Kriminalita v kyberprostoru

Ing. Dušan Navrátil

Kyberkriminalita

Kyberkriminalita neboli kybernetická kriminalita je definovaná jako „trestní činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některé z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.“

Kyberkriminalita

Kyberprostor je velmi výhodné prostředí pro páchání trestné činnosti.

- **anonymita** – vzhledem k tomu, že identita uživatele není jasně prokazatelná a garantovaná žádnou autoritou je totožnost pachatele obtížně vypátratelná a zejména dokazatelná
- **asymetričnost** – činnost v kybernetickém prostoru může mít významný dopad na zamýšlenou oběť, ale i na nezamýšlené oběti
- **neexistence hranic** – aktivity v kybernetickém prostoru nejsou omezovány žádnou jurisdikcí nebo suverenitou, právním systémem nebo kulturou, proto vymahatelnost práva a potrestání pachatele je obtížné mnohdy nemožné
- **nízké náklady** – náklady na kybernetický útok jsou nízké proti zisku a použité know-how je možné využít mnohonásobně použít
- **dělba práce** – pachatelé se specializují na určitou část trestného činu

Kyberkriminalita

Kyberprostor je velmi výhodné prostředí pro páchání trestné činnosti.

- **odbornost –** pachatel nemusí být odborník, ale uživatel nakoupených nástrojů a nebo služeb včetně upgradu, včetně možnosti „udělaných na míru“
- **snadné toky peněz** – díky kryptoměně rychlé, anonymní a globální toky peněz
- **byznys** – kyberkriminalita nese dnes všechny znaky byznysu
- **kriminální činnost státních aktérů** – mnohdy nemožnost postihnout takového pachatele
- **symbióza mezi státem kyberzločinci** – téměř nemožnost potrestat pachatele
- **nedostatečná legislativa** – legislativa má zpoždění vůči kyberkriminalitě
- **nepřipravenost represivních složek** – tyto složky mají nedostatečné kapacity, znalosti, zkušenosti a dostatek odborníků proti stále se vyvíjejícímu kyberzločinu
- **obtížná mezinárodní spolupráce** – někdy objektivně a někdy záměrně

Kyberkriminalita

Kyberprostor je velmi výhodné prostředí pro páchání trestné činnosti.

- **rychlost –** možnost podniknout útok a zmizet
- **snadná komunikace –** utajená komunikace na darkwebových globálních diskuzních fórech
- **snadné obchodování** – utajené obchodování na globálních darknetových tržištích a snadná „doprava“ nakoupených produktů po internetu – prodej zranitelností
- **využití umělé inteligence** – tvorba plně automatizovaných produktů
- **šifrování** – obtížně nebo vůbec nerozluštitelné šifrování používané kyberzločinci (kvantové počítače)
- **náskok** - neustálý náskok kyberzločinců nad represivními složkami (obecně platí, že kyberútočník má vždy náskok před obráncem)
- **investice** – vzhledem k obrovským ziskům kyberzločinci mohou značně investovat do nových nástrojů pro kybernetické útoky, a proto i obránci musí investovat do své bezpečnosti
- **výhody pro klasickou kriminalitu** – pomáhá páchat klasickou kriminalitu

Aktéři provádějící kyberkriminalitu

- vysoce kvalifikovaní jednotlivci nebo skupiny, kteří dokážou zašifrovávat a šířit software pro útoky na počítačové sítě a systémy, a to buď za účelem páchání trestné činnosti, nebo k tomu, aby ji umožnili jiným
- jednotlivci nebo skupiny s vysokou úrovní dovedností, ale nízkými kriminálními úmysly, například protestní hacktivisté
- jednotlivci nebo skupiny s nízkou úrovní dovedností, ale schopností používat kybernetické nástroje vyvinuté ostatními
- organizované zločinecké skupiny
- kyberteroristé, kteří mají v úmyslu způsobit maximální narušení a dopad;
- jiné státy a státem sponzorované skupiny zahajující kybernetické útoky s cílem shromažďovat informace o vládních, obraně, ekonomických a průmyslových aktivech, kompromitovat je, nebo narušovat provoz, nebo je destruovat
- insidři nebo zaměstnanci s privilegovaným přístupem k počítačům a sítím.

Kyberiminalita z pohledu využívání kyberprostoru.

Cyber-dependent (kyberneticky závislá) je kriminalita, 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 kriminalit, 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 kriminalita která je realizovaná ve fyzickém světě. Při realizaci hrozby, kromě realizace v reálném světě je využíván i kyberprostor.

Cyber-dependent (kyberneticky závislá) kriminalita

- **hacking** - nezákonné vniknutí do počítačových sítí

- **narušení nebo snížení funkčnosti** počítače a síťového prostoru

  - infikováním malwarem
  - útoky Denial of Service (DOS) nebo Distributed Denial of Service (DDOS).

Hacking

Hacking je forma narušení zaměřená na počítače, včetně mobilních telefonů a osobních tabletů. Jedná se o neoprávněné použití nebo přístup k počítačům nebo sítím využitím zjištěných slabých míst zabezpečení.

