Informatikai betörések, adatszivárgások, ipari kémkedések

Tények és igazságok
a múlt és jelen tükrében

Török Szilárd
ügyvezető
torok.szilard@constantine.hu

Constantine
biztos, ami biztos

Előadás célja

- Magyar információ-biztonsági szemlélet és megtörtént események ismertetése
- Milyen legális hacker szolgáltatások léteznek, mire használhatók
- Milyen formában zajlanak adatszivárgások itthon és milyen módon lehetséges védekezni ellenük
- Információ-biztonság és a jog közeledjen egymáshoz
- **az előadás alapján valósabb információ-biztonsági kép alakuljon ki Önben!**

a „Múlt” itthon

-1993: szoftver feltörések, átalakítások és illegális másolások kialakulása

1993-1997: hazai internet hálózatok kialakulásával megjelentek a betörési kísérletek, felfedezték a haladó programozók a számítógép oldali tudás hálózati használatát. Jelentősebb hazai példák: NASA / JATE, Soros Alapítvány / C3.hu, Kormányzati tűzfalrendszer, harcok az egyetemi hálózatok feletti uralomért (1997-)

1997-1999: Cyber kultúra és harcosai a Telko cégek ellen fordultak: Matáv és Mobil szolgáltatók hackelése: ingyenes mobil (450-900Mhz) és vezetékes beszélgetés, hangposta-üzenés, világkártya. Gellérthegy/AH, nexus.hu Digitális adatszivárgások (eladtak teljes ügyfél adatbázisokat). ATM hibák és trükkök. HIP 1997

1999: Megjelent Magyarországon az első Legal Hacker szolgáltatás. Index vs Internetto háború, hackme.telnet.hu háttértörténete, első komolyabb backdoor-ok nagy cégeknél, álbetörések (Index.hu), elender.hu, TV2 interjú

a „Múlt” itthon (folytatás)

2000-2002 (választásokig)

Megjelentek az első komolyabb ipari kémkedések IT segítséggel.
Néhány esemény: synergon.hu és egy 2009-es hacker előadás összefüggése, Tőzsdei rendszerek, OTP Home Bank / Index.hu, Távol-Keleti oktatási szerverek, Italgyárak, Választások 2002 védelme(?)

2002-től csak kérdések formájában

Magyar hacker konferencia: miért nincs ott a „szakma” színe-java?
Kik felügyelik a hazai legnagyobb warez rendszereket?
Ki láthatják az ügyvédek szerződéseit?
Hallott pl. 2008-ban Magyarországi internetes banki lopásról?
Valóban használnak a bűnözők informatikai alapú támadásokat, rendszer módosításokat a sikeresség érdekében? És milyenekre?
Ki/kik az Anonymous? mi közük lehet a Hackerekhez?

Jelen kérdései

Hacker, Cracker zsoldos vagy ellenség:

- Miért találná meg az összes hibát valaki, amikor a hiba meglétéből él?
- Hogy lehet egy ügyfél elégedett a megvásárolt Etikus Hack szolgáltatással, amikor rendszerében sosem látott betörést?
- Azokat a hibákat keresi és találja meg a fizetett hacker amik valóban kockázatosak?
- Kockázat egy hacker munkatárs/ismerős? Megvehetőek?

Mielőtt a rossz biztosító ügynök „mindenhonnan tégla eshet a fejedre” hibájába esnénk: Minden biztonsági kérdést kövessen a kockázat elemzése! Ne érzelmi vagy indulat alapon (pl. félelem, bosszúság) rendeljünk szolgáltatásokat.

Legal Hack az informatikai biztonsági szakma „krémje”, de a valódi feladatok és elvégzett munkák max 5-10%-át teszi ki. Meglepő, de ez így van rendjén!

Legal Hacking körülményei

- Törvényes, jogilag pontosan definiált betörési teszt, kizárólag a Megrendelő kérései alapján elvégezve!
- Valós és szimulált tesztek, vizsgálatok
- Speciális szolgáltatások
- Eredményét mérni idő alapon lehetséges
- Megmutathatja egy IT rendszer „ellenálló képességét”

Legal Hacking Szolgáltatások

- Külső betörési tesztek
- Belső tesztek, ellenőrzések
- Fejlesztési tanácsadás, együttműködés
- Betörések, más típusú támadások lenyomozása, helyreállítás
- „Bér Hacker” konstrukciók
- Folyamatos vizsgálatok: újratesztelések a szinten tartás és a megelőzés céljából

Esettanulmányok 1.

Nagyvállalat ügyfélszolgálati rendszerének vizsgálata

- Tűzfal ami véd, de még se...
- No User probléma
- Session ID-k csapdái
- Certificate használat
- Logout: fontos kilépni?

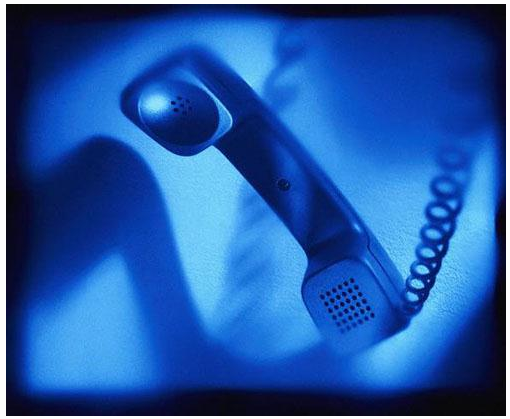
Esettanulmányok 2.

Több ezer számítógépes nagyvállalati hálózat feltörése kívülről

- DNS eltérítések, e-mail szerver ugrópont
- Web-es hibák kihasználása
- Trójai levél és/vagy file bejuttatás
- 2 napon belül a middle-ware-n információk nélkül
- Valódi cél lehetne maga az anyavállalat!

