



2. fejezet

A Biztonsági háziprend és a felelősség

A kudarc gyakran csupán ideiglenes állapot.
A feladás teszi véglegessé.

(Marlene vos Savant)

**A fejezet elolvasása után tudnunk kell
a választ az alábbi kérdésekre, és el is kell
tudnunk magyarázni azt:**

- ***Mi a biztonsági háziprend szerepe
a hálózatunkban?***
- ***Hogyan készítsünk biztonsági háziprendet?***
- ***Miként kell kezelni a biztonsági háziprend
megsértését?***

Hálózatunk biztonságossá és védetté tételenek első és legalapvetőbb tenyér döje a biztonsági politika (*security policy*) kialakítása. A részét képező házirendek biztosítják az alapjait a cégnkön és hálózatunkon belüli elfogadható és megfelelő viselkedés definiálásának. Szintén a házirendek alkotják azt a „törvénykönyvet”, amelynek paragrafusaival ítéltetünk meg minden mást.

Tegyük fel, hogy a környezetünkben uralkodó írott és íratlan szabályokhoz hasonló lenne a biztonsági házirend. Milyen lenne így az élet? Amint valami hasznosat akarnánk végrehajtani, bizony kibírhatatlanná válna. A biztonsági házirendnek tehát azt kell leírnia, hogy mi az elfogadható, és mi nem az a hálózatunkon belül. Ez a biztonsági házirend szerepének legalapvetőbb definíciója, azonban számos más ok miatt is hasznos a létrehozása:

- leírja a folyamatokkal szembeni elvárásokat,
- definiálja az elfogadható viselkedést,
- üzemeltetési és üzleti egyetértést fogalmaz meg,
- a nem elfogadható viselkedés esetén ennek alapján lehet fegyelmi eljárást kezdeni,
- a vállalat biztonsági rendszerének minden csoportjához hozzárendeli a szerepköröket és felelősségeket,
- a nem elfogadható viselkedés bekövetkeztekor segít a jogi lépések megtételében,
- a hálózat biztonsága szempontjából alapvető elvek és fogalmak definícióját nyújtja,
- lehetővé teszi a szükséges eszközök meghatározását, a hálózati biztonság pénzügyi szükségleteinek igazolásával.

A biztonsági házirend teszi lehetővé a vállalat dolgozói számára annak pontos megértését, hogy ki miért felelős, megadva egyúttal a belső szervezeti egységek folyamatait és módszereit is. Például az ügyfélszolgálati részleg ebből értheti meg az érzékeny vásárlói adatok védelméért való felelősséget, a személyzeti osztály a munkavállalók által elvárt adatkezelési módot, míg a gyártási és tervezési részleg ebből tudhatja meg, miként kell megvédeni a költséges kutatási és fejlesztési eredményeket. A biztonsági házirend legfontosabb eredménye természetesen az, amit az IT-részleg hasznosíthat belőle. Az informatikusok ebből tudhatják meg, hogyan kell beállítaniuk a szervereket, milyen eszközökre van szükségük, milyen tűzfalszabályokat kell alkalmazniuk, hogyan állítsák be a virtuális magánhálózatot (VPN) stb. – a lista végtelen.

Most persze azonnal felmerül a kérdés, hogy mik a leggyakrabban használt biztonsági eljárások, s az IT-infrastruktúra mely területein érdemes megfontolni az ilyen házirendek használatát. A SANS Biztonsági

Házirend Projektje (*Security Policy Project* – <http://www.sans.org/resources/policies>) számos biztonsági házirendet tesz elérhetővé. Közülük a legelterjedtebbeket tartalmazza a 2.1. táblázat.

2.1 táblázat. Leggyakoribb biztonsági házirendek

Házirend neve	Leírás
Elfogadható titkosítás	Javaslatot tesz a titkosításra használt algoritmusok azokra való korlátozására, amelyek nyilvánosan végzett alapos ellenőrzésen estek át, és hatékony működésük is bizonyított. Ugyanez a házirend rendelkezik az érvényes törvények és szabályzatok betartásának alapelveiről is.
Indokolható használat	Megadja, hogy kik jogosultak a vállalat tulajdonát képező számítástechnikai eszközök és a hálózat használatára. Tartalmazza a vállalat területén és a munkavállalók otthonában található vállalati eszközök használati korlátait egyaránt.
Analóg vonal	Leírja az analóg és ISDN-telefonvonal elfogadható használatát, valamint a jóváhagyási eljárás elveit és folyamatát. Külön szabályok rendelkeznek a kifejezetten a faxokhoz rendelt vonalakról, valamint a számítógépekhez csatlakozó vonalakról.
Alkalmazás-szolgáltatók	Leírja a vállalat elvárásait az alkalmazásszolgáltatókkal (<i>ASP – application service provider</i>) szemben. (Az ASP-cégek szolgáltatásalapú alkalmazást biztosítanak a hálózati technológiák, a hardver és a náluk telepített szoftver segítségével.) Ez a házirend a külön elkészítendő ASP-szabályokra hivatkozik, és annak rendelkezéseit alkalmazza.
ASP-szabályok	Azokat a minimális biztonsági követelményeket határozza meg, amelyekkel egy ASP-nek rendelkeznie kell ahhoz, hogy szolgáltatásainak igénybe vétele egyáltalán szóba kerülhessen.
Felügyelet	Az informatikai biztonsági részleg tagjainak a vállalat által birtokolt, illetve a vállalat területén elhelyezett rendszerek biztonsági ellenőrzésével kapcsolatos jogosultságait határozza meg.
Automatikusan továbbított e-levél	Megtiltja a bizalmas vállalati információk jogosulatlan vagy akaratlan csatolását.
Adatbázis-jogosultságok	A vállalati hálózatok valamelyikén futó programok adatbázis-eléréshez használt felhasználói neveinek és jelszavainak (vagyis a jogosultságoknak) biztonságos tárolásával és lekérdezésével kapcsolatos követelményeket adja meg.
Behívási hozzáférés	Azokat a szabályokat határozza meg, amelyek a feljogosított személyek által használt behívó vonali kapcsolatok gondatlanságból bekövetkező veszélyeltől óvják meg az elektronikus adatokat.
Extranet	Megadja azokat a szabályokat, amelyek a más cégek számára az üzleti folyamatok végrehajtása érdekében a vállalati hálózathoz való hozzáférést szabályozzák.
Információ-besorolás	Segíti az alkalmazottakat annak megismerésében, hogy mely információkat adhatnak meg külső embereknek. Ugyancsak megadja a megfelelő feljogsítás nélkül ki nem adható információk relatív érzékenységét.

Házirend neve	Leírás
Belső labor-biztonság	Rögzíti a laborokra érvényes információs biztonsági követelményeket, megakadályozandó a bizalmas információk és technológiák kijutását, illetve a termelési szolgáltatások és más érdekek labortevékenységektől való védelmét biztosítandó.
Vírusvédelem	Meghatározza a vállalat hálózataira csatlakozó számítógépekkel szemben megfogalmazott követelményeket, amelyek a vírusok kellő hatékonyságú észlelését és védelmét teszik lehetővé.
Jelszó	Az erős jelszavak létrehozásával, védelmével és cseréjük gyakoriságával kapcsolatos szabályok gyűjteménye.
Távoli hozzáférés	A vállalati hálózat bármely gépről való elérésének szabályai. Ezek arra valók, hogy csökkentsék a vállalat bizalmas vagy másként érzékeny adatainak, szellemi tulajdonának elvesztésével, illetve a cégt megítélésével, valamint a kritikus belső rendszerek károsodásával és hasonlókkal kapcsolatos károk bekövetkezésének valószínűségét.
Kockázat-felmérés	Felhatalmazza az információs biztonsági részleget arra, hogy rendszeres információbiztonsági kockázatelemzést végezzen azzal a céllal, hogy meghatározhassa a sérülékeny területeket, és megfelelő óvintézkedéseket tehessen ellenük.
Útválasztó- és kapcsoló-biztonság	A termeléssel vagy a termelési kapacitással kapcsolatos hálózathoz csatlakozó valamennyi útválasztó (router) és kapcsoló (switch) minimális biztonsági konfigurációját határozza meg.
Kiszolgáló-biztonság	A vállalat által birtokolt vagy a telephelyein, illetve a vállalati webszolgáltatók telephelyén elhelyezett kiszolgálók alapkonfigurációjával kapcsolatos szabályokat határozza meg.
Virtuális magánhálózat	Megadja a távoli elérésű vállalati hálózathoz való csatlakozáshoz szükséges IPsec vagy L2TP virtuális magánhálózati szabályait.
Vezeték nélküli kommunikáció	A vállalati hálózathoz biztonságos vezeték nélküli kommunikációs eszközökkel történő hozzáférés szabályait írja le.

A vállalatnál minden személy és részleg érintett a biztonsági házirendben, amint az a következő listából is látszik:

- **Általános felhasználó** – Mivel minden felhasználó hozzáfér a hálózati erőforrásokhoz, így a házirend őket érinti elsősortban.
- **Vállalatvezetés** – A vállalatvezetés felel a vállalati erőforrások és adatok védelméért, miközben tekintettel kell lennie a gazdasági kihatásokra is.
- **Könyvelők, jogászok és befektetők** – Meg kell érteniük, hogy a vállalatok önvédelmi képessége a házirendektől függ, felismerve egyúttal, hogy a biztonsági házirendnek erre erős pozitív kihatása van.
- **Biztonsági csoport** – A házirend ennek a csoportnak a szerepét a biztonsági házirend betartatójaként határozza meg.

A továbbiakban a biztonsági házirendek kialakítása során felmerülő első fontos kérdésre próbálunk választ találni: kiben és miben bíthatunk meg?

2.1. A BIZALMI VISZONYOK MEGHATÁROZÁSA

A bizalom számos különböző megközelítésből is a biztonság központi téma, amit a biztonsági házirendek tárgyalása során végig szem előtt kell tartanunk. Ha tökéletes világban élnénk, egyáltalán nem lenne szükség bizalmi viszonyokra – egyszerűen mindenben megbíznánk és mindenki minden helyesen cselekedne. Sajnos, ez a megközelítés egyáltalán nem valószerű, ráadásul a különböző egyéb tényezőket – például a hálózati erőforrások hibáit – sem veszi figyelembe. Ez utóbbit másként is megfogalmazhatjuk: nagyon jó lenne, ha megbízhatnánk a hálózati erőforrásokban, a hálózatot alkotó hardver és szoftver meghibásodása azonban egyáltalán nem kivételes esemény.

A biztonsági házirend azzal az alapfeltételezéssel is elkészíthető, hogy a szervezetnél senkiben sem lehet megbízni. Rendkívül valószínűtlen azonban, hogy egy ilyen házirend képes lenne elérni célját. Ismert tény, hogy a felhasználók rendre igyekeznek megkerülni a túlságosan szigorú szabályokat, ezért a hálózati biztonságot egyensúlyba kell hozni a bizalmi viszonyokkal. Ez az egyensúly minden vállalat esetén más és más, de a biztonság igénye mindenütt ugyanaz.

