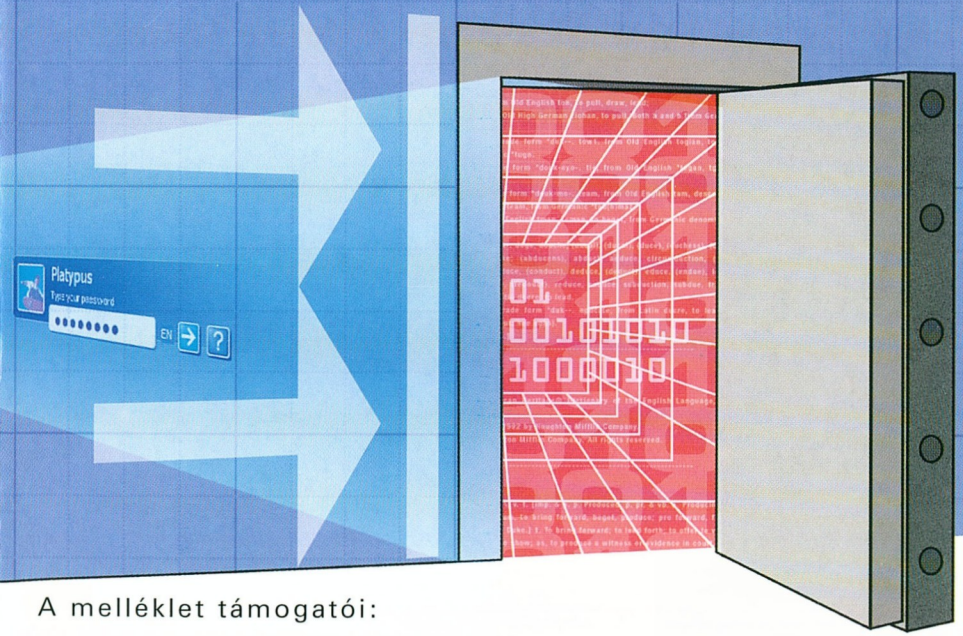
IDG
COMPUTERWORLD
SZÁMÍTÁSTECHNIKA

Komplett adatbiztonság



A melléklet támogatói:

A cél: minden bit a helyén legyen

Az információ-, illetve adatbiztonság témája napjainkban igen felkapott. Távoli szemlélő azt gondolhatná, ez egy újabb marketingfogás, amivel a vásárlókat újabb pénzek elköltésére ösztönözhetik.
Hogy ez nem így van, arról a hírekből nap mint nap értesülhetünk: újabb vírusok bukkannak föl, megváltoztatják egy-egy cég honlapját, ellopnak adatokat.
A világban minden új dolog hasonló lépéseken megy át, amíg a mindennapok eszközévé válik.
Ezen lépések egyike, amikor az eszköz biztonságos használatának mivolta kerül előtérbe. Így volt ez az autókkal is. Először örültek, hogy megy, aztán szépen lassan kidolgoztak egy sor eszközt és szabályt, amelyek kellenek a biztonságos használathoz. A fiatalabbak már nem emlékeznek arra, amikor még nem volt légzsák, biztonsági öv, ABS – de volt idő, amikor még közönséges ablaküveg volt az autókban.
Ugyanez a lépés megtörtént a repülőgépek világában is: az első években aki csak akart, épített egy repülő szerkezetet, amivel aztán vagy tudott repülni, vagy nem. Később sorban jöttek a biztonságot szolgáló eszközök, eljárások, amelyek nélkül ma már elképzelhetetlen a repülés.
Az informatika a fejlődés hasonló stádiumában van: ma már számtalan különféle működő eszközünk van, otthon és nagyvállalatoknál egyaránt. Már többek, mint játékszerek, hiszen működőképességük lényegesen befolyásolja életünket.
Kis mellékletünkben négy cég ismerteti eljárásait, eszközeit, amelyeket betartva, használva informatikai infrastruktúránk magasabb osztályba léphet.
Egyúttal ezen kiadványunk a gerince a 2003. március 19-én megrendezésre kerülő Adatbiztonsági Konferenciánknak is.

Makk Attila

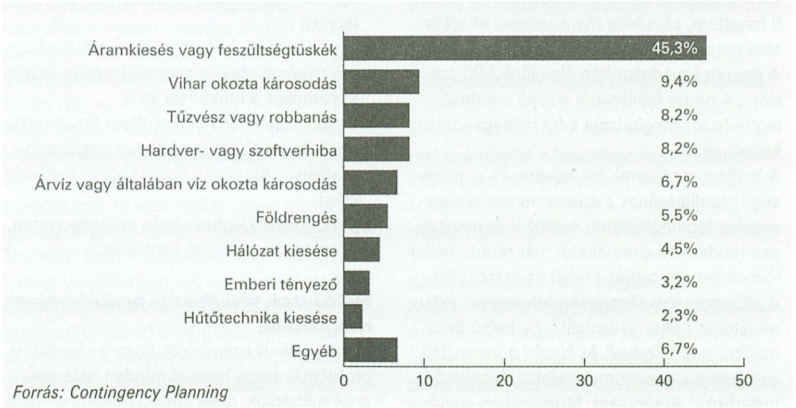
A számítógépekre leselkedő láthatalan veszély

A feszültségvédelem a létfontosságú számítógépek és hálózati rendszerek biztonságos működésének legelső védelmi vonala.

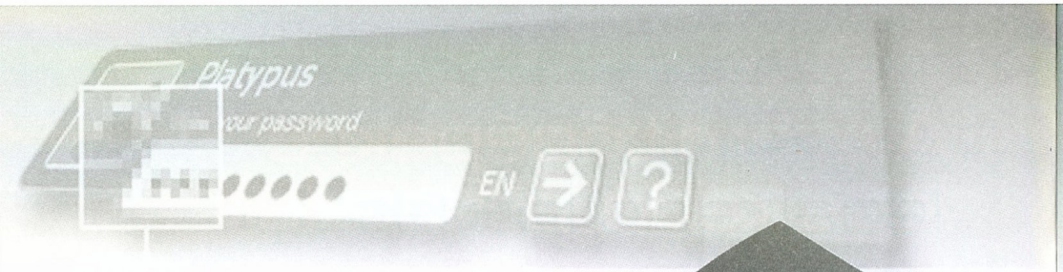
Úgy tartja a mondás, hogy számítógépes hálózatból kétféle van: az egyik fajtában már támadt hiba és adatvesztés feszültségproblémák miatt, a másik fajtában csak ezután fog. Kétségtelen tény, hogy a számítógépes hálózatok akaratlan leállását és adatvesztését leggyakrabban tápellátási problémák okozzák. A Contingency Planning Research szerint a tápellátási zavarokból és feszültségtüskéktől származik az adatvesztések 45,3 százaléka, s persze az adatvesztéshez hardverhiba, állási idő is társul, meg az óhatatlan újraprogramozás. Ma már minden felelősségteljes rendszergazda készít biztonsági másolatot a fontos adatokról, azt azonban még mindig sokan figyelmen kívül hagyják, hogy tápellátás nélkül nem működnek a számítógépek; hiába van mentés, az adatok mégsem érhetők el.

A tápellátási zavarok okozzák az adatvesztések túlnyomó részét.

Milyen hatással van a feszültségingadozás az érzékeny berendezésekre? Egy rövid ideig tartó, pillanatnyi feszültségingadozás is nagy károkat okozhat! Az IBM által készített egyik tanulmány szerint egy átlagos számítógép havonta több mint 120-szor van kitéve feszültségingadozásnak, s ez sokféle hatással járhat, a billentyűzet lefagyásától kezdve a gyenge hardverteljesítményen át egészen a berendezések súlyos károsodásáig és visszaállíthatatlan, sérült állományok létrejöttéig. A rendszergazdák hosszú órákat töltenek a különféle problémák felkutatásával és elhárításával, s azok sokszor végül is nem észlelt tápellátási problémákra vezethetők vissza. Egyre több vállalkozás sikere függ a számítógépektől, emiatt manapság soha nem látott méreteket öltött a feszültségvédelem iránti igény.



Forrás: Contingency Planning



Az elektronika korában tehát két sajátos tényt kell szem előtt tartaniuk a számítógépet használó vállalkozásoknak: egyrészt azt, hogy a fogyasztói energiahálózat nem ad káros ingadozásoktól mentes, az érzékeny számítógépek által megkövetelt egyenletes feszültséget, másrészt azt, hogy végső soron a vásárló felelős a maga eszközeinek biztonságos és hibátlan működéséért. A Gallup Intézet felmérése szerint a megkérdezett vállalatok több mint fele óránkénti 5000 amerikai dollárra vagy még többre becsüli a gépek leállásából eredő költségeket. A feszültségvédelem szükségességét tehát nem nehéz igazolni.
Hálózati környezetben az eszközök sokszor más-más telephelyen működnek, az eddig csupán egyetlen elektromos hálózatot, emeletet, épületet vagy telephelyet érintő áramellátási zavar tehát az egész rendszert károsíthatja. Ha a hálózati gerinc egyetlen kritikus elemében támadt feszültségesés vagy feszültségtüske észrevétlenül megrongál egy érzékeny alkatrészt, akkor megszakadhat a hálózati forgalom, és a hiba megkeresése és elhárítása rengeteg időt vesz el a rendszergazdától. A feszültségvédelemben élen járó APC szerint: „A gépek leállásából adódó veszteség legtöbbször meghaladja a feszültségvédelem költségeit."
A kritikus rendszerek folyamatos és jó minőségű tápellátásának a szünetmentes tápegységek a legmegfelelőbb eszközei. A nagygépes rendszerek üzemeltetői már régóta nélkülözhetetlennek tartják ezeket az eszközöket. A szünetmentes tápegység folyamatos akkumulátoros háttérrel szolgál (egy belső akkumulátor segítségével) és kiszűri a potenciálisan ártalmas elektromos zajokat, feszültséghullámokat és tüskéket. Mostanában egyre több kritikus adat kerül fel a hálózatokra, s a hálózati rendszergazdák felismerték, hogy a szünetmentes tápegységek (UPS) nemcsak a hagyományos nagygépes rendszerekben fontosak, hanem a nagygépes rendszerek szerepét sok helyütt átvevő kiszolgálók, hálózati perifériák (tárolóeszközök, szalagos egységek, koncentrátorok, kapcsolók, útválasztók) és sok PC-s munkaállomás működtetésében is. Ma már könnyebben rászánhatjuk magunkat az UPS vásárlására, hiszen az új modellek minden eddigieknél költséghatékonyabbak, és tulajdonságaik mindenféle környezetben megfelelnek a követelményeknek:

- egyszerű, automatikus („plug-and-play") telepítés;
- a működés közben cserélhető akkumulátorok minimalizálják a szerelési igényt és maximalizálják a működési időt;
- a tápellátás-felügyeleti szoftver figyelmezteti a felhasználókat, ha baj van, vagy automatikusan elmenti a használatban levő adatokat;
- a moduláris kiépítés révén szükség szerint növelhető a tápellátó kapacitás.

Hálózatok tápellátási problémáinak megoldása

Mindig tartsuk szem előtt, hogy a tápellátási problémák káros hatásai minden hálózattípust sújthatnak. A feszültségvédelmi stratégia

kialakításában azonban a hálózat mérete a legfontosabb szempont.

Kis munkacsoportok

Az ilyen, általában kisvállalkozások által használt és távoli telephelyeken előforduló hálózatok húsznál kevesebb, egyenrangú (peer-to-peer) csomópontból állnak, nem tartoznak hozzájuk sem dedikált kiszolgálók, sem összetett felügyeleti rendszerek. A rendszergazdák általában a különféle számítógépeken tárolt adatok értéke és az állásidőből eredő veszteségek felhasználókra vetített összege alapján határozzák meg a feszültségvédelmi kívánalmakat. A tápellátási igények meghatározásakor figyelembe kell vennünk azt, hogy mekkora veszteséget okoz a közösen használt perifériák elérhetetlenségéből vagy hibájából eredő termeléskiesés. Egy alapszintű asztali UPS mindössze 5-10 százalékkal növeli egy új PC beszerzési árát, másfelől megkétszerezheti az üzemkész időt. A kevésbé kritikus eszközök érzékeny hardverelemeit egy jó minőségű, feszültségingadozás ellen védő csatlakozó (surge suppressor) még gazdaságosabban megvédheti a veszélyes feszültséghullámoktól és tüskéktől – az áramkimaradástól, feszültségeséstől és túlfeszültségtől azonban nem.

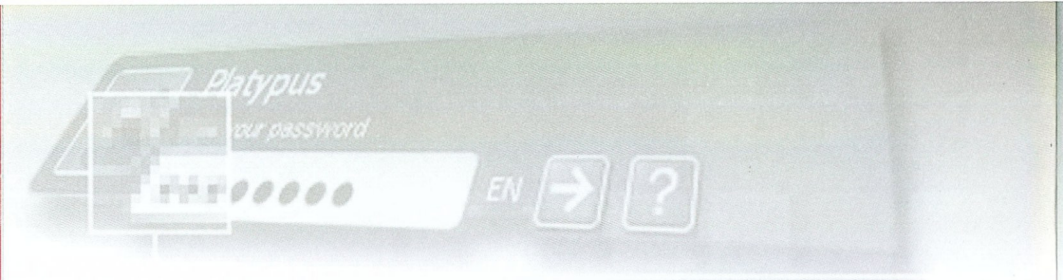
Kisméretű, kiszolgálóra épülő helyi hálózatok

A 250-nél kevesebb csomópontból álló kisméretű helyi hálózatok (LAN) sokféle vállalati igényt kielégítenek: betölthetik egy kisvállalat teljes hálózatának szerepét vagy egy nagyvállalati környezet egyik távoli telephelyi hálózatáét. Ezek a hálózatok nemcsak a kiszolgálótól valamint a fontos adatok tárolását és a felügyeletet végző munkaállomásoktól függnek, hanem az információk hálózatbeli áramlásáról gondoskodó tárolóeszközöktől és koncentrátoroktól is. Ha ezek közül bármelyik hibás lesz vagy leáll, akkor a felhasználók nem érhetik el az adatokat, s a kiszolgálóra sem menthetik ki őket, ez pedig végső soron adatvesztéssel jár – vagy ami még rosszabb: sérült állományokkal és adatbbázisokkal.

Az ilyen hálózatokhoz tervezett UPS-ek az akkumulátoros háttér és a túlfeszültség elleni védelem mellett további biztonsági funkciókkal is szolgálnak. Ahol több száz felhasználó munkája hiúsulhat meg, ott a vezetőknek hatékony feszültségszabályozási megoldásról, többféle működés közbeni funkcióról kell gondoskodniuk, valamint olyan tápellátásfelügyeletről, amellyel a rendszer távolról is ellenőrizhető és irányítható. A felügyeleti szoftvernek személyhívón értesítenie kell a rendszergazdát a feszültségproblémákról, illetve hosszabb áramszünet esetén automatikusan és biztonságosan le kell állítania a számítógépeket.

Közepes méretű helyi hálózatok

A 250–1000 csomópontból álló LAN-ok a kisméretű LAN-ok bonyolultabb változatai: felügyeleti rendszerük összetettebb, gyakran több, egymástól eltérő operációs rendszerű kiszolgálóból állnak, s bonyolult tárolórend-



szerek – például redundáns lemezalrendszerek (RAID) – csatlakoznak hozzájuk. A különböző hálózati zónák közötti kommunikációról a kokoncentrátorok és kapcsolók mellett útválasztók és hidak gondoskodnak.
A felhasználók munkája ezekben a hálózatokban is attól függ, hogy a kiszolgálók (a felhasználók több kiszolgálóra is bejelentkezhetnek), azután a kiszolgálókhoz csatlakoztatott tárolóeszközök és a munkaállomást a kiszolgálóval összekötő hálózati eszközök hibátlanul működnek-e.
Az ekkora hálózatok védelméről gondoskodó UPS-ektől a rendszergazdák sokszor azt várják, hogy a könnyebb telepítés kedvéért keretbe lehessen szerelni őket. S a rendszergazdának biztosnak kell lennie afelől, hogy a tápellátás-felügyeleti szoftver több kiszolgálóval és a kiszolgálón futtatott többféle operációs rendszerrel is kommunikál. A webes felügyeleti eszközök is egyre hasznosabbnak bizonyulnak a platformfüggetlen ellenőrzésben és jelentéskészítésben.

Vállalati hálózatok

A vállalati hálózatok feszültségvédelme bizonyos tekintetben egyszerűbb feladat, hiszen ezekben a hálózatokban a kritikus adatok legnagyobb részét egyetlen helyen, például egy adatközpontban tárolják.
Ma már nemcsak a nagyvállalatok működtetnek – az ISP- és ASP-központokban – adatközpontokat (data center), hanem a korszerű informatikai környezetet kiépítő kis- és középvállalkozásokok is.
S így van ez akkor is, ha az adatközpontot „szerverszobának", router-teremnek nevezik. (Az „adatközpont" annak a helyiségnek a neve, amelyben a vállalakozás informatikai eszköztárát üzemeltetik; itt van a kiszolgálópark, s itt vannak a hálózati eszközök, a távközlési berendezések, a szünetmentes áramforrások, az egy- vagy háromfázisú villamosenergia-ellátás, a légkondicionálás stb.)
Az adatközpont kiépítésében kulcskérdés, hogy a beruházó mennyire átgondoltan indít-

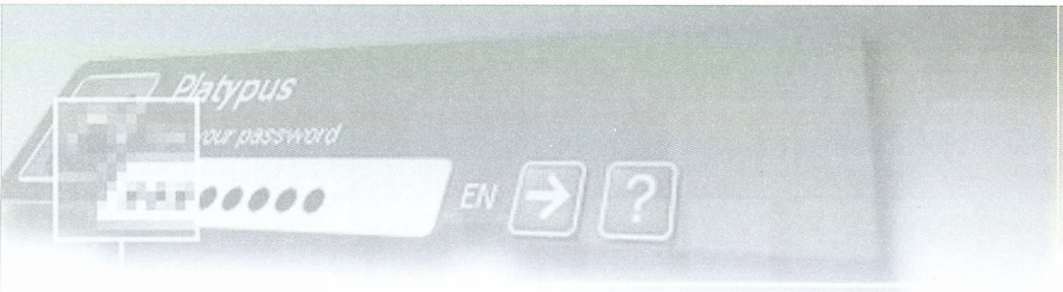
ja el a tervezést, majd a létesítmény felépítését. A gyakorlat szerint az üzemeltetésben jó néhány olyan szempont is lényegessé válik, amelyre a tervezéskor még nem kellett – vagy éppen nem lehetett – jobban figyelni.i. Már a helyiség kiválasztása is sok mindent eldönthet: ne legyen nagyobb területű az éppen szükségesnél,

másfelől meg bővíthető legyen; bármikor lehessen növelni a külső energiaellátás és szünetmentes áramforrások teljesítményét; gyorsan ki lehessen alakítani a helyiségben az infrastruktúrát, és persze könnyű legyen ebből a helyiségből egy másikba átköltözni. Ezek a követelmények persze ellentmondanak egymásnak, hiszen nincs gumiból sem a helyiség, sem az adatközpont eszközei.

A gyors felépíthetőség, az optimális helykihasználás, az igény szerinti bővíthetőség, az egyszerű költöztethetőség, a felügyelhetőség, a csekély beruházási és üzemeltetési költségek együttes követelménye erősen próbára teszi az informatikai szakembereket és az adatközpontok tervezőit – hiszen a szünetmentes áramforrásnak, a klímaberendezésnek akkor is működnie kell, ha az adatközpontnak csak tízszázalékos a kiépítettsége és a terhelése.

A minden kívánalomnak eleget tevő megoldást az APC InfraStruXure (ISX) rendszere kínálja.

Az APC tervezőmérnökei azzal előzték meg a mai gyakorlatban használatos megoldásokat, hogy az ISX architektúrával méretezhetővé tették a szünetmentes feszültségellátást, és a speciális keretekkel gyorsan beépíthetővé tették a szabványos (19 hüvelykes)



IT-eszközöket. Ezzel a megoldással az adatközpontok úgy bővíthetők, mintha valóban valamiféle IT-Legóval dolgoznánk; az ISX-rendszerek legfontosabb jellemzője a rugalmasság, a méretezhetőség, a költséghatékonyság, a testre szabhatóság, a könnyű felügyelet, az egyszerű és gyors szervizlehetőség.

Az InfraStruXure tulajdonképpen a logika diadala. Nem technológiai csoda, inkább logikusan felépített, optimálisan szervezett mód az IT-erőforrások elhelyezésére és szerelhetőségére.

Mielőtt UPS-t választanánk

Az alábbiakban összefoglaljuk, milyen szempontokat kell figyelembe venni az UPS kiválasztásakor.

