Kyberprostor – dějiště neviditelných konfliktů

Ing. Dušan Navrátil

Kybernetické útoky Na Ministerstvo České republiky

příklad kyberšpionáže.

Kybernetický útoky na nemocnice v ČR

příklad kyberkriminality

- **11. 12. 2019 – Nemocnice v Benešově**
- **Co se stalo: - Emotet – získal přístup**
  - Trickbot – sbíral data a připravoval útok
  - Ryuk – ransomware - zašifroval data
- **Dopad: Výrazné omezení provozu nemocnice**
- **Finanční dopad: 40-50 milionů Kč**
- **Doba trvání narušení: Nemocnice obnovila provoz koncem prosince 2019, proces obnovy infrastruktury pokračoval dále i v lednu 2020**

12. 3. 2020 – FN Brno

- **Co se stalo: Kolem 01:00 v noci útočník získal práva doménového admina a začal šířit ransomware, IT odd. situaci zachytilo a začalo odpojovat systémy**
- **Dopad: Odložení plávaných úkonů, nemožnost ukládat data, celkové výrazné omezení všech činností**
- **Finanční dopad: odhadem řádově stovky milionů**
- **Některé části nemocnice byly více jak týden po útoku stále odstaveny**

Válka na Ukrajině

příklad hybridní války v kyberprostoru jako součást válečného konfliktu

- **2014 leden - První známý modulární malware BlackEnergy: intenzivní útoky na cíle na Ukrajině a v Polsku**
- **2014 únor - Začátek okupace Krymu.**
- **2014 duben - Začátek války na Donbase.**
- **2014 květen - Kyberútoky za účelem manipulace prezidentských voleb.**
- **2015 prosinec - Malware BlackEnergy cílí na čtyři distribuční stanice energetické infrastruktury na Ukrajině a způsobí částečný blackout.**
- **2016 prosinec - Malware Industroyer od stejných autorů jako BlackEnergy cílí na systémy přenosové sítě na Ukrajině, způsobí částečný blackout a napadené systémy šifruje. Dále Android aplikace, kterou využívá Ukrajinské dělostřelectvo k nastavení 122 mm houfnic, obsahuje spyware, který nepříteli skrytě odesílá polohu mobilního telefonu; na tuto pak nepřítel soustředí konvenční útok**
- **2017 červen - Malware NofPetya se v rámci útoku na dodavatelský řetězec prostřednictvím aktualizace účetního software MeDoc šíří do až 80 % ukrajinských společností, kde šifruje napadené systémy. 2017 červen Malware NofPetya se v rámci útoku na dodavatelský řetězec prostřednictvím aktualizace účetního software MeDoc šíří do až 80 % ukrajinských společností, kde šifruje napadené systémy.**

- **2022 - leden Malware WhisperGate cílí na státní úřady na Ukrajině, exfiltruje databáze o státních zaměstnancích, policistech a vojácích (včetně například adres) a poté data na napadených systémech šifruje.**
- **23. únor - V předvečer vojenské invaze na Ukrajinu malware HermeticWiper (sestaven 28. 12. 2021) cíleně útočí na organizace na jejím území. Zároveň probíhá masívní DDoS útok na webové servery úřadů.**
- **24. únor - Přibližně hodinu před (konvenčním) útokem kybernetický útok na systémy poskytovatele satelitních služeb Viasat, který využívala mimo jiné ukrajinská armáda ke komunikaci, vyřazuje tento z provozu. Malware IsaacWiper (sestaven 19. 10. 2021 jinou skupinou než HermeticWiper) šifruje napadené systémy. Začátek invaze na Ukrajinu.**
- **březen - Kybernetické útoky na sdělovací prostředky za účelem jejich vyřazení z provozu (i konvenční útok na vysílač v Kyjevě) a pokusy ochromit instituce vlády i místní samosprávy. Malware CaddyWiper infiltruje systémy několika ukrajinských institucí. E-mailem a na sociálních sítích cílená kampaň nabádá vzdát se a spolupracovat s ruskou armádou, podpořeno deep-fake videem „s prezidentem Zelenským“. Odhalení a rozbití farem s falešnými účty. Kybernetický útok proti Ukrtelecom**
- **duben - Multiplatformní malware Industroyer2 útočí na systémy přenosové sítě a způsobuje částečný blackout. Lokální poskytovatelé datového připojení v Chersonské oblasti jsou donuceni přesměrovat datovou komunikaci přes Krym a území RF**
- **červenec - Falešná Android aplikace (spyware) a web pod hlavičkou pluku Azov sbírá informace o největších aktivistech.**

Definice kyberprostoru – existuje mnoho definic

Dle Zákona o kybernetické bezpečnosti (ZKB)

Kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Jiná definice

Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje:

a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery atd..),

b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému,

c) spojení počítačových sítí,

d) uživatelské vstupy a uzly zprostředkovatelů spojení,

e) informace – uživatelská data.

