Kybernetické útoky, kyberkriminalita

Ing. Dušan Navrátil

Kybernetické útoky

Útočníci:

- **Státní aktéři**
- **Státem sponzorované skupiny**
- **Hacktivisté**
- **Kyberzločinci**
- **Teroristé**
- **Script kiddies**

Kybernetické útoky

Některé způsoby kybernetických útoků

Kybernetické útoky

Kybernetická špionáž: Státní aktéři v informačních sítích.

- **Útočníci: státní aktéři, státem sponzorované skupiny, konkurenti**
- **Metody: zranitelnost nultého dne, pokročilé spear-phishingové kampaně, útoky typu watering hole a další**
- **Dopady: ztráta dat, kompromitace citlivých a event. utajovaných informací, ztráta obchodních tajemství vedoucí ke ztrátě konkurenceschopnosti**

Kybernetickou špionáží se rozumí celá škála aktivit v kyberprostoru, jejichž cílem je přístup k citlivým, eventuelně utajovaným informacím a následné využiti těchto informací ve prospěch útočníka. Nejčastějšími aktéry kybernetické špionáže jsou tzv. skupiny Advaced Persistent Treat (APT).

U kybernetické špionáže platí, že nejčastějším vektorem útoku vedoucím k pvotnímu prolomení systému jsou metody sociálního inženýrství, z nichž nejčastější je spear-phishig.

Kybernetické útoky

Úniky dat: Nespočet možností pro další zneužití

- **Útočníci: státní aktéři, státem podporované skupiny, kyberzločinci, script kiddies,teroristé**
- **Metody: útoky hrubou silou, SQL injection a další**
- **Dopady: odcizení osobních údajů, jejich možné zneužití následným spear-phishingovým útokem, krádežím identit či tzv. credential stuffing**

Úniky dat jsou nebezpečné kvůli možnosti jejího dalšího zneužití. Mohou být zneužity k:

Následné spear-phoshingové kampani a zvýšení pravděpodobnosti, že oběť na odkaz klikne nebo si nakaženou přílohu stáhne.

Krádeží identity oběti.

Credential stuffingu, kdy útočníci zkoušejí uniklá hesla uživatelů použít pro přístup do jejich dalších účtů. Pokud uživatel používá jedno heslo do různých systémů, útočníkovi usnadní práci.

Vybudování vlastní databáze hesel specifický region-slovníkové útoky

Sestavení teroristy tzv. kill listů a extrémisty tzv. black listů.

Krádeží financí z elektronických peněženek.

Kybernetické útoky

Útoky skrze slabá místa v dodavatelském řetězci: oklikou ke skutečnému cíli.

- **Útočníci: Státní aktéři, státem sponzorované skupiny, kyberzločinci**
- **Metody: phishing a spear-phishing na zaměstnance dodavatelských organizací**
- **Dopady: ztráta dat, kompromitace strategických informací, ohrožení konkurenceschopnosti, sabotáž, vydírání atd.**

Dodavatelský řetězec může být zneužit k získání přístupu ke státním institucím, ale také k průmyslovým a dalším subjektům.

Důvody mohou být různé-snaha získat data až po přístup do systému se záměrem sabotáže (způsobení materiálních škod).

Dodavatelský řetězec je zranirelný na softwarové i hardwarové úrovni.

Kybernetické útoky

Kybernetické útoky na volební proces: Útoky na základní pilíř demokracie

- **Útočníci: státní aktéři, státem sponzorované skupiny, haktivisté, script kiddies**
- **Metody phishing, spear-phishing, DoS/DDos**
- **Dopady: omezení dostupnosti výsledků voleb, odcizení politicky citlivých materiálu ke zdiskreditování některého z kandidátů, šíření dezinformací, nedůvěra ve zvolené představitele, narušení zpracování výsledků voleb, snížení důvěry v demokratický proces**

Události posledních let změnily pohled mnoha západních zemí na bezpečnost volebního procesu.

Kybernetické útoky na americkou Demokratickou stranu v roce 2016 nebo na volební štáb francouzského prezidenta Macrona o rok později se v tomto ohledu staly předělem.

