Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

ellopott adataink - tanulunk-e a más kárán?

döntések, következmények, elrettentő példák...

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

azért gyűltünk itt ma össze...

1. bevezető: technikák, felelősség, következmények :-P
2. a helyzet reménytelen, de nem súlyos ;-)
3. amikor a profik hibáznak :-O
4. zsarolás a cégek ellen :-(
5. felhasználói hozzáállás, fegyelem :-/
6. konklúzió \o/

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

bevezető :-P

- idén 30 éves a Brain vírus
- a védekezés régen sokkal könnyebb volt (2015. 310 millió)
- egyre gyarapszik az ismeret, a teendő
- a hozzáállás nagyon sokszor nem megfelelő

"A szerencse az, amikor a felkészültség találkozik a lehetőséggel, vagyis először mindig tanulni kell."

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

a helyzet reménytelen, de nem súlyos I. ;-)

2014. ITV News Consumer Limited beszámoló
- A britek hatoda (16%) volt már kiberáldozat
- Nem védik az eszközeiket (pl. okostelefon és tablet)
- A mobiltelefonos adathalászat +80% egy év alatt
- 83% becsapták PC vagy laptop használat közben
- 21% okostelefonos, 17% tabletes támadás

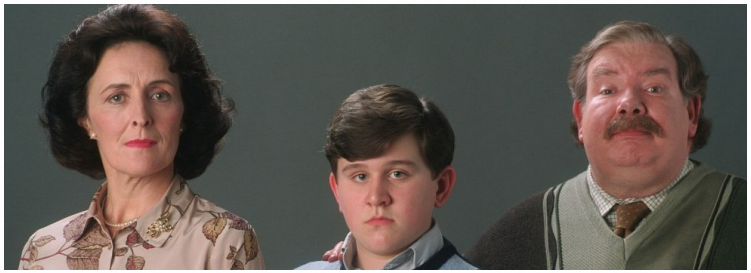
2014. A svájci KPMG International felmérése
- 300 IT és HR vezető, 500-10,000 fős nagyvállalatoktól
- 60% nincs elegendő szakember a védelemhez
- 70%-a nincs adatvédelmi stratégia, megoldás
- 50% hackereket alkalmazna, börtönviseltet is

2014. EY, 13. Globális Visszaélési Felmérés, magyar kutatás
- A hazai vállalatok többsége alulértékeli a kiberbűnözés veszélyeit
- Csak 35% tartja kockázatosnak a saját vállalatára nézve
- Közép-Kelet-Európában 45%, nyugat-európában 50%-a aggódik

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

a helyzet reménytelen, de nem súlyos II. ;-)

2015-ös nemzetközi felmérés:
- A vállalatok 82%-a azt hiszi, túl kicsi célpontnak
- A valóság ezzel szemben
- Az 50 főnél kisebb cégek 41%-nál már volt fenyegetés
- A rosszindulatú támadások pénzügyi veszteséggel is járnak
- 2014-ben a rendszerek feltörésének átlagos költségvonzata 6,500 USD (1.8 millió HUF) összegű volt



2016. Nemzeti Kibervédelmi Intézet (NKI) éves jelentés
- Ötezer magyar weboldalt ért tavaly támadás! (2016.02.20. MTI)
- A legjellemzőbb a weblapfeltörés, a túlterheléses támadás
- Gyakoriak a zsaroló szándékú támadások
- Nagy számú adatlopási kísérlet, pl. hazai banki ügyfelek ellen

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

amikor a profik hibáznak I. :-O

2013. október - Adobe
- Előbb "csak" 2, utána 38 millió ellopott ügyféladat
- Utána forráskódok is, nyilvánosságra kerülnek a jelszavak
- Sok felhasználó a jelszó-emlékeztetőkben egy az egyben megadta a jelszavát!