- *Milyen hosszú legyen az áthidalási idő?* Az áramkimaradások általában nem tartanak tovább néhány percnél, mégis minden helyzetet egyedileg kell értékelni. A hálózati rendszergazdának általában legalább 5-10 perc akkumulátoros áthidalásra van szüksége ahhoz, hogy kézzel vagy automatikusan – egy tápellátás-felügyeleti szoftverrel – leállíthassa a rendszert. Más elektronikus berendezésekkel másképpen kell eljárni aszerint, hogy a felhasználók szempontjából mennyire fontos a folyamatos működésük.
- *Kell-e távolról ellenőrizni és irányítani a rendszer tápellátását?* A tápellátás-felügyeleti szoftver különböző beépített biztonsági funkcióival ugyanis távolról is elvégezhetjük ezt a feladatot, egy kiszolgálón, egy PC-n vagy a weben át.
- *Soroljuk fel az UPS-re kapcsolandó valamennyi eszközt!* Mint már említettük, számbe kell vennünk minden olyan eszközt, amely létfontosságú adatokat tárol vagy kritikus műveleteket végez — az összes biztonsági berendezést, a megjelenítőket és az alapinformációt hordozó telekommunikációs távközlési hálózati hardvert.
- *Hogyan válasszuk ki az eszközeinknek megfelelő UPS-t?* A nagyobb UPS-gyártók aszerint kategorizálják készülékeiket, hogy azok milyen számítógépes eszköz – asztali, hálózati, vállalati stb. – védelmére vannak tervezve. Néhány asztali rendszernek már a dobozáról is leolvasható, hogy milyen PC-konfigurációval működik együtt. Nagyobb hálózatok vagy összetettebb konfigurációk használatakor meg kell határoznunk a rendszer teljes tápellátás-igényét.
- Minden elektronikus eszköznek van egy *virtuális címkéje, s azon rajta van a bemeneti feszültség- és tápigény* voltamperben (VA), amperben (A) vagy wattban (W). Mivel az UPS-eket általában voltamperben rangsoroljuk, szorozzuk össze a feszültségértéket az amperekkel, s ezzel megkapjuk a voltamperértéket. Ha csak a wattérték van megadva, akkor azt szorozzuk meg 1,4-del.
- *Adjuk össze az eszközeink VA igényét.*
- *Válasszunk olyan UPS-t,* amelynek volt-amper-kapacitása legalább akkora, mint a teljes rendszer igénye. Ha már tudjuk, hogy később majd bővíteni fogjuk a rendszert, akkor érdemes eleve nagyobb kapacitású UPS-t beszerezni.
- *Hol működnek a táplálandó eszközök?* Ha az összes kritikus eszköz egy helyre került, akkor érdemes őket egyetlen nagyobb UPS-hez csatlakoztatni. Ha az eszközök különböző helyeken vannak, akkor rendszerint gazdaságosabb több kisebb UPS-t beszerezni.

InfraStruXure™

POWER RACK AIR

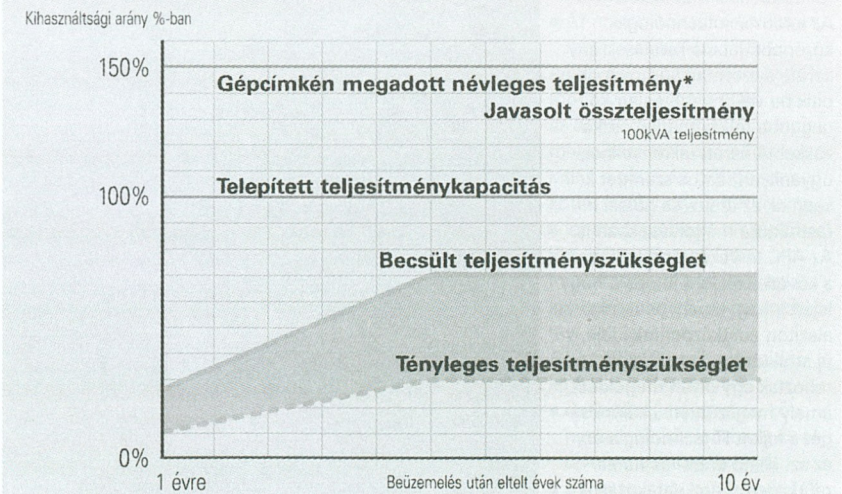
On-demand scalable, manageable, pre-engineered solutions

APC InfraStruXure™ a standard elemekből felépülő, igény szerint méretezhető, felügyelhető megoldás, avagy a Lego-elv szabadsága az adatközpontok kiépítésében.

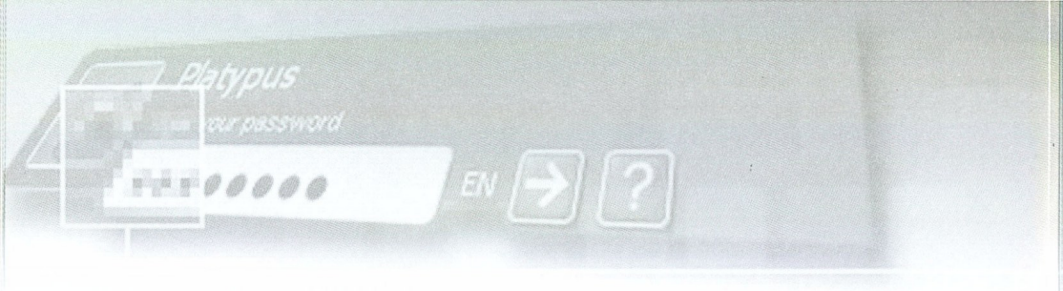
Az adatközpontok vadonatúj struktúrájának kidolgozása előtt az APC szakemberei alapos kutatást végeztek. Több mint 500 gyakorlott szakembert kérdeztek meg arról, hogy az adatközpontok tulajdonosai, üzemeltetői vajon milyen gondokkal küzdenek. A válaszok kiértékelésében az alábbi 5 problémakört tartották a legfontosabbnak:

1. élettartam-költségek
2. adaptálhatóság/skálázhatóság
3. rendelkezésre állás
4. felügyelhetőség
5. üzemeltetés/szervizlehetőségek

A túlméretezés költsége



* A telepített szünetmentes tápellátás rendszer gyártócímkén megadott névleges teljesítménye. Ez nagyobb lehet, mint a tervezett teljesítménykapacitás, mivel a tervben gondolnak a teljesítmény-csökkenésre és a berendezések redundanciájára is.

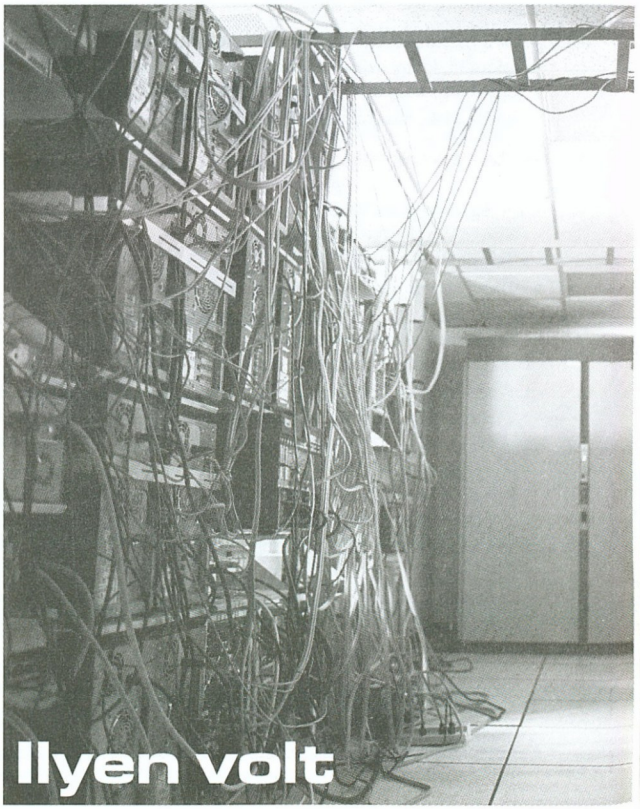


Az 1980-as években a számítástechnikai ipar temékei nem voltak sem szabványosak, sem integráltak. Sokkal összetettebbek voltak, mint manapság, nagy volt az erőforrásigényük és nehezen lehetett őket kezelni.

Amíg az információtechnológia akadálytalanul fejlődött a korszerű, könnyen felügyelhető, méretezhető eszközök irányában, addig az őket támogató áram- és hűtőrendszerek nem követték ezt a fejlődési irányt és ütemet. Az összetett villamos és mechanikai infrastruktúrák voltaképpen még mindig a hagyományos, gyakran 20-30 éves technológiájú áram- és hűtőrendszerekkel működnek.

Az információtechnológia középpontjába a keretszekrény került, s azt mind sűrűbben telepítik be vékonyabb és egyre nagyobb teljesítményű eszközökkel. A keretszekrényeknek ugyanilyen fontos szerepet kell kapniuk az áram- és hűtési infrastruktúra megoldásokban is.

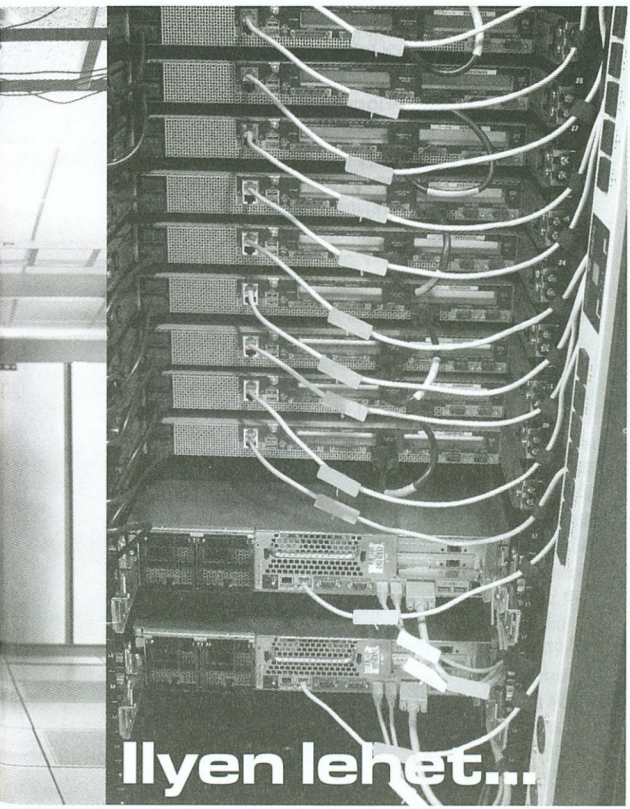
Az APC tervezőmérnökei arra a következtetésre jutottak, hogy lejárt a hagyományos módon kialakított adatközpontok ideje, s új struktúrára van szükség. Létrehoztak egy olyan megoldást, amely megszünteti a különbséget a fejlett IT-technológia és az azt ellátó áram- és hűtési rendszerek iránti várakozások között. Az APC úgy tartja, hogy nem a felhasznált alkotóelemektől lesz valóban jó egy megoldás, hanem az integráció művészetétől és tudományától, mert az teszi hatékonnyá az együttműködést a különféle részek között. Az APC által kifejlesztett InfraStruXure™ igény szerint méretezhető, könnyen felügyelhető, standard elemekből felépülő áram- és hűtési architektúra. Az Áram, Keret és Levegő hár-



mas egységéből felépülő keretoptimalizált InfraStruXure™ tökéletes, biztos alapul szolgál a teljes IT-rendszer felépítéséhez.

A régi rendszerek problémái

- Az IT-környezet „melegfoltjai" váratlan leállásokat okoznak.
- A túlméretezett áram- és hűtési megoldások fölösleges beruházási és működési költségeket követelnek meg.
- A nem pontosan beállított rendelkezésre állás a kritikus alkalmazások leállását okozhatja.
- A keretes IT-eszközök számának és mélységének növekedésétől a kábelek ellepik a keretszekrényt.
- Integrált megoldások híján a rendszer a külső erőforrások függvényévé válhat.
- A nem megfelelő felépítés értékes területek kihasználatlanságához vezet.
- Az összetett rendszerekben gyakoribb az emberi hiba és hosszabb a javítási idő.
- Az áramkörök túlterhelése váratlan leállásokkal járhat.



A „fizess, ahogyan növekszel" modell már régóta jelen van az üzleti világban, technológiai megoldást azonban eddig nem kínált a piac. Az ISX gondoskodik arról, hogy a beruházás a lehető legjobban megtérüljön (ROI = Return On Investment), s a lehető legkisebbre szorítja le az üzemeltetési költségeket.

Az InfraStruXure™ megoldás legfontosabb erényei:

- optimalizálja a keretes környezet hűtési elosztását és eltávolítja a meleg levegőt.
- a „fizess, ahogyan növekszel" méretezhetőség optimalizálja a beruházási és működési költségeket.

InfraStruXure™ típusok	A típus kis adatközpont	B típus közepes adatközp., szerverszoba	C típus nagy adatközpont
Áram	3 kilowatt	10 kilowatt	50 kilowatt
Levegő	3,5 kilowatt	16 kilowatt	65 kilowatt
Keretszekrény	4	8	28

- a keretes felépítés lehetővé teszi a rendelkezésre állás szintjének pontos meghatározását; a helyiség alapú felépítés erre nem ad módot.
- a keretszekrény mélységének növelése jobb kábel- és áramelosztást ad.
- a webes „Build-out-tool" tervezési eszközzel teljesen integrált rendszer építhető fel.
- a keretes felépítés nagyon jól kihasználja a helyet.
- a szabványosított, integrált megoldás csökkenti az emberi hiba gyakoriságát és a javítási időt.
- a keretszintű tápellátás- és környezetfigyelés révén csökkent a leállások száma.

Függetlenül a vállalkozás méretétől

A Lego-elv arról is kezeskedik, hogy a vállalkozások IT-szakemberei megtalálják a nekik legjobb ISX-változatot. Egy olyan kisvállalkozás, amelynek az induláskor egy kiszolgálója és néhány PC-je van, biztosan talál hosszú távon is optimálisan működtethető ISX-megoldást.

Az ISX-rendszerek legfontosabb jellemzői a rugalmasság, a méretezhetőség, a költséghatékonyság, a testre szabhatóság, a könnyű felügyelhetőség és az egyszerű, gyors szervizlehetőség.

Az APC három InfraStruXure™ architektúrára épülő megoldást dolgozott ki, s ezek mindegyike nagyfokú méretezhetőséget kínál már alapkiépítésben is.

Mit kínál Önnek az ISX?

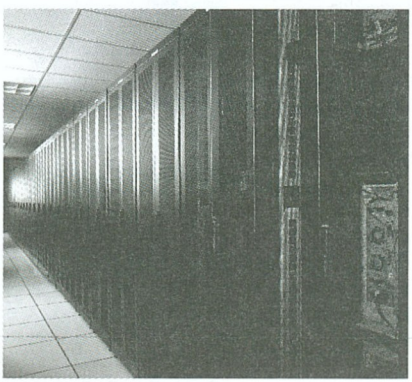
Optimalizálhatja kezdeti beruházásait a „fizess, ahogyan növekszel" megoldással; ez olyan kapacitás kiépítésére ad módot, amelyre éppen szüksége van.

Alapos, előrelátó, a teljes IT-infrastruktúrát átfogó felügyeletettel láthatja el folyamato-

san változó igényeihez alkalmazkodó eszközeit és azok környezetét.
Pillanatnyi igényeihez alakíthatja az infrastruktúrát, s ehhez nem kell feladnia korábbi beruházásait.
Az előre kialakított, moduláris alkotóelemek felhasználásával javíthatja a rendelkezésre állás költséghatékonyságát.
Kihasználhatja a szekrényes, a mai információtechnológiai követelményeknek megfelelő optimalizált áram- és hűtőarchitektúrát.
Igényeinek megfelelő, testreszabott áram- és hűtőarchitektúrát alakíthat ki a rendelésre konfigurált, egyszerűen kezelhető online tervezési eszközzel (a Build-out toollal).

POWER – RACK – AIR

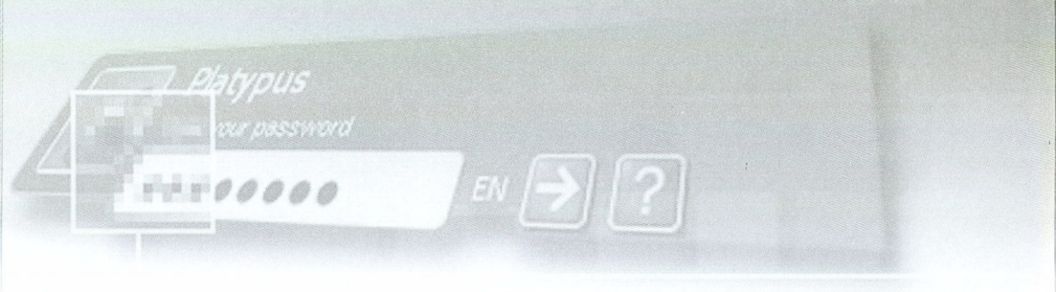
Az APC új megoldása, mint a logón is láthatják, három dolgon alapul: tápfeszültség, rackszekrény és levegő. Az informatikai biztonsághoz hogyan jönnek ezek a heterogén fogalmak?

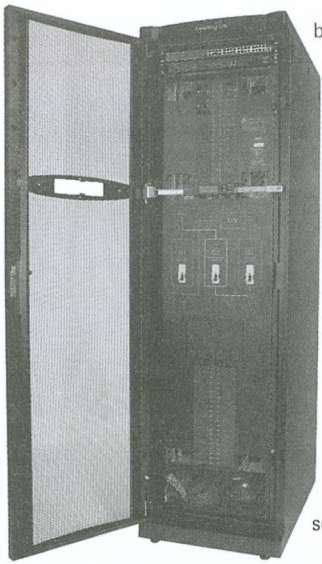


Noha a legtöbb felhasználóban nem tudatosul, de a számítógépnek létfontosságú eleme a tápfeszültség: kevesebb memóriával, kevesebb merevlemezzel lehet működni. Ahol redundáns tápegység van, ott abból is egy meghibásodhat, az üzem attól még megy tovább. De ha nincs tápfeszültség, akkor a legdrágább számítógép sem több egy halom közönséges veszélyesnek is tekinthető hulladéknál. Ez fokozottan igaz a kiszolgálókra: ezek tevékenysége különösen értékes, kiesésük pedig általában a kényelmetlenségnél jelentősebb kárt okoz. Hiszen szerverek nemcsak weboldalak mögött állnak: erőművek, közlekedési vállalatok, telekommunikációs szolgáltatók, kis- és nagykereskedők és még sok ezer cég tevékenysége alapul kisebb-nagyobb kiszolgálókon. Természetesen a többségük alkalmaz szünetmentes tápegységeket a szervereik, számítógépes hálózatuk infrastruktúrájának védelmére.
Ahol több kiszolgálót használnak, ott már érdemes rackszekrénybe szerelni ezeket. A szerverek gyártói is egyre több modellt hoznak ki, ami rackszekrénybe szerelhető.
Noha nem kézzelfogható, de a nagy teljesítményű számítógépekhez sok levegő kell: az asztali számítógépekben is hatalmas ventilátorok mozgatják a levegőt, természetesen a sokkal nagyobb teljesítményű kiszolgálók sem lehetnek meg friss – és hűvös! – levegő nélkül.

Energia

Az InfarStruXure™ megoldás az energiaellátásra igen kényelmes megoldást ad.
A rackszekrényekbe építhető tápegységekkel egyrészt igen nagy teljesítményt lehet elérni, másrészt igen rugalmas a rendszer, igen jó a





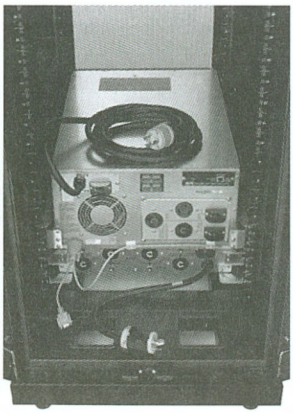
bővíthetőség. Ha valaki hosszabb távra tervez azzal, hogy időről időre új szolgáltatásokat állít be, újabb számítógépeket helyez üzembe, akkor az InfrStruXure™ alkalmazásával újabb és újabb modulok hozzáadásával egyszerűen megoldhatja a szükséges többletenergia beépítését.

