Kyberprostor – dějiště neviditelných konfliktů

Ing. Dušan Navrátil

„Žvásty o nejrůznějších kybernetických útocích jsou tak trochu móda.“

Miloš Zeman, prezident České republiky, 5. 2. 2017

Jsou zprávy o kybernetických útocích žvásty-?

Leden 2022

- Více než polovina zdravotnických zařízení připojených k internetu obsahuje zranitelnosti
- Ukrajinské státní instituce se staly obětí wiperu a defacementu
- Albánská prokuratura vyšetřuje únik osobních údajů až pětiny obyvatel země
- Severokorejský malware Konni byl použit při útoku na ruské ministerstvo zahraničí

Únor 2022

- Ukrajinu, Litvu a Lotyšsko zasáhl destruktivní Wiper. Na Ukrajinu cílí ruské i běloruské skupiny
- Anonymous a další hacktivisté pomáhají Ukrajině. Kyjev rekrutuje hackery k útokům na Rusko
- V souvislosti s krizí na Ukrajině hrozí ruský útok na bankovní systémy EU a USA
- Ruská státem podporovaná skupina cílí na ukrajinské instituce a organizace
- Britské ministerstvo zahraničí terčem závažného kyberútoku
- Malware ShadowPad spojen s čínským Ministerstvem státní bezpečnosti a čínskou armádou

Březen 2022

- Při útoku na satelitní společnost Viasat na Ukrajině byl použit nový malware AcidRain
- Ukrajina byla terčem destruktivních kybernetických útoků pomocí wiperů
- Čínské kyberútoky na evropské diplomaty byly spojeny s konfliktem na Ukrajině
- Čínská APT skupina se zaměřila na ukrajinské cíle
- Anonymous kompromitovali sítě ruské společnosti Transněft a ruské centrální banky a zveřejnili desítky GB dat

Duben 2022

- České weby byly napadeny DDoS útoky ze strany Ruska
- Neutajované a část utajovaných sítí maďarského ministerstva zahraničí kompromitovali ruští útočníci
- Německá policie rozbila darknetový černý trh Hydra
- Některé ransomwarové gangy útočí na Rusko. Microsoft zasáhl infrastrukturu APT28

Květen 2022

- Ředitelství silnic a dálnic bylo cílem ransomwarového útoku
- Ruská skupina Killnet provedla sérii DDoS útoků
- Kybernetický útok na satelitní systémy společnosti VIASAT byl atribuován Ruské federaci
- Ruská APT29 útočí na evropské diplomaty pomocí spear-phishingu
- Čínští hackeři útočí na ruské vládní a vojenské představitele
- Ruští hackeři zveřejnili e-maily předních zastánců Brexitu
- Západní sankce na Ruskou federaci komplikují činnost ransomwarových gangů

Červen 2022

- Litva zaznamenala nárůst DDoS útoků v důsledku zákazu přepravy zboží do Kaliningradu
- Proruská hackerská skupina Cyber Spetsnaz provádí kyberšpionážní útoky vůči NATO a západním státům
- US Cyber Command provedlo ofenzivní kybernetické operace v kontextu rusko-ukrajinského konfliktu
- Čínská APT skupina používá ransomware k zakrytí špionážních operací
- Ransomwarové skupiny cílí spíše na malé a slabé státy

Červenec 2022

- SKUPINA PREDATORY Sparrow provedla kyberútok vedoucí k požáru v íránské ocelárně
- APT29 provedla kyberútoky zneužívající cloudové služby Google drive a DropBox
- Ruská kyberkriminální skupina TrickBot systematicky útočí na ukrajinské cíle
- Čínské APT skupiny zintenzivňují útoky na ruské subjekty

Srpen 2022

- Tchaj-wan se stal cílem rušivých útoků během návštěvy Nancy Pelosi
- Čínská špionáž v USA sílí, Huawei byl zapojen do potenciálního ohrožení bezpečnosti jaderných zbraní
- Německá komora průmyslu a obchodu byla zasažena masivním kybernetickým útokem
- Webový prohlížeč čínské aplikace TikTok umí sledovat veškeré stisky na klávesnici uživatelů

Září 2022

- Albánie obvinila Írán z kyberútoků na vládní infrastrukturu, přerušila s ním diplomatické styky
- Společnost Mandiant odhalila napojení části ruských hacktivistických skupin na ruskou GRU
- Z portugalského Generálního štábu útočníci odcizili utajované dokumenty NATO
- Černá Hora byla terčem kybernetických útoků vůči vládnímu sektoru
- Čínské a severokorejské skupiny útočí na energetický sektor

