INTEGRÁLT MEGOLDÁSOK

KOCKÁZAT ÉS VÉDELEM

Az utóbbi években alapvetően megváltozott a biztonsággal kapcsolatos vélekedés. Ma már természetes, hogy a legkülönbözőbb élethelyzetekben merül fel a biztonság és a kockázatarányos védelem kérdése. A szervezeteknek ma már nemcsak jó termékekre van szükségük, hanem megfelelő integrált biztonsági megoldásokra is.

Ahogy telnek a napok, egyre több információ támasztja alá azt a feltételezést, hogy a Nemzetbiztonsági Hivatal informatikai rendszerébe nem kívülről telepítették a kémprogramot, hanem azt valószínűleg egy volt NBH-s alkalmazott helyezte el a hivatal operációs rendszereiben. Olyan speciális ugyanis a hivatal informatikai rendszere, hogy csak házon belül lehetett kémprogrammal betörni az informatikai hálózatba, ráadásul annak, aki ezt tette, ismernie kellett a hivatal operációs rendszerét is. Az ilyen hírek hallatán jogosan merül fel mindenkiben a kérdés: Hogy fordulhat mindez elő? Ha már az NBH sem tudja megvédeni a saját rendszereit, akkor hogyan érezhetné magát biztonságban az átlagember?

De miért léphetnek fel egyáltalán biztonsági problémák? Az egyik ok lehet, hogy az adott rendszer védelme nem arányos a releváns fenyegető kockázatokkal, nem állnak rendelkezésre a szükséges biztonsági eszközök, nincsenek megfelelően konfigurálva azok. Szintén gyakori hiba, hogy senki sem gondoskodik a biztonsági megoldások naprakészségéről, így előbb-utóbb teljesen elavulnak, és már nem tudják megfelelően ellátni a feladatukat. Hasonlóképpen ide vezethet, ha a szervezet túlságosan megbízik a védelmi rendszerében, és nem feltételezi, hogy bárki is árthat neki, ezért nem foglalkozik annak rendszeres ellenőrzésével és naprakészen tartásával. Az is elképzelhető, hogy a felső vezetőkben nem tudatosul kellőképpen a védekezés fontossága. Mindebből látszik, hogy a fizikai és a logikai sebezhetőségek nagy része végül visszavezethető humán tényezőkre. Ha az emberi veszélyforrásokat nem kezelik megfelelően, akkor nem érhető el megnyugtató, teljes körű biztonság.

> ■ AZ ÖSSZETETT BIZTONSÁGI KÉRDÉSEKNÉL A TAPASZTALAT ÉS AZ EMBERI INTÚÍCIÓ ÖNMAGÁBAN MÁR KEVÉS.

Közeledő technológiák

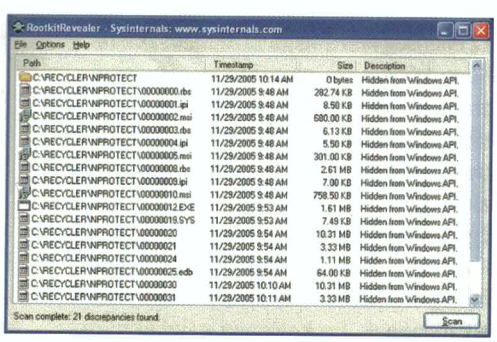
■ Szun-Ce, a híres ókori kínai hadvezér és hadászati szakértő írta (A háború művészetében), hogy a haditudomány arra tanít bennünket, ne abban bízzunk, hogy az ellenség nem fog jönni, hanem abban, hogy készen állunk a fogadására; sem annak az eshetőségében, hogy nem fog támadni, hanem inkább abban a tényben, hogy bevehetetlenné tettük a pozíciónkat.

Egy szervezetnél ma már rengeteg különböző – fizikai, logikai és szervezeti, illetve humán – biztonsági megoldást alkalmaznak. Ezeknek az önállóan működő megoldásoknak az adattartalma

A rootkitek olykor sikerrel elrejtik a vírusokat, férgeket, trójaiakat

Testvérként figyelemmel kísérhette a felhasználók szokásait. Jól jellemzi egy átlagfelhasználó kiszolgáltatottságát, hogy bár a Sony végfelhasználói szerződésének egyik apró betűs pontjában szerepel, hogy telepít egy szoftvert a számítógépre, ám annak a funkcionalitása nincs egyértelműen megjelölve, és arról sem esik szó, hogy a későbbiekben ezt lehetetlen lesz eltávolítani. Bár a Sony kezdetben még tagadta a kényes esetet, a bizonyítékok súlya alatt meghajolva visszavonta a DRM másolásvédelmét. Erre egyébként az ellene indított perek sorozata is rákényszerítette.