Hacking lze použít k:

- **shromažďování osobních údajů nebo informace použitelné pro zločince;**
- **změna webové stránky**
- **využití napadeného počítače k DDoS útoku – vytvoření botnetové sítě**
- **využití napadeného počítače k těžbě kryptoměn**

Narušení funkčnosti počítače

Malware (škodlivý software) se šíří mezi počítači a narušuje činnost počítače. Malware může být destruktivní, například mazat soubory nebo způsobovat pády systému, ale může být také použit ke krádeži osobních údajů. Některé programy mají dvojí použití. Mají legitimní funkci, ale mohou být také použity pro kriminální účely. Mezi typy malwaru patří:

- **Viry** jsou jedním z nejznámějších typů malwaru. Mohou způsobit mírnou počítačovou dysfunkci, ale mohou mít také závažnější účinky, pokud jde o poškození nebo smazání hardwaru, softwaru nebo souboru. Jsou to samoreprodukující se programy, které se šíří v rámci počítačů a mezi nimi. Vyžadují hostitele (jako je soubor) v počítači, aby fungoval jako přenašeč, ale nemohou infikovat počítač bez lidského zásahu ke spuštění nebo otevření infikovaného souboru.

- **Červi** jsou také programy, které se samy replikují, ale mohou se šířit autonomně v rámci počítačů i mezi nimi, aniž by vyžadovaly hostitele nebo jakoukoli lidskou činnost. Dopad červů proto může být závažnější než viry a způsobit zničení celých sítí. Červy lze také použít k vypuštění trojských koní do systému sítě.

• **Trojské koně** jsou škodlivé počítačové programy, které se prezentují jako užitečné, rutinní nebo zajímavé, aby přesvědčily oběť, aby si je nainstalovala. Tento malware může provádět funkce, jako je krádež dat, bez vědomí uživatele a může uživatele oklamat provedením rutinního úkolu, zatímco ve skutečnosti provádí skrytou neoprávněnou akci.

• **Spyware** je software, který narušuje soukromí uživatelů tím, že shromažďuje citlivé nebo osobní informace z infikovaných systémů a monitoruje navštívené webové stránky. Tyto informace pak mohou být předány třetí straně Spyware může být někdy skryt v adwaru (bezplatný a někdy nechtěný software, který vyžaduje sledování reklam, abyste jej mohli používat). Jedním z příkladů spywaru je software pro zaznamenávání klíčů, který zachycuje a předává stisknuté klávesy provedené na počítači, což umožňuje shromažďování citlivých dat, jako jsou hesla nebo podrobnosti o bankovních účtech.

•**Backdoor** jsou zadní vrátka pro útočníky. Jedná se o způsob přímého připojení k zařízení. V případě, že útočník tato zadní vrátka do počítačového systému objeví, zmocní se celého systému a může ovládat počítač stejně jako uživatel sedící přímo u něj. Do počítačového systému se dostane pomocí trojského koně, který se snaží otevírat komunikační porty za cílem usnadnit útočníkovi ovládání infikovaného systému na dálku. [16] RAT je zkratka pro anglické slovní spojení Remote Administration Tool.

- **RAT je nástroj umožňující se vzdáleně připojit k zařízení a díky tomu může sdílet obrazovku, přenášet soubory apod. RAT se do počítačového systému dostane pomocí implementace nebo aktualizace softwaru. Uživatel nic nezpozoruje, protože tento nástroj běží tajně na pozadí. Útočníkovi umožní shromáždit potřebná data nebo provádět další útoky prostřednictvím tohoto počítače. V poslední době byl RAT spojován i s útoky, kdy útočník po zmocnění se daného počítače chtěl po uživateli výkupné s příslibem, že mu počítač, resp. přístup do počítače vrátí.**

- **Rootkity a keylogger jsou skupiny spadající do malwaru. Rootkity jsou sada počítačových programů, které slouží k maskování přítomnosti škodlivého softwaru v infikovaném počítačovém systému. Rootkity mají tu vlastnost, že dokáží měnit chování celého počítačového systému. Keylogger je software, který snímá údery na klávesnici. Většinou je užíván za účelem zjištění přihlašovacích údajů uživatele.**

- **Ransomware může kromě dostupnosti narušit i integritu a důvěrnost dat. Ransomware je druh malwaru, který blokuje přístup k počítačovému systému nebo šifruje data na pevném disku. Následně je uživatel vyzván pod výhružkou útočníka k zaplacení tzv. výkupného. V poslední době se používá Doxware, který vyhrožuje uživateli zveřejněním jeho odcizených osobních údajů, pokud uživatel nezaplatí požadované výkupné. Také vyhrožuje zveřejněním důvěrných dat zákazníků a spolupracujících organizací. Většinou dochází k útoku pomocí phishingu, velmi nebezpečný je spear phishing využívající sociálního inženýrství, který svoji nebezpečnost znásobil využíváním umělé inteligence.**