Z obou volebních štábu byly ukradeny a následně zveřejněny politicky citlivé dokumenty a v případě prezidenta Macrona byly některé z nich zfalšovány.

Cílem útočníků v obou případech bylo velmi pravděpodobně zdiskreditovat prezidentské kandidáty.

Při volbách v ČR od roku 2017 dochází k DDoS útokům na veřejné adresy ČSU.

Kybernetické útoky

DDoS: Exponenciální nárůst síly útoků

- **Útočníci: kyberzločinci, státní aktéři, státem sponzorované skupiny, hacktivisté, script kiddies, teroristé**
- **Metody. Botnety, DNS amplification, SYNFlood**
- **Dopady: narušení dostupnosti služeb, finanční ztráty, odlákání pozornosti od jiného útoku, poškození konkurence**

Základem kybernetické bezpečnosti je zabezpečení dostupnosti, integrity a důvěryhodnosti informací.

DDoS (distributed denial of servise) útoky omezují první zásadu kybernetické bezpečnosti – dostupnost služeb a sním spojených informací.

DDoS útoky jsou poměrně časté. Doprovázejí jiné kybernetické útoky, odvádějí pozornost od jiných útoků, jsou využívány hacktivisty jako virtuální blokáda a projev protestu, soukromými společnostmi pro oslabení konkurence nebo jako politický nástroj pro projevení nesouhlasu.

Kybernetické útoky

- **Ransomwarové útoky: v současné době nejrozšířenělší útoky**
- **Útočníci: kyberzločinci, státní aktéři, státem sponzorované skupiny**
- **Metody: phishing, sper-phishing, neautorizované využívání přístupových údajů, ransomware**
- **Dopady: nedostupt kritických dat (zašifrování) – dočasná nebo trvalá, únik dat na veřejnost**

Dochází ke komplexnímu ovládnutí systému, znepřístupnění dat, krádeži dat, event. záměně data a napadení HW přídavných zařízení.

Záměrem je většinou získání finančních prostředků vydíráním, ale muže být také záměr zničení dat a dlouhodobá nefunkčnost organizace.

Reálné dopady jsou, že organizace přestává fungovat, fyzické škody na majetku event. zdraví a ohrožení životů, reputační dopady a finanční dopady.

Většinou dochází k dělbě práce mezi útočníky se specializací.

Kybernetické útoky

Malware na nelegální těžbu kryptoměn: neviditelný zločin

- **Útočníci: kyberzločinci**
- **Metody: útok na výpočetní výkon napadených zařízení nebo napadení webové stránky využívající počítač**
- **Dopady: nelegitimní využívání výpočetního výkonu obětí, bez zřetelných dopadů na důvěrnost a integritu, hypotetická možnost omezení dostupnosti informačních systémů**

Malware na těžbu kryptoměn (kryptomining) je nová hrozba, která napadá počítače, mobilní zařízení nebo síťové servery a využívá výkonu těchto zařízení k těžbě kryptoměn.

Hlavním motivem malwaru je zisk, nicméně podstatnou odlišností proti podobně motivovaným útokům je, že tento malware je navržen tak, aby zůstal před uživateli zcela skrytý.

Kybernetické útoky

Cíle kybernetických útoků

Kybernetické útoky

Uživatelé: Brána do sítě organizací

- **Útočníci: kyberzločinci, státní aktéři, státem sponzorované skupiny**
- **Metody: phishing, spear-phishing, watering hole**
- **Dopady: poskytnutí přístupu sítí organizace útočníkům**

V oblasti kybernetické bezpečnosti se největší zranitelnost obvykle považují koncoví uživatelé informačních technologií. Útočníci jsou si této slabiny vědomi a využívají uživatelů jako bránu do sítí organizací, které chtějí kompromitovat.

Útočníci proti uživatelům většinou využívají sociální inženýrství, tedy technik manipulace osoby k tomu, aby se chovala způsobem, který není v jejím zájmu. V kontextu kybernetické bezpečnosti jde většinou o snahu získat z cílové oběti konkrétní informace (např. heslo) nebo uživatele přesvědčit ke stažení přílohy obsahující malware. Mezi nejvíce užívané techniky sociálního v kybernetickém prostoru patří phishing a spear- phishing.