Fontos momentum, hogy a lemezkiadó szoftverlejátszó programja olyan sebezhetőséget nyitott a számítógépeken, amit nem sokkal később a külön erre a célra írt vírusok már ki is használtak, így szinte láthatatlanul tudtak beférkőzni ezekbe a rendszerekbe. Egy ilyen rootkites megoldás eltávolítása rendkívül kényes és komoly szaktudást igénylő folyamat, mivel a kártevő roppant komplex módon épül be a rendszerbe. Tapasztalatlan felhasználóknak megfelelő segédeszköz nélkül semmiképpen nem javasolt.



Munkában egy rootkitfelismerő alkalmazás

ROOTKITEK MACINTOSH KÖRNYEZETBEN

Sajnos már Apple OS X alatt is létezik néhány kísérleti (PoC, Proof of Concept) rootkit. Ezek hatása eddig jelentéktelen volt, és emiatt a Mac-használók tábora lebecsüli a veszélyt, hiszen ahhoz, hogy sikeresen feltelepüljenek, rootjogosultságra lenne szükségük, de ezt nem képesek megszerezni. Egy Mac-felhasználónak nehezebb kiváltságos felhasználóként dolgoznia (hacsak nem állítja be ezt saját magának): ennek ellenére naivság lenne azt gondolni, hogy őket soha nem fogják tudni rászedni oly módon, hogy átkapcsolva a rootjogosultságokra, egy rootkit-program is képes legyen települni a rendszerben.

A rootkitek és vírusok

■ Bár a rootkitek csak néhány éve kerültek az érdeklődés középpontjába, valószínűleg már korábban is használatban voltak, csak nem mindig vettük észre őket. Greg Hoglund, független biztonsági szakértő egyenesen úgy véli, hogy a Windows-alapú rootkitalkalmazások titokban ugyan, de már évek óta széles körű használatban vannak. Hoglund már 1999-ben figyelmeztetett a probléma veszélyességére, sőt demonstrációs céllal több rootkitet is írt, például a széles körben ismert Hacker Defendert. Manapság egyértelműen tapasztalható, hogy a víruskészítők egyre fertőzőbb és ellenállóbb kártevőket készítenek, s ezek mind az üzleti, mind pedig az otthoni felhasználókra veszélyt jelentenek.

A sötét oldal vírusírói, hackerei és a vírusvédelmi alkalmazások fejlesztői folyamatos versenyfutásban vannak egymással. Nehezíti a küzdelmet, hogy a rootkitek több fajtája nyílt forráskódú, azaz mindenki számára hozzáférhető, emiatt bárki kisebb módosításokkal új kártevőt hozhat létre. További kellemetlen adalék, hogy egy-egy ilyen fejlett vírus a fertőzés után képes eltüntetni magát az operációs rendszer elől, miközben a háttérben tovább végzi kártékony tevékenységét.

Hogyan védekezhetünk?

■ Fontos tisztázni, hogy egy rootkit önmagától nem képes települni a rendszerünkre, csak ha az már korábban megfertőződött. Mivel elvileg még egy naprakész vírusvédelmi rendszer esetén is van esély egy olyan új vírus bejutására, amelyre még nem létezik felismerés, lehetőség nyílik a rootkit bejutására is. Jó hír lehet, hogy egy használható rootkit valamilyen módon mindig észlelhető lesz, mivel a működése közben szükséges információkat továbbítania, kommunikálnia kell. Egyre több vírusvédelmi fejlesztőcég ismerte fel a téma jelentőségét, és fejlesztette ki a rootkiteket leleplező programját, s már nem segédprogramként kínálja ezt, hanem egyenesen integrálják ezt a képességet a keresők alapfeladatai közé.

A rootkitfelismerő programok képesek észlelni a különféle rendszereltérítéseket (hooksokat). Az egyik legeredményesebb rootkitleleplező módszer a számítógép pillanatnyi állapotának (futó folyamatok, automatikus indításra jogosult alkalmazások listája, Registry-bejegyzések, memóriafoglaltság stb.) mentését összehasonlítani egy garantáltan tiszta (pl. CD, DVD) lemezről történő indulás utáni hasonló mintavétellel. Ha ebben a két lementett állapotban nem egyeznek a futó folyamatok, a felhasznált memóriaterület, vagy bármilyen egyéb eltérésre fény derül, az további alapos nyomozásra adhat okot.

CSIZMAZIA ISTVÁN,
vírusvédelmi szakértő
Sicontact Kft.