Kybernetická kriminalita v ČR

V roce 2019 došlo k dalšímu nárůstu počtu kybernetických útoků proti naší zemi, z nichž některé lze označit za velmi vážné. Řada veřejných i soukromých institucí se musela vyrovnávat s obranou před těmito útoky a odstraňováním jejich následků. NÚKIB v průběhu roku řešil 78 kybernetických incidentů. Jeho pracovníci pomáhali napadeným institucím státní správy, územní samosprávy, nemocnicím i firmám s obnovováním jejich systémů, a to jak formou doporučení a metodické pomoci, tak i fyzicky přímo na místech incidentů. Úřad byl této podpory schopen jen díky týmové práci, maximálnímu úsilí a pracovnímu nasazení všech jeho zaměstnanců.

V prosinci 2019 došlo ke kybernetickému útoku proti systémům Nemocnice Rudolfa a Stefanie Benešov, spádové nemocnici až pro 400 000 lidí. Ransomware zašifroval data na serverech, nemocničních přístrojích a pracovních stanicích. V ordinacích nebylo možné provádět standardní ošetření, rušily se plánované operace a hospitalizovaní pacienti museli být převezeni do okolních nemocnic, včetně pacientů na jednotce intenzivní péče. Obnovení plného provozu trvalo téměř měsíc a následky útoku byly vyčísleny na 40–50 milionů korun.

Ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019

V současné době dochází k nebývalému nárůstu digitálních technologií.

V souvislosti s pandemií koronaviru se rozšiřuje práce z domova, porady se dělají on-line, lidé nakupují v e-shopech, školy a vzdělávací instituce přechází na on-line výuku a řada povolání hledá nové možnosti v on-line světě. To vše se děje v tzv. kyberprostoru, jehož hlavní vstupní branou je internet.

Je reálný předpoklad, že využívání digitálních technologií se bude neustále rozšiřovat. Ten, kdo je zvládne efektivně využívat pro své účely, bude mít větší šanci na lepší uplatnění v zaměstnání i mimo něj. Lidé si tento fakt uvědomují a zvyšují si své digitální kompetence, nejvíce se však zaměřují na ty oblasti kompetencí, které přímo souvisejí s využíváním digitálních technologií: informační a datová gramotnost, komunikace a spolupráce a tvorba digitálního obsahu.

Odvrácenou stranou je, že oblast digitální bezpečnosti je často podceňována. Lidé si neuvědomují, že na internetu a někdy i ve svých zařízeních mají velké množství dat, včetně těch osobních, o které mohou přijít. Prostřednictvím internetu provádí finanční transakce, sdílí své názory, komunikují s dalšími lidmi. Navíc do online prostředí umisťují soukromé fotografie a videa… S tím vším jsou spojena určitá rizika, kvůli kterým mohou přijít o své finance, data a dokonce si i poškodit pověst.

Trocha terminologie nikoho nezabije

Kyberprostor je virtuální počítačový svět, přesněji elektronické médium tvořící světovou, globální počítačovou síť, která je základem online komunikace. Je to rozsáhlá počítačová síť tvořena menšími, po světě rozesetými počítačovými sítěmi, které užívají TCP/IP protokol. Ten jim umožňuje komunikaci a výměnu dat.

Jedna z hlavních vlastností struktury kyberprostoru je otevřenost širokému okruhu uživatelů v interaktivním a virtuálním prostředí. Další vlastností je anonymita, která umožňuje v podstatě jakékoliv jednání bez zodpovědnosti.

Kyberprostor umožňuje uživatelům komunikovat, sdílet a vyměňovat si informace a nápady, hrát hry, účastnit se diskuzí na sociálních fórech, provádět obchodní transakce atd. Je virtuálním počítačovým světem tvořeným daty a informacemi. Lidé zde mohou komunikovat např. pomocí emailu nebo nakupovat v internetových obchodech.

Zdroj: Wikipedie

Kybernetická bezpečnost

je odvětví výpočetní techniky známé jako informační bezpečnost a uplatňované jak v případě počítačů, tak i sítí. Cílem informační bezpečnosti je ochrana informací a majetku před krádeží, korupcí nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné jeho předpokládaným uživatelům. Počátky tohoto odvětví se objevily v 80. letech, kdy se s rozmachem výpočetní techniky začaly skladovat informace do výpočetních systémů. Jednalo se například o evidence plateb, informace o zákaznících či armádní tajemství.

Kybernetická kriminalita

představuje trestnou činnost, která zahrnuje počítač nebo síťové zařízení. Patří sem i zločiny prováděné prostřednictvím internetu, jako například podvody či krádeže osobních údajů a identity nebo kreditní karty. Velké množství útoků je prováděno za účelem získání peněžních prostředků.

