KYBERPROSTOR II

Mgr. et Mgr. Jakub Fučík

Globální doména v rámci informačního prostředí, která je definována nezávislou sítí informačně-technologických infrastruktur, jakými jsou Internet, telekomunikační sítě, počítačové systémy a vestavěné procesy a řídící jednotky (MO USA)

Charakteristika kyberprostoru

- Vytvořen člověkem
- Komplexní struktura
- Specifické hranice

Kybernetický prostor

- **Provázané vrstvy (dimenze):**
  - **Fyzická infrastruktura** (kabeláž, routery, satelity atd.)
  - **Vrstva protokolů**, zabezpečující komunikaci mezi prvky
  - **Sémantická vrstva**, zahrnující data uložená, zpracovávaná, přenášená
  - **Pragmatická, kognitivní vrstva** - interakce s člověkem:
    - Vstupy
    - Vytváří kyberprostor
    - Je kyberprostorem ovlivňován – zdroj informací
    - Manipulace

Kybernetický prostor jako pátá doména – pro a proti

- - Kyberprostor je stvořen, užíván, měněn lidmi
- - Časově proměnný, nestabilní, nespojitý
- - Prostor pro kybernetické operace je dán zranitelností informačních systémů
- - **Tvárný** - podstatou je architektura, připojení, administrace, řízení přístupu – lze realizovat vlastní zabezpečení
- - Segmenty kyberprostoru mohou být vytvářeny, ale i ničeny
- - je obsažen ve všech ostatních doménách
- + Operace se vedou jako v jiných doménách – (průzkum, útok, obrana)

Základní pojmy

- **Kybernetická bezpečnost** (Cyber security)
  Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.

- **Kybernetická obrana** **(**Cyber defence)
  Obrana proti kybernetickému útoku a zmírňování jeho následků. Také rezistence subjektu na útok a schopnost se účinně bránit

Základní pojmy

- **Kritická infrastruktura (**Critical infrastructure)
  Systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva.

- **Kritická komunikační infrastruktura** (státu) (Critical communication infrastructure)
  V případě státu: zákonem jasně vymezený komplex služeb nebo sítí elektronických komunikací, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.

Kybernetické útoky

- Nepřátelské aktivity v kyberprostoru
- 2 druhy
  - kybernetická špionáž
  - kybernetické útoky

Základní otázky

- Co/kdo je hrozbou?
- Jaké jsou chyby v zabezpečení?
- Jaké jsou následky útoku?

Hrozba

- Detekce kybernetického útoku
- Určení „útočníka“ – státní vs. nestátní aktér
- Možnost přisouzení?

Zranitelnost

- 3 hlavní oblasti
  - Úmyslné nebo neúmyslné aktivity osoby s (legálním) přístupem do systému
  - Dodavatelský (zásobovací) řetězec
  - Vnitřní chyby a nedostatky v systému

Následky

- Přímé a nepřímé
- Zamýšlené vs. nezamýšlené
- Collateral damage

Kybernetické válečnictví (cyberwarfare)

- Z logiky věcí vyplývá, že je podmnožinou kyberprostoru
- Nemá smysl jej uvažovat samostatně, ale ve spojení s vojenskou operací
- **Kybernetická válka** (Cyber war)
  - Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků.
  - Válečné akty v a kolem kyberprostoru prostředky ICT (tj v rámci kyberprostoru, z kyberprostoru ven, a zvenku do kyberprostoru). V širším smyslu, podpora vojenských operací v tradičních doménách prostřednictvím operací vedených v kyberprostoru.

Kybernetické operace

- Vytváření kyberprostoru (není analogie s jinými doménami)
- Pasivní obrana
- Aktivní obrana
- Vytěžování nebo operační příprava prostředí
- Útok
- Definování potřebných schopností k vedení misí v, prostřednictvím a z kyberprostoru
- **Informační operace** – využití Internetu, sociálních sítí

Kybernetické operace

- Úkolem je zajistit operační volnost
- Kybernetický útok může zneškodnit segmenty kyberprostoru klíčové pro splnění mise
- **Fyzický efekt** (zničení zařízení)
- **Logický efekt** (zničení dat, znemožnění přenosu dat, zničení nebo ochromené informačního systému pro podporu rozhodování)
- **Kognitivní efekt** – informační válka, působení na rozhodovací procesy a schopnosti

Specifika kybernetických operací

Obrana:

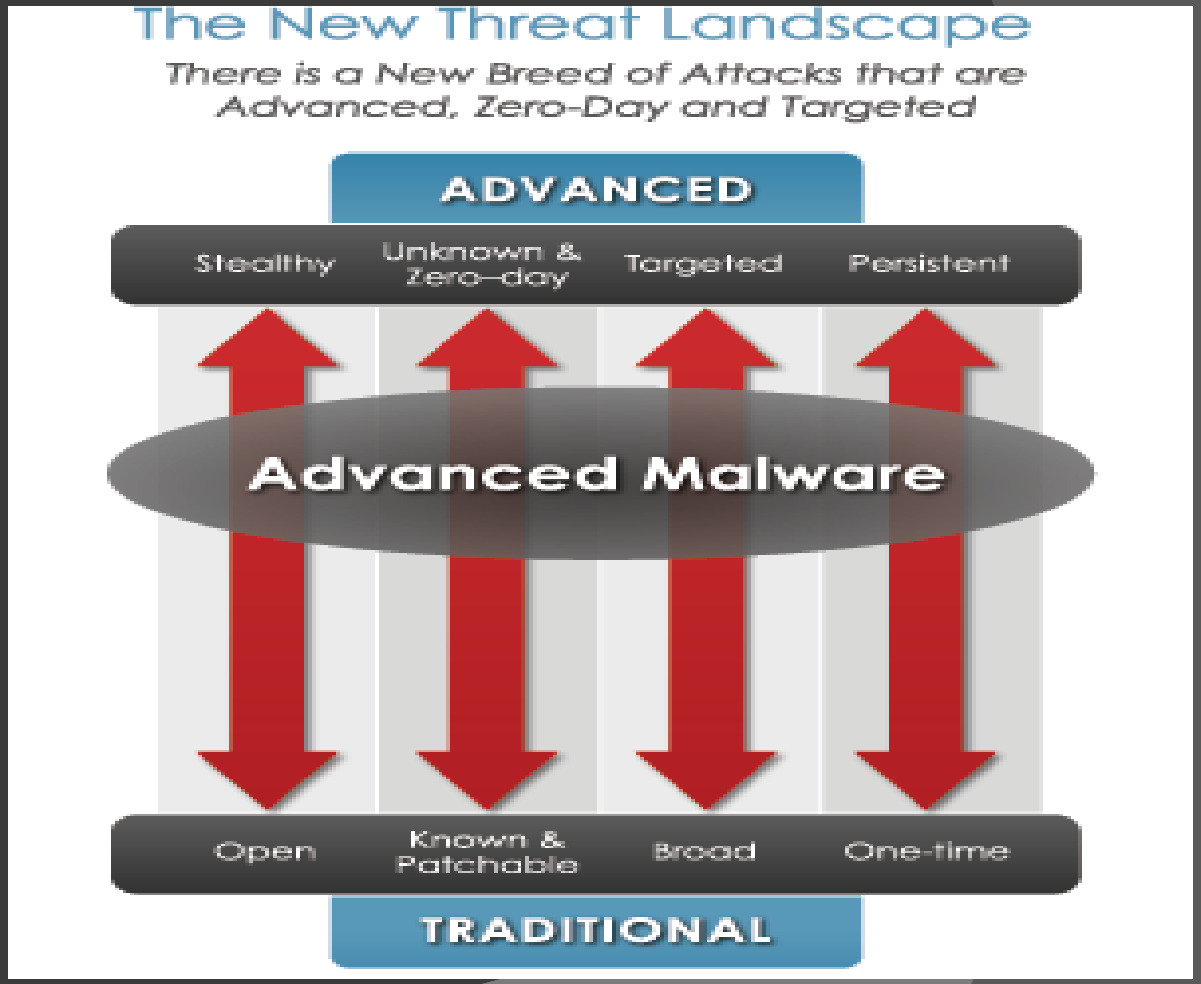
- Útočník se dostane jen tam, kam jej pustím, ale
- Sofistikovaný malware je těžké detekovat
- Samotné fyzické oddělení (air-gap) nezaručí bezpečnost

Útok:

- Musím znát zranitelnosti protivníka (průzkum v kyberprostoru, zpravodajství)
- Teprve pak lze vyvíjet kybernetickou zbraň
- Doručení
- Spuštění
- Těžko předvídatelný efekt, na rozdíl od konvenčních zbraní