Rackszekrény

Ráadásul nem csak arról van szó, hogy a rackszekrényekbe betesszük a gépeinket, szünetmentes tápegységeinket: az egész olyan, mint egy gigantikus építőkocka készlet. A szekrények és beléjük építhető szünetmentes tápegységek mellett szinte minden olyan elemet tartalmaz, ami egy számítóközpont berendezéséhez kell. Így megtaláljuk a szekrények mellett a tápfeszültség elosztására szolgáló kábeleket, a különböző egységes csatlakozókat. Azt hiszem sokan jártak már úgy, hogy kihúztak a kábelrengeteg végén egy kábelt – és akkor vették észre, hogy nem azt kellett volna...
A rackszekrény igen jól használja ki a rendelkezésre álló alapterületet. Ezért noha látszólag drága megoldás, hosszabb távon mindenképpen megéri: egyrészt ugyanannyi eszköz (szünetmentes áramforrások, kiszolgálók, hálózati eszközök) elhelyezése akár tizedakkora helyen is megoldható. Márpedig egy adatközpont kiépítése elég drága, és ha egy jelentősen kisebb helyiséget kell berendezni, az komoly előny.

Levegő

Az InfraStruXure™ komoly megoldást jelent a szellőzés problémájára is. Hiszen ahogy a kiszolgálók egyre kisebb méretűek és nagyobb teljesítményűek lesznek, egyre több hőt kell elvezetni a rackszekrényekből. Ezért az építőkészlet tartalmaz különböző, a rackszekrénybe építhető ventilátorokat is. Ezek 9 kW teljesítmény által keltett meleg levegőt tudnak kiszellőztetni. A hűtés mind álpadlós, mind álpadló nélküli helyiségekben használható.
A teljes rendszer komplex adatközpont, számítógépterem felépítésére nyújt segítséget. Ha ismerjük szükségleteinket, és a rendelkezésre álló helyiséget, akkor az APC weboldalán meg is tervezhetjük a rendszert.
A teljes rendszernek nagy előnye, hogy egész üzemállapotát egyetlen helyről kísérhetjük figyelemmel: egy monitoron áttekinthető a teljes üzemállapot. Ehhez kapcsolható az EMU (Environmental Monitoring Unit), ami a szekrényekben uralkodó hőmérsékletről, páratartalomról ad folyamatos tájékoztatást. ■



Fenyegetések az internet világában

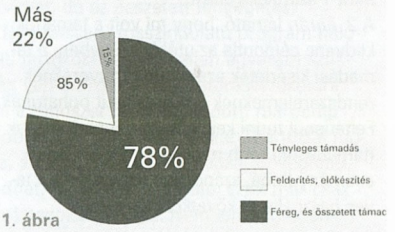
A Symantec februárban megjelentetett egy tanulmányt, amely komplex képet próbál adni a ma élő, elsősorban az internet felől fenyegető veszélyekről.

A tanulmány a 2002 második felében észlelt jelenségek alapján készült, és első részében a mai internetes, számítógépes támadások trendjét elemzi. Ez valós támadások, próbálkozások feldolgozásán alapul. Az adatok forrásául 30 országban mintegy 400 cég és 1000 behatolásérzékelő rendszer szolgált.
A második részben a várható fenyegetéseket másik oldalról elemzik, a dokumentált program, rendszerhibák, illetve a rosszindulatú kódok felől. Ezeknek az adatbázisa több mint 6000 tételt tartalmaz.
A tanulmány három fő részre osztja az informatikai infrastruktúrára leselkedő veszélyeket.

Hálózati támadások

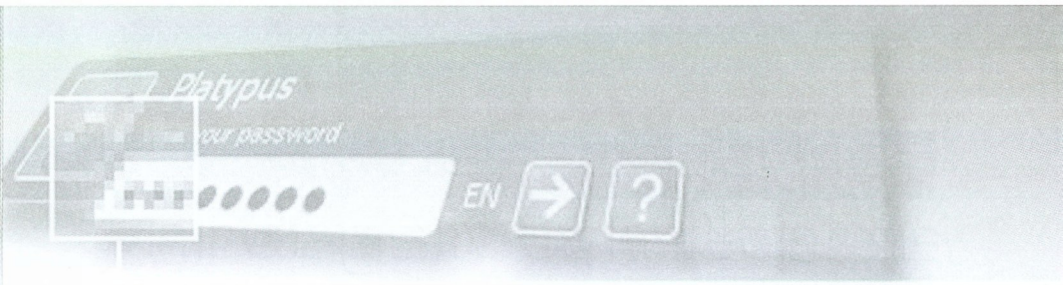
A *cyber attack* néven emlegetett hálózati támadásokról a tanulmány megállapítja, hogy a számuk enyhén csökkenő tendenciát mutat (a férgektől és az összetett támadásoktól eltekintve). Persze vannak rosszabb hetek, hónapok, de az utolsó hat hónap az előző hat hónappal összehasonlítva enyhe csökkenést mutat. A támadások túlnyomó többsége inkább valamiféle támadást előkészítő, felderítő eljárás volt, mindössze 15 százalék volt a valódi támadás. Az előkészítő, hálózati infrastruktúrát felderítő tevékenység többnyire nem minősül a biztonságot súlyosan sértő eseménynek, mivel az esetek többségében nem követi semmi tényleges akció. A támadási kísérletek 99 százaléka tartozik a nem veszélyes kategóriába, a súlyosnak minősíthető esetek száma pedig enyhén csökkenő tendenciát mutat *(1. ábra)*.

Támadástípusok
(2002. július 1. és 2003. december 31. között)



1. ábra

A támadók próbálkozásai gyakorlatilag a hét bármely napján, a nap bármely órájában előfordulnak. Az adatok szerint sokkal kevesebb a behatolási kísérlet szombat-vasárnap, mintegy fele a hétköznapi kísérleteknek. A hét első napjain hajszálnyival több kísérletet észleltek. Érdekes módon, a hétvégi behatolási kísérlet nemcsak kevesebb, hanem sokkal erőtlenebb is: a komolyabb próbálkozásokból (súlyosnak minősített esetekből) hétvégén negyedannyit észleltek.
A támadások gyakorisága és súlyossága igen erősen függ az adott cég, intézmény jellegétől, méretétől, ügyfélkörétől: a támadók kedvencei az energiaipari cégek, ide tartoznak az erőművek, nagy olajipari cégek. Az utóbbi időben a különböző nonprofit szervezetek is egyre többször válnak célponttá. A célpontok toplistáján harmadik helyen a telekommunikációs ipar képviselői állnak.
A támadások többsége továbbra is jellemzően néhány országból indul; az első tíz országból indítják a támadások 80 százalékát. Ebben az Egyesült Államoké az első hely, az utóbbi hónapokban Dél-Korea „megszerezte" a második helyet és Kína a harmadik a listán. Ugyanakkor a cyber terroristák listáján sze-



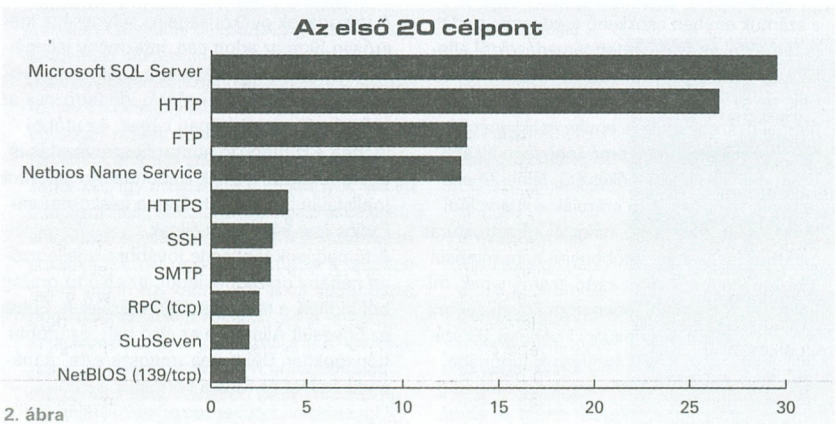
replő országokból a támadások kevesebb mint 1 százaléka eredt.
A *2. ábrán* látható, hogy mi volt a támadók kedvenc célpontja az utóbbi fél évben, a támadási kísérletek ezeknek a szoftvereknek, rendszerelemeknek gyengeségeit puhatolták. Feltétlenül tudni kell, hogy a jelentett esetek (támadások) több mint 50 százaléka belső esemény (hiba, szándékos vagy véletlen téves használat...) következménye volt.

Rendszerhibák, hibás kódok

A rendszerhibák, sérülékenységek tekintetében sem szívderítő a helyzet. Az elmúlt évben 2524 új, a biztonságot sértő hibát dokumentáltak, 80 százalékkal többet, mint 2001-ben. Nem mindegy, hogy ezek a biztonsági rések mekkorák: sajnos 2002-ben sokkal jobban növekedett a komolynak minősített biztonsági rések száma, mint a kevésbé veszélyeseké. A Symantec szerint ez a trend a webes alkalmazások erőltetett ütemű fejlesztéséből is adódik, mert ezek a távolból is kihasználható hibákat tartalmaznak. A biztonsági rések kihasználása általában egyszerű. Az utóbbi időben feltárt biztonsági rések a jövőben komoly biztonsági kockázatot rejtenek.

Rosszindulatú kódok

A legnagyobb fenyegetést továbbra is rosszindulatú kódok – nemcsak az újak, hanem a régiek is – jelentik, mert ezek kihasználják az óvatlanul ki nem javított rendszerhibát. Az önmagukat levélben továbbító rosszindulatú kódok száma mintegy nyolcszorosára nőtt 2002 első félévéhez képest, továbbá megnőtt azoknak a vírusoknak (férgeknek) a száma is, amelyek információkat, dokumentumokat lopnak el a megfertőzött gépről. Az új technológiák új lehetőségeket adnak a rosszindulatú programok készítőinek, emiatt a jövőben felkészülhetünk arra, hogy például a mobil eszközöket, a speciális pont-pont kapcsolatokat új támadások fogják érni. ■



2. ábra

Integrált biztonsági megoldások

Az informatikai rendszerek igen összetettek, minden egyes részük más-más módon támadható. Ezzel a védelemnek is lépést kell tartania; erre szolgál az integrált védelem.

Felhasználók integrált védelme

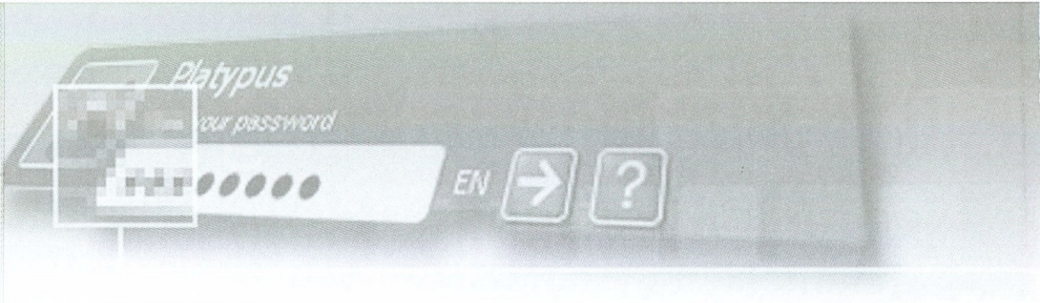
A vállalatok informatikai rendszerét egyre összetettebb fenyegetések veszélyeztetik, ugyankkor egyre több dolgozó végzi munkáját a munkahelyétől távol, otthon vagy útközben. A munkavégzés ilyen módja kétségtelenül hatékony, de a távolból dolgozó és az utazó alkalmazottak veszélynek teszik ki a vállalatot — akár egy védtelen, nagy sebességű kapcsolaton (ADSL-en vagy kábelmodemen) keresztül, akár egy fertőzött laptop munkahelyre való bevitelével — és ez a veszély nem elhanyagolható. Az alkalmazottak azonban a számítógépükre letöltött fertőzött elektronikus levéllel vagy óvatlanul megnyitott weblappal a munkahelyen belül is éppen ilyen könnyen megnyithatják az utat a hálózaton keresztül terjedő veszély előtt.

Egy valós esemény

Képzeljük csak el! Egyik alkalmazottunk a távolban dolgozik a noteszgépén. Kap egy fertőzött mellékletet tartalmazó levelet. Nem kell megnyitnia a mellékletet, egyes levelezőprogramokban elég csak az előnézeti ablakban megnéznie, és a Nimda máris észrevétlenül a gépére kerül. Ezután az alkalmazott vagy felkapcsolódik egy tökéletesen megalkotott VPN-en át a noteszgépéről a vállalati hálózatra, vagy másnap beviszi a gépet a munkahelyére, a tűzfallal, és más eszközökkel védett tartományon belülre. A víruselhárító szoftver el tudja ugyan fogni a vírust, de az összetett fenyegetés, a Nimda-szerű rosszindulatú program hálózati fertőzőképessége ellen egyaránt szükség van a tűzfalra és a betörésérzékelőre. Ha a rendszer megfertőződött, márpedig a noteszgéppel a féreg bekerült a tűzfal mögé, a fertőzés az egész hálózaton végigterjedhet, mivel a felhasználói szint már csak korlátozottan védett. Nem lehet minden egyes hálózati csomópontot, számítógépet külön tűzfal mögé tenni. Vagy igen?
Ha a felhasználói szinten is valamiféle összetett védelem dolgozna, akkor a következő történhetne: a felhasználóhoz érkező adatoknak először át kell haladniuk a felhasználói tűzfalon, emellett az érkező jelzés a hálózati támadások, az érkező adatok, vírusok szempontjából is ellenőrzésre kerülnek. Ha „megszólal" a betörésjelző, a felhasználói tűzfal megakadályozza az érintett IP-cím felőli hálózati hozzáférést. Vírus esetén pedig a rendszer kijavítja vagy elszigeteli a fertőzött állományt. A felismert fenyegetés megmarad a felhasználói szinten, és az akció elhal, mielőtt átterjedhetne a vállalati hálózat többi részére.

Az általános cél

Az összetett veszélyek a vírusok, a férgek, a trójaiak és a rosszakaratú kódok tulajdonságait ötvözik a szerverek és a rendszerben meglévő biztonsági hibák, sérülékenységek kihasználásával, és így indítják, viszik át és terjesztik támadásaikat. Az egyetlen védelem ellenük az integrált védelem alkalmazása valamennyi szinten – az internetátjárón, a hálózati kiszolgálókon és a munkaállomásokon is.



Az informatikai védelem és a valós helyzet

Ma, amikor

- nő az e-üzlet fontossága,
- eltűnőben van a hálózat határa,
- a határok eltűnésével lényeges elem lett az üzlet folyamatossága,
- egyre gyakoribbá és összetettebbé válnak az információ elleni támadások és egyre nagyobb veszteséget okoznak,

a legtöbb informatikai részlegnek várhatóan több lesz a feladata, a pénzügyi és a személyi erőforrása azonban csökkenni fog.

A mai védelmi környezet következményei

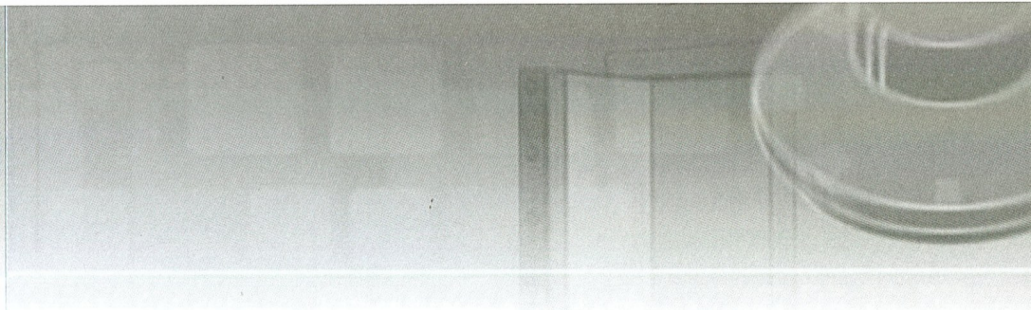
A különböző szállítóktól származó, önálló termékekből összetevődő hálózati védelemnek több sajátossága van.

1. Az informatikai személyzet gazdaságtalanul dolgozik: az informatika területén dolgozóknak megvásárolt többféle termék azt jelenti, hogy többet kell telepíteniük, többször kell kezelniük és felügyelniük a hasonló adatokat. Az egyedülálló termékeknek kicsi a „rálátásuk" a védett környezet egészére. Egy járvány kitörésekor a különféle szállítók által végzett gyorsjavításokat különböző módszerekkel kell bevizsgálni.
2. A védelem gyengébb a vártnál: ha több gyártótól szerezzük be a termékeket, nem várhatjuk azt, hogy ezek zökkenőmentesen együttműködjenek vagy kommunikáljanak egymással.
3. Többe kerül: az informatikai részlegeknek nagyobb közvetlen és közvetett költséggel jár a különféle, önálló termékek hadrendbe állítása, kezelése és frissítése, mint amennyibe egy integrált megoldásé kerülne.

A végeredmény az, hogy a nem integrált, önálló termékek kezelése nem hatékony, nő a rendszer kezelésének és támogatásának a költsége, valamint a birtoklás összköltsége. Az integrált védelem nemcsak széles körű védelmet és reagálást kínál, hanem a kezelésre fordított erőforrások optimalizálását is, hiszen a különböző védelmi módszerek telepítése, a készülő jelentések és a frissítések mind egyetlen felületről kezelhetők. Ez pénz- és időmegtakarítással jár, és csökkenti annak a lehetőségét, hogy a hálózat felhasználói szintje védtelen maradjon.
A felhasználói szinten történő vírusellenes védelem már nem elegendő a felhasználói réteg megvédésére. Mivel a felhasználók a vállalati tűzfal mindkét oldalán előfordulnak, éppúgy sebezhetőek, mint a hálózat többi része, sőt az összetett veszélyek szaporodásával sebezhetőségük is nő.

Három jó ok egy ügyféltűzfal alkalmazására

1. *A távmunkások számának növekedése*
   VPN és más „always-on" kapcsolatok a vállalati hálózat hátsó ajtajaként is működhetnek, illetéktelenek könnyen hozzáférhetnek egy noteszgépen keresztül a vállalat titkos információihoz.
2. *Összetett fenyegetések*
   Azokat a fenyegetéseket, amelyeket az ügyfél-vírusvédelem nem állít meg, megállítja az ügyféltűzfal, és így nem fertőznek meg másokat sem.
3. *DDoS támadások*
   PC-k és laptopok könnyen részesei lehetnek egy ilyen támadásnak.



Átfogó ügyfélvédelem

A *Symantec Client Security* a maga nemében egyedülálló integrált védelmi megoldás a hálózat és a távoli felhasználók számára.
A *Symantec Client Security* egyesíti a vírusellenes, betörésjelző és tűzfalmegoldásokat annak érdekében, hogy a felhasználói szinten is érvényesíthetőek legyenek a rendszabályok, és a központosított frissítés és terjesztés révén gondoskodjon a jobb reagálásról. A védelem megnövelése érdekében a *Symantec Client Security* a vírusellenes védelmet összetett hálózati védelemmé bővíti.

A Symantec Client Security további előnyei

- A központosított kezelés gyorsabb reagálást tesz lehetővé a többszörös veszélyekre
- Az egy gyártótól származó többféle védelmi eljárás olcsóbban, jobb védelmet ad
- A különböző területekről érkező jelzések (víruskereső, tűzfal, behatolásjelző...) egy rendszerben keletkeznek, az összefüggések könnyebben felismerhetők
- Egyszerűbb a védelem kezelése a különféle elosztott hálózatokon
- A kezelés egyszerűbb egyetlen segítségnyújtó kapcsolaton át.

A VÁLLALAT ÚJ, INTEGRÁLT MEGOLDÁSÚ VÉDELME

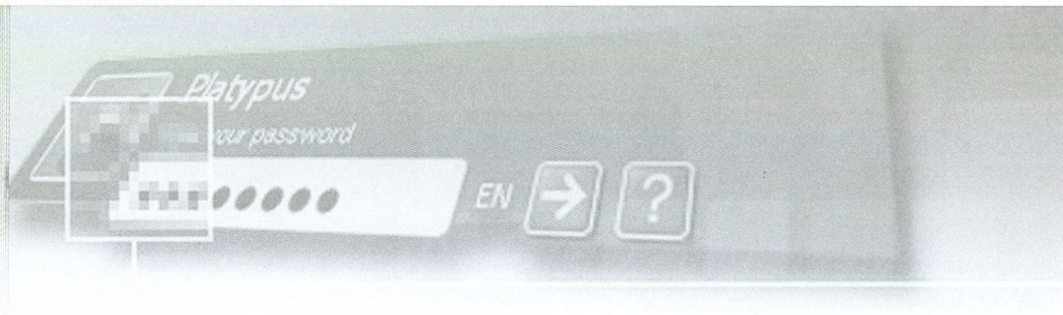
A szervezetek munkájuk, adatmegosztásuk, mindennapi kommunikációjuk során egyre inkább függenek a hálózatoktól. A feladat magától értetődik: csak azok az emberek férhessenek hozzá az adatokhoz, akiknek megfelelő jogosultságuk van, de aki jogosult, az férjen hozzá az adatokhoz. A mai hálózatok bonyolultsága és a biztonságot fenyegető új kockázatok megjelenése napról napra nehezebbé teszi ezt a feladatot.