Kyberpodvody/zločiny

jsou chápány jako trestná či škodlivá jednání, která spočívají v získávání informací nebo v manipulaci s nimi za účelem dosažení zisku a která jsou uskutečňována prostřednictvím síťových technologií.

NÁŠ PŘÍBĚH

USB Killer

Tak jako téměř každý den i tohle dopoledne si Jitka užívala se svým malým synkem Radimem na dětském hřišti. Byl teplý začátek září a hřiště skoro plné. Děti vesele skotačily a maminky probíraly zážitky z prázdninových cest. Jitka se pomalu chystala se synkem k odchodu, když v tom k ní Radim přiběhl a nadšeně jí ukazoval svůj objev: „Maminko, podívej, co jsem našel!“ Držel v ruce malou barevnou tyčinku a radostně s ní mával nad hlavou. Jitka se nejprve trochu lekla, že její dítko někomu sebralo oblíbenou hračku, ale při bližším ohledání zjistila, že tohle hračka určitě nebude.

„Ráďo, myslím, že jsi našel něco, co někdo ztratil. Zkusíme zjistit, komu to patří.“ Barevná tyčinka byla totiž ve skutečnosti USB flashdisk v docela pěkném pouzdře z měkkého plastu.

Dotazování na ztrátu v okolí hřiště se nesetkalo s odezvou. Jitka se tedy rozhodla, že nejprve zjistí, co na nalezeném datovém médiu je uloženo. Pak podle toho zkusí dohledat majitele. Doma tedy po obědě otevřela notebook, po startu systému vsunula flashdisk do konektoru a spustila prohlížeč souborů. Chvilku se nic nedělo. Po chvíli ale najednou počítač problikl, zhasl a zcela ztichl. Jitka hned zkusila opětovný start, nic. Jitka si pomyslela, že se asi vybila baterie. Připojila tedy napájecí zdroj a pokusila se počítač znovu nastartovat. Stále bez odezvy. Jitce to připadalo divné, protože počítač byl relativně nový. Po chvilce zkoušení proto rezignovala a zavolala prodejci s popisem problému.

Notebook putoval do opravy a už za dva dny bylo jasno. Počítač byl na odpis. A diagnóza? Jitce zničil počítač ten krásně barevný USB disk!

Zdánlivý disk nebyl totiž ve skutečnosti paměťové médium, ale tzv. USB killer. To je zařízení, které po připojení k počítači dokáže po několika sekundách vygenerovat silný elektrický výboj, který dokáže zničit obvody na základní desce počítače, případně i další jeho komponenty.

Kybernetické útoky

Kybernetické útoky jsou chápány jako trestná či škodlivá jednání, která jsou uskutečňována prostřednictvím síťových technologií. Jejich podstata tkví v získávání informací nebo v manipulaci s nimi za účelem dosažení zisku či jiné výhody.

Nejčastěji jsou kybernetické útoky prováděny s následujícími cíli:

- Sledování aktivit, které děláte na internetu
- Zcizení, případně i zveřejnění vašich hesel a prolomení bezpečnosti uživatelských účtů
- Zcizení financí z vašeho bankovního účtu
- Podvodné vylákání finančních prostředků
- Zpomalení nebo zablokování počítače nebo serveru
- Znemožnění přístupu k určité internetové službě
- Zcizení identity, vydávání se za jinou osobu (např. na sociální síti)
- Agresivní zobrazování reklamy v zařízení
- Zneužití e-mailových účtů
- Zcizení vašich dat a dalších informací o vaší osobě či organizaci
- Rozesílání nevyžádaných informací a/nebo nebezpečných souborů vašim kontaktům
- Zablokování/zašifrování firemních systémů a požadování finančních prostředků za odblokování
- Kybernetická šikana
- Další nelegální aktivity (organizovaný zločin, šíření poplašných zpráv, zneužívání dětí, dětská pornografie)

Kdo stojí za kybernetickými podvody

Obvykle je to hacker. Ten v akčních filmech často vystupuje jako sympatický týpek, který se dokáže dostat k zásadním informacím vlády a pomůže tak dopadnout zločince, který chce zničit celou naši planetu. Pravdou je, že se v případě hackera jedná o velice schopného programátora, který je odborníkem na manipulace nebo úpravy počítačových systémů a sítí. Nehoní zločince, naopak on sám je zločincem, který využívá své počítačové dovednosti k získání neoprávněného přístupu k cizím počítačům a sítím. Zajímá se především o citlivé informace, jako jsou hesla, údaje o platebních kartách nebo soukromé fotografie. Jedná tak pro zábavu, zisk nebo ve snaze způsobit škodu.

Kybernetické útoky se týkají každého z nás

Uvedených cílů kybernetických útoků útočníci dosahují celou řadou různých technik a nástrojů.

Malware (velká skupina různých typů škodlivého softwaru)
Většina kybernetických útoků se týká i běžných uživatelů. Příkladem může být malware, což je zastřešující výraz pro jakýkoli typ škodlivého softwaru, jehož cílem je poškodit nebo zneužít libovolné programovatelné zařízení, službu nebo síť.