Esettanulmányok 3.

Pénzügyi rendszer védelme



- 5-10 perc alatt adminisztrációs user és jelszó számítógép nélkül
- 2 perc alatt saját internet kapcsolat, kikerülve a bank „kötelező” internetét
- Kb. 1-2 óra alatt a vírusvédelmi rendszer kikapcsolható

Home Banking és társai

- SSL spoof
- Digitális kulcsok, Cert. auth hiányosságok
- Különféle banki rendszerek időzítési és szinkronizálási hibáinak következményei
- ATM bizonylatok trükkje 10 éve...

Állandó a lemaradás? Miért is?

- Rendszergazdák/Informatika versus Biztonsági Osztály
- Felső vezetés még mindig nem tulajdonít komoly jelentőséget az Informatikai Biztonság szerepének
- Mindennapi trükkök és fejlődésük (GSM alapú, WiFi, elektromos hálózat, stb.)
- SPAM és botnet hálózatok
- Őrzők őrzőjének hiánya
- Megélhetési IT bűnözők

Belső fenyegetések, Adatszivárgás

A belső fenyegetettség elleni védelem aktuális kérdései:

- Szabályozások és jogi lehetőségek
- Kockázat analízis, kockázat menedzsment
- Jogosultság szerinti megközelítés
- Jogosultak tevékenységeinek nyomon követése a kihirdetett biztonságpolitika alapján

Belső és külső fenyegetések elemzése

Kockázat analízis

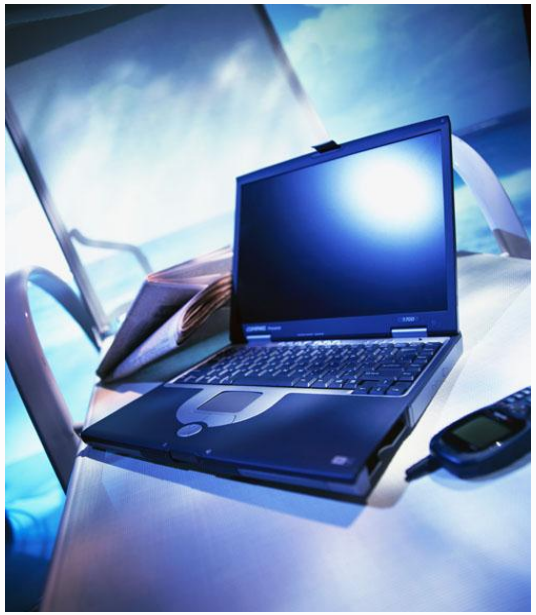
A kockázatok azonosítása és értékelése. Fenyegetettség, sebezhetőség, vagyon.

Kockázat menedzsment

A megfelelő mechanizmusok implementálásával a kockázat elfogadható szintűre csökkentése.

DLP megoldások lehetőségei

- Képesek minden számítógépes kimeneti pontot figyelni (USB drive-ok, CD, Infra, Bluetooth, Nyomtatók)
- Bizalmas fájl nyomon követése, akár copy/paste vagy hálózaton történő követés
- Otthoni megfigyelési mód
- Szöveges/tartalom elemzés mindenhol
- Titkosítást „kikényszeríthető”
- „Ügyeskedő felhasználó” biztosak
- Akár bonyolult életszerű folyamatokat is lehetséges szabályozni, védeni
- Képesek megfigyelni, blokkolni, de akár bizonyítékot is eltárolni



Constantine
biztos, ami biztos

Ki figyel kit és hogyan „megelőzésként”?

- Államigazgatási,pénzügyi és nagyvállalati szektorok DLP alapú megfigyelő rendszerei (amikről az Adatvédelmi Iroda sem tudott tavaly)
- Kommunikációt monitorozó rendszerek (ADSL, GSM, stb.)
- Fekete dobozok (FAX/Copy)
- Billentyűzet figyelő eszközök
- Kamerák és mentéseik
- Beléptető rendszerek
- Napló elemző rendszerek

Constantine
biztos, ami biztos

Megoldások

Röviden, azaz a „hárombetűs” szakmai megoldások:
IPS, DLP, H-DLP, DRM, SSL, CERT, Crypto, stb.

Hatásos megoldások egyike:
Jogász és Informatikai biztonsági szakma együttműködése.

4-8 éves távlatban:
Kormányzati cselekvés, ehhez új program, majd a megfelelő jogi környezet megteremtése.

Bizonyítsuk be itt és most, hogy az IT biztonságtól olcsóbb az állam!

Központi adatbank/e-tár; egységes e-beszerzés, e-pályázatkezelés, projektmenedzsment és kontrolling; működő állami PKI; központi kockázatelemzés és kezelés; valódi jogkörrel bíró ellenőrző szerv.

Legfrissebb e-közigazgatási szabályozás

Jó kezdés a következő évek tekintetében:

A Kormány **223/2009. (X. 14.) Korm. rendelete** az elektronikus közszolgáltatás biztonságáról :

Nemzeti hálózatbiztonsági központ

8. § (1) A kormány a magyar kritikus információs infrastruktúrák védelme, valamint a központi rendszeren megvalósuló kommunikáció biztonsága, a vírus-és más támadások káros hatásainak korlátozása érdekében nemzetközi együttműködéssel hálózatbiztonsági központot (a továbbiakban: Központ) működtet.

PTA & CERT-Hungary, mint kormányzati CERT

Informáljunk mindenkit a jelentősebb volumenű informatikai incidensekről!
Ne hallgassuk el, mert hosszú távon több kárt okoz.
Tudatosságunk növeli az általános biztonságot és az igényt rá!

Köszönöm a figyelmüket!

Török Szilárd
ügyvezető
torok.szilard@constantine.hu

Constantine
biztos, ami biztos