Amikor a biztonsági házirendbe beépítendő bizalom szintjét akarjuk meghatározni, a következő kérdéseket gondoljuk végig, és a válaszokat tartsuk szem előtt a megfogalmazás során:

- a hálózat minden egyes részére határozzuk meg, kinek legyen hozzáférése,
- határozzuk meg, hogy pontosan mihez és miként férhetnek hozzá,
- hozzuk egyensúlyba az emberekbe és erőforrásokba vetett bizalmat,
- a felhasználók és erőforrások hozzáférését a bizalom szintje határozza meg,
- biztosítsuk, hogy a bizalommal ne éljenek vissza,
- határozzuk meg, mit értünk a hálózat és erőforrásainak helyes használata alatt.

E rövid listán kívül még számos más kérdést is figyelembe kell vennünk, beleértve a vállalati politikát és a felhasználói reakciókat is. A biztonsági házirend nem képes minden lehetséges megfontolásnak eleget tenni, de rendkívül fontos annak megértése, hogy milyen hatással lesz az emberekre.

A SANS biztonsági házirend projekt szerint a biztonsági házirendnek az engedélyeket kell megfogalmaznia, nem pedig a tiltásokat. Ahol csak lehetséges, minden adjunk példákat is az engedélyezett és tiltott viselkedésre. Ezzel a módszerrel elkerülhetők a félreértesek. Ha a biztonsági házirend nem engedélyezi kifejezetten az adott viselkedést, akkor az tilos. Ugyancsak le kell írni azt is, hogy a házirendben lefektetett célok miként érhetők el. A biztonsági házirend fejezetét és azok rövid tartalmi javaslatait a 2.2. táblázatban soroljuk fel.

2.2. táblázat. A biztonsági házirend általános tartalmi javaslata

Fejezetcím	Tartalmi javaslat
Áttekintés	Bizonyítja a házirend szükségességének okát, és azonosítja az érintett kockázati területeket.
Célkitűzés	Elmagyarázza, hogy miért jött létre a házirend, és mi a célja.
Hatályosság	Meghatározza az érintettek körét, ami egy kis csoporttól akár a teljes vállalatig terjedhet.
Szabályok	Ez maga a szabályzat. Gyakran különálló alfejezetekre tördeljük, és példákkal illusztráljuk a jobb megértés vagy a pontosabb meghatározás érdekében.
Büntetések	A házirend be nem tartásáért adható büntetéseket határozza meg. Általában „az eddig felsoroltak mellett...” sablon szerint fogalmazzuk meg, így a büntetések akár együttesen is alkalmazhatók. Leggyakrabban az elbocsátás a legsúlyosabb büntetés, de néhány esetben a büntetőjogi felelősségre vonás kezdeményezése is szerepelhet.
Meghatározások	A nem teljesen nyilvánvaló vagy kétértelmű fogalmak, illetve azok meghatározása.
Változásjegyzék	A végzett változtatások, valamint okai és időpontjai vannak itt felsorolva. Erre azért van szükség, mert a házirend megsértése esetén a cselekményt nem a felfelmeréskor, hanem a bekövetkezéskor érvényes szabályok szerint kell kivizsgálni.

A biztonsági házirend tehát meghatározza a szervezet által védendőnek ítélt erőforrásokat, valamint a védelmük érdekében tett intézkedéseket. Magyarul, a házirend a biztonság kialakítása érdekében hozott döntések során alkotott szabályzat. Nyilvánosságra kell hozni, és a vállalat valamennyi alkalmazottjával, illetve a rendszer minden felhasználójával meg kell ismertetni. A vezetésnek biztosítania kell, hogy mindenki elolvashassa, megérthesse és elfogadhassa a házirend betartásában játszott szerepét, és megismerhesse a megsértésének következményeit.

Amint arról már volt szó, a két véglet az, hogy mindenben megbízhatunk, vagy senkiben sem bízhatunk meg. Egyik megoldás sem működik hatékonyan, ha a működőképességet megőrizve akarunk biztonságot. Mindegyik felhasználó másként szemléli a hálózat biztonsági igényeit,

s mindegyikükben megtalálható az öröklelem egy adott szintje. A felhasználók egrészt félhetnek attól, hogy a biztonsági intézkedések miatt a munkájuk megnehezedik, de félhetnek a büntetéstől is, ami egy hiba elkövetéséért vagy feledékenységükért járhat. Mindehhez társul az emberekben különböző szinten meglévő ellenséges hozzáállás bármiféle, a munkavégzésüket érintő korlátozással szemben. Ezek a viselkedések teljesen természetes érzelmi reakciók, amelyeket meg kell érteni és a házirend kialakítása során megfelelően kell kezelni a vállalat védelmi egyensúlyának megteremtése érdekében. A házirendek megalkotásába ezért ajánlatos bevonni a 2.3. táblázatban felsorolt csoportok képviselőit, növelve ezzel elkötelezettségüket a szabályok betartásában.

2.3. táblázat. A házirendet bíráló testület tagjai (a SANS biztonsági házirend projekt alapján)

Képviselet	Feladatkör
Vezetőség	Bárki, aki képes betartatni a házirendet. Általában a személyi döntésért felelős részleg vezető beosztású tisztségviselője.
Információbiztonsági részleg	Bárki, aki technikai részletekkel is szolgálhat.
Felhasználói területek	Bárki, aki a felhasználókkal azonos szemszögből képes véleményezni a szabályokat.
Jogi osztály	Valószínűleg csak időnként van rá szükség. Bárki lehet, aki képes a házirend érvényes jogszabályoknak való megfelelősegét vizsgálni. Multinacionális vállalatok esetén ezen vizsgálat nehézsége exponenciálisan növekszik. ¹
Sajtóosztály (propaganda)	Bárki, aki képes javaslatokat tenni azzal kapcsolatban, hogy miként lehet a házirendet „eladni”, vagyis miként lehet azt megismertetni a vállalat alkalmazottaival, és hogyan lehet rávenni őket az együttműködésre.

Az emberek alkotta aknamező elkerülhető, ha az érintett csoportoktól a házirend fejlesztése során kikérjük a véleményüket. Ez lehetővé teszi számunkra azt is, hogy némi társadalomkutatást végezzünk, a „jó fiúkat” kiválasztandó, akik részt vehetnek a fejlesztésben. Ebben az esetben sokkal könnyebben fogják később elfogadni a biztonsági megszorítások léttét.

A továbbiakban azokat a tényleges biztonsági házirendeket vizsgáljuk meg közelebbről, amelyeket a jelenlegi cégem (a Granite Systems) használ. Ez segíthet minket annak meghatározásában, hogy miként kell a biztonságot kezelni.

¹ Mivel a könyv szerzője alapvetően az angolszász joggyakorlatnak megfelelően érinti a jogi kérdéseket, illetve annak megfelelően alkotja meg a mintaszabályzatokat is, így különösen indokolt az amerikai példák, mintaszabályzatok jogi felülvizsgálata. (A lektor meg.)

2.2. INDOKOLHATÓ HASZNÁLATI HÁZIREND

A SANS (<http://www.sans.org>) a honlapján ingyenesen elérhetővé teszi a biztonsági házirendek egész seregét. A most ismertetésre kerülő is ezekre a nyilvánosan elérhető házirendekre épül. Ne feledjük azonban, hogy a biztonsági politika minden személyre szabott kell legyen, így az itteni min-ták szolgai másolása erősen ellenjavallt, ezek csupán ötletadási célzattal szerepelnek itt. A honlap meglátogatása az ebben a részben tanultakat egészítheti hasznosan ki. A Granite Systems (<http://www.granitesystems.net>) a SANS ajánlásaira alapozta a saját házirendjét, és nagylelkűen hozzájárult ahhoz, hogy a belső gyakorlata ebben a könyvben nyilvánosan is elérhető legyen.

Ebben a szabályzatban a cég IT-biztonsági részlegét egyszerűen *vállalati biztonsági csoport* néven emlegetjük. Maga a *Granite Systems* és minden egyes vállalatspecifikus részlege dőlt betűvel található a házirendben. Ha valaki egyébként változtatás nélkül akarná felhasználni ezt a szabályzatot, akkor elegendő ezeket kicserélnie a megfelelő nevekre.

2.2.1. ÁTTEKINTÉS

Az indokolható használati házirend kiadásával a *vállalati biztonsági csoport* szándéka nem az, hogy a *Granite Systems* vállalat meghirdetett céljaival, a nyíltsággal, bizalommal és sérthetetlenséggel ellentétes korlátozásokat vezessen be. A részleg elkötelezetted abban, hogy a vállalat alkalmazottait, partnereit és magát a vállalatot megvédje az egyes személyek szándékos vagy véletlen, illegális vagy káros cselekményeinek következményeitől.

A különböző internet/intranet/extranet rendszerek, beleértve a számítástechnikai eszközöket, szoftvereket, operációs rendszereket, adattárolókat, valamint az elektronikus levelezést, webböngészést és állományátvitelt biztosító hálózati témaszám fiókokat a *Granite Systems* tulajdonát képezik. Ezen rendszereket a vállalat, kliensei és fogyasztói érdekeit szolgáló üzleti céllal engedélyezi használni.

A hatékony biztonság kizárálag az egész vállalatot felölelő együttes csapatmunka eredményeként teremthető meg, amelyhez szükség van az információval, illetve információs rendszerekkel kapcsolatba kerülő vállalati alkalmazottaknak, szerződött és üzleti partnereknek és egyéb jogviszonyban álló tagoknak a közreműködésére és támogatására. minden egyes számítógép-felhasználónak a saját felelőssége, hogy ismerje a szabályzat útmutatásait, és tevékenységét a benne foglaltaknak megfelelően végezze.

2.2.2. CÉLKITŰZÉS

Jelen házirend célja a *Granite Systems* vállalatnál elhelyezett számítástechnikai eszközök indokolható használatának megfogalmazása. E szabályok célja a *Granite Systems* vállalat alkalmazottainak védelme. A helytelen használat a vállalat számára biztonsági kockázatot jelent, beleértve, de nem ezekre korlátozódva, a vírustámadásokat, a hálózati rendszerek és szolgáltatások veszélyeztetését és a jogi következményeket egyaránt.

2.2.3. HATÁLYOSSÁG

Jelen házirend hatálya kiterjed a *Granite Systems* vállalat valamennyi alkalmazottjára, szerződéses munkatársára, konzultánsára, időszaki és egyéb munkására, beleértve a más cégek által alkalmazottakat is. Hatálya kiterjed a vállalat által bérelt, lízingelt vagy birtokolt valamennyi eszközre, beleértve azokat a magántulajdonú saját eszközöket is, amelyek a vállalat IT-infrastruktúrájával kapcsolatba kerülhetnek.