A változó környezet és az összetett fenyegetések szükségessé teszik az integrált védelmet

A vállalati hálózatok kereskedelmi és együttműködési célra való felhasználásának képessége nagymértékben előmozdítja a vállalkozást, és afféle „hiperkapcsolt vállalat" széles körű megjelenéséhez vezet. Az ilyen vállalkozások igényeinek kielégítésére a hálózat átjáró-, szerver-, valamint felhasználói szintjeinek szorosan össze kell kapcsolódniuk, vagyis a létfontosságú információk a belső hálózat több szintjén megtalálhatók, és ezek mindegyike megköveteli a saját védelmet. Ezzel egyidejűleg mindennapossá válnak a hálózatot fenyegető egyre rafináltabb veszélyek, olyan támadási módszerekkel, amelyek több módon próbálják felderíteni és kihasználni a hálózat sebezhető pontjait. Például a vírusok, a férgek, valamint a trójaiak, amelyek többnyire önmagukat sokszorosító és terjesztő fájlokban vagy programokban rejtőznek, és igen könnyen elterjedhetnek a gyanútlan számítógép-használók révén. A védelmi eljárások gyenge pontjainak kihasználására tervezett, egymástól függetlenül dolgozó, összetett fenyegetések több eljárást használnak a támadásra és saját maguk elterjesztésére, ezáltal igen gyorsan elterjednek és kiterjedt károkat okoznak.

A kockázatokról

A hálózat sebezhetőségének több szintjével és az egyre gyarapodó támadási eljárásokkal a vállalatok kockázata is egyre nő. A hálózati



támadások több módon is befolyásolhatják az üzletmenetet.

- Az üzleti műveletek leállítása. A támadások okozta kimaradás termelési és bevételi veszteségekkel járhat, a megtámadott hálózat helyreállítási költségei pedig megnövelik a pénzügyi terheket.
- A törvényi felelősség és az esetleges pereskedés. A sikerrel megtámadott cégeket gyakran fogják perbe vagy idézik a bíróság elé tanúként.
- Csökken a versenyképesség. Ma már többnyire az információ a vállalat legértékesebb kincse (gondoljunk az előfizetők, beszállítók listájára).
- A márkanév károsodása. Egy márkanév sérülése a vállalat piaci helyzetének romlásához vezethet. Ha egy cégtől például hitelkártya-információkat loptak el, nehéz lesz visszaszereznie a márkába vetett bizalmat.

A jelenlegi biztonsági megoldások nem alkalmasak az összetett fenyegetések elleni védelemre és magasabb birtoklási költséggel járnak. Ez nehezen kezelhető védelmi helyzetet eredményez, és hatása nem felel meg a biztonsági elvárásoknak.

A logikus megoldás: az integrált védelem

Az integrált védelem elve az e-üzlettel kapcsolatos új feladatok megoldására alakult ki. Az integrált védelem a teljes védettség érdekében a különféle biztonsági eljárásokat egyesíti a szabályzatnak való megfeleléssel, a segítségnyújtással és a fejlett kutatással. A költségek és az előnyök legkedvezőbb aránya mellett a leghatékonyabb biztonságot ez adja. Kész a legnagyobb védekezésre, az informatikai rendszer több szintjén egymást kiegészítő funkciókkal működik. A hálózatot érő támadások hatásának minimalizálása érdekében összetett tevékenységével valamennyi rétegben hatékonyabb védelemre képes a fenyegetések sokasága ellen.

Az integrálható védelmi eljárások:

Tűzfalak – a hálózatba belépő és az azt elhagyó információ szűrésével a teljes hálózati forgalmat ellenőrzik a jogosulatlan hozzáférés megakadályozása érdekében.

Behatolásérzékelés – felismeri a jogosulatlan hozzáférést, riaszt és jelentést készít a támadások mintázatának és módszerének elemezhetősége céljából.

Tartalomszűrés – felismeri és megakadályozza a nemkívánatos forgalmat.

Virtuális magánhálózatok (VPN) – a hálózat határain túlnyúló kapcsolatokat védi, lehetővé teszi a biztonságos vállalati kommunikációt az interneten át.

Sérülékenység kezelése – felderíti a védelem réseit és megoldást javasol rájuk.

Víruselhárítás – védelmet ad a vírusok, férgek és trójaiak ellen.

Miért szükséges az integrált védelem?

Az egy megoldássá egyesített védelmi eljárások a bonyolultság és a költségek csökkentése mellett átfogóbb védelmet adnak. Az integrált megoldás szükségtelenné teszi a különböző szállítóktól származó termékek egyenkénti kezelését és a közöttük fellépő együttműködési problémák megoldását. Mivel az integrált védelem a hálózat valamennyi rétegén alkalmazható, ezért növeli a vagyonvédelmet és csökkenti az üzletmenet megszakadásának a kockázatát is. Az integrált megoldásnak köszönhetően nő a gyakran túlterhelt

informatikai részleg hatékonysága is, és az informatikai személyzet más stratégiai feladatokra tud összpontosítani.
A védelmi tevékenység hatékonyságának növelésére, a támadások hatásának minimalizálására és a szervezetek általános védelmi helyzetének javítására ma egy integrált védelmi keretrendszer nyújtja a legtöbbet. Eljött az ilyen megoldások ideje.

Integrált biztonsági megoldások: Symantec Client Security

A *Symantec Client Security* az integrált biztonsági megoldások egyéni felhasználóknak szóló megvalósítása.
Ez a csomag együtt tartalmazza a ügyfélgépek számára az integrált antivírus, tűzfal és behatolásérzékelést.
A Symantec Client Security az első olyan megoldáscsomag, amely integrált biztonsági megoldást kínál a hálózati és távoli ügyfélgépeknek is. Több biztonsági technológia egyidejű központosított telepítését, terjesztését, beállítását és szabályzatkezelését teszi lehetővé.

- Integrálja a Symantec antivírus, tűzfal és behatolásérzékelő technológiáit, így biztosítja az ügyfélgépeken a biztonsági szabályzat betartását.
- A nagyvállalati hálózatban az integrált menedzsment- és válaszlépés-szolgáltatásokkal fejlett védelmet ad az ügyfélgépeken az összetett internetes fenyegetések ellen.
- Az adminisztrátor erőforrásait optimalizálja, és csökkenti az ügyfélgépek hálózati védelmének adminisztrációs, rendszertámogatási és általános biztonsági költségeit.
- Mindez a Symantec Security Response támogatásával végezhető, amely a veezető internetes biztonsági kutató és rendszertámogató szervezet.

A Symantec Client Security kiváló védelmet nyújt az ügyfélgépeken az összetett internetes fenyegetések ellen. Integrációja a piacvezető biztonsági technológiákkal az ügyfélgépek szintjén széles körű biztonságot ad, miközben csökkenti az általános biztonsági költségeket.
A Symantec Client Security közös terítési és frissítési funkciót kínál a Symantec antivírus, tűzfal és behatolásérzékelő technológiái számára, így csökkenti az üresjáratokat, a kockázatot és az adminisztratív terheket, melyek rendesen a különböző szállítóktól származó egyedi termékek menedzseléséhez kapcsolódnak. A Symantec Client Security automatikusan megvizsgálja az állományokat az ismert és ismeretlen vírusok után kutatva, blokkolja a gyanús kimenő és bejövő forgalmat, a jogosulatlan behatolást és a port scant. A Symantec Client Securityt támogatja a Symantec Security Response, az iparágvezető általános kutató és rendszertámogató szervezet. A frissítések a Symantec Client Securityhez egyetlen, integrált mechanizmuson keresztül jutnak el, ez a LiveUpdate; amely biztosítja a gyors terítést és a biztonsági szabályzatok betartását.
A Symantec System Center központosított ügyfélbiztonsági menedzsmentje a biztonsági funkciók széles körű áttekintését teszi lehetővé, valamint fejlett menedzsment- és válaszlépés-lehetőségeket biztosít még az összetett internetes fenyegetések ellen is. A rendszergazda erőforrásait optimálisan használja ki, mivel a többrétű biztonsági technológiák te-

lepítése, a jelentéskészítés és a -frissítés mind egyetlen konzolról történik.
A Symantec Client Security egyedi backend infrastuktúra technológiákat használ a Symantectől, többek között NAVEX-et, a Digital Immune Systemet és a Bloodhoundot. Ezek a technológiák az ismert és ismeretlen fenyegetésektől egyaránt védelmeznek.

Integrált biztonsági megoldások: Symantec Gateway Security

A *Symantec Gateway Security* széles körű átjáróvédelem egy teljesen integrált biztonsági berendezésben.
Ez a könnyen kezelhető berendezés széles körű átjáróvédelmet ad a vállalatoknak, és kielégíti a kis- és közepes vállalkozások, valamint a nagyvállalkozások fiókirodáink egyedi biztonsági igényeit.

- Az adminisztrációt könnyűvé és egyszerűvé teszi egy grafikus menedzsmentfelület használatával, s ezzel minden biztonsági funkció kezelhető.
- Rugalmas és nagy teljesítményű, miközben kompatibilis a piacvezető tűzfal-, magas rendelkezésre állási és terhelésmegosztási opciókkal.
- Mögötte áll a Symantec Security Response, a világ vezető internetes biztonsági kutató és rendszertámogató szervezete.
- Az internetátjárót megvédi minden típusú web- és e-mail fenyegetés ellen.

A Symantec Gateway Security az első széles körű átjáróvédelmi megoldás egy egyszerű, könnyen kezelhető berendezésben, amely a kis- és közepes vállalkozások egyedi biztonsági igényeit célozza meg az 5 elemi hálózati biztonsági funkció ötvözésével. A teljesen integrált rackbe szerelhető egység a legmodernebb tűzfal, antivírus, internettartalom-szűrés, behatolásérzékelés és virtuális magánhálózat technológiák alkalmazásával véd a legújabb többrétű biztonsági fenyegetések ellen.
Ahogy az egy valódi plug-and-protect megoldáshoz illik, a berendezés vezérli és figyeli a web- és e-mail fenyegetések minden típusát, beleértve a féregvírusokat, a rosszindulatú kódot, a biztonsági rések támadását, és az olyan összetett fenyegetéseket is, mint a Nimda vagy a Code Red. A közös menedzsment konzol használatával minden biztonsági funkció könnyen beállítható és módosítható akár helyben, akár távolról, és az olyan frissítések, mint az új vírusok definíciói és behatolásérzékelési „ujjlenyomatok" automatikusan teríthetők a LiveUpdate segítségével.
A Symantec Gateway Security az internet és a vállalati hálózat vagy a belső hálózat egyes szegmensei közötti átjáró biztonságossá tételének rugalmas megoldása olyan szervezeteknek, amelyeknek már van tűzfala. A berendezés teljesen kompatibilis a vezető gyártók termékeivel, így egy második védelmi vonalat alkot, továbbá olyan védelmet ad, amelyet azok egymagukban nem tudnának adni.
A Symantec Gateway Security az a megoldás, amely az egyszerű, grafikus menedzsmentfelület mögé a létező legjobb biztonsági technológiát integrálja, és gondoskodik arról, hogy minden komponens tökéletesen együttműködjön. Ez növeli a biztonságot, mégis könnyen kezelhető, továbbá biztosítja a hálózat optimális működését és a befektetés lehető legjobb megtérülését. ■

A Symantec szemlélete az információk védelméről

Az adatbiztonság területének két fontos fogalma az incidens és az esemény. A teljes rendszer adatbiztonságához ezeket a tényezőket pontosan kell használni, és megkülönböztetni.

A biztonság kézben tartása minden eddiginél nagyobb felelősség.
Nagy összegeket költöttek a felismerést és a megelőzést szolgáló alkalmazásokra, mégis mindig küzdeni kell a környezet biztonságának megőrzéséért? Nos, ezzel nincs egyedül.

Mennyi összetevő

Az incidens és az esemény két igen eltérő fogalom, és sajnos gyakran összekeverik őket. Meg kell találni az események szénakazlában a védelmi incidenseket jelentő „tűket".
Események. A vállalatnál működő, a rendszereket és a hálózati forgalmat vizsgáló védelmi eszközök gyanúsnak tűnő tevékenység észlelésekor jeleznek. Az ilyen, egy-egy védelmi eseményt képviselő jelzésből a legtöbb vállalatnál naponta sokezernyi adódik. *Eseménynek nevezzük a rendszerben vagy a hálózaton megfigyelhető bármely történést.*
Két példa a mindennapos eseményekre:
- hibás vagy túl hosszú hálózati csomag
- elrontott bejelentkezés a számítógépre

Az eltorzult csomagok általában ártalmatlanok, de egyes esetekben káros hatásuk is lehet; például jelezhetnek egy átmenetitár-túlcsordulásos támadást is. Azok a cégek, amelyek az összefüggések ismerete nélkül csak az események felügyeletére összpontosítanak, az összehangolatlansággal kínlódnak, és hamis találatokra pazarolják el az időt.
Incidensek. Gyakran történnek olyan események, melyek egyenként szemlélve elszigeteltnek és összefüggéstelennek tűnhetnek. Az incidensek bekövetkezése összefüggést teremt az események között, így a rendszer biztonsági felelősei észlelhetik azokat. *Egy incidens egy vagy több, az elfogadható kockázati mérték megtartása érdekében beavatkozást és lezárást igénylő védelmi eseményből vagy körülményből áll.*
Incidens lehet:
- jelentős, az üzletet veszélyeztető és beavatkozást igénylő fenyegetések
- nap mint nap előforduló helyzetek, amelyek csak *elhanyagolásuk* esetén veszélyesek az üzletmenetre.

Néhány példa az egy vagy több eseményből álló incidensre:
- nagymértékű vírus- vagy féregfertőzés
- szolgáltatás leállása
- egy alkalmazott visszaélése a rendszeren
- támadásérzékeny alkalmazások futtatása a rendszeren

Hatékony incidenskezelés

A sok, egymáshoz kapcsolódó eseményt (támadást, sérülékenységet, szabályzatsértést) mindig együtt kell szemlélni ahhoz, hogy felfedezzük az incidenst.
Nem az a kérdés, hogy találkozunk-e incidensekkel, hanem az, hogy ez mikor következik be.

A Symantec Incident Manager

A nagy hálózattal rendelkező vállalatoknál naponta nagy tömegű védelmi esemény jelentkezik. A teljes bejövő adatmennyiség áttekintése nehéz feladat; ezen a ponton tud segíteni a *Symantec Incident Manager*. A Symantec Incident Manager összevonja a több gyártótól származó különféle egyedi termékek által jelzett védelmi eseményeket, felismeri a fontossági sorrendet, és nyomon követi az incidenseket azok lezárásig. ■

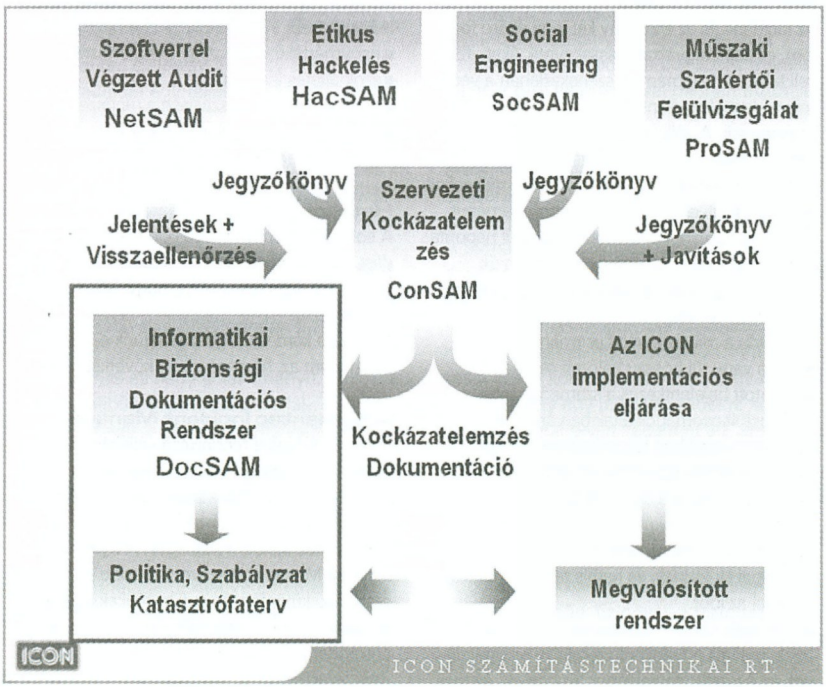
Platypus

Az ICON Intelligens etikus hackelés szolgáltatása

IT-biztonság napjainkban

Napjainkban sajnos a biztonság kérdése már nem elvont fogalom. Elég meghallgatni a híreket, böngészni az interneten, számos riasztó hírt találunk nap mint nap. Sok intézmény, vállalat időben reagált a külső fenyegetettségekre, fizikai biztonságát videós megfigyelőrendszerrel, riasztó- és tűzvédelmi rendszerrel erősítette meg.

Látható, hogy számos helyen az emberi erővel való védelemnek is jelentős teret adnak. Ezek azonban a lehetséges támadásoknak csak kisebbik, elsősorban a fizikai részét akadályozzák meg. Ezzel szemben az informatikai rendszert, melyet a korábbiakhoz képest sokkal több támadás érhet, ezzel a módszerrel nem sok sikerrel védhetjük. Ráadásul a támadások jelentős része a statisztikák szerint belülről, a felhasználók akaratlagos vagy véletlen tevékenységeiből indul. Egyes irodalmi adatok szerint az okozott károk több mint négyötöde ilyen, belső károkozásból származik. Az informatikai iparágra vetített változások már ma szemmel láthatók.
Az üzleti folyamatokat ma már nem lehet elvá-



lasztani a hozzájuk rendelt információtechnológiai struktúrától. Az informatikai eszközök, rendszerek kiesése az egyes intézményi feladatok ellátásának megszűntét okozza. Az e-mailt már nemcsak emlékeztetők és feljegyzések küldésére használjuk, hanem szerződések, gazdasági információk, értékkel bíró dokumentumok továbbítására is. Minőségi változás következett be: míg korábban a kereskedelemben főleg cégismertetők, prospektusok terjesztésére használták a világhálót, ma a web egyre több helyen kínál elektronikus kereskedelmi (e-Commerce) funkciókat is.

Az ICON Rt. – a KFKI Számítástechnikai csoport tagja – közel öt éve hozta létre önálló IT-biztonsági üzletetágát, amely a piaci igényeket követve, töretlen lendülettel növekedve mára a honi biztonsági piac meghatározó szereplőjévé nőtte ki magát. Szakemberei számos komplex projektnek köszönhetően jelentős rendszerintegrátori tapasztalattal, valamint referenciával bírnak mind a kormányzati, mind a versenyszektorban.

Az elmúlt két évben a statisztikák szerint minden ötödik vállalat jelentős anyagi kárt szenvedett informatikai biztonsági problémák következtében. A megkérdezett nagyvállalatok döntő többsége, 90%-a úgy vélte, hogy az elmúlt egy év során csorba esett informatikai rendszerének biztonságán, 80% pedig elismerte, hogy a rendszerében lezajlott hacker tevékenység anyagi kárral járt. 2002-ben is a webkiszolgálók voltak az internetes kalózok kedvenc áldozatai: a megkérdezettek 38%-a tapasztalt valamilyen, a webszolgáltatást fenyegető támadást.

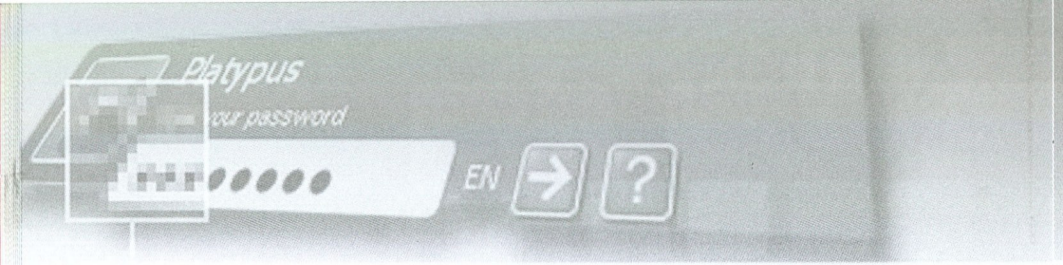
A fentiek ismeretében cikkünkben megpróbálunk rávilágítani az IT-védelem globális egészére úgy, hogy különböző részeit – úgymint egy vállalat vagy intézmény biztonsági szintjének értékelése, a biztonsági rendszer tesztelése, ellenőrzése, különböző eljárások és eszközök, távfelügyelet és egyéb eljárások – kiemeljük, és ezeken keresztül értelmezzük a komplex feladatot.

Hogyan értékeljük a rendszer biztonságát?