Pozn. Otázka je, zda analogová data a komunikace jsou součástí kyberprostoru.

Význačnou a charakteristickou vlastností kyberprostoru je, že žádná jediná centrální moc nekontroluje všechny sítě, které tvoří tuto doménu, tudíž nekontroluje kyberprostor.

Stejně jako v reálném světě neexistuje světová vláda, ani kyberprostor postrádá institucionálně předem definované hierarchické centrum.

Západ, Čína a Rusko vnímají kyberprostor jinak. Proto v současné době obtížné, až nemožné vytvořit mezinárodní dohody a standarty.

Všichni tři aktéři se shodují na tom, že kyberprostor (či prostředky, které nabízí) lze využít ke kybernetickým útokům, kybernetické válce, nebo jako psychologickou zbraň, a to v obdobích války a míru.

Západ vychází ze svých základních hodnot, kterými jsou demokracie, lidská práva, právní stát, svoboda projevu, přístup k informacím, právo na soukromí. Lidská práva a základní svobody jednotlivců musí být respektovány a dodržovány stejným způsobem on-line i off-line.

Čína vnímá kyberprostor jako hrozbu pro stát/ Komunistickou stranu. To znamená, že není vnímán pozitivně, jak ho vnímá Západ, jako nástroj liberalizace. Z vojenského hlediska je považován za nové bojiště a skvělý nástroj pro armádu. V rámci mezinárodního prostředí Čína vnímá kyberprostor jako nové citlivé místo u svých soupeřů (nikoliv však u sebe – hrozba pro Čínu samotnou je odlišná, přichází zevnitř, ze společnosti). Přístup ke kyberprostoru je útočný a jako hrozba č. 1 jsou vnímány USA. Zásadním je snaha o dosažení kontroly sítí a technologická převaha. Čína přemýšlí v dlouhodobém horizontu, uvažuje o převzetí iniciativy, zahrnuje kyberprostor do svého vojenského přemýšlení. Její přístup se zaměřuje spíše na ovlivnění protivníkova rozhodování (v duchu čínského strategického myšlení, které má svoje počátky u Sun-C (Umění války), je kladem větší důraz na přemýšlení, než na bojování). Záměrně nepoužívá slovo cyber, ale slovo informationization, by zdůraznila jiné pojetí.

Rusko přistupuje ke kyberprostoru zejména ze svého vnímání pocitu ohrožení. Podobně jako Čína vidí Rusko kyberprostor jako určitou hrozbu pro svoji vnitřní stabilitu. Kyberprostor využívá k ke kybernetické špionáži, k destruktivním kybernetickým útokům a úspěšným dezinformačním kampaním. Nemůže soupeřit na poli technologií.

Jiné vnímání kyberprostoru Čínou a Ruskem je zásadní globální problém. Např. pojem válka je vnímán podobně, což umožňuje mezinárodní dohody. Např. různý vyklad pojmu demokratické volby v dohodě v Postupimi (1945) byl jedním z důvodů Studené války. Nejednotnost vnímání kyberprostoru přináší problém v uzavírání mezinárodní dohod.

Boj o rozvojové země, kam se přikloní v chápání a standardů kyberprostoru. Důležitá je kybernetická diplomacie. Nutnost pravidel např. z hlediska kyberkriminality, řešení anonymity atd. OSN

Aktéři v kybernetickém prostoru

. státní aktéři a státem sponzorované skupiny

Jsou to nejsofistikovanější a nejnebezpečnější útočníci z hlediska jejich působení a náročnosti jejich odhalení. Tito útočníci disponují zdroji, intelektuálnějšími i finančními pro dlouhodobé, vytrvalé a vysoce sofistikované kampaně. Většinou se jedná o precizně cílené operace ve snaze získat přístup k politicky, vojensky či diplomaticky významným informacím, nebo kompromitovat aktivity oponenta, zničit informace nebo narušit schopnost např. komunikace. Státní aktéři mohou být reprezentováni příslušníky zpravodajských služeb cizí moci, vojenskými složkami, ale také „volnou“ skupinou, která je neprovázána se státním aparátem, aby bylo možno odmítnout zodpovědnost v případě prozrazení.

. kyberzločinci

Motivem je zejména osobní obohacení. Nejčastěji útočí s cílem monetizovat data, která zašifrují data, formou výpalného získávají finanční prostředky. Používají sociální inženýrství malware. Využívají dělbu práce a jejich služby je možno objednat. Využívají i jiných způsobů, třeba krádež identity a další. Každý může být cílem útoku!