2.2.4. ÁLTALÁNOS HASZNÁLAT ÉS TULAJDONJOG

1. Jóllehet a *vállalati biztonsági csoport* ésszerű szinten kívánja biztosítani a személyes titok védelmét, a felhasználóknak tisztában kell lenniük azzal, hogy a vállalati rendszerek felhasználásával létrehozott adatok a *Granite Systems* tulajdonát képezik. A vállalati hálózat védelmének szükségessége miatt a vezetőség nem garantálhatja a vállalat bármely hálózati eszközén tárolt információk bizalmas voltát.
2. A munkavállalók felelősek a személyi használat indokoltságával kapcsolatos ésszerű döntések meghozataláért. Az egyes részlegek kötelesek elkészíteni az internet/intranet/extranet rendszerek használatával kapcsolatos előírásokat. Amennyiben hiányoznának a vonatkozó házirendi szabályok, a munkavállalók a személyi használatra vonatkozó előírásokat kötelesek betartani. Kétség esetén a munkavállalonak kötelessége megkérdezni munkahelyi vezetőjét vagy felügyelőjét.
3. A *vállalati biztonsági csoport* azt ajánlja, hogy a felhasználók által érzékenyek vagy sérülékenyek tartott adatok titkosítva legyenek tárolva. A vonatkozó információbesorolási vezérelveket az ugyancsak a *vállalati biztonsági csoport* által kiadott Információbesorolási házirend tartalmazza. Az e-levelek és dokumentumok titkosításával kapcsolatban lásd a csoport Elővigyázatossági ajánlását.



Megjegyzés

Számos esetben találkozhatunk olyan biztonsági házirenddel, amely a szervezet egy másik biztonsági házirendjére hivatkozik. Ezt nemcsak célszerűnek tartjuk, de egyben ez az ajánlott megoldás. Ez teszi ugyanis lehetővé, hogy a házirend mindenki csak az adott területre összpontosítható. Vegyük például az előző pontot, amely az adatok titkosítására hivatkozik. A valóságban a szervezet valamennyi munkatársának kötelező az elfogadható használat házirendjének elolvasása és aláírása. Ha azonban azt vizsgáljuk, hogy valószínűleg kiktől várható el az adatok titkosítása, akkor egy teljesen más listát és más típusú személyeket kapunk. Ezek a szabályzatok ezért külön lettek elkészítve, elkerülendő (vagy kiváltandó) a felhasználók összeavarását.

4. Biztonsági és hálózati karbantartási okokból a *Granite Systems* vállalat felhatalmazott munkatársai bármikor ellenőrizhetik az eszközöket, rendszereket és a hálózati forgalmat, a vállalati biztonsági csoport Felügyeleti házirendjének megfelelően.
5. A *Granite Systems* vállalat fenntartja magának a jogot, hogy bármely hálózatot vagy csatolt rendszert ellenőrizzen akár rendszeres, akár véletlen szerű jelleggel, így felügyelve a jelen szabályzat betartását.



Megjegyzés

A 4. és 5. paragrafus különösen fontos, hiszen így értesíthető minden személy arról, hogy a vállalat rendszeresen, illetve szükség esetén bármilyen módon megfigyelheti és ellenőrizheti a hálózatot. Ezen állításokra azért van szükség, mert jogilag így lehet felhívni az alkalmazottak figyelmét arra, hogy valamiképpen megfigyelés alatt is állhatnak.

2.2.5. BIZTONSÁGI ÉS TULAJDONJOGI INFORMÁCIÓK

1. Az internettel/intranettel/extranettel kapcsolatos rendszerek információs felhasználói felületei minősíthetők bizalmasnak és nem bizalmasnak egyaránt, amint azt a vállalat Emberi erőforrások házirendjében található adatbesorolási vezérelvek meghatározzák. Bizalmas információk (nem kizárolagosan) például az alábbiak:

- vállalati titkos és bizalmas adatok,
- vállalati stratégiák és fejlődési irányvonalak,
- versenytárs-érzékeny vagy versenyképességi analízis,
- kereskedelmi titkok, szabadalmak és teszteredmények,
- specifikációk, működési paraméterek,
- fogyasztók listája és adataik,
- kutatási adatok.

A munkavállalóknak minden szükséges lépést meg kell tenniük annak érdekében, hogy az ilyen jellegű információhoz való jogosulatlan hozzáférést megakadályozzák. Amennyiben egy munkavállalonak tudomására jut, hogy ilyen jellegű információ valószínűsíthetően kikerült a vállalattól, haladéktalanul értesítenie kell gyanújáról a *vállalati biztonsági csoportot*.

2. A jelszavakat titokban kell tartani, és a bejelentkezési információk nem oszthatók meg. A jogosultságokkal rendelkező felhasználók felelőssége a saját bejelentkező nevük és jelszavuk biztonságának megőrzése. A rendszerszintű jelszavakat negyedévente, a felhasználószintű jelszavakat pedig minden hat hónapban egyszer cserálni kell.
3. minden számítógépről, hordozható gépről és munkaállomásról abban az esetben, ha felügyelet nélkül marad, ki kell jelentkezni (Ctrl-Alt-Delete a Windows 2000 és XP felhasználók esetén), vagy zárolással, illetve jelszóval védett képernyővédővel kell biztosítani úgy, hogy az legkésőbb 10 perc elteltével automatikusan aktiválódjék.

Megjegyzés

A 2. és 3. paragrafusban eleve azt feltételeztük, hogy a vállalat rendszere az ajánlott módszer szerint működik. Ez azt jelenti, hogy a szerverek megkövetlik a felhasználóktól a jelszavak rendszeres cseréjét, amely jelszavak a később ismertetett „jelszószabályzat” előírásainak megfelelnek.

2.

4. Az információ titkosítása kizárálag az Engedélyezett titkosítási lehetőségek házirendben leírtaknak megfelelően történhet.
5. Mivel a hordozható számítógépeken tárolt információ különösen sérülékeny, így ezeket különleges gondossággal kell kezelni. A hordozható gépeket a „Laptop-biztonsági javaslatok” dokumentumban foglaltak szerint javasolt használni.
6. A *Granite Systems* vállalat e-levélcímét használó alkalmazottak kötelesek a hírcsoportokba irányuló leveleik végén elhelyezni egy nyilatkozatot, amelyben kijelentik, hogy a levélben található vélemények a sajátjuknak tekintendők, és nem feltétlenül tükrözik a *Granite Systems* vállalat véleményét. Kivételt a vállalat üzleti ügyeiben történő e-levelek jelentenek.

7. A munkavállalónak a *Granite Systems* vállalat internet/intranet/extranet rendszerére csatlakozó bármely gép használata esetén – birtokolja azt akár a vállalat, akár a munkavállaló – az adott gépen folyamatosan üzemeltetnie kell a jóváhagyott víruskereső szoftverek egyikét, amely a legfrissebb vírusadatbázist használja.



Ez a paragrafus azért szükséges, mert a felhasználók leveleiket különböző gépeken és különböző fizikai helyeken töltik le. Tegyük fel, hogy egy felhasználó a saját ingyenes webes postafiókját a munkahelyén nézi meg, és anélkül tölt le egy vírust is tartalmazó levelet, hogy a fertőzöttségét észlelné. A paragrafus célja tehát az, hogy legalább a munkahelyen egy elfogadott víruskereső észlelje az állomány vírusos voltát. Ha azonban a felhasználó ugyanezen e-levelet ott-honról egy olyan gépre tölti le, amelyet a vállalati hálózathoz való csatlakozáshoz is használ, akkor figyelemmel kell lennie erre a lehetőségre, illetve a megsérítéséért járó lehetséges büntetésekre.

8. A munkavállalóknak különösen óvatosnak kell lenniük az ismeretlen feladótól érkező e-levelek csatolmányai kent érkező állományok megnyitásakor, amelyek vírusokat, e-levélbombákat vagy trójai kódot tartalmazhatnak. Kétség esetén a munkavállalóknak tanácsos külön megvizsgálniuk a dokumentum vírusmentességét, és megnyitása előtt konzultálni a vállalati biztonsági csoporttal.

2.2.6. VISSZAÉLÉSEK

Az ebben a pontban felsorolt cselekmények általában tiltottak. Egyes munkavállalók kaphatnak a tiltások alól felmentést, ha arra munkakörük megfelelő betöltése miatt szükségük van. (A rendszergazdának például meg kell legyen a joga arra, hogy egy adott gép hálózati elérését megszüntesse, amennyiben az a gép akadályozza a termelési folyamatokat.)

A *Granite Systems* vállalat egyetlen munkavállalója sem jogosult a területi, hazai vagy nemzetközi jogszabályba ütköző tevékenység folytatására a vállalat által birtokolt erőforrások felhasználása során.

Az alábbiakban felsorolt lista semmiképpen sem tekinthető teljesnek vagy kizárolagosnak, csupán megkíséri a visszaélés kategóriájába eső cselekmények keretét megrajzolni. Amennyiben bármely munkavállalónak egy cselekmény engedélyezhetőségével kapcsolatos kérdése lenne, a vállalati biztonsági csoporttal kell előzetesen tisztáznia azt.

Rendszer és hálózati cselekedetek

A következő cselekmények kivétel nélkül szigorúan tiltottak.

1. Tilos bármely személy vagy társaság szerzői, kereskedelmi, szabadalmi vagy más szellemi tulajdonjogának, illetve más hasonló törvénynek vagy szabályozásnak a megsértése, beleértve, de nem csak ezekre korlátozódva a „kalóz” vagy más olyan szoftvertermék installálását vagy közreadását, amelynek használati jogát a *Granite Systems* vállalat nem, vagy nem kellően szerezte meg.
2. Szigorúan tilos a szerzői jogvédelem alá tartozó bármilyen anyag lemásolása, beleértve, de nem csak ezekre korlátozódva az újságokból, könyvekből vagy más jogvédett termékekben származó képek vagy jogvédett zene digitalizálását, közreadását, illetve minden olyan jogvédett szoftver installálása, amelyhez a *Granite Systems* vagy a végfelhasználó nem rendelkezik érvényes licencsel.
3. Illegális a szoftverek, technikai információk, titkosított szoftver vagy technológia nemzetközi vagy regionális exporttörvénybe ütköző exportálása.

Bármely kérdéses anyag exportálása előtt az illetékes menedzserrel kell konzultálni.



Az első néhány paragrafus a vállalat és a biztonsági házirend szempontjából több ok miatt is fontos. Végük mondjuk a talán leglátványosabb, és jogilag legaktívabb alábbi három, az interneten elérhető szervezetet:

- Recording Industry Association of America (<http://www.riaa.org>),
- Report Cable Theft (<http://www.cabletheft.com>),
- Business Software Alliance (<http://www.bsa.org>).

Ezek a szervezetek figyelemmel kísérik a szerzői jogok megsértését, kalózkodást, lopást, más hasonló cselekményeket, és jogi eljárást kezdenek azokkal szemben, akik ilyen cselekményekben részesek. Ezek a személyek és vállalkozások voltak ezen szervezetek első jogi célpontjai, velük szemben sikerrel jártak, s jelenleg az oktatási intézményekben és a kampuszokon folyó (etikus vagy rosszindulatú) kalóztevékenység irányába kezdenek fordulni.

