/levelezési listákra a csoport/lista témájába nem vágó üzenet küldése);

m) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

A felhasználók kötelességei

8. §

A NIIF felhasználók kötelesek jelen Szabályzat megismerésére és megtartására.

9. §

Az a felhasználó, aki a NIIF hálózaton keresztül más hálózati szolgáltató szolgáltatásait is igénybe veszi, az idegen hálózatra érvényes szabályokat is köteles megtartani.

10. §

A NIIF felhasználó a polgári jog általános szabályai szerint felel minden általa - a NIIF Irodának vagy harmadik félnek - okozott kárért.

11. §

A NIIF felhasználó köteles a NIIF Irodát, illetve a NIIF tagintézményeket a Szabályzat megsértése és az esetleges káresetek kiderítésében, valamint lehetőség szerint a bekövetkezett károk következményei felszámolásában segíteni.

A Szabályzat betartatása, a Szabályzat megsértésének szankcionálása

12. §

A Szabályzat megsértésének gyanúja vagy erre vonatkozó - a NIIF Irodához vagy a NIIF tagintézményhez tett - bejelentés esetén az érintett NIIF tagintézmény az esetet kivizsgálja és megteszi a szükséges intézkedéseket. A NIIF tagintézmény a Szabályzat gondatlan megsértése esetén az elkövetőt figyelmeztetésben részesíti. A Szabályzat figyelmeztetést követő ismételt megsértése szándékos elkövetésnek minősül. A NIIF felhasználó a Szabályzat szándékos megsértése esetén a NIIF szolgáltatásokból ideiglenesen vagy véglegesen kizárható.

13. §

A NIIF tagintézmények kötelesek a Szabályzat több intézményt érintő súlyos megsértése esetén a NIIF Irodát tájékoztatni. Az ilyen esetet a NIIF Iroda és az érintett NIIF tagintézmény közösen vizsgálja ki. Amennyiben a Szabályzat több intézményt érintő súlyos megsértése más hálózatot is érint, akkor annak illetékeseivel a NIIF Iroda és az érintett NIIF tagintézmény együttműködni köteles.

14. §

A NIIF Irodának a Szabályzat súlyos megsértése esetén joga van a NIIF tagintézmény hálózati hozzáférését azonnal korlátozni. A hálózathoz való hozzáférés korlátozása esetén a NIIF tagintézményt kártérítési igény nem illeti meg, ugyanakkor a NIIF Iroda a korlátozás okáról az érintett NIIF tagintézményt a lehető legrövidebb időn belül tájékoztatni köteles.

15. §

A NIIF Iroda a Szabályzat megsértéséből eredő károkozás megelőzésére és a bekövetkezett károk következményeinek mielőbbi és minél eredményesebb felszámolására törekszik, illetve a Szabályzat megsértése esetén - amennyiben annak feltételei fennállnak - a polgári jog szabályai szerint felelősségre vonást kezdeményez.

16. §

A NIIF Iroda és a NIIF tagintézmények a mindenkori műszaki lehetőségeknek megfelelően törekednek arra, hogy a hálózaton áthaladó, illetve a hálózaton elérhető információkhoz, adatokhoz illetéktelenek ne férjenek hozzá.

17. §

A NIIF Irodában, illetve a NIIF tagintézményekben a NIIF hálózat működtetéséért felelős személyek a felhasználók adataihoz csak technikai vagy biztonsági okokból férhetnek hozzá, illetve akkor, ha a Szabályzat megsértésének gyanúja merül fel. Az adatokhoz való hozzáférés csak a szükséges mértékben és az érintettek megfelelő tájékoztatásával megengedett. A hálózat működtetéséért felelős személyek az ilyen módon tudomásukra jutott információkat másokkal nem közölhetik, azokat nem hozhatják nyilvánosságra. Kivételt képez, ha a Szabályzat

megsértésének gyanúja merül fel, ebben az esetben az információk a kivizsgálásra illetékes személyekkel közölhetők.

18. §

A NIIF Műszaki Tanács által létrehozott NIIF Etikai Bizottság a NIIF Iroda, a NIIF tagintézmény vagy a NIIF felhasználó kérésére állást foglal a Szabályzatot érintő vitatott kérdésekben. Az Etikai Bizottságnak nem feladata a konkrét esetekben hozott döntések felülvizsgálata.

Záró rendelkezések

19. §

Jelen Szabályzat közzétételét követően a Hungarnet hálózat használatáról szóló szabályzatot („Acceptable Use Policy” - 1997. május 23., 1.0 verzió) nem lehet alkalmazni.

Függelék

Javaslatok, ajánlások a NIIF tagintézmények számára

Ajánlott, hogy minden NIIF tagintézmény hozza létre saját - helyi - hálózat-használati szabályzatát, amelynek a jelen Szabályzattal összhangban kell lennie. A helyi szabályzatok részben vagy egészben tartalmazhatják a jelen Szabályzatot is, de a jelen Szabályzatnak a helyi szabályzaton belül egyértelműen azonosíthatónak és felismerhetőnek kell lennie.
A helyi szabályzatoknak ajánlott tartalmazniuk a következőket:

1. a helyi rendszerek specialitásai és a hálózati sávszélesség korlátai miatt esetleg szükséges további szabályok, korlátozások;
2. a szabályok betartásának ellenőrzési módja; az egyes részfeladatok végrehajtásáért felelős személyek neve, beosztása, elérhetősége;
3. a szabályok megsértése esetén követendő eljárások és alkalmazandó szankciók;
4. a súlyosabb hálózati üzemzavarok, támadások és egyéb veszélyhelyzetek esetében szükséges intézkedések;
5. a felhasználók kötelességei, különösen:

- a helyi hálózati szabályzat és a „netiquette” megismerésének és betartásának kötelessége; együttműködés a hálózat üzemeltetőivel a Szabályzat betartatásának érdekében;
- a biztonsági rendszabályok betartása (pl. az account átruházásának tilalma, a jelszavak rendszeres cseréje, a fölöslegessé vált accountok bejelentése);

6. A felhasználók jogai, különösen:
    - az accounthoz való hozzáférés joga (a technikai lehetőségektől függően);
    - személyi honlap fenntartásának lehetősége (az erőforrások függvényében);
    - a hálózati szolgáltatások használatához szükséges alapismeretek megszerzésének módja és lehetősége;
    - a személyiségi jogok és a levéltitok tiszteletben tartása a hálózat üzemeltetői részéről;
    - a „zaklatás” ellen való védelemkérés lehetősége;
    - a tervezett vagy rendkívüli technikai problémákról (pl. rendszerkarbantartás, levelek elveszése) való tájékoztatás kötelessége a rendszergazdák részéről;
    - a helyi korlátozásokról (pl. levélszűrési rendszer) való tájékoztatás kötelessége a rendszergazdák részéről.