ACPM
Audit Consulting Project Management

BUDAPEST • DUBAI • KIGALI • KUALA LUMPUR
NAIROBI • PRETORIA • SHANGHAI • WIEN

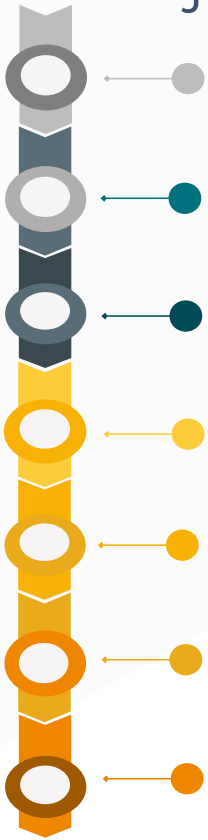
ACPM IT Tanácsadó Kft.

Az orosz-ukrán kiberháború előzményei, történései és lehetséges következményei

Sysadminday
2022. július 15.

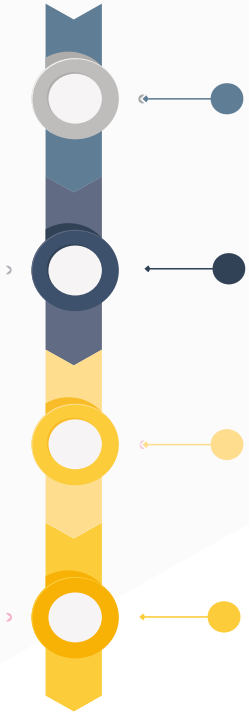
Előzmények – jó ideje nincs új a nap alatt

ACPM
Audit Consulting Project Management



- Az „információs hadviselés” nagyon nem új dolog
- Minden nagyhatalom „tudatosan” fejleszti ezt a kompetenciát
- 2007 Észtországot megtámadta a kibertérben Oroszország
- 2010 US Cyber Command
- 2013 Snowden és az NSA
- 2013 Magyarország Nemzeti Kiberbiztonsági Stratégia
- 2016 NATO Varsói csúcs: az operatív hadviselés területét kiterjesztették a kibertérre is

Előzmények – ne gondoljuk, hogy más nem csinálja



Kína: 2003-4 USA, UK; 2010 google; 2013 Németország; 2021 USA / MS; 2021: USA, Ausztria, Kambodzsa, Kanada, Németország, Indonézia, Malajzia, Norvégia, Szaúd-Arábia, Dél-Afrika, Svájc, UK

USA: 2000 előtt Echelon; 2012-14 EU

Izrael: 2010 Stuxnet Irán / 2021 Irán

Észak Korea: 2014 Lazarus csoport; Sony; Kripto-valuta

Előzmények – Oroszország támadásai

- 2007 Észtország
- 2008 Grúziai háborút megelőző és kísérő kibertámadások
- Amerikai elnökválasztásokhoz / politikához kapcsolódó kampányok, akciók; trollhadsereg
- 2015-2016 Ukrán áramszolgáltatók
- 2016 Kijev központi repülőtér / Ukrán Államkincstár
- 2016-17 Petya / Nopetya bűnözés és/vagy kibertámadás?
- 2020 Solarwinds
- Érdekesség: Ukrajna 2016 óta több esetben támadott vissza, lényegesen kisebb hatással

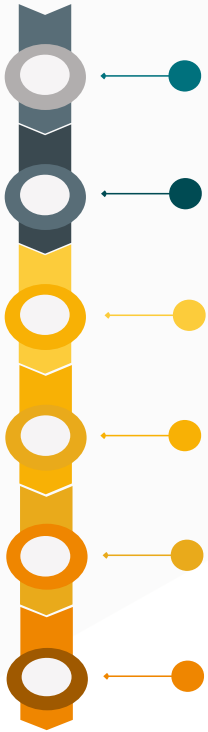
Háború „előkészítése” orosz részről

ACPM
Audit Consulting Project Management

A háború előtt komoly kibertámadást indítottak

2022. január	70 kormányzati weboldal deface-elése; kormányzati, non-profit és információtechnológiai szervezetek támadása; APT támadások
2022. február 15.	Védelmi minisztérium, hadsereg, két legnagyobb bank főként weboldalainak támadása (bank esetén mobil és ATM hálózat is);
2022. február 23.	Újabb DDOS támadások és rombolóvírus támadások (katonai, védelmi, politikai, légiközlekedési és IT célpontok ellen, több 100 szerveren)

