Selhávání lidského faktoru a začínající éra kybernetických válek

Tomáš Pojar

Cevro Institut/CyberGym

Sílící útoky

- Počet útoků se celosvětově zvyšuje, zvyšuje se i jejich účinnost.
- Česká republika neleží na frontové linii, pro české statistiky však platí to samé.
- Co se děje dnes v USA, Izraeli, Británii…, bude se dít pouze s mírným zpožděním i u nás.

Izraelská zkušenost I: „Cyber Command“

- Izrael je ve válce 67 let, od svého vzniku.
- V kybernetické válce je již přes dvacet let.
- Kybernetické bojiště je podobné reálnému bojišti.
- Nelze oddělit ofenzívu a defenzívu.
- Sebelepší stroje nenahradí lidi
- Klíčový faktor: „Boots on the ground“ = vojáci v poli.
- Dnešní válka je vedena na zemi, ve vzduchu, na moři a v kyberprostoru = Cyber Command.

Izraelská zkušenost II: Síla lidského faktoru

- Je nutné poznat nepřítele.
- Čekat na útok znamená prohrát.
- Největší slabina/síla obrany i útoku je lidský faktor.
- Pozor na sociální inženýrství!

- 72 % úspěšných kybernetických útoků je provedeno s pomocí zaměstnanců (vědomou i nevědomou).
- Na každých 10 miliónů USD investovaných do hardwaru a softwaru je pouze 8 dolarů investováno do lidí.
- DELL: během následujících dvou až tří let plánuje 74 % firem zvýšit výdaje na kybernetickou bezpečnost včetně vzdělávání zaměstnanců.

Kritická infrastruktura

- Státní správa
- Obrana a bezpečnost
- Energetika
- Telekomunikace
- Finanční sektor
- Doprava
- Zdravotnictví
- Média

EU Observer: Útok na francouzský televizní kanál TV5 ve středu 8. dubna podtrhuje evropskou zranitelnost z pohledu high-tech kybernetické kriminality.

Státní správa

- **Estonsko 2007**: Vlna kyberútoků na webové stránky estonských organizací a institucí, bank, ministerstev, médií…
- **Gruzie 2008**: Klíčové části gruzínského internetu přesměrovány na servery v Rusku a Turecku. Dočasně se sice podařilo přesměrovat gruzínský internet na servery v Německu, během několika hodin se však hackerům podařilo opět získat kontrolu nad gruzínským internetem prostřednictvím serverů ruských.

- **Ukrajina 2014:** Počet (a síla) kybernetických útoků vedených z Ruska na Ukrajinu se výrazně zvýšil v polovině roku 2014. Cílem nebyla pouze samotná infrastruktura Ukrajiny, ale i další cíle v USA a Evropě.

Energetika a průmysl

- **2010: Objeven červ Stuxnet napadající íránský jaderný program.**
- **2011: Ukradeno 77 millionsů účtů Playstation Network a Sony Online Entertainment včetně informací o kreditních kartách uživatelů. Škoda vyčíslena až na dvě miliardy dolarů.**
- **2012: Na deset dní vyřazeno z provozu třicet tisíc počítačů saudské ho ropného gigantu Aramco.**
- **2014: Podle zprávy Federálního úřadu pro informační bezpečnost způsobily hackeři vážné škody klíčové německé ocelářské firmě.**
- **2015: Masivní blackout , který postihl většinu z 81 tureckých provincií, mohl podle turecké vlády způsobit kyberútok.**

Finanční sektor

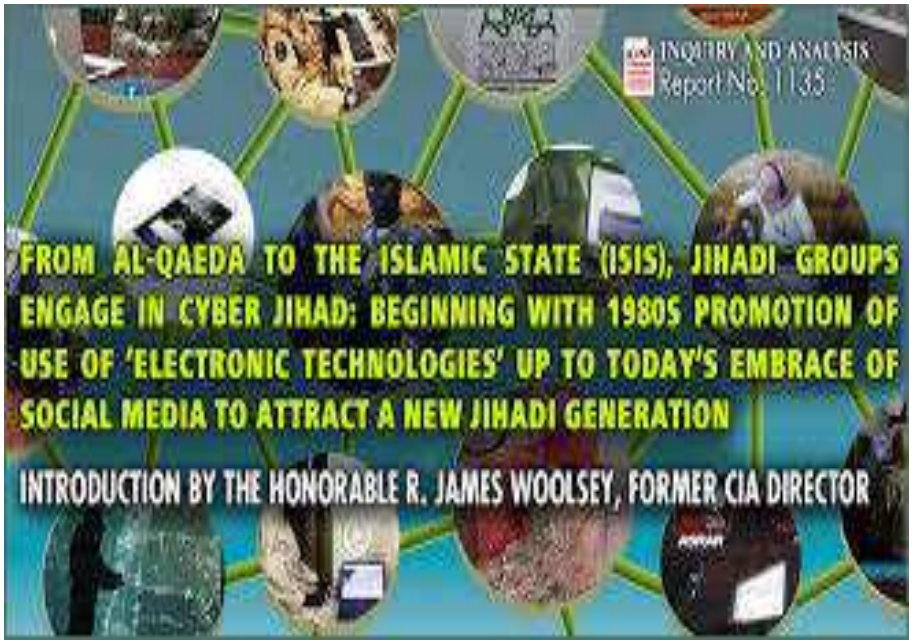
- 2012: Útok ze serverů z Ruska, Albánie a Číny způsobil zmizení až dvou a půl miliardy dolarů z účtů v Evropě, Spojených státech a v Jižní Americe.
- 2013: Informace o 40 miliónech účtů byly ukradeny v důsledku napadení prodejního řetězce Target.
- 2014: J.P. Morgan: Útok na banku postihl 76 miliónů domácností a 7 miliónů firem.
- 2015: Kaspersky - ze stovky bank a finančních institucí zmizela miliarda GBP.

Útoky Cyberhcaliphate v roce 2015

- Nejvyšší velení americké armády
- Newsweek
- Francouzská TV5
- BBC

<u>Cyber Command:</u>

- **Státy: Sýrie, Severní Korea, Írán…**
- **Teroristické organizace: Islámský stát, Al-Kajda, Hizballáh, Hamás….**



Cyber Defense

- Analýza hrozeb
- Aktivní obrana
- Investovat do hardwaru, softwaru a lidí

Nezapomínat na lidi!

- Netýká se pouze IT oddělení
- Netýká se pouze krádeží dat a peněz
- Je třeba myslet na kybernetickou ochranu napříč celou organizací
- Klíčový trojúhelník pro obranu: CEO-CIO-CSO

MBA: Management a kybernetická bezpečnost a

Třísemestrální program

- Vysoká škola CEVRO Institut
- Český institut manažerů informační bezpečnosti (ČIMIB)
- Asociace obranného a bezpečnostního průmyslu (AOBP)
- PricewaterhouseCoopers (PwC)
- Corpus Solutions
- odborníci z Národního centra kybernetické bezpečnosti (NBÚ)

- pro klíčové manažery, bezpečnostní pracovníky a vedoucí pracovníky v ICT v soukromé i veřejné sféře
- zaměřený na ochranu podnikové i státní ICT infrastruktury a pochopení principů řízení kybernetické bezpečnosti
- reflektující nově schválený zákon č. 181/2014 Sb. o kybernetické bezpečnosti účinný od 1. ledna 2015

www.vsci.cz, mba@vsci.cz

Připraveným štěstí přeje!