Az informatikai rendszer biztonságának értékelése azért komplex feladat, mert a rendszer más jellemzői érdeklik a rendszer üzemeltetőjét és más az ügyvezető igazgatót. Ahhoz, hogy megfelelő döntés születhessen a biztonsági fejlesztésekről, esetleg a biztonsági funkció vállalaton kívülre való helyezéséről, célszerű pontos képet alkotni a pillanatnyi helyzetről. Ez a tevékenység a biztonsági vizsgálat, átvilágítás (idegen szóval: audit), amit ma még szinte mindenki másképpen értelmez. Az informatikai biztonsági vizsgálat módszeres és független ellenőrzés annak a meghatározására, hogy az informatikai infrastruktúra és a kapcsolódó eljárások milyen formában és mekkora hatékonysággal szolgálják a biztonságos üzletvitelt. A biztonsági vizsgálat elsődleges követelményeit a módszertani megközelítés – az ICON egyéni módszertanában felhasznált BS7799, Common Criteria –, a megtervezett, széles körű és koordinált lebonyolítás, illetve a függetlenség, azaz a semleges bizatonsági szakértők és a független kritériumok jelentik. Ez nemcsak azt jelenti, hogy tárgyszerű eredményt kapunk, hanem az eredmény más eredményekkel – például egy korábbi időpontban készülttel – össze is hasonlítható.

Mit tartalmazzon egy informatikai biztonsági vizsgálat?

Ahány feladatkör, annyiféle válasz létezik erre a kérdésre. Az ICON létrehozta a jól



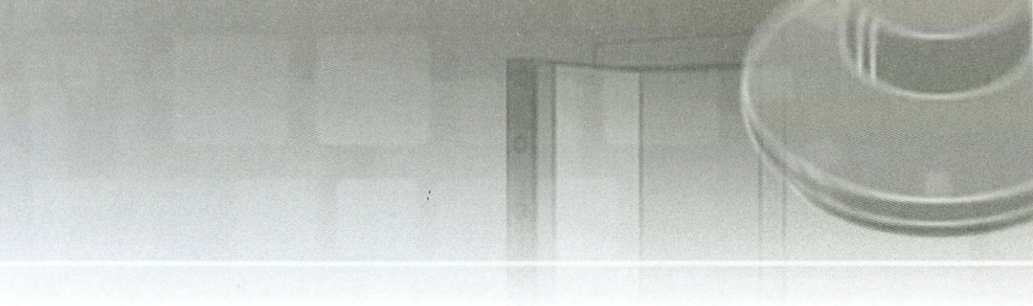
dokumentált SAM Secure Audit Methology programot, amely valójában hosszú évek tapasztalatára épülő módszertan. A program a megközelítés módja és célja szerint több (önmagában is megálló) szolgáltatásból áll. Az első lépésben a rendszer biztonságának és kockázatainak felmérése a feladat, ennek részei a következők:

- Szoftverrel Végzett Felülvizsgálat
- Műszaki Szakértői Felülvizsgálat
- Kockázatelemzés

A következőkben vizsgáljuk meg a három szolgáltatást kicsit alaposabban.

Szoftverrel Végzett Felülvizsgálat

Az informatikai erőforrások sérülékenységei széles skálán mozognak, ezért a biztonsági lyukak felfedezésére olyan szoftvereszközök szükségesek, amelyek módszeresen és célirányosan keresnek sérülékeny pontokat, és ezekről riportok formájában számolnak be. Könnyen belátható, hogy csak az ismert hibák, sérülékenységek meglétének ellenőrzése manuális eljárással sok időbe telik. Az ICON a szolgáltatások elvégzéséhez a többéves biztonsági tapasztalatok alapján kialakított NetSAM nevű szoftveres felülvizsgála-



ti módszertant alkalmazza, így olyan képet kap az informatikai rendszerről, amilyennel egy jól felkészült támadó is találkozik. Megvalósításának az alábbi lépései vannak:

- felmérik az adott informatikai hálózat erőforrásait és felépítését.
- minden egyes előzőleg kijelölt informatikai erőforrást (például router, szerver, ügyfélgépek, hálózati kapcsolók stb.) szoftverrel átvizsgálnak.
- a szoftver által automatikusan készített sérülékenységi jelentést kijavítják, lefordítják magyar nyelvre
- a jelentésből levonják a megfelelő következtetéseket
- a Szoftverrel végzett felülvizsgálat eredményei angol nyelvű jelentések és azok kiértékelt, tömörített magyar nyelvű változatai.
- a szakértők feladatai többrétűek, többek között kijavítják a téves észleléseket, rangsorolják a sérülékenységeket, az eredményt összevetik más hasonló tesztek eredményével, végül következtetéseket vonnak le az adott informatikai erőforrás sérülékenységére nézve.

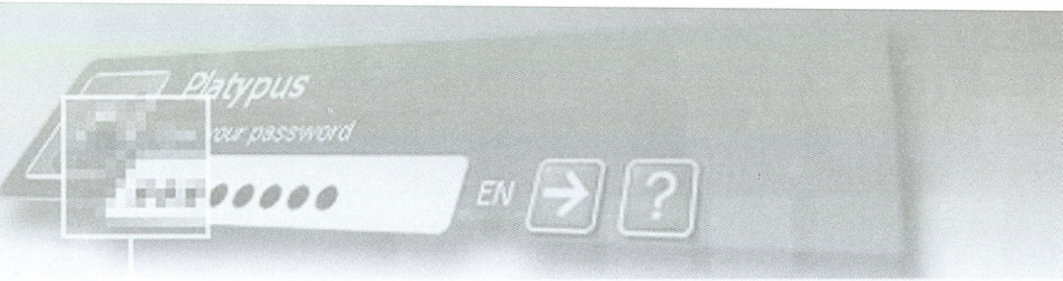
Műszaki Szakértői Felülvizsgálat

Az ICON szakemberi az informatikai rendszerelemek állapotát biztonsági szempontból illetve rendszeradminisztrátori nézőpontból értékelik. A valós folyamatokat, az alrendszerek állapotát és a rendszerelemek tényleges beállításait összevetik az üzemeltetési dokumentációkban foglaltakkal és az általános üzemeltetési szokásokkal. A felülvizsgálat többéves szakmai tapasztalatokra és az ICON ProSAM módszertanára épülve, részletes ellenőrzőlisták alapján történik, amelynek során felhasználják a korábban esetleg végrehajtott Szoftverrel Végzett Felülvizsgálat eredményeit is. A rendszer tehát használható a Szoftverrel Végzett Felülvizsgálat nélkül is, természetesen célszerűbb együtt alkalmazni. Így olyan képet kapnak a rendszerről, ami megmutatja az informatikai szempontból ideális állapothoz képest tapasztalt eltéréseket.

Érdemes megvizsgálni a megvalósítás lépéseit is. A Műszaki Szakértői Felülvizsgálat során egy vagy több szenior (vezető) rendszermérnök valós működési körülményeik között (üzemelés közben) felülvizsgálja a rendszerelemeket informatikai biztonsági szempontból, az észlelt hiányosságokról jelentést készít, illetve javaslatokat tesz a rendszerek biztonságot növelő beállításaira, és dokumentálja azokat. Szükség, illetve igény esetén a dokumentált javaslatok alapján az ICON szenior rendszermérnöke a módosításokat végre is hajtja a rendszerelemen, majd a módosításról jegyzőkönyvet készít.

A műszaki Szakértői Felülvizsgálat a következő informatikai infrastrukturális elemekre terjedhet ki:

Megnevezés	Megjegyzés
Internetkijáratok felülvizsgálata	Router, tűzfal, web, proxy, ftp, mail kiszolgálók
Egyéb hálózati eszközök vizsgálata	Routerek, switchek, intelligens HUB-ok
Szerverek vizsgálata	Windows NT 4.0, Windows 2000, Novell, Linux, UNIX, AS/400, VMS, AIX



A Műszaki Szakértői Felülvizsgálat eredménye egy jegyzőkönyv, amely tartalmazza a talált problémák javasolt megszüntetési módjait.

Kockázatelemzés

A Kockázatelemzés a szervezet ügyvitele szempontjából kritikus üzleti folyamatokra és az azokat kiszolgáló informatikai eszközökre, szolgáltatásokra terjed ki. Célja, hogy pontos képet kapjunk az ügyfél üzletmenetének biztonságát fenyegető informatikai eredetű veszélyekről. Az ICON a szolgáltatások elvégzéséhez az interjúk, konzultációk során a British Standard 7799, Common Criteria nemzetközi módszertanok, valamint a többéves biztonsági tapasztalataink figyelembevételével kialakított saját módszertanát alkalmazza. Így olyan képet képes alkotni a vállalatról, amilyet egy informatikai biztonságban nem járatos menedzser fel tud használni a továbbfejlesztéssel kapcsolatos pénzügyi döntéseihez.
Az Üzleti Kockázatelemzés megvalósításának több fontos lépése van, lássuk most ezeket.

Helyzetfelmérés
Az informatikai biztonsági helyzetfelmérés kiterjed azokra az üzletileg kritikus rendszerelemekre, amelyek biztonságát a későbbiekben garantálni kívánják annak érdekében, hogy ezek sérülése vagy hiánya az üzleti tevékenységet ne akadályozza, vagy ne veszélyeztesse, illetve ezekből illetéktelen kezekbe információ ne kerülhessen.
A helyzetfelmérés során a következőket vizsgálják:

- vállalati eljárások, szabályok, standardok; rendszeradminisztrációs eljárások;
- alkalmazások és az általuk kezelt adatok;
- kritikus üzleti folyamatok;
- változások kezelése;
- dokumentációs rendszer;
- katasztrófatervek;
- fizikai környezet és biztonsága;
- oktatás, képzés

Veszélyforrás-elemzés
Fel kell tárni valamennyi elképzelhető veszélyforrást, fenyegető tényezőt, amelyek kárt okozhatnak az informatikai rendszerben, és ezzel az alkalmazásban vagy az adatokban. A kockázatelemzés ennek a tevékenységnek az eredményeire épül.

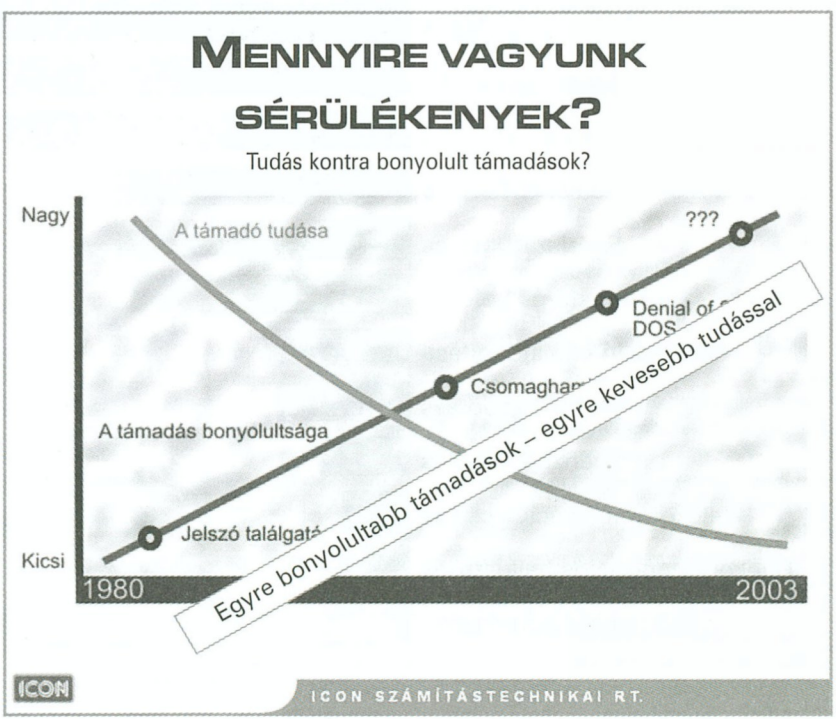
A kockázatelemzés
A feltárt fenyegető tényezőket lehetséges kihatásaik szempontjából értékelik (veszélyforrások által bekövetkező lehetséges biztonsági események gyakorisága és kárértéke), és ebből határozzák meg a fennálló kockázatokat.

Cselekvési terv készítése
A Kockázatelemzés eredménye a kockázatelemzés dokumentációja és a cselekvési terv, amelyből kiindulva meg tudják határozni a biztonsági rendszer kívánt állapotát. Rendszerint közös workshop keretében értékelik az eredményeket, és ekkor választják ki a cselekvési tervből megvalósításra érdemes projekteket is.

Belső szabályozás

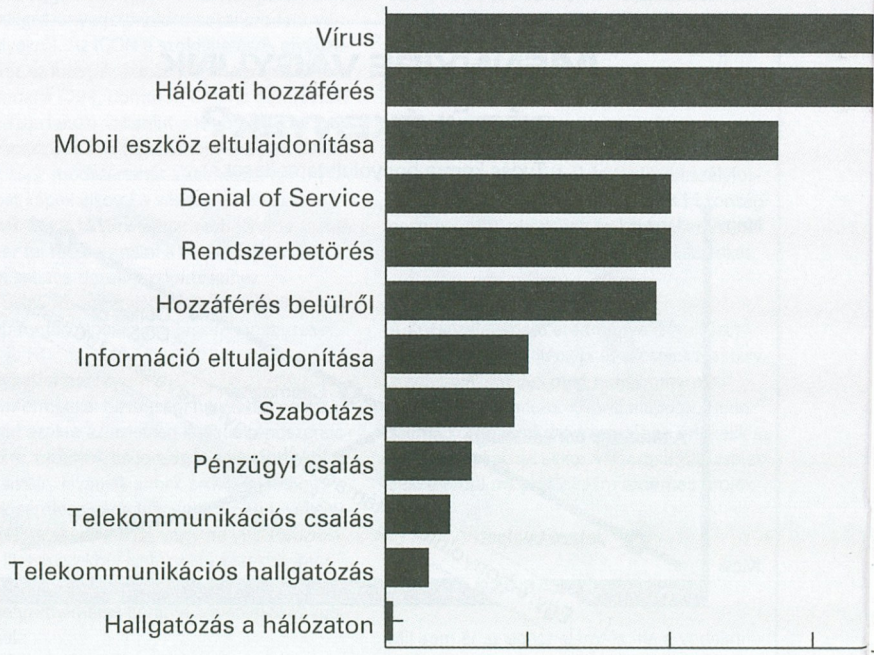
Mit sem ér az egész elemzés, ha a védelmi rendszert bevezetni szándékozó intézmény vagy vállalat nem alakít ki saját belső előírásokat a biztonságos működésre. Az első lé-

pés ezen a területen a *belső informatikai biztonsági politika* meghatározása. Ennek része, hogy a szervezet legfelsőbb vezetése elfogadja és betartassa az irányelveket, azaz deklarálja a vezetői elkötelezettségét, tegyen konkrét intézkedéseket a biztonság megteremtésére, fektesse le az általános irányelveket, definiálja az informatikai szereplők jogait, feladatait és hatásköreit, végül tegye mindezt mindenki számára ismertté és kötelezővé. Mert mit ér a legjobb, legkorszerűbb eszköz, ha használatát nem szabályozzák? Hiába ruháznak be egy hatékony tűzfalba, ha boldogboldogtalan állítgathatja a paramétereit. Mint tudjuk, aminek sok gazdája van, annak nincs gazdája. Nem lesz senki, aki tudná az összes paraméterről, hogy miért van éppen az, és éppen úgy beállítva. A jogok, hatáskörök és feladatok definiálására jó példa, hogy szabályozni kell, ki és hogyan vehet fel új felhasználót az informatikai rendszerbe. Természetesnek tűnik, hogy ez valakinek a joga és kö-

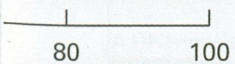


TÁMADÁSOK TÍPUSAI ÉS ELŐFORDULÁSI S

(Forrás: CSI/FBI 2002 Computer Crime and Security Survey
– Computer Security Institute



ZÁZALÉKUK



telessége, és hogy csak megfelelő írásos dokumentum alapján teheti meg; mégis vannak nem kis hálózatok, ahova többen, telefonon érkező kérés alapján vehetnek fel felhasználót.

Ugyancsak lényeges a belső informatikai biztonsági szabályzat kialakítása. Ebben célszerű lefektetni a rendszer biztonságához szükséges kontrollokat, kijelölni a részrendszerek felelőseit, azok feladatát, speciális szabályzatokat tervezni a kritikus rendszerekhez, végül egységes számonkérési és ellenőrzési szabályokat bevezetni.

Az előzőkben vázolt elméleti feladatok után lássunk egy példát arra, hogy miképp lehetséges hatékonyan ellenőrizni rendszerünket. Az ellenőrzéseket az ICON módszertana szerint négyféleképpen lehet elvégezni:

- NetSAM (szoftverrel végzett felülvizsgálat, melynek során a sérülékenységeket vesszük számba)
- ProSAM (lokális szakértői felülvizsgálat rendszeradminisztrátori jogosultsággal)
- HacSAM (etikus hackelés: a hibák jóindulatú feltérképezése és kihasználhatóságuk bizonyítása)
- SocSAM (a biztonság emberi tényezőinek felderítése)

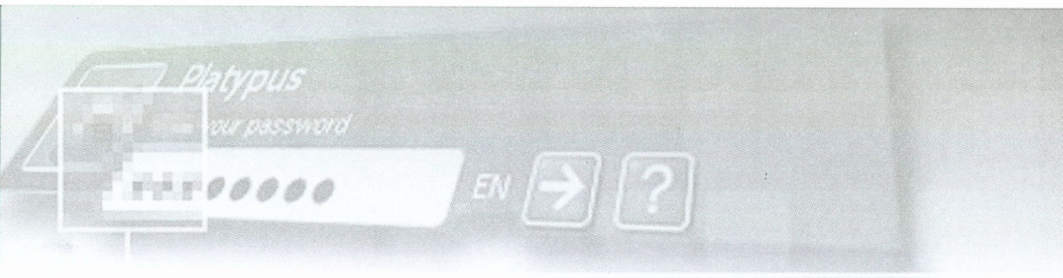
Ezek a szolgáltatások egymásra épülnek, de önmagukban is hasznosan bevethetők. Cikkünkben az egyik legérdekesebb és leglátványosabb módszertani elemet mutatjuk be, azaz az etikus hackelésre (HacSAM) fókuszálunk.

Az etikus hackelés

Mit is nevezünk etikus hackelésnek? A kissé misztikus elnevezés nem más, mint az informatikai biztonsági hibák jóindulatú feltérképezése, ezek kihasználhatóságának bizonyítása. De milyen módszerek és eszközök alkalmazhatók erre a feladatra? Az ICON Rt.-ben létezik egy csapat, amely etikus hack (nevezhetnénk etikus betörésnek is) tevékenységre specializálta magát. Módszereik és eszközeik teljesen hasonlóak azokéhoz, akik illegális módon próbálnak betörni egy hálózatba, gyakorlatilag egy (vagy több) behatolási kísérletet hajtanak végre. Amiben különbözik, hogy a célpont beleegyezésével teszik, és tapasztalataik alapján segítenek a rendszer biztonságát növelni. A háttérben az ICON által kifejlesztett HacSAM módszertan áll. Az alábbiakban a leggyengébb pontokat mutatjuk be, hiszen a vizsgálat is elsősorban ezekre irányul.

WEB és FTP szerverek sérülékenységei

A legelterjedtebb támadási formák a CGI (Common Gateway Interface) szkriptek sérülékenységeit kihasználó támadások. Komoly

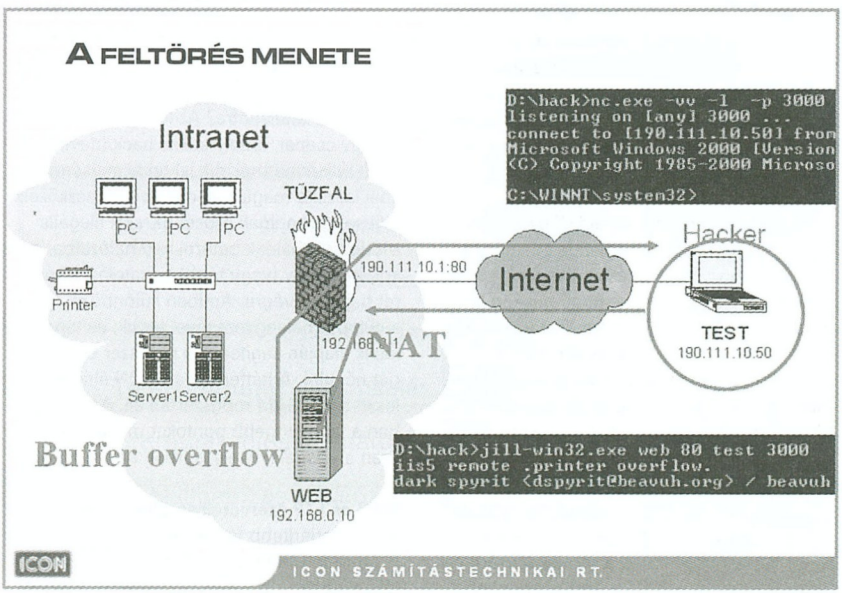


biztonsági rést jelentenek az alapkonfigurációval feltelepített mintafájlok, a mintaadatbázisok és a feleslegesen futó szolgáltatások is. A régebbi verziójú webkiszolgáló szoftverek könnyű prédának számítanak, ugyanis ezeknek a hibái közismertek, az összes informatikai biztonsággal foglalkozó honlap ismerteti. A hacker oldalakon pedig ezek kihasználására találunk részletes leírásokat.