Járulékos áldozatok, rosszkor voltak rossz helyen
- Közös szerveren a Corporate-Car-Online
- Luxus limuzin kölcsönző, 850 ezer ügyfél
- Cégvezetők, sztárok, politikusok: DonaldTrump, Tom Hanks, stb.
- Útvonalak, 241 ezer hitelkártya adata

Összességében:
- Többször kozmetikázott beismerés
- Vétlen szereplők járulékos kára

"A profi az, aki akkor is meg tudja csinálni, amit kell, ha nincs hozzá kedve. Az amatőr az, aki akkor sem tudja megcsinálni, amit kell, ha van hozzá kedve." (James Agate)

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

amikor a profik hibáznak II. :-O

2013. november - TARGET
- 110 millió ügyfél adat
- 40 millió bank- valamint hitelkártyához tartozó adat
- Az incidens teljes költsége 290 millió USD (81 milliárd forint)
- A VISA, MasterCard felé a peren kívüli egyezségek értelmében 39.4 millió dollárt kell fizetnie
- Biztosításaik viszont csak 90 millió dollárra szóltak

Összességében:
- Óriási nagy veszteségek
- Az adatlopások nyilvánosságra kerülése után az üzleteikbe azonnalchipes kártyaolvasókat telepítettek, hogy elkerüljék a további ismételt támadásokat,
- Ez kicsit késő volt

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

amikor a profik hibáznak III. :-O

2014. augusztus - Apple iCloud (Fappening)

- Hírességek (Jennifer Lawrence, Kate Upton, Avril Lavigne) meztelen képei a Reddit és a 4chan oldalain
- Apple: "Nem az iCloud rendszer hibája"
- NakedSecurity szavazás: "94.59% -> legyen 2FA az iCloud-nál is"

2014. szeptember

- A korábban hiányzó brute-force védelem aktiválása a Find My iPhone szolgáltatáson is
- iCloud = 2FA bevezetése
  + e-mail értesítés a bejelentkezésekről

Összességében:

- Felelősség gyors hárítása
- Utólag elvégzett gyors hiánypótló fejlesztések

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

amikor a profik hibáznak IV. :-O

2015. augusztus - Ashley Madison

- Avid Life Media fizetős anonimitást ígérő „félrelépős” szolgáltatása
- 37 millió "ügyfél" adat
- Nevek, e-mailcímek, bankkártya, szexuális preferenciák
- Feltöltött fotók, ügyfelek és a belső munkatársak levelezése
- 9.7 GB adat (Impact Team)
- A 19 dolláros "végleges törlés" nem működött

Összességében:

- Üzemeltetői hibák: e-mail cím regisztráció hitelesítés nélkül, hamis női profilok, el nem végzett törlés
- Rekordszámú celeb a Reputation Management Consultants cégnél
- Retorziók US Army, első öngyilkosságok (Torontó), kezdődő perek

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

amikor a profik hibáznak V. :-O

2013-2014. - SONY Pictures Entertainmaint
- 20 egymást követő támadási sorozat
- Észak-Korea? Lazarus csoport?
- 24 milliárd USD veszteség

Összességében:
- Eleinte tagadás, kozmetikázás, rossz kommunikáció
- A forensics vizsgálat és a biztonsági audit után:
  pár 10 ezer USD költséggel megelőzhető lett volna
  (Shakeel Tufail, HP Enterprise Security Solutions)

Az incidensek után a „Best practice” - lett volna :-)
- Gyors reagálás, őszinte tájékoztatás
- Mulasztások és hibák beismerése és javítása
- Hitelkártya-monitorozás
- Security Incident Response Team (SIRT) megléte, mozgosítása

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

zsarolás a cégek ellen I. :-(

2013. november 6. - CryptoLocker VS. rendőrség
- Swansea (Massachusetts, U.S.A.) szólt az FBI-nak
- De előbb kifizették a 2 bitcoin - 750 USD váltságdíjat