4. Tilos rosszindulatú programok szerverre vagy hálózatba juttatása (például vírusok, trójai programok, e-levélbombák, egyebek).
5. Tilos a saját bejelentkezési jelszót bárki más tudomására hozni, vagy a témaszám bárki más általi használatát lehetővé tenni, beleértve a családtagokat vagy a közös háztartásban élőket is, ha a munkát otthonról kell folytatni.

Megjegyzés



Jegyezzük meg, hogy a vállaltnál soha senki nem fogja megkérdezni a jelszavunkat. Amennyiben bármilyen technikai nehézség adódna, az erre jogosult alkalmazottak egyszerűen kicserélik a jelszavunkat. Éppen ezért soha senkinek nem szabad elárulni a jelszót, s ha valaki mégis megkérdezné, azonnal tegyük róla jelentést.

6. A *Granite Systems* számítástechnikai vagyonának felhasználásával a felhasználó tartózkodási helyén érvényes, a szexuális zaklatásra vagy munkahelyi ellenségeskedésre vonatkozó törvényeket sértő anyagok átvitele vagy beszerzése.
7. A *Granite Systems* bármely témaszámáról termékekre, szolgáltatásokra vagy árucikkekre vonatkozó csalárd ajánlat tétele.
8. Tilos a garanciával kapcsolatban bármilyen kijelentést tenni, legyen az utalás vagy kifejezetted hivatkozás, kivéve munkakörből adódó kötelezettség részeként tett kijelentéseket.
9. Tilos a biztonság megsértése vagy a hálózati kommunikáció megrongálása. A biztonság megsértése körébe tartozó cselekmény például olyan adathoz való hozzáférés, amelyre a munkavállalónak nincs jogosultsága, vagy belépés olyan szerverre vagy témaszámmal, amelyre a felhasználónak nincs kifejezetted jogosultsága, kivéve ha ezen cselekmények a szokásos munkavégzés miatt szükségesek. Ezen bekezdés szempontjából „megrongálásnak” minősül más, itt fel nem sorolt cselekmény mellett a hálózat lehallgatása, elárasztásos támadások, csomagok meghamisítása, szolgáltatás megtagadása és az útválasztási információk rosszindulatú okok miatt történő meghamisítása.
10. Portok letapogatása vagy a biztonsági letapogatás a *vállalati biztonsági csoport* előzetes értesítése nélkül kifejezetten tilos.
11. Tilos a hálózat bármilyen formában történő megfigyelése, amelynek során nem a munkavállaló géphez címzett adat kerül elfogásra, kivéve ha a munkavállaló munkaköri leírásában ez a tevékenység kifejezetten szerepel.
12. Bármely gépen, hálózaton vagy témaszámon a felhasználói azonosítás vagy a biztonsági rendszer megkerülése.
13. Tilos a szolgáltatás megtagadása vagy befolyásolása a munkavállaló gépének kivételével (például szolgáltatásmegtagadási támadás).
14. Tilos bármely program/parancsállomány/parancs használata, vagy bármely üzenet küldése egy felhasználó terminálkapcsolatát befolyásoló vagy ellehetetlenítő szándékkal, történék bármilyen módon, helyileg vagy az interneten/intraneten/extraneten keresztül.

- 15.** Tilos a *Granite Systems* vállalat dolgozóin kívül bárkinek megadni a vállalat munkavállalónak névsorát, vagy bármilyen velük kapcsolatos egyéb információt.

E-levezési és kommunikációs tevékenységek

- Tilos a kéretlen e-levél üzenetek, beleértve az úgynevezett „szemétlevelet” (*junk mail*) is, vagy más hirdetések küldése olyan címekre, amelyek nem kérték kifejezetten az ilyen információk küldését (hulladék e-levél, „szpem”, illetve eredeti írásmóddal *spam*).
- Tilos az e-levélben, telefonon vagy üzenetküldő rendszeren keresztül történő zaklatás bármely formája, alkossa azt a használt nyelvezet, gyakoriság vagy üzenethossz.
- Tilos az e-levél fejlécében található információk meghamisítása vagy jogosulatlan használata.
- Tilos a feladó e-postafiókcímtől eltérő bármely más e-levélcímre történő e-levél megrendelése zaklatási vagy válaszgyűjtési szándékkal.
- Tilos a „lánclevelek”, valamint a bármilyen típusú pilótajátékok létrehozása vagy továbbítása.
- Tilos az eredetileg a *Granite Systems* vállalat hálózatából vagy bármely más internet/intranet/extranet szolgáltatótól érkező e-levél kéretlen továbbküldése a *Granite Systems*, vagy a hálózatához csatlakozó más szervezet nevében, illetve szolgáltatásait hirdetendő.
- Tilos ugyanazon vagy hasonló, nem üzleti célú üzenetek továbbítása több Usenet hírcsoportba (hírcsoport hulladéküzenet).

2.2.7. BÜNTETÉSEK

A szabályzatot megszegő munkavállalók fegyelmi eljárás alanyai lesznek, amelynek határozata alapján a vétkes munkavállaló akár el is bocsátható.

2.

2.2.8. KÖVETKEZTETÉSEK

Minden biztonsági házirendnek néhány közös elemmel kell befejeződni. Ezek tisztázzák a potenciális félreértelemezéseket és feloldják a felhasználó értelmezési nehézségeit, hogy végül megérthesse, pontosan mit szabad és mit nem.

- Büntetések** – A legfontosabb elem a szabályzat megszegése esetén a munkavállalót terhelő következmények és büntetések ismertetése.
- Meghatározások** – Nem minden felhasználó vagy alkalmazott képes a szabályzatban használt terminológia pontos megértésére, ezért komoly

haszonnal jár, és a téves értelmezések és félreértek elkerülhetők, ha lehetőleg iparspecifikus fogalmak használatával pontosan meghatározzuk a használt kifejezéseket.

- 3. Változásjegyzék** – A szabályzatok bármikor megváltozhatnak. A változások forrása is megváltozhat idővel. Okai között szerepelhet a vezetőség megváltozása, új törvények életbe lépése vagy régebbi törvények pontosítása, a hálózatunk biztonsága ellen irányuló új fenyegetések megjelenése, a vállalat döntése, hogy minőségbiztosítási vagy egyéb tanúsítványt szerez, vagy csak egyszerűen egy olyan új technológiát fejlesztett ki, amelyet szintén szabályozni kell. A változás tényét viszont tanácsos dokumentálni.

Jóllehet a szabályzatok általában felzaklatják az embereket, akik rendszerint úgy gondolják, hogy joguk van bizonyos dolgokra a munkáltatójuktól, pedig ilyen jogai nincsenek – ők azért vannak, hogy a vállalatot segítsék az üzleti érdekeinek elérésében. Ez az alapvető igazság teszi lehetővé, hogy a házirend egyaránt védje a vállalatot, alkalmazottait, és bárki mást, aki kapcsolatba kerül vele.

2.3. A JELSZAVAK SZABÁLYOZÁSA

SANS (<http://www.sans.org>) a honlapján ingyenesen elérhetővé teszi a biztonsági házirendek egész seregét. A most ismertetésre kerülő is ezekre a nyilvánosan elérhető házirendekre épül. A honlap meglátogatása és az ebben található megjegyzések együttesen segíthetnek a saját ötletek kidolgozásában. A Granite Systems (<http://www.granitesystems.net>) a SANS ajánlásaira alapozta a saját házirendjét, és hozzájárult ahhoz, hogy itt nyilvánosságra hozzuk.

Ebben a szabályzatban a cég IT-biztonsági részlegét egyszerűen *vállalati biztonsági csoport* néven emlegetjük. Maga a *Granite Systems*, és minden egyes vállalatspecifikus részlege dőlt betűvel található a házirendben. Ha valaki egyébként változtatás nélkül akarná felhasználni ezt a szabályzatot (ami a legkevésbé sem ajánlható), akkor elegendő ezeket kicserélnie a megfelelő nevekre.

2.3.1. ÁTTEKINTÉS

A jelszavak a számítógépes biztonság fontos elemét alkotják. A felhasználói témaszámok védelmének első vonala belőlük áll. Egy rosszul megválasztott gyenge jelszó a *Granite Systems* teljes vállalati hálózatát veszélybe sodorja. Éppen ezért a vállalat alkalmazottai (beleértve a szerződéses munkatársakat és a *Granite Systems* rendszereit elérő beszállítókat

is) kötelesek az alábbiakban kifejtett minden szükséges lépést megtenni a saját jelszavaik kiválasztása és védelme érdekében.

2.3.2. CÉLKITŰZÉS

Jelen szabályzat célja az erős jelszavak létrehozási szabályainak, valamint a védelmük érdekében követendő módszerek rögzítése és megváltoztatásuk gyakoriságának előírása.



A jelszavakat rendszeresen cserélni kell, mert a támadók a felhasználói jelszavakat próbálják meg elsőként feltörni. A legtöbb rendszer egy adott, előre beállított idő elteltével automatikusan felszólítja a felhasználókat a jelszavuk megváltoztatására. A gyakorlatban a legtöbb modern operációs rendszer a felhasználói jelszavakat intelligens módon kezeli, így például megtiltja a könnyen feltörhető vagy egy szótárban megtalálható szavak használatát. Ha valaki nem használja ezeket a lehetőségeket vagy nem tudja, hogy a rendszere egyáltalán lehetővé teszi-e a használatukat, akkor javasoljuk neki ennek kiderítését, és a lehetőség aktiválását.



2.3.3. HATÁLYOSSÁG

Jelen szabályzat hatálya kiterjed minden olyan személyre, aki bármilyen témaszámért (esetleg jelszót igénylő vagy támogató hozzáférési módról) felelős vagy rendelkezik ilyennel a *Granite Systems* területén elhelyezett, a hálózatát elérő vagy a vállalat nem nyilvános információit tároló bármely eszközön.

2.

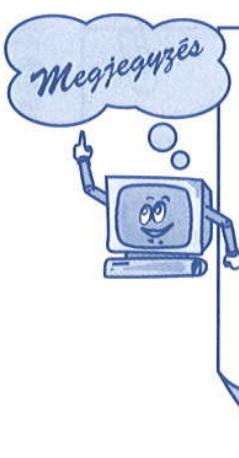


A témaszám meghatározható és kiterjeszthető az e-levélcímekre, állományátviteli protokollt használó átvitel jelszavaira, megosztott könyvtárakra, billentyűzárakra, és egyéb hasonló lehetőségekre is. Az ilyen jellegű erőforrások használatát lehetővé tevő valamennyi jelszót valamelyen jelszószabályzat szerint kell kezelni, amint azt később bemutatjuk.

2.3.4. ÁLTALÁNOS SZABÁLYOK

Valamennyi rendszerszintű jelszót (például a rendszerjelszavakat, alkalmazás-adminisztrátori jelszavakat, szolgáltatások jelszavait stb.) legalább negyedévente ki kell cserélni.

- A termelést érintő rendszerszintű jelszavak mindegyikét kötelezően tárolni kell a *vállalati biztonsági csoport* által kezelt globális jelszóadatbázisban.