Az FTP szervereknél tipikus hiba az anonymous login engedélyezettsége. A korábbi FTP-verziók jelentős részénél találtak olyan hibát, aminek segítségével anonymous felhasználóként DoS támadást indíthatunk a szerver ellen, s ennek eredményeképpen root jogosultságokhoz jutunk a rendszeren. Nagy kockázatot hordoz még a könyvtárszerkezet jogosultságainak nem megfelelő beállítása.

Trójai falovak keresése, elhelyezése, kihasználása. A trójai falovak segítségével átvehetjük az irányítást a célerőforráson, bármit megtehetünk, ami root/adminisztrátori jogosultságokkal lehetséges. Ahhoz, hogy trójai szoftvereket helyezzünk el egy rendszeren, elég egy létező buffer overflow támadást kihasználni, aminek következtében root/adminisztrátori jogokat kapunk az adott hoston.

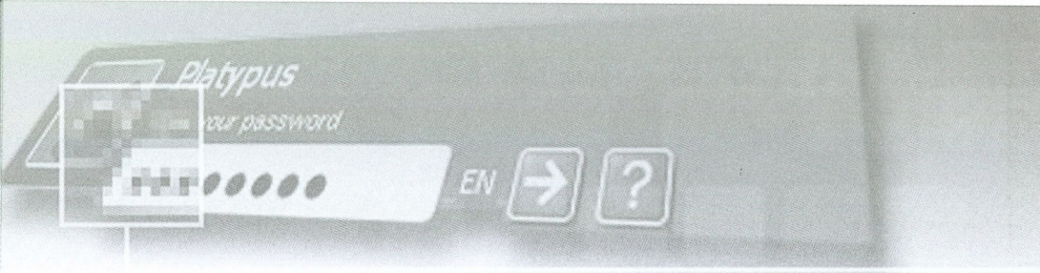
Jelszófeltörések. Különböző módszerek léteznek: password file megszerzése, hallgatózás a hálózaton, registry megszerzése, folyamatos próbálkozás szótár alapján vagy pedig úgynevezett brute force technika segítségé-



vel. Ez utóbbi azt jelenti, hogy a karakterek bizonyos kombinációit végigpróbáljuk. A jelszavak feltöréséhez többféle közkézen forgó szoftvert használhatunk.
A munkaállomásokra kötött modemeken keresztüli támadások. Telefonszám-tartományok végighívása, ahol az adatgyűjtő szoftver feljegyzi, ha a telefonszámon modem jelentkezett be. Ezek a támadások súlyos károkat okozhatnak, mivel a munkaállomásokon általában nincs komoly védelmi szoftver.
Vírusok. A régi boot, DoS, makrovírusok helyett ma már a különböző rendszerkomponensek, a levelező szerverek/kliensek, valamint a böngészők hibáit kihasználó kódok, trójaiak, férgek élik világukat. Sokszor szükségtelen a rendszer direkt feltörése, ha a rendelkezésre álló dedikált csatornákon (pl. levelezés, web-böngészés) a szükséges adatok (jelszavak, rendszerinformációk, konkrét állományok) kijuttathatóak. Egyes vírusok kifejezetten trójai programok bejuttatására specializálódtak.
Látható, hogy egy informatikai hálózat veszélyeztetettségét csak folyamatos felülvizsgálat segítségével lehet felmérni. Ezeknek a vizsgálatoknak nem szabad csak az internet felőli tűzfalakra, webszerverekre korlátozódniuk, hanem célszerű a teljes belső informatikai infrastruktúrára is kiterjeszteni őket. A felülvizsgálatoknak érdemes pontosan kidolgozott módszertanra épülniük.
Cikkünkben természetesen nem csak a vizsgálatokra és az ellenőrzésre mutatunk be módszereket, hanem kész megoldásokkal is szolgálunk.

A PKI-rendszer

Az ICON Rt. szállította, és integrálta az országban az első elektronikus aláírást biztosító kormányzati PKI (Public Key Infrastructure) rendszert a Belügyminisztérium Magyar Igazolvány szolgáltatásához, ahol kollégáik speciális rendszerintegrátori szemlélete segített a rendszer alkalmazás szintű integrációjában. Következőkben tekintsük át, a különböző alkalmazások miképp működnek együtt a PKI-rendszerrel:
E-mail titkosítás és digitális aláírás: a PKI-rendszer együttműködik az ismert és széles körben használt levelező szerverekkel és kliensekkel (például a Microsoft Exchange-el, az Outlook Express-szel, a Netscape Messangerrel vagy a Lotus Notesszal). Ugyancsak problémamentes az együttműködés a web hozzáférés során. Az internet-böngészők és a webszerverek PKI-rendszert alkalmaznak a hitelesség megállapításához, a bizalmasság megőrzéséhez és olyan alkalmazásokhoz, mint például az online-banking vagy az online-shopping. Adattitkosításra tipikusan Secure Sockets Layer (SSL)-t használnak. VPN (a hagyományos internetkapcsolaton is működő telephelyeket és felhasználókat összekötő virtuális privát hálózatok) esetében a PKI-technológia lehetővé teszi a titkosítást és a hitelesség megállapítását a nyilvános hálózatokban is. A távoli hozzáférés (RAS) esetén a PKI biztosítja a felhasználók azonosítását, és lehetőséget nyújt a VPN alapjául szolgáló, titkosított adatkapcsolat kialakítására. Fájlok, levelek digitális aláírásával, illetve titkosításával a letöltött programok vagy a megkapott levelek megbízhatósága jelentősen növelhető, mert ezek a technológiák lehetővé teszik a csomag érintetlenségének ellenőrzését.
Roppant fontos a védelem szempontjából a felhasználók azonosítása, azaz a hozzáférés-védelem: a munkaállomások, tartományok, alkalma-



zások korábbi jelszavas védelme számos esetben nem bizonyult elegendőnek. Ez smart-kártyával kiegészítve már eleget tesz a kétfaktorú felhasználóazonosítás követelményeinek, miszerint a biztonságos azonosításhoz „valamit tudni és valamit birtokolni" kell.
A jelenleg ajánlott, alkalmas technológiák:

Proxy interfész	Motorola, MIFARE, HID
PKI chip	Schlumberger, Oberthur - ICON HYDRA, ActivCard,
PKI szerveroldal	RSA Security Microsoft W2K, RSA KEON, Baltimore UniCert

Az előzőekben már tettünk említést az egyik legbiztosabb védelemről, az intelligens chipkártyáról, a továbbiakban ennek integrálásáról szólunk.

A beléptetőrendszer integrációja
A stabil működés olyan védett rendszert feltételez, amely képes garantálni a titkosságot, a hitelességet, a szabályozott hozzáférést, az adatok integritását és a letagadhatatlanságot. A digitális tanúsítvány és a nyilvános kulcsú kriptográfia alkalmazásával ezen elvárások mindegyikének eleget lehet tenni. A nyilvános kulcsú kriptográfia szervezeti szintű alkalmazásához ki kell alakítani

TERVEZÉSI FÁZIS ➡ **TÁMADÁSI FÁZIS** ➡ **JELENTÉSI FÁZIS**

Közös tevékenység

1. Jogalap megteremtése
2. Műszaki előkészítés
3. Katasztrófaelhárítási terv

Megrendelő tevékenysége

1. Mentés
2. Kritikus üzleti tevékenység meghatározása
3. Katasztrófaterv végrehajtása

ICON tevékenysége

Információszerzés
1. IT módszerekkel
2. Social engineeringgel
3. Egyéb módszerekkel

ICON tevékenysége

1. Hálózati forgalom elemzése
2. Támadott rendszerelemek típusainak felderítése
3. Web-, levelezőszerver sérülékenységek, konf. kihasználása
4. Buffer overflow
5. CGI exploit
6. DDOS támadások
7. Jelszómegfejtés
8. Modern pool támadás
9. Vírusteszt
10. Hamisított levél küldése
11. Hordozható számítógép vizsgálata adatszerzés
12. Információszerzés a szervezetben (Soc. E.)

Dokumentum:
- Információszerzés eredménye
- Támadások, eszközök listája
- Támadások eredményei
- Egyéb eredmények
- Talált sérülékenységek összefoglalása
- Megoldási javaslatok

Az eredmények prezentációja

a nyilvános kulcsú infrastruktúrát (PKI), amely a felhasználókra, az alkalmazásokra és a rendszerekre vonatkozó tanúsítványok és titkosítási kulcsok kezelését, elosztását segítő alapvető szolgáltatásokat biztosítja. Az utóbbi néhány évben a világ számos országában megtörtént e technológia jogi szabályozása – 2001-ben nálunk is. A törvényhozás által jóváhagyott szabályozó dokumentum a „2001./XXXV. Törvény az elektronikus aláírásról" címet viseli.

De hol kapcsolódik a fizikai biztonság az informatikai biztonsághoz? A kapcsolódás egyik pontja a kártya. A technológiai fejlődés lehetővé teszi, hogy a PKI-rendszerhez tartozó tanúsítványt és a hozzá tartozó kulcspárt egy rendkívül jól védett fizikai eszközön, smart-kártyán tároljuk. Az új technológia mára azt is megoldja, hogy ugyanazt a kártyát használjuk a fizikai beléptetőrendszerhez is. A kártya az úgynevezett hibrid kártya, mely egyszerre tartalmazza a beléptetőkártyához tartozó rádiófrekvenciás (proxy) interfészt (illetve mágnescsíkot) és a PKI csipet.

1999-ben az ICON kifejlesztette az ICON HYDRA smart card csomagot a Microsoft és a Schlumberger kártyagyártó cég segítségével. A termék második verziójának számos érdekessége és előnye van.

Az Oberthur kártyát használó HYDRA 2 többek között a fizikai kialakítása – az ultravékony kártya illeszkedik a hagyományos olvasókhoz, a külső réteg alkalmas személyes azonosítók felvitelére –, illetve elektronikus tulajdonságai – beépített közelítő chip az ajtónyitáshoz, Cryptochip a PKI funkciókhoz, EMV-kompatibilis chip az e-paymenthez, illetve JAVA-kompatibilitás a számos különböző alkalmazáshoz – a legkritikusabb védelmi rendszerek számára is optimális megoldást jelent.

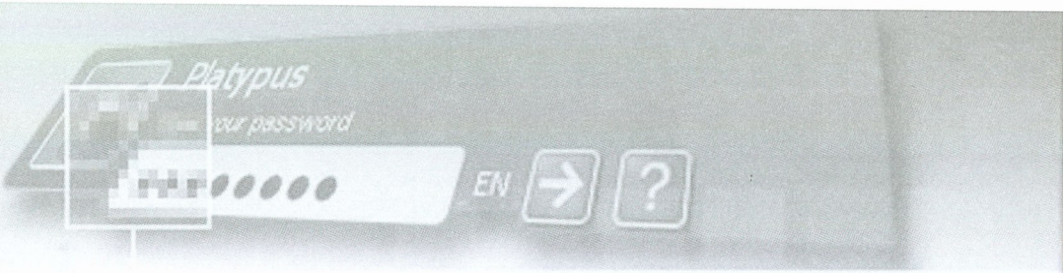
Nem tértünk még ki egy roppant fontos területre, a távfelügyeletre. Számos területen – bankok, közintézmények – rájöttek már arra, hogy a különböző védelmi rendszerek üzemeltetését nem célszerű és gazdaságos házon belül megoldani – gondoljunk csak a különböző őrző-védő szolgálatokra –, hanem érdemesebb azt külső, erre a területre szakosodott cégre bízni. Az IT-biztonság esetében ezt a távfelügyelet jelenti.

Az ICON-nak erre is van kész megoldása.

Hatékony módszer – a távfelügyelet

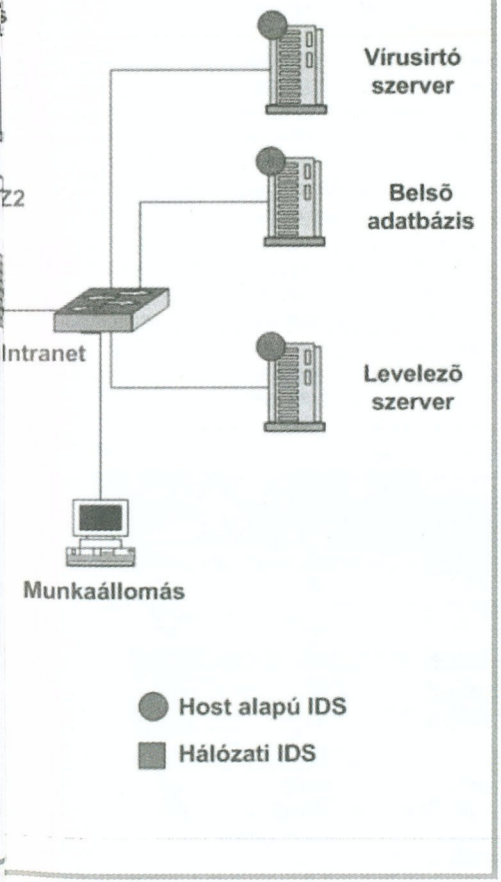
Az elmúlt hónapokban számos, „SP-re végződő" szolgáltatásról lehetett hallani. Összesítve ezeket a szakma xSP-knek nevezi, ideértve az ASP, MSP és egyéb titokzatos rövidítésű szolgáltatásokat. Ezek közül az ICON különösen ígéretesnek tartja a *menedzselt informatikai biztonsági szolgáltatásokat.* Míg a „hagyományos" ASP modell ugyanis a korábbiakhoz képest egy forradalmi váltást feltételez a vállalatok részéről – nevezetesen azt, hogy irodai és egyéb kulcsalkalmazásaikat külső szolgáltatótól béreljék – a menedzselt biztonsági szolgáltatások (angol rövidítéssel MSSP- Managed Security Services Provider) csak egy szűk szakterületet fednek le, ráadásul épp azokat, melyeket a legtöbb vállalat nem tekint kulcs kompetencia területének. Ilyenek például:

- 7x24 biztonsági felügyelet és biztonsági rendszer menedzsment
- tűzfalak szabályrendszerének menedzselése
- azonnali incidenskezelés



TIPIKUS TÁVFELÜGYELETI RENDSZER

Vázlat 1.0



- a menedzsment számára készülő rendszeres biztonsági jelentések
- periodikus sérülékenység elemzés
- vírusminták naprakészen tartása
- rendszeres vizsgálatok

Az MSSP modell gyakorlatilag egy eszközökkel és képzett szakemberekkel jól ellátott távfelügyeleti központ, amely úgy alakítja ki szolgáltatásait, hogy azok megoszthatóak legyenek az ügyfelek között. Az ICON és ügyfelei között precíz SLA (Service Level Agreement) szabályozza a szolgáltatás minőségét.
Az SLA-nak több előnye is van. Egyrészt lehetővé teszi, hogy a szolgáltatóra jóval nagyobb felelősséget ruházzanak, mint egy átlagos biztonsági alkalmazottra.
S mivel az SLA csak dokumentált eljárásokra, eszkalációs utakra épülhet, sok vállalatnál már az is nagy előny, ha ezeket az eljárásokat az SLA megkötésekor végre egyszer alaposan átgondolják. Az ICON ezt a folyamatot egy szabványos környezettanulmány elkészítésével kezdi, amely már önmagában nagy értéket jelent az informatikai rendszerének biztonsági állapotáért aggódó cégvezető számára.
Van néhány olyan hajtóerő, amely az MSSP piac erősödésének irányában hat, például egyre több felhasználó egyre bonyolultabb informatikai alkalmazást használ, s egyre több üzleti folyamat épül az internetre és az informatikára. Ezek együttesen egyre több és komplexebb fenyegetettséget jelentenek. Ide sorolható a magas szintű szakértelem általános hiánya (sok kisebb vállalat egyáltalán nem képes önálló informatikai biztonsági szakembert megfizetni. Ugyanakkor egyre több vállalat működése függ az informatikai

rendszerektől), az informatikai biztonság, mint szakterület „töredezettsége" (azaz túl sok mindenhez kellene érteniük a vállalati informatikusoknak, egy személy nem is lenne elegendő) a felügyeleti központok méretgazdaságossági problémái (7x24 órás felügyeletet ellátó központ kiépítése csak a legnagyobb vállalatoknak éri meg, az MSSP viszont ezeket az erőforrásokat képes megosztani ügyfelei között). Észre kell venni azt is, hogy a védelmi rendszerek az átlagos felhasználó számára áttekinthetetlenül bonyolultak és drágák.
Az eszközök megvásárlása helyett kezdenek tért hódítani a bérletszerű konstrukciók. („Mivel nem biztos, hogy két év múlva is ezt az eszközt használom majd, minek fektessem tehát ebbe a drága és gyorsan amortizálódó eszközbe a pénzem?") A védelmi rendszerek gyártói felismerték ugyan ezeket a problémákat, de a megoldásban csak odáig jutottak, hogy saját eszközeik távoli menedzselhetőségét megkönnyítették. Az ICON tapasztalata szerint legalábbis a különböző technológiai területeken (a vírusvédelemtől kezdve a tűzfal technológiákon át a VPN-ig) ez volt az elmúlt egy év legfontosabb fejlődési tendenciája. Azonban a tipikus vállalat nem csak egyféle terméket használ, s a heterogén biztonsági rendszerek menedzselése a mai napig nem megoldott.
Az ICON a BME SEARCH biztonsági kutatólaboratóriummal közösen speciális távfelügyeleti rendszert fejlesztett ki, mely azért különleges, mert gyártófüggetlen, azaz szinte bármilyen meglevő védelmi eszközzel együttműködik, legyen az Checkpoint vagy CISCO tűzfal, McAfee vírusvédelmi rendszer, vagy csak egyszerűen a Windows beépített naplófunkciója. Terveik szerint a szoftvernek kiadják egy ingyenes, mindenki által használható változatát is. A vállalati felhasználók számára pedig havi átalánydíj ellenében a komplett felügyeleti szolgáltatáscsomagot kínálják. A szolgáltatás ára a felügyelt rendszer komplexitásától és az ügyfél által kiválasztott szolgáltatás szintjétől függ. ■

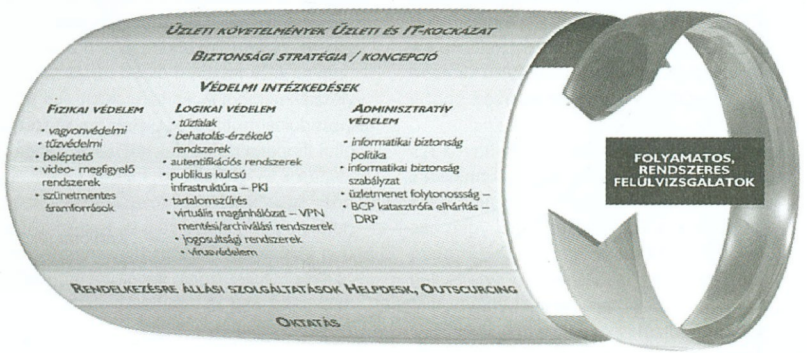
	Hydra2		
	Light	Classic	Deluxe
Windows 2000/XP logon	☑	☑	☑
E-mail digitális aláírása, titkosítása	☑	☑	☑
Távoli elérés és VPN csatorna	☑	☑	☑
Web felülethez azonosítás	☑	☑	☑
Web kapcsolat titkosítás SSL	☑	☑	☑
Web form aláírása	☑	☑	☑
File és Directory titkosítás			☑
File tárolás (meghajtóként)			☑
Statikus jelszó tárolás		☑	☑
Single SignOn	részben	részben	☑
Eurocar-Mastercard (EMV)	☑	☑	☑
Belső vállalati credit tárolás			☑
Ajtónyitás (fizikai beléptető)	☑	☑	☑

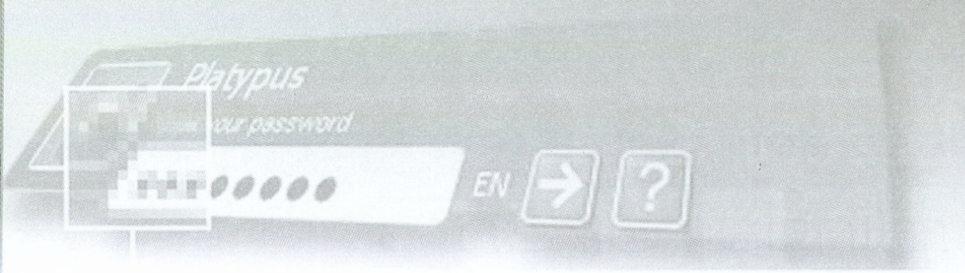
Biztonság minden síkon

Tudás alapú gazdaságunkban az információ a szervezetek legértékesebb erőforrása, tőkéje. Fizikai, pénzügyi értékeinkhez hasonló módon az információt is védenünk, biztosítanunk kell. A hagyományos értékek biztosításához hasonlóan az információbiztonsági kiadások is felesleges költségnek tűnhetnek mindaddig, amíg nincs baj. Utólag viszont már hiába sajnálkozunk azon, hogy mennyivel olcsóbb lett volna a megelőzés és a védelem.

