Informatikai adatvédelem a gyakorlatban

Dr. Kőrös Zsolt

ügyvezető igazgató

NOREG

Információvédelmi Kft.

SZIGORÚAN BIZALMAS

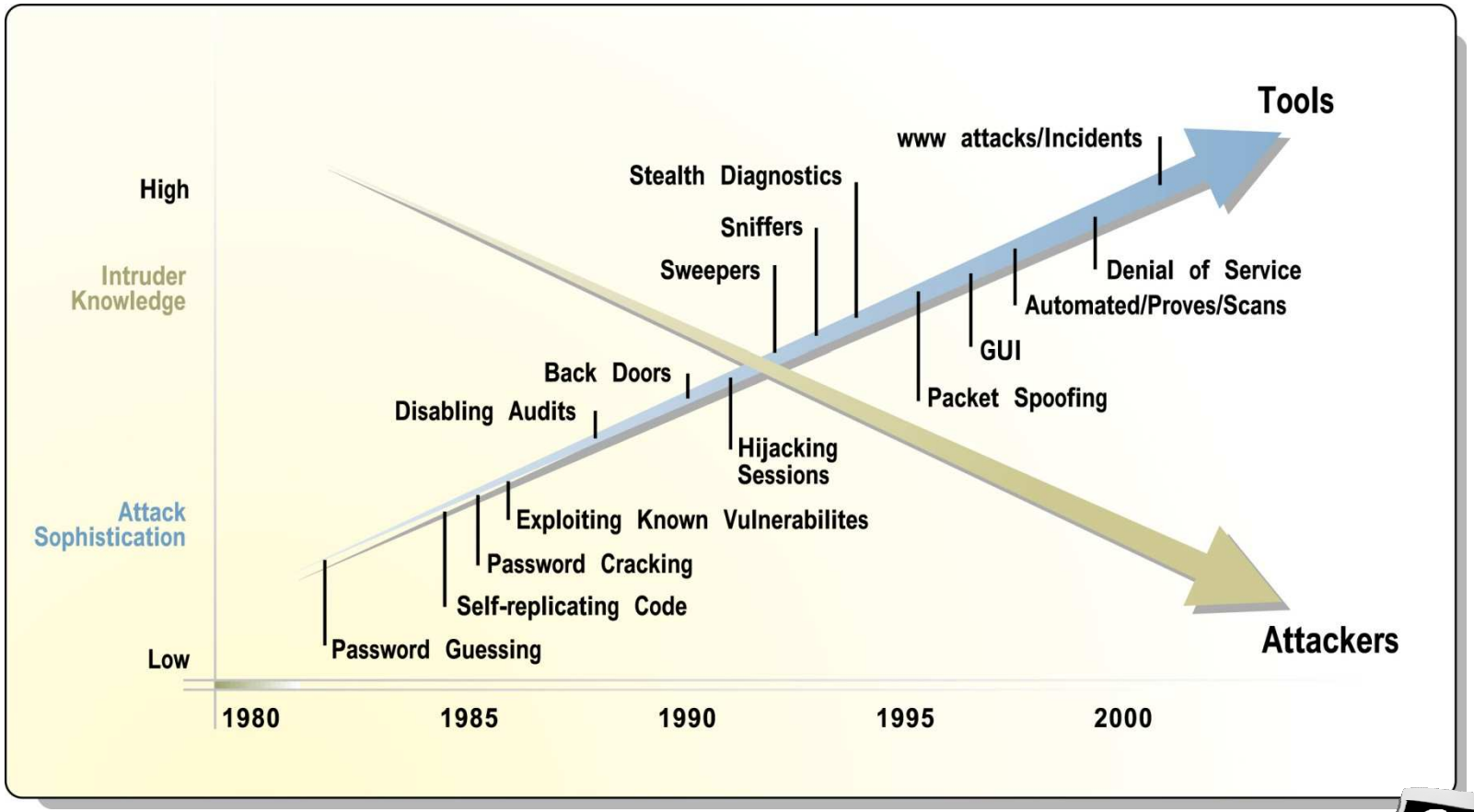
Az informatika térhódításának következményei