Nincs minden szervezetnek ilyen jól hangzó „globális jelszóadatbázisa” a jelszavak nyomon követésére, s erre a legtöbb szervezet esetén valójában nincs is szükség. Valamilyen módon azonban nyilván kell tartani mind az ilyen jelszavakat, mind pedig lecserélésük gyakoriságát. Csak ez teszi lehetővé, hogy a szabályzat betartását ellenőrizni lehessen. Természetesen bármilyen eszközzel is tartanánk nyilván ezt az információt, a hozzáférést erősen korlátozni kell.

- minden felhasználói szintű (például e-levél, web, munkaállomás) jelszót legalább hathavonta egyszer cserélni kell. A csere ajánlott gyakorisága négy hónap.
- A csoporttagságuk vagy valamilyen alkalmazás következtében rendszerszintű jogosultságokkal rendelkező (például adminisztrátor vagy root) témaszámhoz egyedi jelszót kell hozzárendelni, amely nem lehet azonos az ezen témaszámot használó felhasználó egyetlen másik jelszavával sem.
- A jelszavakat tilos e-levélüzenetben vagy más elektronikus kommunikáció segítségével elküldeni.
- A jelszavakat tilos bárki ne elárulni, függetlenül az illető vállalaton belüli pozíciójától. Ha valaki mégis megkérdezné a jelszavakat, a munkatársak még a jelszó elárulása előtt kötelesek értesíteni a *vállalati biztonsági csoportot*.
- Az SNMP-jelszó (*community string*), amennyiben ezt a protokollt kell használni bármely eszközökhez is, nem lehet az alapértelmezett „public”, „private” és „system” egyike sem, továbbá tilos az interaktív bejelentkezésre használt bármely jelszóval megegyezőségük is. Amennyiben lehetséges, a kulcsos kivonatoló titkosítást kell használni (például SNMPv2).

Megjegyzés



Az utolsó szabály az eszköz alapértelmezett jelszavának kötelező megváltoztatását írja elő. Ez rendkívül fontos, mégis meglepő, hogy milyen sok szervezet hagyja meg az alapértelmezett jelszavakat. Valahányszor egy olyan eszközzel találkoznánk, amelynek nem ismerjük az alapértelmezett jelszavát, a <http://www.cirt.net/cgi-bin/passwd.pl> webhelyen kereshetjük azt meg.

A könyv fordításakor 218 gyártó 1299 alapértelmezett jelszavát lehetett meg-találni ezen az állandóan bővülő oldalon, amely a vezeték nélküli eszközöket és jelszavaikat (SSID – service set identifier; szolgáltatáscsoport-azonosító) is tartalmazza.

Minden felhasználói és rendszerszintű jelszó meg kell feleljen a következő pontban közölt előírásoknak.

2.3.5. A JELSZÓKÉSZÍTÉS ÁLTALÁNOS ALAPELVEI

A *Granite Systems* vállalatnál számos különböző célra használunk jelszavakat. Leggyakoribb alkalmazásuk a felhasználói szintű témaszámok, webes témaszámok, e-levél-postafiókok, képernyővédő, hangüzenetek és helyi útválasztó-belépések védelme. Mivel nagyon kevés rendszer támogatja az egyszeri zsetonok (*token*) – vagyis egyszer használatos dinamikus jelszavak – használatát, így mindenkinél elő kell tudni állítani minél nehezebben feltörhető, úgynevezett erős jelszavakat.

A gyenge, könnyen feltörhető jelszavakra az alábbiak egyike (vagy köztük több) jellemző:

- A jelszó nyolc karakternél kevesebbet tartalmaz.
- A jelszó egy (angol vagy más nyelvű) szótárban található szóval meggyezik.
- A jelszó például az alábbi gyakran használt kifejezések közül kerül ki:
 - családtagok, háziállatok, barátok, munkatársak, filmbeli szereplők stb. neve,
 - számítógépes fogalmak és nevek, parancsok, társaságok, hardver vagy szoftver neve,
 - a vállalat, vagy tevékenységének, üzletágának neve,
 - születésnapok vagy más személyi információk, például telefonszámok, címek,
 - betű- vagy számjegyminták, mint például aaabbb, qwert, xcvbnm, 123321 és hasonlók,



- a fenti példák bármelyike visszafelé betűzve,
- a fentiek bármelyike egy számjeggyel megelőzve vagy kiegészítve (például titok2, vagy 4titok),
- sportegyesületek, sportolók, egyéb ismert személyiségek neve.

A 10. fejezetben (kereskedelmi eszközök) még beszélünk a szólistárkról és szótárákról, azonban a jelszavak kapcsán itt is érdemes szóba hozni ezeket. A szólista, amint neve is mutatja, egyszerűen a szavak egy adott listája. Ezek a szavak származhatnak szótárból, állhatnak sportegyesületek neveiből, iparágazati fogalmakból, szleng szavakból, nevekből, egyebekből. Számos ilyen lista (sok különböző nyelven!) található az interneten, egyik remek élő forrás a <http://wordlist.sourceforge.net>.

A kalózok is ilyen listák segítségével hajtanak végre támadásokat, azt remélve, hogy valakinek a jelszava a listában szereplő szóból származik. A nagyobb hatékonyság érdekében még számjegyeket is beszúrnak a szavakba. A szabályzat előző pontjára azért van szükség, hogy a jelszavak a kalózok ezen tevékenységétől védve legyenek.

Az erős jelszavakra az alábbiak (illetve közülük egyszerre minél több) jellemzők:

- kis- és nagybetűket (a-z, A-Z) egyaránt tartalmaznak,
- számjegyeket (0-9) és írásjeleket (- *.:>,:?;#&@(){}[]~””+!%/=) is tartalmaznak a betűk mellett,
- legalább nyolc karakter hosszúságúak,
- nem hasonlítanak egyetlen nyelv szavára, tájszavára sem, nem részei egyetlen zsargonnak, argónak stb.,
- semmilyen személyes információhoz, családtag nevéhez stb. nem köthetők.

A jelszavakat soha nem szabad leírni vagy elektronikusan (olvasható formában) tárolni. Törekedni kell a könnyen megjegyezhető jelszavak készítésére. Egy módszer lehet például a jelszót egy dal címéhez, szövegéhez vagy más, könnyen fejben tartható fogalomhoz hozzákötni. Tegyük fel például, hogy a választott szöveg „egyszer a nap úgy elfáradt, elaludt mély, zöld tó ölén” – az ebből készült jelszó pedig: „1xaNÚe,emZTö”, esetleg „1xanÚGYef,elMÉZtö”, vagy valami ehhez hasonló. Nem feltétlenül kell ragaszkodni a szavak kezdőbetűihez sem, a lényeg csupán az, hogy könnyen megjegyezhessük.



Soha ne használjuk az itt megadott példák egyikét sem, mivel valaki felveheti azokat a saját szólistájára, és így nem biztonságos!!!

2.3.6. JELSZÓVÉDELMI SZABÁLYOK

Soha ne használja a *Granite Systems* rendszereiben érvényes bármelyik jelszavát egyetlen más, nem a *Granite Systems* vállalatnál lévő (például otthoni internetszolgáltatónál lévő, valamilyen védett weboldalakhoz kiválasztott stb.) hozzáférési jelszavaként sem. Amennyiben lehetséges, a *Granite Systems* vállalaton belül se használja ugyanazt a jelszót két vagy több rendszerbeli azonosítására. Például válasszon egy adott jelszót az e-levelezéshez és egy másikat a webes felületen történő belépéshez. A Windows tartományi jelszava és a UNIX-rendszerbeli jelszava szintén legyen különböző.

A *Granite Systems* vállalatnál használt egyetlen jelszavát se adja meg senkinek, beleértve az adminisztratív munkatársait vagy a titkárњjét is. minden jelszót érzékeny, biztonságos *Granite Systems* belső információként kell kezelni.

Az alábbiakban felsoroljuk a tiltott tevékenységeket:

- telefonon keresztül soha ne árulja el a jelszavát senkinek,
- soha ne árulja el a jelszavát e-levélben,
- soha ne árulja el a jelszavát a főnökének,
- soha ne beszéljen a jelszaváról mások előtt,
- soha ne áruljon el a jelszóval kapcsolatos adatokat, mintákat (például „nagyon hasonlít a családnevemhez”),
- soha ne írja le a jelszavát a kérdőívekre vagy a biztonsági űrlapokra sem,
- soha ne árulja el a jelszavát még a családtagjainak sem,
- soha ne adja meg a jelszavát a munkatársainak, még akkor sem, ha szabadságra indul.

Amennyiben valaki meg akarja tudni az Ön jelszavát, hivatkozzon erre a szabályzatra, és szólítsa fel az illetőt arra, hogy vegye fel a kapcsolatot a vállalati biztonsági csoporttal.

Ne használja a „jelszó megjegyzése” lehetőséget egyetlen alkalmazásnál sem (például Netscape, Outlook, Eudora).

Ismételten jegyezze meg, hogy soha ne írja le a jelszavát és soha ne tárolja azt a hivatalában. Ne tárolja a titkosítatlan jelszavakat egyetlen számítógépen sem, beleértve a kézi gépeket (*palmtop*) és más hasonló eszközöket is. Titkosított jelszavak is csak a *vállalati biztonsági csoport* által jóváhagyott módszerrel kódolva tárolhatók.

Legalább hathavonta változtassa meg a jelszavát (kivéve a rendszer-szintű jelszavakat, amelyeket negyedévente kötelező megváltoztatni). A jelszóváltás ajánlott gyakorisága azonban négy hónap.

Ha egy témaszámáról vagy jelszóról azt gyanítjuk, hogy feltörték, a gyánukat azonnal jelentsük a *vállalati biztonsági csoportnak*, és azonnal változtassuk meg a jelszót.

Jelszótörő vagy jelszófelfedő programok rendszeres vagy véletlenszerű használatára a *vállalati biztonsági csoport* vagy képviselője jogosult. Amennyiben ezen ellenőrzés során egy jelszót sikerül felfedni, a jelszó tulajdonosát fel kell szólítani az azonnali jelszóváltásra.

2.3.7. BÜNTETÉSEK

A jelen szabályzat bármely pontját megsértő munkavállalóval szemben fegyelmi eljárás indítható, melynek kimenetele akár azonnali elbocsátásra is vezethet.

2.3.8. KÖVETKEZTETÉSEK

Minden biztonsági házirendnek néhány közös elemmel kell befejeződni. Ezek tisztázzák a potenciális félreértelmezéseket és a felhasználó értelmezési nehézségeit, hogy végül megérthesse, pontosan mit szabad és mit nem.

- Büntetések** – A legfontosabb elem a szabályzat megszegése esetén a munkavállalót terhelő következmények és büntetések ismertetése.
- Meghatározások** – Nem minden felhasználó vagy alkalmazott képes a szabályzatban használt terminológia pontos megértésére, ezért komoly haszonnal jár, és elkerülhetők a téves értelmezések és félreértelek, ha a lehetőség szerint iparspecifikus fogalmak használatával pontosan meghatározzuk a használt kifejezéseket.
- Változásjegyzék** – A szabályzatok bármikor megváltozhatnak. A változások forrása idővel megváltozhat. Okai között szerepelhet a vezetőség megváltozása, új törvények életbe lépése vagy régebbi törvények pontosítása, a hálózatunk biztonsága ellen irányuló új fenyegetések megjelenése, a vállalat döntése, hogy minőségbiztosítási vagy egyéb tanúsítványt szerez,

vagy csak egyszerűen egy olyan új technológiát fejlesztett ki, amelyet szintén szabályozni kell. A változás tényét viszont tanácsos dokumentálni.