A vállalati rendszerek megtervezésében, kiépítésében és üzemeltetésében alapteényezővé vált a rendszerbiztonság. Az erről való gondoskodás többrétű feladat, ezért beszél a Synergon „360 fokos" biztonságról.
A logikai védelem hardveres és szoftveres védelmi megoldásokból, tűzfalakból, vírusfigyelő rendszerekből, behatolásjelző alkalmazásokból áll; a fizikai védelem pedig fizikai eszközökkel szabályozza a védendő rendszerekhez való hozzáférést. A biztonság harmadik területe az adminisztratív védelem: ez határozza meg az informatikai üzemeltetés munkarendjét, az esetleges vészhelyzetekben elvégzendő feladatok sorrendjét, s ehhez a területhez tartozik a cég informatikai politikájának meghatározása is.
Az informatikai biztonsághoz vezető lépésekből az első a kockázatelemzés: a védendő rendszer jellemzőinek meghatározása, a jellemzőkhöz illő, és a sajátságos igényeknek is megfelelő konkrét megoldások kiválasztása. Emellett szükség van az üzemeltetők és a felhasználók megfelelő szintű oktatására, a telepített eszközök, megoldások folyamatos frissítésére és a teljes rendszer auditálására is.

Mivel a tökéletes védelem ára végtelen, így a cél nem is a tökéletes, hanem az optimális biztonsági szint elérése, melyet a különböző kockázati tényezők potenciális kárértékeinek és a megelőzéshez szükséges intézkedések költségeinek gondos mérlegelése alapján kell kiszámítanunk. A megfelelően átgondolt információbiztonsági kiadások tehát jó pénzügyi befektetésnek tekinthetők.



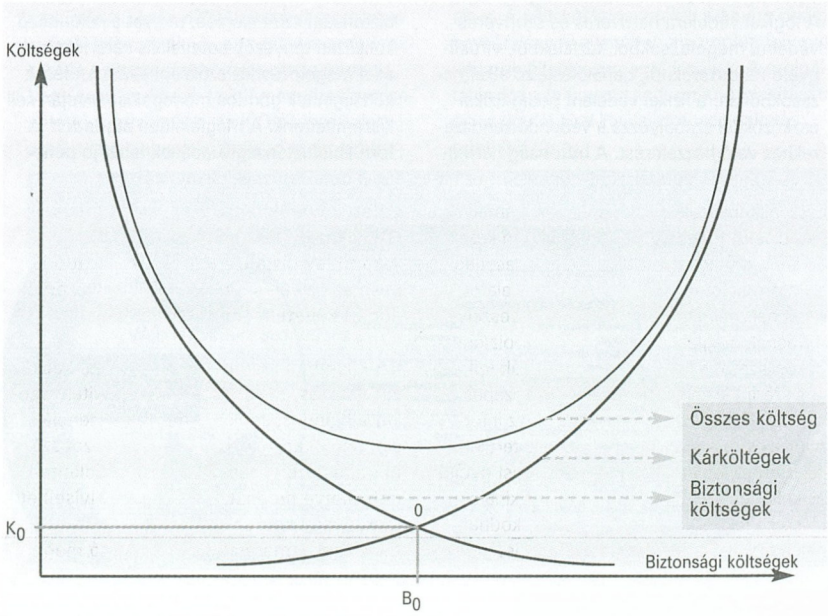


Elérhető biztonság

Az ügyfél tevékenységének alapos megismerése nélkül bajos valóban teljes körű és költséghatékony biztonsági megoldást kiépíteni. S az alapos megismeréshez a biztonság kérdését üzleti oldalról kell megközelíteni.
A Synergon is ezt az irányzatot követi, s az ügyfélcég munkájához pontosan hozzáigazítja a megfelelő biztonsági követelményeket és megoldásokat. Szakértői első lépésként átvizsgálják az ügyfél mostani informatikai rendszerét, majd ellenőrzik a rendszerből a napi működésben kinyerhető adatokat, hogy vajon valódiak és megbízhatók-e. Végül ellenőrzik az információkat elérők körét – hogy az adatokhoz valóban csak azok férhessenek hozzá, akiknek a munkájához ez szükséges. A vállalati rendszerek fejlődése miatt a Synergon megvizsgálja a megrendelő rendszereinek teljes biztonsági életciklusát is, hiszen a támadók módszerei is folyamatosan fejlődnek.

Az információval járó kockázat

A vállalkozás szempontjából kétségkívül az információ a legfőbb érték; a versenyelőny megszerzéséhez és megtartásához folyamatosan és biztonságosan kell működnie az információs rendszernek. Ehhez azonban azt is pontosan tudni kell, hogy az adatok és a rendszerek közül mit kell megvédeni és hogyan. Megfelelő forgatókönyvet kell



Siker Macedóniában

A Matáv tulajdonába került macedón Maktel telekommunikációs vállalatban a Synergon végezte el a teljes informatikai rendszer biztonsági felmérését és fejlesztését. A Compaq 2001 végén kérte fel erre a feladatra. 2002 januárjában, az előzetes megbeszélések sikeres lezárulta után a Synergon szakemberei – a Compaq minőségbiztosításával – megkezdék Szkopjében a munkát.

Az egyik feladatuk a Maktel teljes informatikai rendszerének átvilágítása volt; a vegyes eszközparkot üzemeltetési kontroll és biztonsági kockázatok szempontjából is meg kellett vizsgálniuk. A helyi szakemberek folyamatosan fejlesztették az egymástól elszigetelten működő s egymással nehezen kommunikáló szigetrendszerek helyébe lépő integrált rendszereket. A felmérések szerint azonban az informatikai biztonsági intézkedések nem voltak egységesek, csak ötletszerűek, inkább csak műszaki kérdésekre szorítkoztak, s nem terjedtek ki az adminisztratív szabályozásra. Az eredeti, 38 aktívan használt alkalmazást például később még ki kellett egészíteni az informatikai részlegtől független vállalati egységekben használatos programokkal is.

A vizsgálatban a Synergon szakemberei jó néhány megbeszélést tartottak a csúcsvezetőkkel a vállalat üzleti és informatikai folyamatainak összefüggéseinek tisztázására. S ugyanilyen nagy feladat volt az informatikai rendszerek kockázatfelmérése is. A kockázatelemzésből adódtak később a Maktel által bevezetendő védelmi intézkedések, azokból pedig a vállalat Informatikai Biztonsági Szabályzata. A végeredmény két dokumentum volt: az első bemutatta a felmérések eredményét, a másik megfogalmazta a vállalat biztonsági szabályzatát. A Maktel szakemberei igen hasznosnak találták ezt a több mint 100 oldalas jelentést, s arra támaszkodva a helyi informatikai vezető már kidolgozhatta a továbblépéshez szükséges stratégiát.

összeállítani azokra a helyzetekre is, amelyekben elvész, megsérül vagy illetéktelen kezekbe kerül a megvédendő információ, esetleg az információt tároló rendszer válik valami miatt használhatatlanná. A többféle veszélyforrásnak megfelelően az információbiztonsági kockázatot a legcélszerűbb integrált felfogás szerint kezelni. Mivel a kis- és közepes méretű vállalkozások legtöbbjének az informatika csupán eszköz s nem munkaterület, azért érdemes a megfelelő tudásbázist gyűjtő és kellő technológiai megoldásokat kínáló külső cégekhez fordulni; ők gondoskodhatnak a fizikai és a logikai védelemről is.

Üzleti követelmények, avagy üzleti és IT-kockázat

A komplex biztonsági megoldás kezdő lépése az üzleti és a működési környezetből adódó **követelmények** azonosítása.

Ezt követheti egy üzleti/informatikai **kockázatelemzés,** melynek célja azonosítani azokat a hiányosságokat, amelyek potenciálisan nagy kárt okozhatnak a szervezet számára, és ezért magas kockázatot jelentenek, illetve meghatározni a még elviselhető maradvány kockázati értéket.

Csak ezek ismeretében valósítható meg

Szakavatott vizsgálódó

A CISA, vagyis a Certified Information System Auditor munkája éppoly felelősségteljes, mint egy pénzügyi auditoré. Neki kell megállapítania, hogy a vizsgált informatikai rendszer megfelel-e a felállított követelményeknek és szabályoknak. Az 1969-ben az Egyesült Államokban alapított ISACA több tízezer tagja közül 26 ezren szereztek CISA minősítést. Ennek a címnek a megszerzése nem könnyű feladat, hiszen négy óra alatt kétszáz kérdésre kell felelnie a vizsgázónak. A kérdések egyebek között a nemzetközi IT-auditálási szabályokat firtatják, azután az információvagyon kezelését és megőrzését, a katasztrófaelhárítást, a folyamatos üzletmenet fenntartását és az üzleti alkalmazások fejlesztését. A sikeresen letett vizsga öt évig érvényes, s a minősítéshez további ötéves szakmai gyakorlatot is igazolni kell. Az ISACA kreditrendszerrel ellenőrzi a továbbképzést, és ha a minősített személy nem gyűjt kellően sok kreditpontot, akkor megvonja tőle a minősítést.

a kockázatarányos védelem elve: optimális biztonsági költségek – megfelelő védelmi szint mellett.

A követelmények és a kockázatok ismeretében dolgozható ki a szervezet **információbiztonsági stratégiája és koncepciója,** amelyek az elérendő biztonsági célokat és a megvalósítás koncepcionális tervét tartalmazzák.

A következő lépés a **védelmi intézkedések** kidolgozása és szükséges kontrollok implementálása. Ezeket három csoportba soroljuk: fizikai, logikai és adminisztratív védelmi intézkedések.

Védelem fizikai szinten

A fizikai védelmi intézkedések **az információ feldolgozását kiszolgáló berendezések, helyiségek és az alkalmazottak védelmét szolgálják. Ilyenek például a vagyonvédelmi, a tűzjelző-, a beléptető- és a videomegfigyelő rendszerek vagy akár a szünetmentes áramforrások, védett kábelrendezők, klímaberendezések.**

Az információ nem csak elektronikusan, hanem fizikai mivoltában is sérülhet, ha megsérül, netán megsemmisül a hordozóeszköze. A sokféle fenyegetésnek megfelelően sokrétű lehet a fizikai védelem is. A vagyonvédelmi rendszerek a létesítményekbe való behatolást jelzik, az intelligens tűzjelző rendszer pedig – a különböző oltórendszerekkel együtt – a tűzkárok megelőzésében vagy csökkentésében jut szerephez. A megfigyelő videorendszer – folyamatos vagy csak változásra induló üzemmódban – feljegyezheti a megfigyelt területen történteket. A beléptetőrendszer a kialakított biztonsági előírásoknak megfelelően – ha kell, napszakonként és területenként – korlátozhatja a jogosultak belépését. A CMC rendszer az adatátviteli és adattároló szekrények működését ellenőrzi, s mivel saját IP-címe van,

azért a hálózat bármely pontjáról vezérelhető. A rendszerek távfelügyelete RS–485 protokollal, illetve telefonvonalon keresztül intézhető, s az események számítógépen rögzíthetők.

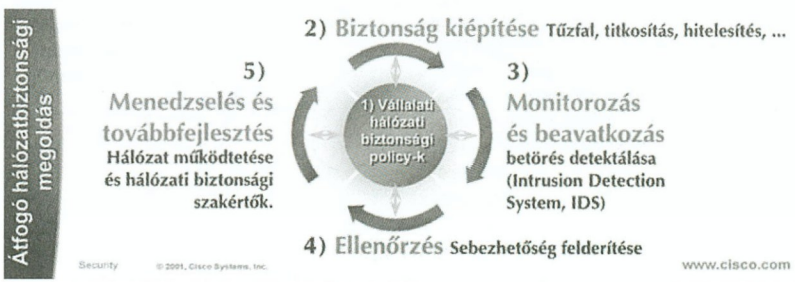
Résmentes védőgát

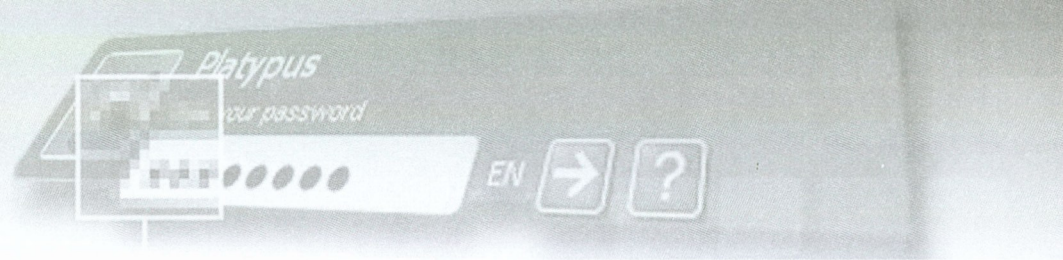
***A logikai védelmi intézkedések,* megoldások az adatok bizalmas kezelését, sértetlenségének megőrzését és folyamatos rendelkezésre állását biztosítják. Néhány példa a teljesség igénye nélkül: vírusvédelem, tűzfalak, behatolásérzékelő rendszerek, autentikációs rendszerek, publikus kulcsú infrastruktúra a digitális aláírás és titkosítás megvalósítására, tartalomszűrés, virtuális magánhálózat a bizalmas kommunikációhoz, mentési/archiválási rendszerek stb. Ide sorolható még a különböző rendszerszoftverek biztonsági követelményeknek megfelelő konfigurálása, illetve a biztonsági szabályzat szerinti jogosultsági rendszerek kialakítása, a nagy tömegű naplóadatok (logok) hatékony elemzésének megvalósítása.**

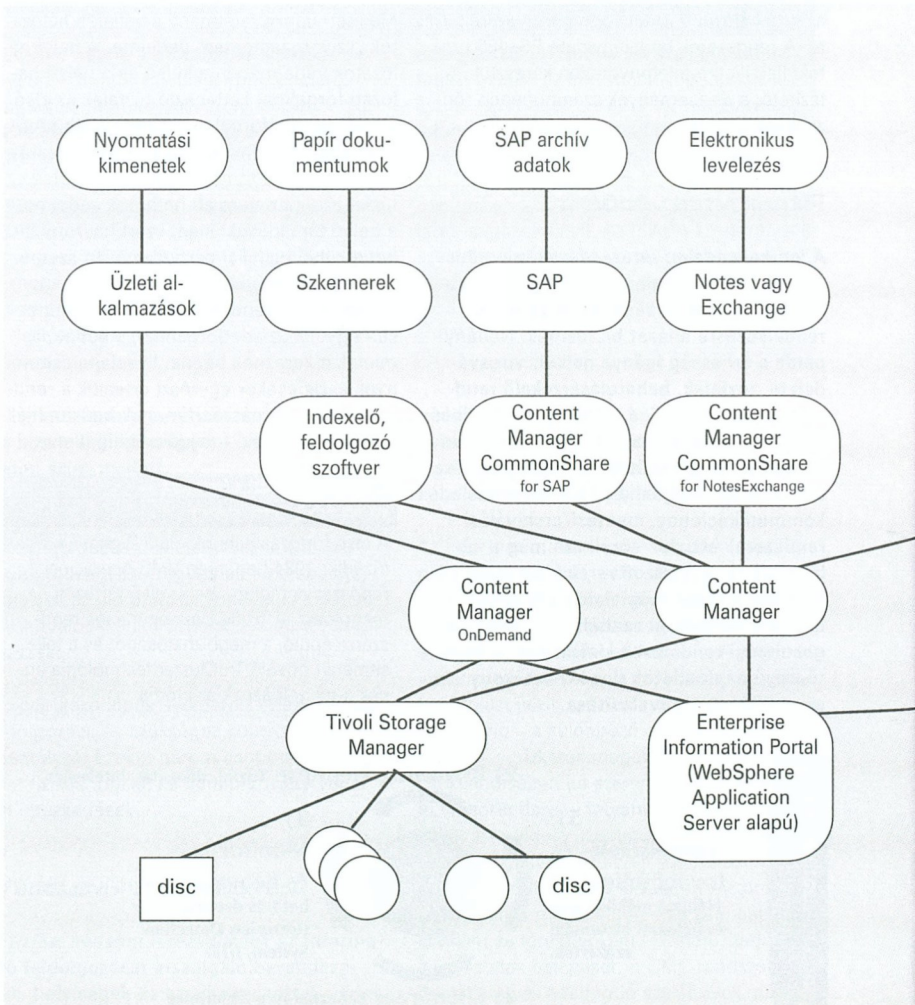
Ma már alapkövetelmény a vállalati hálózatok „szivárgásmentes" védelme. A helyi hálózatok védelmében a külső és a belső hálózati forgalmat kettéosztó tűzfalak az első vonal. Az adatforgalom szűrése több szempont szerint is elvégezhető, s ezzel jóval kisebbé tehető a támadási felület. A külső tűzfal azonban nem ad hathatós védelmet a belső támadások ellen, ezért hasznos lehet a külső tűzfallal párhuzamosan személyes tűzfalat is alkalmazni. A behatolásérzékelő rendszerek (IDS) folyamatosan figyelik az adatforgalmat, s behatolási mintákat keresnek benne. Ilyesfajta események észlelésekor egyrészt értesítik a rendszergazdákat, másrészt maguk beállíthatják a tűzfal megfelelő tulajdonságait, illetve

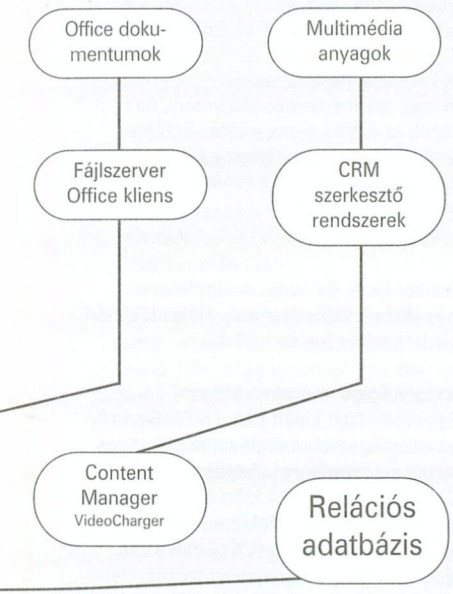
Compaq cluster – fürtözött erő

A első fürtözéstechnológia a Digital nevéhez fűződik: 1984-ben, még VMS operációs rendszerrel mutatta be az első fürtözött megoldást. A Tru64 Unix operációs rendszerre épülő, a megbízhatóságot és a teljesítményt növelő TruCluster technológia ennek a megoldásnak az utódja.




Platypus
EN

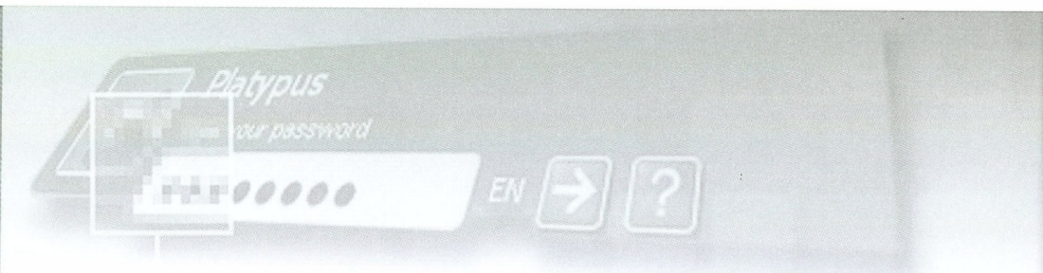

Nyomtatási kimenetek
Papír dokumentumok
SAP archív adatok
Elektronikus levelezés
Üzleti alkalmazások
Szkennerek
SAP
Notes vagy Exchange
Indexelő, feldolgozó szoftver
Content Manager CommonShare for SAP
Content Manager CommonShare for NotesExchange
Content Manager OnDemand
Content Manager
Tivoli Storage Manager
Enterprise Information Portal (WebSphere Application Server alapú)
disc
disc



megszakíthatják a kapcsolatot. A letapogató alkalmazások (szkenneralkalmazások) hasznos felvilágosítással szolgálhatnak a védendő rendszerek valós védettségéről; ezek az alkalmazások a másutt már felismert fogyatékosságokat keresik.
A technológiai megoldásoknál semmivel sem kevésbé fontos az emberi oldal: a felhasználók képzése, a gondoskodás a megfelelő eszközökről és a követelmények betartásának ellenőrzése. A megfelelő emberi és műszaki tényezők együtt tehetik csakugyan „jól záróvá" a vállalat informatikai rendszerét.