Megnőtt az informatikától való függőség

Az informatikai kockázat

üzleti kockázattá vált

Az automatikus eszközök növelik a veszélyt



Source: Carnegie Mellon University

Kiemelt Internetes fenyegetések

- SPAM (60-90%)
- Adathalászat (81% éves növekedés)
- Internetezéskor a munkatársak nyomot hagynak magukról (adware)
- Webes levelező rendszeren történő adatszivárgás
- Interneten letölthető kártékony programok (spyware, keylogger, …)

Kockázatok és kihívások a modern informatikában

- Biztonsági kockázat
  - P2P fájlcserélő hálózatok
  - Kémprogramok
  - Illetéktelen hozzáférés
  - Jelszóhalászat (phishing)
  - Azonnali üzenetküldők

- A Kazaa letöltések 45%-a tartalmaz rosszindulatú kódot. *(TruSecure)*

- A vállalatok 45%-a tapasztalt illetéktelen belső hozzáférést az elmúlt egy év során. *(CSI/FBI Computer Crime & Security Survey)*

Kockázatok és kihívások a modern informatikában

- Jogi felelősség
  - Pornográf tartalmak
  - Zene (MP3)
  - Fájlmegosztás
  - Azonnali üzenetküldők
  - Üzleti titok védelme

- A P2P keresések 73%-a pornográf tartalomra irányul. *(Palisade Systems)*

Kockázatok és kihívások a modern informatikában

- Sávszélesség pazarlás
  - Valós idejű média közvetítések (Internet rádió és TV)
  - Fájlcsere
- A dolgozók 44%-a rádiózik vagy TV-zik az Interneten. (*Nielsen NetRatings)*

Kockázatok és kihívások a modern informatikában

- Termelékenység
  - Chat, fórumozás
  - Játék

- A vállalatok 70%-a tapasztal engedély nélküli azonnali üzenetküldő használatot. *(Gartner)*

Jogosulatlan hozzáférések

	Belső	***Külső***	
	Alkalmazottak, szerződéses partnerek	**Diákok, „computer zsenik”**	***Szervezetlen***
	Kíváncsiság	**DoS, feltört WEB-site-ok**	
	Volt-alkalmazottak, szerződéses partnerek	**Idegen hatalmak, kémek, terroristák, konkurencia**	***Szervezett***
	Bosszú, károkozás	**Haszonszerzés, kémkedés**	

Hogyan védekezzünk?

- Mérjük fel a kockázatok valós szintjét
- Hajtsuk végre a szükséges védelmi intézkedéseket
  - Szabályzások kialakítása
  - Technikai megoldások bevezetése
- Vizsgáljuk felül rendszeresen a biztonság szintjét

IT biztonsági audit célja

- Részrehajlás mentes jelentés készítése arról, hogy a cég védelmi elvárásainak az informatikai rendszer védelmi adottságai megfelelnek-e vagy sem
- Az informatikai biztonság szintjének emelése
- Törvényeknek, jogszabályoknak, rendeleteknek való megfelelés
- Vezetőség tájékoztatása a szervezet informatikai biztonságának helyzetéről, hogy dönteni tudjon a kockázatok csökkentéséről

Szervezeti, adminisztratív hiányosságok (példák)

- A szabályozás hiánya, vagy elégtelensége
- A szabályok és eljárások ismeretének hiánya
- A biztonság ellenőrzésének hiánya, vagy elégtelensége
- Illetéktelenek rendelkezése jogosultságokkal
- Az erőforrások ellenőrizetlen használata

Emberi hibák (példák)

- Az IT biztonsági utasítások be nem tartása
- Adatok, vagy berendezések károsítása hanyagság miatt
- Rossz jelszókezelés
- Gondatlan információkezelés
- A külsősök miatti kockázat
- Az IT rendszer nem megfelelő használata