A felhasználók állandóan meg fogják kísérelni a jelszószabályzatban lefektetett korlátozások könnyítését – senki sem szereti időről időre újra megtanulni az ilyen szabályzat által rákényszerített erős jelszavait. Amennyiben a felhasználó mégis képes megjegyezni egy olyan jelszót, amely megfelel ezeknek az alapelveknek, akkor sincs miért aggódni – hamarosan azt is meg kell változtatnia!

A felhasználók szerencsétlenségére ismerniük és követniük kell ezt a szabályzatot. Ne feledjük, a jelszavak biztonsága a hálózat védelmére tett legelső helyes lépés. Ennek megfelelően a felhasználókkal szembeni helyes elvárások megfogalmazása nagymértékben hozzásegíthet minket a szervezetünk általános biztonságának megőrzéséhez.

A következő részben a virtuális magánhálózatok (VPN) biztonsági szabályzatát vizsgáljuk meg, kitérve arra is, hogy mire kell ügyelnünk a megfogalmazása során.

2.4. A VIRTUÁLIS MAGÁNHÁLÓZAT (VPN) BIZTONSÁGI SZABÁLYZATA

A 7. fejezetben részletesen is foglalkozunk a virtuális magánhálózat (*VPN – Virtual Private Network*) biztonsági kérdéseivel. A szabályzatokkal azonban ez a fejezet foglalkozik, a virtuális magánhálózatokat pedig egyre többen használják, így az erre vonatkozó szabályzatra is kell mutatnunk egy példát. mindenekelőtt azonban röviden áttekintjük, pontosan mit is jelent a virtuális magánhálózat. Részletesebb információk a 7. fejezetben találhatók.

A VPN egyre népszerűbbé és egyre érettebbé vált az elmúlt néhány évben. Számos vállalat használja ezeket a távoli kisebb irodák vagy különböző felhasználóik távoli csatlakoztatására. A kapcsolat az IPSec (*IP Security – IP biztonság*) vagy az L2TP (*Layer Two Tunneling Protocol – második szintű alagútprotokoll*) technikák használata miatt tekinthető biztonságosnak, és a nagy sebességű internetkapcsolati lehetőségek, mint például a DSL vagy a kábeles összeköttetés miatt egyre elfogadhatóbb alternatívát jelent a teljesítmény szempontjából is. Éppen ezért egyre fontosabbá válik, hogy a rajta keresztül zajló forgalom kellő biztonsága érdekében kidolgozzuk a használatukat szabályozó házirendet.

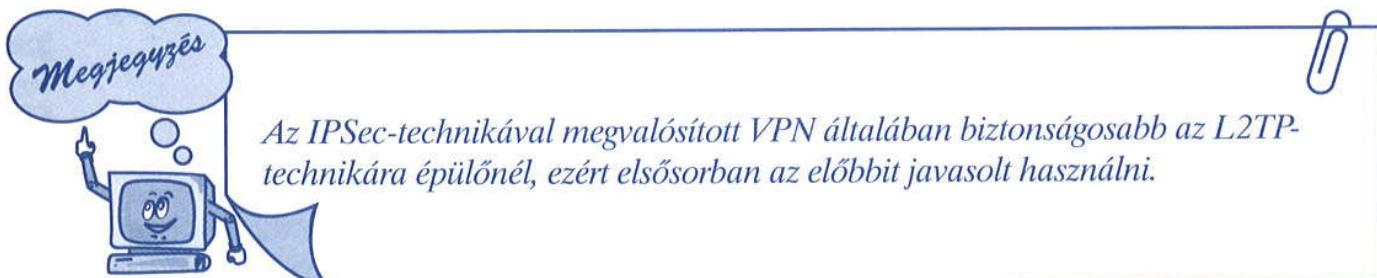
A SANS (<http://www.sans.org>) a honlapján ingyenesen elérhetővé teszi a biztonsági házirendek egész seregét. A most ismertetésre kerülő is ezekre épül. A honlap meglátogatása és az itt leírt megjegyzések együtte-

sen segíthetnek a saját ötletek kidolgozásában. A *Granite Systems* (<http://www.granitesystems.net>) a SANS ajánlásaira alapozta a saját házirendjét, és hozzájárult ahhoz, hogy itt nyilvánosságra hozzuk.

Ebben a szabályzatban a cég IT-biztonsági részlegét egyszerűen *vállalati biztonsági csoport* néven emlegetjük. Maga a *Granite Systems*, és minden egyes vállalatspecifikus részlege dőlt betűvel található a házirendben. Ha valaki egyébként változtatás nélkül akarná felhasználni ezt a szabályzatot, akkor elegendő ezeket kicserélnie a megfelelő nevekre.

2.4.1. CÉLKITŰZÉS

Jelen szabályzat célja a *Granite Systems* vállalat hálózatához az IPSec vagy L2TP segítségével csatlakozó virtuális magánhálózat (VPN) összeköttetésekkel kapcsolatos biztonsági előírások összefoglalása.



Az IPSec-technikával megvalósított VPN általában biztonságosabb az L2TP-technikára épülőnél, ezért elsősorban az előbbit javasolt használni.

2.4.2. HATÁLYOSSÁG

Jelen házirend hatálya kiterjed a *Granite Systems* vállalat valamennyi olyan alkalmazottjára, szerződéses munkatársára, konzultánsára, időszaki és egyéb munkatársára (beleértve a más cégek által alkalmazottakat is), akiknek a *Granite Systems* vállalat hálózatához VPN-hozzáférésük van. A hatálya kiterjed minden VPN-koncentrátoron vagy VPN-re alkalmas tűzfalon keresztül megvalósított VPN-implementációra.

2.4.3. ÁLTALÁNOS SZABÁLYOK

A *Granite Systems* vállalat engedéllyel rendelkező munkavállalói és partnerei használhatják ki a VPN előnyeit. Maga a VPN egy felhasználó által kezelt szolgáltatás. Ez azt jelenti, hogy a felhasználó felelősségi körébe tartozik egy internetszolgáltató (*ISP – internet service provider*) kiválasztása, valamint a szükséges szoftverek beszerzése és telepítése, valamint az ezzel kapcsolatos díjak fizetése.



Jóllehet egyes vállalatok átvállalják a munkavállalóiktól a behívó vagy a kábel-s internetszolgáltatás díjának kifizetését, ez azonban esetére különbözik. A legtöbb vállalat a munkavállalókra hagyja ezek fizetését, s így ezt a tényt is rögzítenie kell a vállalati biztonsági politikában.

Továbbá:

1. A VPN-hozzáféréssel rendelkező felhasználók felelőssége annak biztosítása, hogy illetéktelenek a VPN segítségével ne férhessenek hozzá a vállalat belső hálózatához.
2. A VPN-hozzáférést vagy egy alkalomra szóló jelszavas hitelesítéssel (például zsetoneszköz), vagy erős kulccsal alkotott kétkulcsú (nyílt/privát) titkosító rendszerrel kell védeni.
3. A vállalat hálózatához csatlakozó VPN az aktív működése idején az adott számítógép adatforgalmát a VPN-csatornán keresztül küldi, minden más forgalmat eldob.
4. A kettős (megosztott) csatlakozás tilos, kizárálag egy hálózati csatlakozás engedélyezett.
5. A megosztott csatlakozás egyike a VPN kétállapotú (be- vagy kikapcsolt) konfigurációs lehetőségeinek. Tulajdonképpen azt jelenti, hogy bekapcsolt állapotában a felhasználók egyidejűleg csatlakozhatnak a vállalat hálózatához és az internethez. Ez viszont a vállalati hálózat biztonságára nézve veszélyt jelent, mivel az adott kapcsolatot fenntartó géphez hozzáférést szerzett támadó a VPN-en keresztül a teljes vállalati hálózathoz is hozzáfér. Ennek megfelelően az ajánlott gyakorlat a megosztott csatlakozási lehetőség kikapcsolása.
6. A VPN-koncentrátorok felállítása és menedzselése a *Granite Systems* hálózatüzemeltető csoportjának a feladata.
7. A *Granite Systems* belső hálózataihoz VPN vagy más technológia segítségével csatlakozó valamennyi számítógépen a vállalat szabályzataiban meghatározott (és a vállalat belső hálózatán letölthető) egyik vírusvédelmi szoftver legfrissebb változatát kötelező használni. Ez a szabály a személyi tulajdonú gépekre is vonatkozik.
8. A VPN-felhasználóknak a *Granite Systems* hálózatával fenntartott kapcsolata automatikusan bont 30 percnyi télenség után. A felhasználónak ezután újra kell csatlakoznia és bejelentkeznie. A pingötés és más mesterséges hálózati technikák használata a csatlakozás életben tartására nem megengedett.

9. A nem a *Granite Systems* által birtokolt eszközök felhasználói a saját rendezéseiket a vállalat hálózatbiztonsági és VPN-szabályzatának megfelelően kell beállítaniuk.
10. Kizárolag a *vállalati biztonsági csoport* által elfogadott VPN-kliensszoftverek használhatók.
11. A VPN-technológia saját eszközökkel történő használata esetén a felhasználóknak tudomásul kell venniük azt, hogy a saját gépeik a *Granite Systems* hálózatához tartozókká válnak, így azokra is a vállalati eszközökkel pontosan megegyező szabályok és előírások vonatkoznak. Ez azt jelenti, hogy saját gépeiket a vállalati biztonsági szabályzatoknak megfelelően kell konfigurálniuk.

2.4.4. KÖVETKEZTETÉSEK

Minden biztonsági házirendnek néhány közös elemmel kell befejeződni. Ezek tisztázzák a potenciális félreértelmezéseket és a felhasználó értelmezési nehézségeit, hogy végül megérthesse, pontosan mit szabad és mit nem.

- 1. Büntetések** – A legfontosabb elem a szabályzat megszegése esetén a munkavállalót terhelő következmények és büntetések ismertetése.
- 2. Meghatározások** – Nem minden felhasználó vagy alkalmazott képes a szabályzatban használt terminológia pontos megértésére, ezért komoly haszonnal jár, és elkerülhetők a téves értelmezések és félreértések, ha lehetőleg iparspecifikus fogalmakkal pontosan meghatározzuk a használt kifejezéseket.
- 3. Változásjegyzék** – A szabályzatok bármikor megváltozhatnak. A változások forrása idővel megváltozhat. Okai között szerepelhet a vezetőség megváltozása, új törvények életbe lépése vagy régebbi törvények pontosítása, a hálózatunk biztonsága ellen irányuló új fenyegetések megjelenése, a vállalat döntése, hogy minőségbiztosítási vagy egyéb tanúsítványt szerez, vagy csak egyszerűen egy olyan új technológiát fejlesztett ki, amelyet szintén szabályozni kell. A változás tényét viszont tanácsos dokumentálni.