Cyber-enabled (kyberneticky umožněná) kriminalita

Jedná se o zločiny, které nezávisí na počítačích nebo sítích, ale byly transformovány co do rozsahu nebo formy použitím internetu a komunikačních technologií. Spadají do následujících kategorií:

- **Ekonomická kyberkriminalita, včetně:**
  - **Podvod**
  - **Trestná činnost v oblasti duševního vlastnictví - pirátství, padělání atd.**

- **Online tržiště s nelegálním zbožím**

- **Škodlivá a urážlivá komunikace, včetně:**
  - **Komunikace zasílané prostřednictvím sociálních médií nebo jiných elektronických prostředků**
  - **Kyberšikana/trolling**
  - **Virtuální mobbing**

Cyber-enabled (kyberneticky umožněná) kriminalita

- **Trestné činy, které se konkrétně zaměřují na jednotlivce, včetně kybernetického násilí na ženách a dívkách („VAWG“):**
  - **Zveřejňování soukromých sexuálních obrázků bez souhlasu**
  - **Kybernetické pronásledování a obtěžování**
  - **Nátlak a kontrola**

- **Dětské sexuální delikty a erotické obrázky dětí, včetně:**
  - **Sexuální zneužívání dětí**
  - **Online péče**
  - **Zakázané a erotické obrázky dětí**

- **Extrémní pornografie, obscénní publikace a zakázané obrázky**

Kyberkriminalita

Kybernetická kriminalita jako služba – Cybercrime-as-a-service je obchodní model, který umožňuje prakticky komukoliv s dostatečnými finančními prostředky využívání nástrojů i služeb k provádění kybernetických útoků. Škodlivá kybernetická činnost se tak stává stále dostupnější, a to i pro relativně nezkušené útočníky. Vzhledem k narůstající popularitě tohoto modelu, která s sebou přináší velké zisky, roste také konkurence, což zpětně vede k širší nabídce produktů, ale i ke snižování ceny. To pak následně činí poskytované služby a nástroje dostupnější širšímu okruhu potenciálních zájemců.

- **DDos-as-a-servis – nabízí přístup k infikovaným zařízením připojených k internetu tzv. (botnet), za účelem provádění DDos útoků**
- **Acces-as-a-service – nabízí přístupy ke kompromitovaným účtům či systémům**
- **Malwere-as-a-servise – nabízí malwere k následnému využití v rámci kybernetických útoků**
- **Phishing-as-a-service – nabízí kompletní phishingové služby od detailních návodů až po předpřipravené e-maily či legitimně vypadající škodlivé stránky**
- **Vishing-as-a servise – nabízí pronájem hlasových systémů určených pro provádění vishingu**

Kyberkriminalita

S rozvojem odvětví „as-a-service“ se stále více komoditizují i hackerská tržiště, která fungují jako běžné podniky. Prodejci nástrojů na páchání kyberzločinů inzerují nejen své služby, ale také vystavují nabídky práce, aby získali útočníky s odlišnými dovednostmi. Některá tržiště nyní mají speciální stránky s poptávkami pomoci a nábory zaměstnanců, kde také zájemci o práci zde inzerují své dovednosti a kvalifikace.

Rozvíjející se ekonomika podsvětí nejenže podnítila růst ransomwaru a odvětví „as-a-service“, ale také zvýšila poptávku po krádežích přihlašovacích údajů. S rozšířením webových služeb lze různé typy přihlašovacích údajů a dat, zejména cookies, využít mnoha způsoby k získání lepší pozice při útocích na sítě, a to i při obcházení vícefaktorového ověřování. Krádeže přístupových údajů také zůstávají jedním z nejjednodušších způsobů, jak začínající zločinci mohou získat přístup na hackerská tržiště a začít svou „kariéru“.

Kyberkriminalita

Revoluční přechod na Cybercrime-as-a servis způsobily velmi úspěšné a výnosné Ransonwareové útoky

Dřívější ransomwaroví útočníci byli poměrně limitováni v rozsahu činnosti, protože jejich operace byly centralizované a členové skupiny vykonávali každý aspekt útoku. Když se ale ransomware stal nesmírně ziskovým, hledali způsoby, jak svou produkci rozšířit. Začali tedy části svých činností outsourcovat a vytvořili celou infrastrukturu na podporu ransomwaru. Nyní si z úspěchu této infrastruktury vzali příklad další kyberzločinci a následují je. To je vývoj zhruba posledních tří let.

Trošku pesimismu, ale musíme byt optimisty a něco pro to udělat

Cyber útočníci jsou tak nejen stále efektivnější, chytřejší, kreativnější ale také čím dál tím hlouběji pronikají do počítačových systémů, a to takovou rychlostí, než jaké jsou možnosti kybernetické bezpečnosti.

Nadále plati pravidlo, že bezpečnost reaguje na aktuální typy útoků, učí se z nich a prakticky stále dobíhá pomyslný ujíždějící vlak s útočníky. Otázka je, jak daleko za tím vlakem běží odborníci na kybernetickou bezpečnost, zda se chytají nástupního madla, nebo vidí koncová světla vlaku?

Dotazy?
Diskuze!