Říjen 2022

- Výpadky telekomunikační a internetové sítě na Ukrajině doprovázely kybernetické útoky
- DDOS útoky proruské skupiny anonymous.ru zasáhly slovenské subjekty
- Společnost Meta nalezla 400 škodlivých aplikací určených ke krádeži přihlašovacích údajů
- Čínský majitel TikToku plánoval využít aplikaci k cílenému sledování jednotlivců v USA
- Dánský region zakázal nákupy kamerových systémů čínské společnosti Hikvision
- Podle norského premiéra je Rusko kybernetickou hrozbou pro tamní ropný a plynárenský sektoru

Listopad 2022

- Společnost Microsoft obvinila Čínu z rozsáhlého zneužívání zranitelností nultého dne
- Útoky ransomwaru Prestige na Ukrajinu a Polsko provedla ruská APT skupina Iridium
- Nový spyware pro Android pochází od čínských aktérů
- FBI varuje před rizikem zneužití sociální sítě TikTok čínskou vládou
- Instituce evropských států varují před povinnými aplikacemi Kataru pro návštěvníky MS ve fotbale
- Evropský parlament se stal cílem proruských hacktivistů. Šlo o reakci na označení Ruska za stát podporující terorismus
- Spojené státy zakážou import elektronických zařízení čínských firem a Spojené království jejich instalaci do vládních institucí

Prosinec 2022

- **Ruská APT skupina Seaborgium útočila na dodavatele armády Spojených států**
- **Ruští aktéři se snaží koupit zranitelnosti nultého dne k aplikaci Signal na šedém trhu**
- **Čínský aktér využívá USB zařízení ke kyberšpionáži proti cílům v jihovýchodní Asii. Útoky mířily i vůči cílům v Evropě a USA**
- **Kanadská pobočka Amnesty International byla zasažena kyberútokem, zřejmě ze strany čínského aktéra**
- **Kyberšpionážní skupina Cloud Atlas útočí proti Rusku, Bělorusku a jejich spojencům**
- **Po kyberútoku na dvojici švédských okresů byl vyhlášen stav krize**

Definice některých pojmů

Kybernetický prostor (Cyber space) je globálně propojený prostor, který se skládá z internetu a dalších počítačových sítí, digitálních zařízení, systémů, služeb a procesů na nich. Tím poskytuje globální infrastrukturu pro široké spektrum osobních, podnikatelských aktivit a pro jejich propojení.

Kybernetický prostor je veřejný, není nikým vlastněn – úřadem, - vládou, osobou nebo národem. Bezpečnostní aktivity v tomto prostoru musí být mezi různými zúčastněnými subjekty a na různých úrovních. Tyto subjekty by měly mezi sebou sdílet informace o rizicích a společně připravovat koordinovaná opatření proti abnormalitám a bezpečnostním incidentům.

Kybernetická hrozba (Cyber Treat) je hrozba, která se nachází v kybernetickém prostoru.

Kybernetické riziko (Cyber ¨Risk) je způsobené kybernetickou hrozbou. Je to pravděpodobnost škodlivých následků vyplývajících z hrozby.

Zranitelnost (Vulnrability) je slabé místo informačního systému nebo opatření, které může být využito hrozbou. Slabá místa mohou vést k neautorizovanému přístupu ke zdrojům systému.

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

Kybernetická bezpečnost (Cyber Security) je souhrn právních, organizačních, technických a vzdělávacích prostředků, směřujících k zajištění ochrany kybernetického prostoru.

Vlastní kybernetická bezpečnost chrání sféry vlivu soukromých osob, veřejného sektoru a veřejných institucí a představuje pojetí bezpečnosti na rozhraní mezi bezpečností v ekonomickém, politickém, či vojenském smyslu.

Kybernetická bezpečnostní událost (Cyber security Event) je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

Kybernetický bezpečnostní incident (Cyber Security Insurance) je kybernetická událost, která způsobuje ztrátu informační bezpečnosti nebo má dopady na procesní aktivity organizace.

Kybernetická bezpečnost je zastřešující termín pro široké spektrum bezpečnostních činnosti. Zajišťování kybernetické bezpečnosti de facto znamená snahu o zabránění útočníkovi v průniku do infrastruktury. Zahrnuje preventivní a reaktivní aktivity státu (a nejen státu) v oblasti ochrany dat, informací, systému, služeb a sítí. Smyslem je neustále navyšování integrity, odolnosti a robustnosti informační a komunikační infrastruktury.

Kybernetická kriminalita je trestná činnost, kterou, kterou lze definovat jako neautorizovaný přístup k datovému nosiči. Pod kybernetickou kriminalitou si můžeme představit např. neautorizované čtení, nakládání, vymazání zneužití, změny apod.