A VPN-technológia egyike a jelenleg leggyorsabban fejlődő területeknél. Amint arról már volt szó, a vállalatok egyre növekvő számban alkalmazzák, ezért alapvető fontosságú a használatukat szabályozó házirendekek elkészítése. Mind gazdasági, mind biztonsági szempontból meglehetősen sokba kerülhet, ha a VPN kapcsán hibát követünk el.

A következőkben ismertetendő házirendet akkor kell alkalmazni, ha a vállalatunk hálózatához üzleti partnereink és más harmadik fél csatlakozására is szükség van – ez ugyanis meglehetősen érzékeny terület.

2.5. AZ EXTRANET CSATLAKOZÁS HÁZIRENDJE

Jelen szabályzat a nem a vállalatunk által alkalmazottak számára adja meg a „miként kezeljük” kérdésre a választ, illetve rögzíti a követelményeket ahhoz, hogy elérhessék hálózati erőforrásainkat, egyáltalán, hogy csatlakozhassanak a hálózatunkhoz. A „kik” és a „miértek” az ilyen igények esetén meglehetősen tág határok között mozoghatnak. Ezen igények felmerülése esetén az 1. fejezetben a bizalomról írottakat érdemes a döntés meghozatala előtt átutanulmányozni. Ilyen igennel általában a következő felek jelentkeznek:

- a vállalatunk számára munkát végző szerződéses partnerek,
- különböző üzleti partnerek,
- az általában nagy és különleges kezelést igénylő vásárlóink.

Az itt bemutatott házirend az ilyen igények megválasztásához szükséges előírásokat, valamint az igénylő által betartandó követelményeket rögzíti. Ugyancsak lehetővé teszi az IT-személyzet számára a követelődző és rámenős emberek kezelését. Ez a szabályzat tehát egyfajta virtuális csodaszernek tekinthető.

A SANS (<http://www.sans.org>) a honlapján ingyenesen elérhetővé teszi a biztonsági házirendekek egész seregét. A most ismertetésre kerülő is ezekre a nyilvánosan elérhető házirendekre épül. A honlap meglátogatása és az itt található megjegyzések együttesen segíthetnek a saját ötletek kidolgozásában. A *Granite Systems* (<http://www.granitesystems.net>) a SANS ajánlásaira alapozta a saját házirendjét, és hozzájárult ahhoz, hogy itt nyilvánosságra hozzuk.

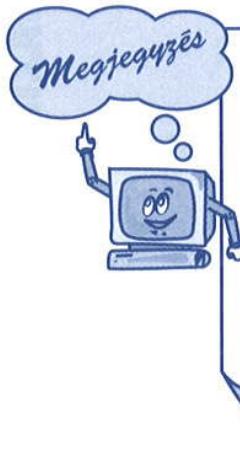
Ebben a szabályzatban a cég IT-biztonsági részlegét egyszerűen *vállalati biztonsági csoport* néven emlegetjük. Maga a *Granite Systems*, és minden egyes vállalatspecifikus részlege dőlt betűvel található a házirendben. Ha valaki egyébként változtatás nélkül akarná felhasználni ezt a szabályzatot, akkor elegendő ezeket kicserélnie a megfelelő nevekre.

2.5.1. CÉLKITŰZÉS

Jelen házirend írja le azokat a szabályokat, amelyek alapján más, a *Granite Systems* vállalattal üzleti kapcsolatban álló vállalatok vagy a konzultánsok az üzleti tevékenység végrehajtása érdekében hozzákapcsolódhatnak a vállalat hálózatához.

2.5.2. HATÁLYOSSÁG

Ez a házirend szabályozza a *Granite Systems* vállalat nem nyilvános hálózatához való hozzáférést igénylő harmadik fél tevékenységét, függetlenül attól, hogy dedikált telekommunikációs vonalat (például ISDN), közvetlen hálózati vonalat vagy VPN-technológiát használ-e a csatlakozáshoz. A vállalat számára internetszolgáltatást nyújtó harmadik félhez (internetszolgáltatóhoz), vagy a nyilvános telefonhálózathoz való csatlakozást jelen házirend *nem* szabályozza.



Az utolsó mondathoz némi magyarázat szükséges, miért is kell a szabályzatnak kivételt tennie a vállalat internetelérését és telefon-összeköttetését lehetővé tevő vállalatokkal szemben. A kivételre azért van szükség, mert ezek a cégek a vállalat által megvásárolt szolgáltatást nyújtják. Ha a vállalat arra kötelezné őket, hogy a szolgáltatás nyújtása érdekében kövessék ezt a szabályzatot, akkor aligha sikerülne valaha is hozzájutni ezekhez a szolgáltatásokhoz.

2.5.3. BIZTONSÁGI ÁTVIZSGÁLÁS

Minden új extranet csatlakozási kérést a vállalati biztonsági csoport biztonsági átvizsgálásnak vet alá, amely biztosítja, hogy valamennyi hozzáférés a lehetséges legjobb módon illeszkedjen az üzleti követelményekhez, valamint hogy a legszűkebb hozzáférés alapelveit követi.

2.5.4. A MÁSIK FÉL CSATLAKOZÁSI SZERZŐDÉSE

A *Granite Systems* és más felek között minden új csatlakozási kérés teljesítéséhez arra van szükség, hogy a *Granite Systems* és a másik fél képviselői aláírják a csatlakozási szerződést. Az aláírók egyike a vállalat költségviselő szervezeti egységének alelnöke, a másik fél részéről pedig az adott fél törvényes képviseletére felhatalmazott személy kell legyen. Az aláírt szerződést a vállalat jogi osztályán is, és a vállalati biztonsági csoportnál is irattárazni kell.

2.5.5. ÜZLETI ÉRDEK

Minden üzemelő extranet csatlakozáshoz társulnia kell a valódi üzleti indoklásnak. Ezt írásban kell elkészíteni, és a *vállalat biztonsági igazgatójának* jóvá kell hagynia. Ebben az indoklásban pontosan fel kell sorolni azokat a hálózati erőforrásokat, amelyek elérését igénylik.

2.5.6. KAPCSOLATTARTÁSI PONT

A *Granite Systems gazdasági osztályának* kötelessége kijelölni azt a személyt, aki az adott extranet kapcsolattal összefüggő ügyekben tartja a kapcsolatot a másik féllel. A kapcsolattartó a *gazdasági osztály* nevében jár el és felel a jelen szabályzat és a másik féllel kötött csatlakozási szerződés azon pontjaiért, amelyek a hatáskörébe tartoznak. Amennyiben a kapcsolattartó személye megváltozik, az érintett másik felet erről azonnal értesíteni kell.

2.5.7. A CSATLAKOZÁS LÉTREHOZÁSA

A *Granite Systems* vállalat másik fél számára kiépítendő csatlakozást létrehozni kívánó *költségviselő szervezeti egységei* az új kapcsolat iránti kérelmüköt a *vállalati biztonsági csoportnak* nyújtják be. A szervezeti egység vállalja a *biztonsági csoport* felé, hogy a projekt eredendő biztonsági kérdéseit kezeli. Igény esetén teljes és maradéktalan információt kell szolgáltatnia a kért kapcsolat természetét illetően.

Minden jóváhagyott kapcsolatot a legkisebb hozzáférés elve alapján kell létesíteni, összhangban a jóváhagyott üzleti követelményekkel és a biztonsági átvizsgálással. Semmi esetre sem ruházható át a *Granite Systems* hálózatának vagy erőforrásainak védelme a másik félre.

2.5.8. A HOZZÁFÉRÉS ÉS A CSATLAKOZÁS MÓDOSÍTÁSA

A hozzáférés megváltoztatására irányuló minden kéréshez csatolni kell az érvényes üzleti indoklást, s valamennyi ilyen kérést biztonsági ellenőrzésnek kell alávetni. A változásokat vállalati változáskezelési folyamat-ként kell megvalósítani. A *költségviselő szervezeti egység* felelőssége a *vállalati biztonsági csoport* értesítése minden olyan esetben, amikor az eredetileg átadott információk biztonsági és csatlakozási téma-köröket érintő része módosul.

2.5.9. A HOZZÁFÉRÉS VISSZAVONÁSA

Ha nincs már többé szükség a hozzáférésre, a *Granite Systems* vállalaton belüli költségviselő szervezeti egységének értesítenie kell a kapcsolatért felelős extranetcsoportot, s ezzel a hozzáférés megszűnik. Ez jelenthet a meglévő jogosultságok módosításától kezdve egészen a kiépített vonal lebontásáig bármit. A *vállalati biztonsági csoportnak* évente felül kell vizsgálnia valamennyi létező kapcsolatát, így biztosítva egyrészt azt, hogy mindegyikre ténylegesen szükség van, másrészt azt, hogy a hozzáférés az igényeknek megfelel. A szükségtelen és a *Granite Systems* vállalat üzleti érdekeihez már nem szükséges kapcsolatok azonnal felszámolódnak. Amennyiben egy biztonsági incidens vagy a felülvizsgálat eredménye azt mutatja, hogy a kapcsolat már nem él, és a vállalat üzleti érdekeihez nincs rá szükség, s így a kapcsolat felszámolására vagy a megadott jogosultságok megváltoztatására van szükség, a *vállalati biztonsági csoport* bármilyen további intézkedés előtt értesíti a kapcsolattartó személyt, vagy a költségviselő szervezetet.

2.5.10. KÖVETKEZTETÉSEK

Minden biztonsági házirendnek néhány közös elemmel kell befejeződni. Ezek tisztázzák a potenciális félreértelemezéseket és a felhasználó értelmezési nehézségeit, hogy végül megérthesse, pontosan mit szabad és mit nem.

- Büntetések** – A legfontosabb elem a szabályzat megszegése esetén a munkavállalót terhelő következmények és büntetések ismertetése.
- Meghatározások** – Nem minden felhasználó vagy alkalmazott képes a szabályzatban használt terminológia pontos megértésére, ezért komoly haszonnal jár, és elkerülhetők a téves értelmezések és félreértesek, ha lehetőleg iparspecifikus fogalmak használatával pontosan meghatározzuk a használt kifejezéseket.
- Változásjegyzék** – A szabályzatok bármikor megváltozhatnak. A változások forrása idővel megváltohat. Okai között szerepelhet a vezetőség megváltozása, új törvények életbe lépése vagy régebbi törvények pontosítása, a hálózatunk biztonsága ellen irányuló új fenyegetések megjelenése, a vállalat döntése, hogy minőségbiztosítási vagy egyéb tanúsítványt szerez, vagy csak egyszerűen egy olyan új technológiát fejlesztett ki, amelyet szintén szabályozni kell. A változás tényét viszont tanácsos dokumentálni.