Orosz – ukrán kiberháború



- 2022. február 24-től háború (kiber) is
- Ukrán oldalon a NATO kibervédelmi csoportja vélhetően segített
- Mindkét oldalon beszállnak hacktivista csoportok
- Anonymus belép ukrán oldalon
- Nemzetközi hacktivista toborzás (akár pénzért is)
- Meglepően(?) gyors és érdekes eredmények ukrán oldalon

ACPM
Audit Consulting Project Management

- Atomhatalmak / más országok / kritikus infrastruktúra / … otthonról történő hackelése kockázatos!

Kérjük ezt ne próbáljátok ki otthon!

(És a képpel ellentétben a barátotoknál se!)

Háborús történések

ACPM
Audit Consulting Project Management

- Számos orosz kormányzati weboldal (Kreml, Kormány); az állami televízió; vezető média oldalak elesnek
- Orosz IT rendszerekbe történő bejutások, adatlopás: gázállomás, fegyvergyártó cég, orosz gazdaságfejlesztési minisztérium, központi bank, Roszkozmosz műholdak (?)
- Több ezer támadás / incidens orosz rendszerek ellen
- Az ukrán oldal nagyon erősen kommunikál / Az orosz nem igazán
- Meglepőek-e a gyors eredmények?
- **A kibertérben támadóelőny van!**

Érdekes kapcsolódó területek

ACPM
Audit Consulting Project Management

News és Fake news; hírgyártás és terjesztés

Tiltakoznak a szoftverfejlesztők: Protestware

Katonai és civil veszteségek, elért „eredmények”

A közösségi média újra megmutatja, az információ terjesztés jó és rossz oldalát is: élőben közvetített háború

Közösségi média tartalmak és metaadatok használata a hadviselésben / adathalász támadások / túlzott megosztások

(Lehetséges) következmények

ACPM
Audit Consulting Project Management

- Komolyabban vesszük az **IT biztonságot**! (???)
- Komolyabban vesszük a meglévő szabályozási környezetet, ajánlásokat! (?)
- Legalább állami / kritikus infrastruktúra / média / … / szinten komolyabban vesszük a témát. (NIS irányelv, EU Cybersecurity Act, hazai jogszabályok)
- **2022.04.14.**(!) Oroszország benyújt az ENSZ-nek egy globális egyezménytervezetet a bűnözés elleni küzdelemről az informatikai és kommunikációs technológiák területén
- Hazai (és EU) IT ipar fejlesztése
- Tanúsítási rendszerek elterjedése
- Ellátási láncok biztosítása

Miért jó az ACPM csapatban dolgozni?

ACPM
Audit Consulting Project Management

Mert ilyen fancy dolgokkal foglalkozunk:

- IT biztonsági szabályozás, folyamatok, eljárások
- Gyakorlati IT biztonsági vizsgálatok (pl.: etikus hacking, betörés tesztelés, forensics)
- IT biztonsági oktatás
- IT biztonsági kutatás és fejlesztés

✉ hr@acpmit.com

ACPM
Audit Consulting Project Management
BUDAPEST • DUBAI • KIGALI • KUALA LUMPUR
NAIROBI • PRETORIA • SHANGHAI • WIEN

Köszönöm a figyelmet!

ACPM IT Tanácsadó Kft.

Széchenyi István tér 7-8.
Budapest, 1051
www.acpmit.com