Kybernetická obrana je ochrana státu proti pokročilým závažným a nepřátelským kybernetickým útokům. Reaktivní část kybernetické obrany přichází na řadu ve chvíli, kdy útok byl úspěšný a je potřeba ho odrazit nebo vyvinout takové aktivity, aby bylo útoku předejito. Smyslem je aktivní působení v kybernetickém prostoru proti útočícím entitám a proti infrastruktuře používané k útokům. Důležitá je role ostrašení.

Kybernetická špionáž je užití nebo zneužití informačních a komunikačních technologií s cílem získat citlivé informace bez souhlasu držitele. Využívají ji státní i nestátní aktéři za účelem získání významné ekonomické, politické, technologické převahy.

Bezpečnost informací (Information Security) je ochrana důvěrnosti, integrity a dostupnosti informací. Kromě toho může zahrnovat další vlastnosti, např. autenticitu, nepopiratelnost a spolehlivost. Informační bezpečnost je bezpečnost informací v kybernetickém prostoru.

Důvěrnost (Confidentiality) je vlastnost, že informace není dostupná nebo není odhalena neautorizovaným jednotlivcům, entitám nebo procesům.

Integrita (Integrity) je zajištění správnosti a úplnosti informací.

Dostupnost (Availability) je vlastnost přístupnosti a použitelnosti na žádost autorizované entity.

Několiv faktů

Kybernetická bezpečnost naší země nikdy nebude absolutní, ale naší povinností je se k tomu stavu co nejvíce přiblížit

Nelze strojem porazit kybernetické útočníky

Pokud se někdo rozhodne, že bude útočit a destruovat a má dostatek financí, tak uspěje

V kybersvětě neexistují hranice, nelze použít klasické řešení

Bezpečnost je tak účinná, jak silný je nejslabší článek

Množství kybernetických hrozeb roste

Počet kybernetických útoků a jejich důmyslnost roste útočníci přicházejí s novými metodami útoků.

Současně se rozšiřuje možné útočné pole, přibyla např. zařízení internetu věcí. (IoT)

Neočekávejme, že kybernetické hrozby budou v příštích letech ustávat. Útočníci budou hledat nové způsoby, jak prolomit ochranu. Je nutné se jim postavit a nereagovat jen na útoky, které již proběhly, ale předvídat je a být na ně připraveni dříve než nastanou.

Rizika digitalizace

Závislost společnosti (jak soukromé, tak i státní sféry) na informačních a komunikačních technologiích (ICT)

Zabezpečení provozu kritické infrastruktury

Rostoucí podíl HDP závislý na ICT

Zvýšené riziko vážných škod v případě zneužití / cíleného útoku na sítě ICT

Kybernetická bezpečnost zahrnuje ochranu informací, dat, systémů a sítí.

Proč je to důležité?

. Vláda, armáda, policie, finanční instituce, průmysl a další entity kritické pro fungování státu provozují sítě a systémy a shromažďují, zpracovávají a ukládají velké množství informací a dat.

. Vývoj na poli technologií a konektivity zařízení neznamená vyšší zabezpečení, naopak – vede k většímu objemu útoků s významnějšími dopady.

Stát v kybernetickém prostoru již nemá příslovečný monopol na “násilí“, aktéry v kybernetickém prostoru se schopností útočit a páchat značné škody jsou nestátní subjekty – firmy a jednotlivci.

Neexistuje lidská činnost, která by nebyla provázána s digitalizací nebo internetem a neměla zároveň dopad na bezpečnost.

Aktéři v kybernetickém prostoru

- **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.

. 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.

. 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

. kybernetický prostor

Kybernetický prostor byl vyhlášen jako 5. doména na Varšavském sumitu 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.

Přisouzení (atribuce)

Atribuce kybernetického útoku je určení identity útočníka včetně kontextuálních informací, jako jsou motivace, fyzické umístění či detailní informace o způsobu provedení útoku. Vhledem ke specifickým vlastnostem kybernetického prostoru je atribuce složitější než v případě útoků konvenčními prostředky. Kybernetický prostor umožňuje cíleně a velmi dobře kamuflovat identitu, lokaci a další aspekty, běžně vedoucí k určení pachatele. Rozeznat, zda útočníkem je *ad hoc* sdružená skupina hackerů s kriminálním zájmem, či státní aktér s institualizovaným rámcem pro vedení ofenzivních operací v kybernetickém prostoru, je obtížné. O to více, pokud útočníci disponují štědrým rozpočtem a vydávají se skrze své jednání a nástroje jeden za druhého. Působení útočníků pod falešnou vlajkou, maskujících, své aktivity za nástroje užívané jiným aktérem, či využívání cizí infrastruktury, je jednou z největších výzev.

Otázky?

Sakra ptejte se!!!!!