Mindig kényes kérdés marad a vállalaton kívüli személyek hozzáférési jogának engedélyezése. Megtörténhet, hogy az X munkatárs üzleti ügyben Y partnerrel dolgozik, akinek valamelyik hálózati erőforrás elérésére

lenne szüksége, mire X megígéri azt neki. Ennek alternatívájaként valaki a vezetőségből is tehet ilyen ígéretet.

Ezek viszonylag gyakori lehetőségek, és ez a szabályzat igyekszik azt biztosítani, hogy amennyiben felmerülne ilyen igény, akkor a szabályzat értelmében még az ígéret tényleges megadása előtt az egyébként helyénvaló megfelelő gondossággal néhány lépést megtegyünk.

Valószínűleg a leggyorsabban növekvő hitelesítő hatóság a Nemzetközi Szabványügyi Szervezet (*ISO – International Standards Organization*). A következő részben röviden összefoglaljuk, hogy az ISO miként lépett a biztonság porondjára. Azért érdemes erre emlékezni, mert valamilyen szinten egyre több vállalat válik ISO-minősítetté.

2.6. Az ISO-MINŐSÍTÉS ÉS A BIZTONSÁG

Egy nemzetközileg elfogadott szabványnak való megfelelés egyre fontosabbá válik. Ennek eredményeként, s mivel a szabványhoz tartozás az azonnali elfogadottság elterjedt záloga, számos vállalat követi ezt az utat. Az ISO számos szabványt kínál, melyek a maguk helyén kivétel nélkül fontosak. Könyünk témaja szempontjából elsősorban az ISO 17799 szabvány fontos.

Ez a szabvány rendkívül aprólékosan kitér a biztonsággal kapcsolatos valamennyi kérdésre, s jelentős számú ellenőrzési pontot tartalmaz, amelyek kilenc fő csoportba tartoznak.

- **Üzleti folytonossági terv** – Súlyos hiba vagy katasztrófa esetére meghatározza, hogy miként folytatható az üzleti működés.
- **Rendszerhozzáférés ellenőrzése** – A vállalaton belüli különböző típusú információkhoz való hozzáférés ellenőrzését vázolja fel. Még fontosabb, hogy felvázolja az illetéktelen cselekmények felfedhetőségéhez szükséges szabályokat is.
- **Rendszerfejlesztés és -karbantartás** – A vagyon védelmével kapcsolatos folyamatokat fedi le, a vállalat IT-rendszerivel, szoftvereivel és adataival kapcsolatos valamennyi témakörbe beágyazva a biztonságot.
- **Fizikai és környezeti biztonság** – Biztosítja a jogosulatlan hozzáférés vagy károkozás megelőzését, függetlenül attól, milyen szándékkal is következzenek azok be.
- **Megfelelőség** – Lehetővé teszi a vállalat számára annak biztos tudatát (ellenőrzések segítségével), hogy nem sért meg egyetlen polgári törvényt, rendeletet, szabályozást vagy szerződéses kötelezettséget sem, egyidejűleg tájékoztatva is a vonatkozó biztonsági követelményekről.
- **Személyi biztonság** – Az emberi tévedésből, lopásból és visszaélésből eredő kockázat csökkentését taglalja, lehetővé téve így a biztonsági in-

cidensekből és meghibásodásokból eredő károk minimalizálását, valamint az ilyen eseményekből való tapasztalatszerzést.

- **Biztonsági szervezet** – Kifejti, miként kell a vállalaton belül létrehozni és fenntartani az információ biztonságát.
- **Számítógép- és műveletkezelés** – Részletezi, miként lehet minimalizálni a kockázatot és egyidejűleg megnövelni a biztonságot az elkallódás, módosítás és visszaélés megelőzéséhez szükséges információvédelem biztosításával.
- **Vagyonbesorolás és ellenőrzés** – Leírja, miként kell fenntartani a vállalati vagyon megfelelő védelmét, biztosítva egyúttal, hogy az adat- és információvagyon is megfelelő védelmet kapjon.

Az ISO-tanúsítványt csak érintőlegesen tárgyaltuk, maga a szabvány azonban talán egyike a legrészletesebbeknek, amely a használat során még kiegészül. Amennyiben több információra lenne szükség, érdemes meglátogatni az ISO honlapját a <http://www.iso.org> webcímén.

Amikor a biztonsági szabályzatokat el akarjuk juttatni a felhasználókhoz, meg kell határoznunk a lehető leghatékonyabb módszert. Így egyrészt megkönnyítjük az elfogadását, másrészt a felhasználóktól még támogatást is kaphatunk a törekvéseinkhez. Ezt viszont sajnos gyakran könnyebb mondani, mint valóban megtenni.

A biztonsági szabályzatok számos elve és célja a közzététel során könnyen elhomályosulhat. Alapvető fontosságú azonban, hogy mindenki megértse, sőt támogassa ezeket a szabályzatokat. Amennyiben ezt a célt nem sikerülne elérni, minden erőfeszítésünk hiábavaló, a szabályzatokat kárhozatra ítéljük, amennyiben a felhasználók ellenállása miatt meghiúsul a betartásuk, mivel ők már a kezdetektől ellenezték azt.

Az ilyen helyzetek kezelése a személyek közötti kapcsolatok kezeléséhez hasonlatos. Az emberek megfelelő kezelésén túl még az alábbi tanácsokat érdemes megfogadni:

- biztosítsuk, hogy valamennyi szabályzatot ismertetjük az új munkavállalók tájékoztatásakor,
- mindig tegyük lehetővé, hogy a biztonsági szabályzat által érintett személyek tipikus képviselője áttanulmányozhassa és jegyzetekkel ellátva visszajuttassa azt, mielőtt megkísérelnék a bevezetését,
- tartsunk rendszeresen biztonsági szabályzattal kapcsolatos felfrissítő megbeszéléseket.

Általánosságban azt javasolhatjuk, hogy a biztonsági szabályzatok rövidek legyenek, ne haladják meg a kétoldalnyi terjedelmet. Nincs szükség a helyzet szükségtelen bonyolítására. Időnként szükség lehet a terjedelem

HÁLÓZATI BIZTONSÁG

túllépésére, de semmiképpen sem rendszeresen. Végezetül, biztosítsuk azt is, hogy a szabályzatok évente (vagy akár gyakrabban) frissülhessenek, tükrözve az elmúlt időszak tapasztalatait.

2.7. Példák biztonsági szabályzatokra az interneten

Az itt ismertetett valamennyi szabályzat a vállalati követelmények teljesítésének csupán egy (s nem is tökéletes) eszköze. Ami az egyik vállalat esetén működik, nem szükségszerűen a legjobb választás a másiknak. A biztonsági szabályzatokkal kapcsolatban ezért javasolt még az alább sorolt további források elolvasása is:

- http://www.sans.org/rr/catindex.php?cat_id=50 – Ezen az oldalon GIAC tanúsítvánnyal rendelkező szerzők cikkeit és írásait tanulmányozhatjuk.
- <http://www.ietf.org/rfc/rfc2196.txt> – Internet-hozzáféréssel rendelkező hálózatok számára készült számítógép-biztonsági szabályzatok fejlesztési kézikönyve.
- http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf – A szabályzatokkal kapcsolatos gyengeségeket tárgyaló kiadvány.²

Néhány további webhely, ahol biztonsági szabályzatokkal kapcsolatos információk találhatók:

- <http://www.security.kirion.net/securitypolicy>
- <http://www.network-and-it-security-policies.com>
- http://www.brown.edu/Research/UNIX_Admin/cuisp/
- <http://iatservices.missouri.edu/security>
- http://www.utoronto.ca/security/documentation/policies/policy_index.htm
- http://irm.cit.nih.gov/security/sec_policy.html
- <http://w3.arizona.edu/~security/pandp.htm>
- <http://secinf.net/ipsecc.html>
- <http://ist-socrates.berkeley.edu:2002/pols.html>
- http://www.ruskwig.com/security_policies.htm

² A biztonsággal kapcsolatos egyik legnagyobb probléma éppen az, hogy felelőse tökéletesen megbízik egy általa implementált megoldásban. A teljes biztonságot soha nem lehet tökéletesen elérni, legfeljebb némi legközelíteni egy folyamatos cselekvéssor során. A kellően elszánt és felkészült kalóz azonban bármikor képes lehet a biztonsági óvintézkedések kijátszására. A cél ezért valójában nem a kalóztevékenység abszolút megakadályozása, hanem minél nehezebbé tétele kell legyen. A hivatkozott kiadvány elolvasása éppen ezt a szemléletet erősítheti. (A ford. meg.)

2.8. ÖSSZEFoglalás

Ebben a fejezetben a sokak által csupán unalmashoz tartott témáról, a biztonsági politikáról és a szabályzatokról esett szó. Ezek valójában a vállalat biztonságához való hozzáállását tükrözik. Ismertettük a biztonsági szabályzatok megírásával kapcsolatos kulcskérdéseket, például annak meghatározását, hogy kiben és miben lehet megbízni, és kinek a feladata az ilyen szabályzatok megírása és betartatása.

Ebben a fejezetben bemutattunk néhány mintaszabályzatot is. Azokat a területeket igyekeztünk felülni, amelyeken a vállalatoknak általában van még mit csiszolniuk. Ide soroljuk a vállalati IT-erőforrások indokolható használatával, valamint a kellően erős jelszavak megválasztásával kapcsolatos szabályzatokat, a VPN használatának hogyanját és miértjét, végül hogy milyen megszorításokat kell alkalmaznunk a saját hálózatunk és az üzleti partnerek hálózatának összekötésekor.

2.9. Összefoglaló kérdések

1. Mekkora fontossággal bír más szervezetek és munkavállalók bevonása a biztonsági szabályzatok kialakítási munkálataiba?
2. Válaszoljon igennel vagy nemmel a következő kérdésre! Jól ismert tény-e az, hogy a felhasználók a túlságosan erős megszorításokat vezető biztonsági szabályzatokat igyekeznek megkerülni? Indokolja a választ!
3. Mi az az öt legfontosabb tényező, amelyet a biztonsági szabályzatok írása vagy felülvizsgálata során észben kell tartani?
4. Miért kell minden egyes szabályzat részévé tenni a megsértésük esetére alkalmazható büntetések ismertetését is?
5. Milyen jellegű elvárásokat határoz meg az indokolható használati szabályzat a felhasználókkal szemben?
6. Mikor és milyen körülmények között lehet szükség arra, hogy a jelszavunkat másnak eláruljuk?
7. Az alább felsorolt lehetséges jelszavak közül az ismertetett vállalati jelszószabályzati minta szerint melyek minősíthetők kellően erősnek?
 - a) farkascsorda,
 - b) tomi67,
 - c) ferinem12,
 - d) sJ8Dtt&efs,
 - e) 1etlen\$2kedő.
8. Határozza meg, mi az a VPN, és milyen szerepet játszhat a vállalat hálózati infrastruktúrájában!

► HÁLÓZATI BIZTONSÁG •

9. A VPN támogatja a megosztott csatlakozás lehetőségét. Definiálja ezt a technológiát, és magyarázza el, miért használhatja ezt valaki a hálózatban!
10. Milyen gyakorisággal javasolt a biztonsági házirendek frissítése vagy felülvizsgálata?