Védett pontok

Ahogyan az internet egyre fontosabb szerephez jut, a vállalat hálózati erőforrásait mind nehezebb megvédeni a külső és belső támadásoktól. A Synergon az izraeli Check Point Software Technologies megoldásaival kínál ügyfeleinek zökkenőmentes, mégis biztonságos kapcsolódást internethez, intranethez, extranethez. A Next Generation termékcsaládba tartozó Secure Virtual Network alkalmazások a távol dolgozó munkatársak csatlakozását figyelik, valamint a fiókirodák és a partnercégek extranetes hálózatainak csatlakozását. Az OPSEC nyílt biztonsági platform architektúrája révén a Check Point mintegy 300 cég integrált megoldásait is kezeli. A Firewall–1 csomag segítségével ugyanarról a felületről bonyolítható le a hozzáférés ellenőrzése, az érvényesítés, a titkosítás, a hálózati cím fordítása, a tartalombiztonság és az auditálás.
A Firewall–1-es kibővíthető az OPSEC-kerettel, s így együttműködhet harmadik fél által fejlesztett alkalmazásokkal.



Virtuális magánhálózat

A VPN (Virtual Private Network) vagy virtuális magánhálózat lehetővé teszi, hogy olcsó, nyilvános használatú hálózaton keresztül megfelelő biztonságú kapcsolatot alakítsunk ki.
Ekkor a két egymással kapcsolatban lévő végpont valamiféle erős titkosítással kommunikál egymással. Az olcsó átviteli eljárás, tipikusan a nyilvános internetkapcsolat nem tesz lehetővé biztonságos adatforgalmat, hiszen ahhoz sokaknak van hozzáférésük, lehallgathatják, megmásíthatják az üzenetet.
A megfelelő titkosítás lehetővé teszi, hogy az üzenetváltást, ha le is hallgatják, megérteni nem tudják, illetve az üzenetet ne lehessen módosítani, hamisítani.
Ezzel a két fél a nyilvános hálózaton egy virtuális csatornát hoz létre, aminek forgalmát csak ketten tudják értelmezni.
Tipikusan akkor érdemes alkalmazni, ha legalább az egyik kommunikáló végpont helye változik, a gyakorlatban ezek a noteszgéppel, távolról bejelentkező felhasználók.

Magánhálózat interneten át

Az internetes kapcsolatok és a vállalatai erőforrások ötvözésével kialakítható virtuális magánhálózat (VPN) költséghatékony és biztonságos kapcsolódási módszerrel szolgálhat. A virtuális magánhálózat a nyilvános internet adta lehetőségeket használja ki az otthoni és a mobil felhasználók bekapcsolására vagy távoli telephelyek, irodák összekapcsolására. Nem telefonhálózaton alapuló behívásra támaszkodik tehát, s nem is a telephelyek LAN-hálózata között kapcsolatot teremtő bérelt vagy Frame Relay-vonalakra, mint a hagyományos módszerek. A virtuális magánhálózat egyrészt kisebb költséggel jár, másrészt biztonságossá teszi az adatátvitelt; ezt a hagyományos módszerekkel. Nem lehetett elérni, vagy csak IPSec alkalmazásával. A VPN-re támaszkodó megoldások kiépítése rugalmasabb és gyorsabb is, és kapacitása könnyebben hozzáigazítható a mindenkori igényekhez. A Synergon az ügyfelek követelményeit felmérve optimális VPN-szolgáltatásokat kínál, és segíti az ügyfeleket a megoldás kiválasztásában, kialakításában és az integrálás folyamatában.

Biztonságos magánhálózat

A Synergon által kínált Cisco VPN Security Specialization technológiával biztonságos virtuális magánhálózat alakítható ki.
A Cisco berendezései között ott vannak az IPSec VPN-re és tűzfalfeladatok ellátására alkalmas útválasztók, a PIX tűzfalcsalád tagjai, biztonságfelügyeleti eszközök, behatolásjelző alkalmazás és VPN koncentrátor. Mindezeket az eszközöket a Cisco SAFE rendszere fogja össze egyetlen biztonsági architektúrába.
A VPN-kapcsolatnak egyebek között alapfeltétele a kommunikációban részt vevők elkülönülése a hálózat többi adatforgalmától, illetve az adatforgalom valamilyen rendszer szerinti titkosítása. A két feltételt a hagyományos IP-gerinchálózatokon nem lehet egyszerre kielégíteni. A Cisci IPSec VPN-ek révén azonban bármely médium-

mal létrehozható biztonságos magánhálózat – bérelt vonalon, betárcsázós kapcsolattal vagy kívülről csatlakozó internetes kapcsolattal. Az ügyfelek adatforgalmának megfelelően kis és nagy teljesítményű eszközök használhatók, s azok a már meglevő Cisco útválasztóknak szinte mindegyikén át létrehozhatnak IPSec VPN-eket.

Hálózati biztonság

A Synergon által kínált Cisco SAFE az egyik legkorszerűbb és legátfogóbb a ma piacon levő biztonsági megoldások közül; minden részletet ellenőrizhet és szabályozhat a hálózathasználatban.

A védett rendszerbe bejelentkező felhasználót a Secure Acces Control Server kétféle azonosítási móddal fogadhatja: hagyományos, névvel és jelszóval való azonosítással vagy a nagyobb biztonságot kínáló, egyszeri jelszavas, külső kiszolgálón át való azonosítással. A PKI alapú bejelentkezésről a Cisco stratégiai szövetségesei gondoskodhatnak.

A bejelentkezett felhasználó adatait a vállalati címtárból vagy az ACS saját adatbázisából lehet azonosítani. Az egyszer használatos jelszavakhoz megfelelő – Solaris vagy Windows alapú – kiszolgáló is szükséges.

A hálózati erőforrásokat a belső tűzfalak védik, idomulva az egyre gyakoribb belső támadások és jogosulatlan hozzáférésekhez. A Cisco PIX tűzfalak Intel alapon működő, PIX operációs rendszert és tűzfalszoftvert futtató célhardverek. A VPN-kapcsolatokat az IPSec alapú alkalmazások felügyelik, ezek az útválasztókon 1-2 megabit/másodperces sebességgel működnek, tűzfalakon 20 megabit/másodperces sebességgel. A rendszer finomhangolásáról és a behatolások felfedezéséről az IDS eszközök gondoskodnak.

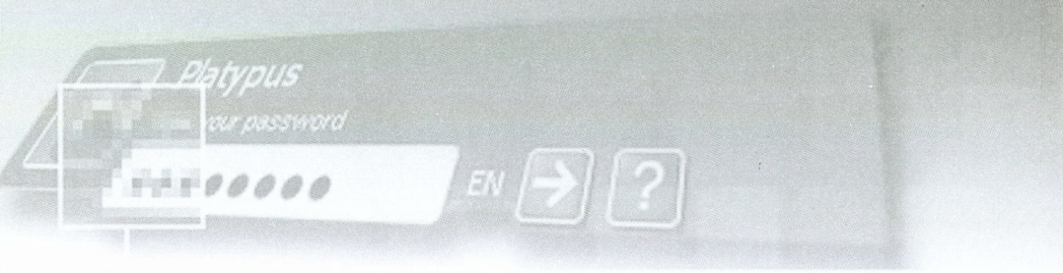
Integrált tartalom

A vállalatoknak igen fontos lehet, hogy integrálják az informatikai rendszerük különböző alkalmazásaiban keletkezett tartalmat; a mostani erős versenyben nem elég az üzleti alkalmazások által előállított és kezelt információkat csak magában az alkalmazásban elérni, hanem azokat egységesítve, egymással összekapcsolva is meg kell jeleníteni, különben a cég hátrányba kerülhet a versenyben. S ez az elektronikus dokumentáció mellett a papír alapú tartalom kezelését és archiválását is megköveteli.

A Synergon erre a meglehetősen összetett feladatra az IBM Content Manager alkalmazáscsomagját választotta. A különböző komponensek együtt teljeskörűen kezelik a papír alapú dokumentációt: elvégzik a szövegfelismerést és az indexelt archiválást, kezelik az elektronikus levelezésben található értékes üzleti információkat, kézi üzemmódban és – szabályrendszerre támaszkodva – automatikus üzemmódban is archiválják a leveleket. A CommonStore for SAP modul kezeli a vállalati SAP rendszerek üzleti adatait. A felhasználók az IBM Enterprise Information Portalon át érik el tárolt adatokat: a portálon egyetlen adatbázisnak látják a különböző rendszerekből kivont tartalmat.

KÖZÉPPONTBAN
AZ ADMINISZTRATÍV VÉDELEM

***Az adminisztratív biztonsági intézkedések* dokumentálják a biztonsági elvárásokat**



(informatikai biztonságipolitika), szabályozzák a biztonsági környezetet, meghatározzák a jogosultságokat, felelősségeket, a kötelezően elvégzendő és a tiltott tevékenységeket (informatikai biztonsági szabályzat). Nagyon fontos kiemelni a nem várt események kezelését célzó üzletmenet-folytonossági tervek jelentőségét, amelyek kidolgozásával a szervezet működőképes maradhat a legkülönbözőbb külső vagy belső incidensek fellépését követően is. Az adminisztratív biztonsági intézkedések bevezetésének elengedhetetlen része az alkalmazottak *oktatása* is, hiszen az intézkedések csak akkor fejthetik ki hatásukat, ha azokat a szervezet valamennyi tagja alkalmazza.

A vállalati informatikai rendszerek biztonságában igen fontos szerepet játszanak a megfelelő adminisztratív védelmi eljárások és módszerek. Ezek az egész védelmi elgondolást áthatják, hiszen az informatikai biztonsági szabályzat magában foglalja a különböző tartományokhoz (doménekhez) tartozó védelmi intézkedéseket, legyenek azok logikai vagy fizikai elemek. A Synergon tapasztalatai szerint a cégek nagy részének gyakorlatában ez meglehetősen elhanyagolt terület. Ahol vannak is (adminisztratív védelem), azok is általában valami sürgető esemény következtében keletkeztek, és ezért nem alaposan átgondolt, hanem ötletszerű megoldást jelentenek. Mint az ilyen megoldások általában, egy problémára egy adott pillanatban megfelelnek, de teljességében nézve nem teszik biztonságosabbá a rendszereket.

Az adminisztratív védelem szemléletmódja a gazdaságosságon alapul: aszerint a vállalatnak olyan szintű biztonságra van szüksége, amely egyrészt megfelelő az ár és teljesítmény viszonyát tekintve, másrészt gondoskodik a teljes rendszer átfogó védelmé-

Intelligens kártyás megoldás az OTP-nél

Az OTP Ingatlan Rt. egy összetett projektkezelő rendszert alkalmaz építési beruházásai és finanszírozási tevékenysége koordinálására és adminisztrálására.
Az internetes-intranetes megoldásban a rendszer megfelelő részeihez nemcsak az OTP Ingatlan Rt. munkatársai, de az ügyfelei is közvetlenül hozzáférhetnek a beépített jogosultsági rendszer engedélyezése alapján.
A helyi igényekhez tartozott annak megoldása is, hogy a projektek döntéshozói jogosultság szerint, biztonságos, egyedi azonosítási eljárás során léphessenek a rendszerbe. Így a döntési folyamat minden lépését rögzíti a rendszer, a döntések és azok következményei azonnal, valós időben jelenhetnek meg, ami azért fontos, mert egy-egy döntés esetenként több százmillió forint sorsát befolyásolhatja.
Az OTP-ben működő rendszer intelligens kártya alapján azonosítja a felhasználókat: a fejlesztők 50 kártyaleolvasót kapcsoltak össze az Oracle adatbázis-kezelőjével és a Microsoft hálózati rendszerrel. A száz felhasználót egy tanúsítványkiadó kiszolgáló fogadja, és ez év január 1-jétől már ki-ki helytől függetlenül jelentkezhet fel a rendszerre, s végezheti vele a munkáját.

ről. A kockázatelemzés – esetleg külső szakemberek bevonásával – megállapíthatja a különféle területek prioritási szintjeit, s azokhoz már hozzárendelhetők a szükséges ráfordítások is. Az alapbiztonság követelményrendszeréről való gondoskodás után kialakítható az igen fontos területeknek a szokásos szintnél erősebb védelme is.

Tűzfalat mindenkinek

A vállalatok adatvagyonának védelme lényegbevágó kérdés, és köze van a cég munkatársainak munkájához is. A legtöbb céget váratlanul érné az, ha egy elégedetlen dolgozó netán összegyűjtené az üzleti adatokat, terveket, stratégiákat, és eltávozna velük a konkurenciához. Az adatokat emiatt nemcsak a külső támadásoktól kell megvédeni, hanem a belső támadásoktól és hibáktól is, egyszersmind gondoskodni kell az adat folyamatos hozzáférhetőségéről és sértetlenségéről.

Az elemzések szerint az adatok károsodása 55 százalékban a belső munkatársak figyelmetlenségéből vagy tévedéséből fakad; az elégedetlen dolgozók 13 százalékban, a tisztességtelen kollegák pedig 14 százalékban hibáztathatók az adatvagyon károsodásáért. Az okozott kár összege is megállapítható; egy nemzetközi tanácsadó cég becslése szerint az átlagos szintű védelmet használó cégekben az évi veszteség a mérleg-főösszeg 2–5 százaléka lehet.

A Synergon ennek a kivédésére dolgozta ki a biztonsági életciklus modellt; eszerint a modell szerint folyamatossá kell tenni a kockázatelemzést, a stratégiai tervezést, a védelmi intézkedések kidolgozását, implementálását, valamint a dolgozóknak e tekintetben adandó támogatást, az oktatást, illetve az auditálást és a felülvizsgálatot.

Mindehhez hozzájárul a „humán tűzfal": a belső munkatársak motiválása, ellenőrzése és képzése. A cég nagy része egyelőre nem sokat törődik ezekkel a teendőkkel, pedig nagyon fontos szerepük van a veszélyelhárításban.

A humán tűzfal méltatlanul mellőzött területe az adat- és információbiztonságnak. Mert gondoljon bele a kedves olvasó: egyes felmérések szerint az informatikai rendszerrel kapcsolatos károk 55%-a, más felmérések szerint több mint 80%-a fakad a saját alkalmazottak, dolgozók tevékenységéből. A felmérések eredményei azért különböznek, mert van aki a kár értékét, van ahol az incidensek számát értékelik, az eredmény akkor is elgondolkodtató.

Milyen tipikus előfordulások vannak, és hogyan előzhetjük meg őket? Gyakorlatilag a károkozás minden formájával találkozhatunk: ilyen a billentyűzetre öntött kávé. A takarítás, bútortologatás közben megsértett, esetleg kiszakított hálózati csatlakozó. A nyomtatóba beszakadt papír házilagos kioperálása húsz centiméteres ollóval, műkörömmel, svájci bicskával.

Természetesen nemcsak a hardver bánja dolgozóink gondatlanságát: a jogosulatlanul használt, tévesen kezelt szoftverek komoly kárt okozhatnak az adatokban. Fontos a jó biztonsági rendszer, hogy jogosulatlan hozzáférésre esély se legyen. Fontos a jó szoftver, aminek felülete felhasználóbarát, hogy ne adjon módot a téves használatra.

Ezenfelül számtalan módja van a szándékos károkozásnak, adatok jogosulatlan kimásolásától a rongálásig vagy megsemmisítésig. A humán tűzfalnak ki kell szűrnie a fegyelmezetlen, elégedetlen, tisztességtelen dolgozókat. A károk nagy része oktatással megelőzhető, de a megfelelően megválasztott eszközök és munkatársak jelentősen csökkentik a belső eredetű károkat.

Folyamatos biztonság

Rendelkezésre állási szolgáltatások. **A biztonságos működés elengedhetetlen feltétele az informatikai rendszerek, így a bennük feldolgozott és tárolt adatok rendelkezésre állása. Kulcsfontosságú biztonsági komponens lehet tehát a rendszerek gazdaságos, professzionális üzemeltetése. Erre, illetve a költséghatékony, szükséges gyorsaságú és minőségű hibaelhárításra több módszer ismert – a szerviz, Help Desk szolgáltatások igénybevételétől a különböző méretű és kompetenciájú saját csapat fenntartásán keresztül, a saját főtevékenységre koncentrálás lehetőségét biztosító teljes outsourcing megoldásig.**

A változékony, bonyolult, vagyis instabil és elromlásra hajlamos informatikai rendszerek megbízható üzemeltetése mindig is nehéz feladatot rótt a szakemberekre. A rendszerüzemeltetés azonban kevéssé vonzó terület, hiszen a közhiedelem szerint egyhangú, fárasztó feladatokat kell hozzá elvégezni, de azokhoz a feladatokhoz nem kell semmiféle különleges szaktudás, sem új ötlet. Optimális esetben a jól szabályozott környezet előre megszabott folyamatoknak enged utat, s a körülményeket a minőségbiztosítás tovább stabilizálja, s mindennek jóvoltából a felhasználó nem is észlelheti a környezetben lejátszódó tranziens jelenségeket.

Ha megtörtént a baj...

Nem felejthetjük el, hogy a biztonság nem statikus állapot. A környezet és a követelmények folyamatosan változnak, így a kialakított információbiztonsági rendszert időről időre felül kell vizsgálni, csak így derülhet fény a már jelen lévő vagy az éppen kialakuló új kockázatokra. Az informatikai biztonsági *felülvizsgálat* magában foglalja az adminisztratív elemek és a technikai megoldások felülvizsgálatát is.

Az informatikai infrastruktúra átfogó kezeléséhez szükséges eszközök sokba kerülnek, ezért nem minden cég engedheti meg magának a használatukat. A Synergon azonban változtatni akar ezen a helyzeten: a kis- és közepes vállalkozásoknak is igyekszik elérhetővé tenni az ITIL (IT Infrastructure Lybrary) kezdeményezésre felépített modelljét.

A szinte szabványként működő, európai kezdeményezéssel életre hívott ITIL-t a Microsoft is támogatja: a maga Operation Framework rendszerének elemeit építette az ITIL-re. A módszer alapelvei meglehetősen egyszerűek: a már megtörtént bajt a probléma pontos behatárolásával és megnevezésével, majd a hozzá való legjobb megoldással lehet leküzdeni.
A cégek többsége ma főleg a felhasználó és a rendszergazda közötti eseti kommunikációra támaszkodik, de ez a módszer nem ad megnyugtató megoldást a netán ismétlődő problémák orvoslására. A Synergon Officium rendszere több kis- és közepes vállalkozást szolgál ki a maga szakembergárdájával és eszközeivel, így magas szintű szolgáltatást adhat a kisebb vállalatoknak is, és naponta több száz vagy több ezer problémával is megbirkózik. ■

IDŐBEN A BIZTONSÁGÉRT

symantec™

ICON

www.icon.hu

Már megint kimaradt...

Garanciális szervíz: www.apcservice.net

Smart-UPS®

Symmetra® Power Array™

az áram. Megelőzhettük volna.

Tegnap du. 3:27-kor néhány pillanatig tartó feszültségkiesés érte a cég szervereit. Ez a számítógépes rendszer egy órás rendkívüli leállását okozta. A cég nem rendelkezett semmilyen feszültségvédelmi megoldással. Ez idő alatt az értékesítési osztály munkája félbeszakadt, az ügyfélkiszolgálás szünetelt. Értékes adatok vesztek el, a céges honlap elérhetetlenné vált. A tápellátásvédelem hiánya ebben az egyetlen esetben 20 millió forintjába került a cégnek.

Az ilyen esetek szerencsére megelőzhetőek. Az APC Smart-UPS® és a Symmetra® Power Array™ garantálják, hogy az Ön kritikus üzleti alkalmazásai folyamatosan elérhetőek és működőképesek maradjanak, még tápellátási zavarok idején is. Elismert tápfelügyeleti megoldásaink megkímélik Önt a felesleges veszteségektől és csökkentik üzemeltetési költségeit.

Az APC megoldást kínál Önnek is!

Az ingyenes termékkatalógus igényléséhez regisztrálja magát a *http://promo.apc.com* címen, a *67189v* kód megadásával.

APC®
Legendary Reliability™

Látogasson el honlapunkra: www.apc.com • ÁRAM-vonal: (06-1) 209-4678
Műszaki tanácsadás: (06-40) 200-262 • Fax: (06-1) 209-4677 • E-mail: apcHUN@apcc.com