2014. február - CryptoLocker VS. ügyvédi iroda
- Goodson ügyvédi iroda (Észak-Karolina, U.S.A.)
- Kifizették a 300 USD (85 ezer HUF) váltságdíjat
- Lekésték a 72 órás, azaz 3 napos határidőt
- A napi munka (Word, Excel) elveszett, mentés nem volt

2015. november - Chimera színrelép
- A titkosított állományokat nem csak zárolja
- De nem fizetésnél a bizalmas vállalati dokumentumokat azonnal fel is tölti egy nyilvános weboldalra
- 638 dollár (180 ezer HUF) összeget követelnek
- Nehezen lekövethető Bitcoin formájában és TOR hálózaton keresztül

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

zsarolás a cégek ellen II. :-(

2015.11.03. "DDoS-as-a-service"
- A DDoS 170%-kal nőtt egy év alatt (Akamai 2015. dec.)
- Nem csak titkosítás miatt szedhetnek váltságdíjat
- Elosztott internetes túlterheléses támadás (distributed denial-of-service)
- ProtonMail: kifizették a 6000 dolláros (1.7 millió HUF) váltságdíjat
- A túlterheléses támadások a fizetés után sem szűntek meg (azonnal)

2015.11.20. Fizess vagy DDoS-oljuk a banki oldalt!
- 3 görögországi bank fenyegetése DDoS támadással
- 20 ezer Bitcoin (7 millió EUR, 2.1 milliárd HUF)
- A bankok egységesen nem fizettek
- Pár órára sikerült blokkolni a webfelületek elérhetőségét

Az új DD4BC "üzletág" terjedése miatt a kritikus infrastruktúrákat üzemeltető vállalatok, valamint a webshopok, egyetemek, pénzintézetek, hotelek, utazási irodák kezdhetnek aggódni...

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

felhasználói hozzáállás, fegyelem :-/

- 16% sosem változtatja meg a jelszavát
- 18% figyelmen kívül hagyja a jelszócsere jelzést

European 2015. Cyber Risk Survey
- Az európai cégek alábecsülik kiberbiztonsági veszélyeket
- A vállalkozások 79% csak alapszintű ismeretek az IT támadásokról
- Nincsenek tisztában a kockázatokkal, lehetséges veszteségekkel

2014. HelpNetSecurity jelentés
- Korábbi IT munkavállalók 25%-a régi jelszavával hozzáfér volt munkahelye hálózatához
- 16%-nak az összes korábbi munkahelyéhez van hozzáférése
- „A komoly adatsértések, incidensek rendre gyenge vagy eltulajdonított belépési adatok miatt következnek be” (Verizon)

2015. január Sailpoint felmérés
- A vállalatoktól elbocsátott dolgozók 14%-a 100 fontért (40 ezer HUF) eladná az általa korábban használt céges jelszavait

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

konklúzió \o/

A biztonság nem egy állapot, hanem egy folyamat!

- Nem érdemes spórolni a biztonságon
- Incidenseknél hiba az eltussolás
- Félelem a tőzsdei árfolyam megrendülésétől, a piac érzékeny
- Fontos a megelőzés, védelmi stratégia, rendszeres dolgozói biztonsági oktatás, pentesting, biztonsági audit

2007. USA: számítógépes csalásból már több pénz folyt be, mint a drogkereskedelemből - 105 milliárd dollár

- Minden egyes kis és közepes vállalat, vállalkozás védelme fontos
- A kiemelt, jelentős célpontok elleni kibertámadások esetében először ugródeszkaként célzottan a sokszor a gyengébben védett beszállítói kört, és az alvállalkozókat támadják

"Mit kell ebből megtanulnom?"
(Al Bundy)

Csizmazia-Darab István
Sicontact Kft., antivirus.blog.hu

köszönöm a figyelmet :-D

csizmazia-darab istván,
it biztonsági szakértő
sicontact kft,
antivirus.blog.hu

csizmazia.istvan@sicontact.hu

"Minden szenvedés oka a nemtudás"
(Zen)