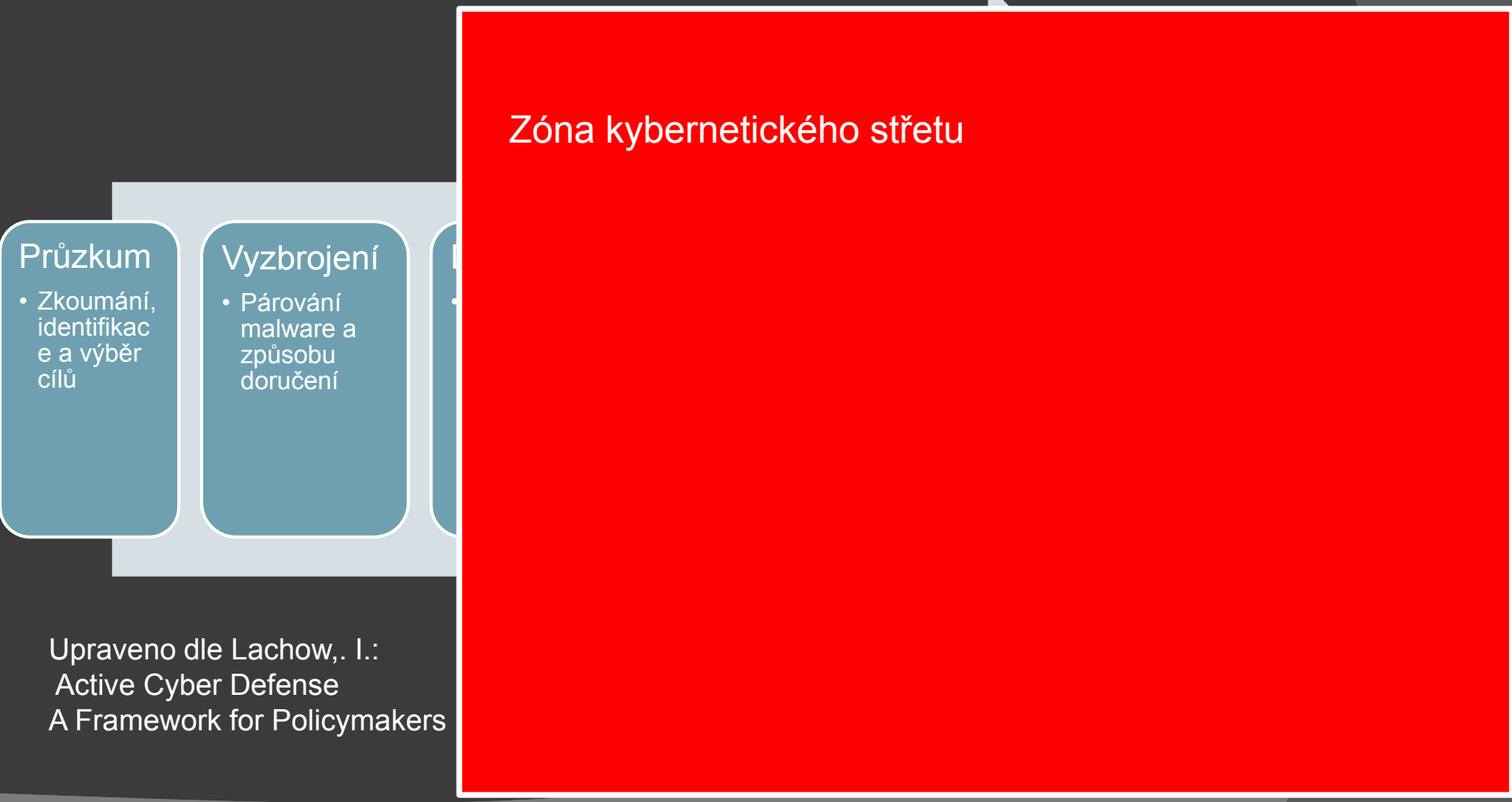
Soudobé kybernetické útoky

- Cílené
- Skryté
- Personalizované
- Zranitelnost nultého dne
- Soustavné



Zdroj: http://www.threatprotectworks.com/Next-Generation-Threats.asp

Fáze pokročilého kybernetického útoku



Upraveno dle Lachow,. I.:
Active Cyber Defense
A Framework for Policymakers

Cyber attack, cyber war - problémy

- **Aplikace mezinárodního práva v kyberprostoru**
  - Chybějící legislativa versus lze aplikovat stávající právní normy?
  - Problém identifikace útočníka (agresora)
  - Problém protiútoku, aktivní obrany
    - Proti komu (problém identifikace útočníka)?
    - Je adekvátní?
    - Je legální?
- **Problém reakce v čase** – systémy umělé inteligence, kontrola člověkem versus automatická reakce
- **Nasazení dronů, umělá inteligence**

DĚKUJI ZA POZORNOST