Kybernetické útoky

- **Veřejný sektor: Pomalu se adaptující prostředí**
- **Útočníci: státní aktéři, státem sponzorované skupiny**
- **Metody: phishing, spear-phishing, DDos a další**
- **Dopady: ztráta dat, kompromitace citlivých a event.utajovaných informací**

Častým cílem kybernetických útokůje veřejný sektor, především v podobě institucí státní správy, které jsou pro útočníky zdrojem, vojensky, politicky i ekonomicky významných informací.

Kybernetické špionážní operace usilující o získání podobných informací jsou dlouhodobého charakteru a vyžadující po útočnících pokročilé schopnosti dlohodobě se vyhýbat odhalení a nepozorovaně z napadeného systému získat data.

Takovou úrovní know-how disponují zejména státní aktéři nebo jimi sponzorované skupiny.

V případě konfliktu patří veřejný sektor mezi prvotní cile kybernetických útoků za účelem ochromení, což se může stát ransomwerovým útokem.

Kybernetické útoky

- **Energetický sektor: Útočné pole se rozšiřuje**
- **Útočníci: státní aktéři, státem sponzorované skupiny**
- **Metody: phishing, spear-phishing, watering hole**
- **Dopady: výpadek dodávek elektřiny nebo plynu, únik informací**

Energetický sektor je pro útočníky sice obtížným, zato lákavým cílem. Pokud provozovatelé sítí v energetickém sektoru dodržují zásady kybernetické bezpečnosti a oddělují průmyslové řídící systémy od podnikových sítí (nevýrobních a neprodukčních včetně internetu), je kybernetický útok velmi obtížný. Na straně útočníka jak vyspělost jeho kybernetických kapacit, tak významné časové a finanční zdroje.

Dnes patří energetický sektor spolu bankovním k těm s nejlepším zabezpečením proti kybernetickým útokům.

Kybernetické útoky

Bankovní sektor: zabezpečený, přesto velmi lákavý cíl

- **Útočníci: kyberzločinci, ale i státní aktér**
- **Metody: phishing, spear-phishing, trojanizace legitimních mobilních aplikací**
- **Dopady: finanční ztráty, ztráta reputace banky, narušení kontinuity činnosti**

Bankovní sektor v ČR, ale i ve světě udělal v kybernetické bezpečnosti obrovský pokrok a je dobře zabezpečen. Na rozdíl od jiných sektorů velmi investoval do kybernetické bezpečnosti. Utajuje kybernetické incidenty, je ochoten v tichosti zaplatit náhrady škod, aby nedošlo ke ztrátě reputace.

Největší zranitelností v bankovním sektoru jsou uživatelé samotní. Útočníci toho využívají ve formě phishingových a spear-phishingových útoků.

Útoky na mobilní internetové bankovnictví, malware zaměřený na bankovní aplikace.

Kybernetické útoky

- **eHealth: Útoky na nejcitlivější osobní data spotenciálem ohrozit život**
- **Útočníci: kyberzločinci, možná i státní aktéři**
- **Metody: phishing, spear-phishing, neautorizované využívání přístupových údajů**
- **Dopady: nedostupnost kritických dat s možnými dopady na efektivitu zdravotnických zařízení a zdraví pacientů, u útoků na důvěrnost dat možnost vydírat a v případě zveřejnění dat zásah do osobního života.**

Vzhledem k možným dopadům útoků a citlivostí dat jsou rizika vyplývající z ohrožení informačních systémů využívaných ve zdravotnictví relativně vyšší než u jiných systémů.

Mezi největší hrozby patří znemožnění činnosti zdravotnického zařízení vyděračským ransomwerovým útokem (zašifrováním dat) způsobujících nedostupnost důležitých informací a únikem, event. zveřejněním citlivých osobních dat.

Výzvou se také stává zabezpečení medicínských Iot zařízení a možnost jejich zneužití.

Kybernetické útoky proti zdravotnickým systémům mohou při nízkých nákladech a malém vynaloženém úsilí přinést relativně velké zisky.

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

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!