Jelszó erősség:

Szerver: Compaq P5500 két Xeon 400Mhz CPU

Crack SW: L0pht Cracker

Password Type	Length	Estimate Time
Dictionary A-Z	8	<1 Sec
	9	<1 Sec
	10	<1 hr 15 min
	14	<3 hrs 10 min
Alpha Numeric A-Z; 0-9	8	<23 hrs 50 min
	12	<34 hrs 50 min
	14	<39 hrs 20 min
Alpha Numeric Plus Special Characters A-Z 0-9 !@#$%^&*()-_+=	8	<130 hrs 10 min
	14	<223 hrs 50 min
Alpha Numeric Plus Advanced Special Characters A-Z, 0-9 !@#$%^&*()-_+= {}`~'"? <>:;|\,./[]	8 **	<2365 hrs 10 min
	13	<2335hrs41min*

Jelszavak – Best Practice

- Legalább 8 karakter hosszú
- Legalább 2-3 havonta változtatva
- Ne legyenek nevek, szavak, szokásos kombinációk
- Keverjük a kis és nagybetűket, speciális karaktereket

Jelszavak – Best Practice

- Sose
  - adjuk át másoknak
  - írjuk le
  - használjunk azonos jelszavakat különböző alkalmazásokhoz
  - küldjük el e-mail-ban

Műszaki hibák (példák)

- A meglévő védelmi eszközök hibája
- Szoftver sebezhetőség
- Adatbázishiba, adatvesztés az adatbázisban
- Hálózati eszköz hiba
- Gyenge, elavult kriptográfiai algoritmus

Titkosítás

- Adattárolók (beépített HDD, biztonsági mentések)
- Adathordozók (pendrive, okostelefon, stb.)
- Kommunikáció (levelezés, adatok átküldése)

Szándékos cselekedetek (példák)

- Adatok, szoftverek, IT berendezések szándékos manipulálása, tönkretétele
- Engedély nélküli belépés épületekbe
- IT rendszer illetéktelen használata
- Lopás
- Vandalizmus

Az informatikai biztonsági audit lépései - helyzetfelmérés

- Helyzetfelmérés - dokumentumok tanulmányozása, helyszíni bejárás, interjúinformatikai szakemberekkel;
- Ügyviteli folyamatok, adatok védelmi igényének meghatározása - interjúk az egyes alkalmazások üzleti felelőseivel
- Hálózati sérülékenység vizsgálat
- Fenyegetettség és kockázat elemzés

Az informatikai biztonsági audit lépései - kockázatkezelés

- Javaslatok:
  a magas kockázatok kezelésére szolgáló védelmi intézkedések kidolgozása, figyelembe véve a megvalósíthatóságot, az erőforrás és költségigényt

Szabályozási rendszer

- „Informatikai Biztonságpolitika”
  - alap dokumentum, az informatikai biztonság iránti elkötelezettséget, felelősségre vonhatóságot, és az információ-rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításához szükséges általános elvárásokat határozza meg

- „Informatikai Biztonsági Stratégia”
  - az IBP-ben megfogalmazott célkitűzések megvalósítási módszerét deklarálja, követelményeket, feltétel- és eszközrendszert, valamint intézkedési tervet javasol a jövőkép elérésére, összhangban az intézmény informatikai stratégiájával

Szabályozási rendszer

- „Informatikai Biztonsági Szabályzata”
  - az ISO 27001 szabvány előírásait és felépítését követve, az információ-rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításához szükséges standardizált elvárásokat határozza meg minden tevékenységre kiterjedően
  - „Informatikai Házirend”
    minden dolgozóra vonatkozó informatikai biztonsággal kapcsolatos felelősségeket és követelményeket határoz meg, és segítséget ad számukra a munkaköri leírásban is vállalt titoktartás betartásához

Köszönöm a figyelmet!

zsolt.koros@noreg.hu

NOREG
Információvédelmi Kft.
SZIGORÚAN BIZALMAS