. bývalí i současní zaměstnanci a dodavatelé

Tito mají přístup k sítím datům, či autentizačním informacím. Jedná se o hrozby zevnitř, tzv, Insider threat, vědomě zneužívající informací či zranitelností. Motivací je obvykle snaha se obohatit, pomstít či např. poukázat na domnělé neetické chování zaměstnavatele.

. hactivisté

Jsou většinou politicky, nábožensky nebo sociálně motivovaní aktéři. Jejich cílem je zlepšení reputace nebo změna, které nejsou schopni docílit běžnými dostupnými a legálními prostředky. Obvykle používají DDoS útoky, kompromitaci webových stránek s podtextem zobrazeným pro uživatele nebo zveřejňování dat za účelem kompromitace nebo odhalení, tzv. *doxing*.

. teroristické skupiny

Které jsou v kybernetickém prostoru aktivní v rovině rekrutace, šíření propagandy, výcviku, získávání finančních prostředků. Týkají se spíše snahy o exfiltraci informací a následné snahy o demoralizaci nepřítele či vyhledávání cílů pro kinetické útoky. Projevy kyberterorismu ve smyslu destruktivního působení jsou vzácné.

Vojenské domény:

. země

. moře

. vzduch

. vesmír

. kyberprostor

Kybernetický prostor byl vyhlášen jako 5. doména na Varšavském summitu NATO (červen 2016). Ve 4 tradičních doménách konfliktu je hranice a limity jasně dané, v kybernetického prostoru však veškeré hranice absentují a limity jsou nejasné. Kybernetický prostor a ICT dnes propojují všechny oblasti boje, zajišťují její funkčnost, a zároveň jsou na něm i kriticky závislé.

Několik základních charakteristik kybernetického prostoru:

. **anonymita** – identita uživatele není jasně prokazatelná a garantovaná žádnou autoritou

. **asymetričnost** – činnost v kybernetickém prostoru může mít významný dopad na ostatní uživatele sítě bez ohledu na význam a důvěryhodnost uživatele, který tuto aktivitu vyvinul

. **neexistence hranic** – aktivity v kybernetickém prostoru nejsou omezovány žádnou jurisdikcí nebo suverenitou, právním systémem nebo kulturou

. **okamžitost** – akce provedená v kybernetickém prostoru může mít okamžitě celosvětový dopad

. **volný vstup i ukončení pobytu v něm** – kdokoliv, kdykoliv může do kybernetického prostoru vstoupit, ale také v něm může ukončit svoji aktivitu

. **interakce** – interaktivní činnost v něm mohou vytvářet znalosti a mohou též vézt k významnému ovlivnění ostatních uživatelů

. **nízké náklady** – finanční náklady na působení v kyberprostoru jsou nízké oproti výsledkům

Bezpečnostní hrozby pro stát, společnost a jednotlivce prudce vrostly využíváním kyberprostoru.

Příklady proměn bezpečnostních hrozeb:

Špionáž – krádeže dat – dešifrování.

Sabotáž – ničení dat – ovlivňování řídících technologických procesů – útoky na informační systémy vedoucí k fyzickému zničení eventuelně k ohrožení životů.

Ovlivňování dodavatelských řetězců.

Psychologická válka – ovlivňování veřejného mínění – ovlivňování voleb – oslabení vůle k odporu – rozložení společnosti – využívání dezinformací – vyvolání stavu nedůvěry v pravdivosti všech informací.

Kriminalita

Hrozby z pohledu využívání kyberprostoru.

Cyber-dependent (kyberneticky závislá) je hrozba, kterou lze realizovat pouze pomocí počítačů, počítačových sítí nebo jiných forem informačních komunikačních technologií (ICT). V podstatě bez internetu by tyto hrozby nemohly být realizovány.

Cyber-enabled (kyberneticky umožněná) je tradiční hrozba, která je ve vnějším fyzickém světě, kterou lze realizovat bez použití počítače. Realizace této hrozby, se však vynálezem a používáním internetu přeneslo na zcela novou úroveň. Její rozsah a dosah se zvýšil pomocí ICT nebo informačních komunikačních technologií.

Cyber-supported (kyberneticky podporovaná) je hrozba která je realizovaná ve fyzickém světě. Při realizaci hrozby, kromě realizace v reálném světě je využíván i kyberprostor.

Nové technologie v kyberprostoru – nové hrozby a rizika

- **umělá inteligence**
- **kvantová výpočetní technika**
- **?**
- **?**

Dotazy?

Diskuze.

Co by jste se chtěli ještě dozvědět?