Takový škodlivý software se snaží infikovat počítač nebo mobilní zařízení. Hackeři malware používají z mnoha různých důvodů, například k získávání osobních údajů či hesel, krádežím peněz nebo k blokování přístupu do zařízení. Před malwarem se můžete chránit pomocí antimalwarového softwaru.

Většinou je šířen za účelem poskytnutí možnosti útočníkovi vzdáleně ovládat nakažené zařízení, snížit výkon systému, nakazit síť nebo v některých scénářích zablokovat přístup k datům.

Do kategorie malware řadíme především tyto skupiny škodlivého softwaru: počítačové viry, počítačové červy, trojské koně, crimeware, špehovací software (spyware), vyděračský software (ransomware) a reklamní software (adware).

Phishing
Phishing je forma útoku, při němž se útočník vydává za důvěryhodnou autoritu, například banku, s cílem vylákat hesla k bankovnímu účtu. K tomuto účelu dokonce vytvoří web, který je na první pohled stejný jako web skutečné banky. Pak pošle podvodný e-mail, který obsahuje formulář k zadání čísla kreditní karty a CVV kódu, nebo odkazuje na jím vytvořený web. Útok pokračuje následnou instalací podvodné aplikace do mobilního telefonu, která dokáže obejít dvoufaktorové SMS ověření. Poté již útočník má vše, co potřebuje k tomu, aby vybral finance z účtu napadené oběti.

Man in the Middle
Principem útoku Man in the Middle je to, že se útočník dostane do digitální cesty (komunikačního kanálu) mezi dvěma účastníky komunikace. Útočník tento kanál může přerušit a přijímat zprávy od obou stran, měnit jejich obsah a vysílat je dále k protistraně.

Může tak snadno namířit obsah a vyznění komunikace ke svému prospěchu. Postižení uživatelé si myslí, že si píší navzájem, ve skutečnosti však dostávají odpovědi od útočníka.

Útoky typu DoS a DDos
Jedná se o útok na internetovou službu s cílem tuto službu znepřístupnit ostatním uživatelům. Útok službu znefunkční nejčastěji prostřednictvím velkého množství požadavků, případně pomocí nějaké chyby v systému služby. Uvedená napadení sice neumožní získat nad službou kontrolu, ale odstaví ji z provozu. Běžným uživatelům se pak takto napadená služba jeví jako nedostupná.

Každý rok se budou zvyšovat počty kybernetické kriminality

/ blížíme se k 10 tisícům podvodů ročně

Útoky na IoT zařízení

IoT zařízení jsou tzv. chytrá zařízení. Do této kategorie spadá široké spektrum různých produktů, od domácích kamer a chytrých reproduktorů přes chytrý zvonek či žárovky až po herní konzole nebo elektronické systémy moderních aut. Tato zařízení se stávají cílem útoků, které zneužívají slabin v jejich nastavení, zabezpečení a malého zájmu jejich majitelů o ochranu proti kybernetickým útokům. Raději nedomýšlejme, co by se mohlo stát, kdyby se takový útočník napojil do elektronického systému vašeho vozu a nečekaně by spustil třeba brzdový manévr.

Úniky dat

Data jsou obvykle to nejcennější, co uživatelé a firmy ve svých počítačích a dalších digitálních zařízeních mají. Proto také k jejich získání směřuje největší množství kybernetických útoků. Oblíbeným cílem jsou údaje o uživatelích či klientech, jejich hesla a osobní data, ale pochopitelně také další zpeněžitelné informace, jako např. firemní know-how, strategické dokumenty a další informace.

Jak se dostane škodlivýsoftware do počítače

Existují různé cesty, obvykle má však formu přílohy v e-mailu. Ta obsahuje datovou část viru, který po stažení provede škodlivou akci. Jakmile oběť otevře soubor, zařízení je infikováno. Škodlivým softwarem mohou být infikovány e-maily, webové stránky, aplikace či soubory.

Co provede škodlivý software v počítači

Škodlivý software může například extrémně zpomalit počítač. Nebo může způsobit to, že vám začnou vyskakovat reklamy, kterých se nemůžete zbavit. To je ten lepší případ. V horším případě dojde ke smazáním dat na disku či k poškození harddisku.

Redakční rada:
Jaroslav Jindra, Jana Kubátová, Petr Klíma, Kateřina Špačková, Pavel Štáfek, Michaela Štáfková

DIGI zpravodaj 10 | Rok vydání: 2021 | www.portaldigi.cz

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

MPSV

MŠMT

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Jak se bránit?

Dbáme na ochranu našeho soukromí a dat a uvědomujeme si rizika kyberprostoru. Věnujeme pozornost bezpečnostním opatřením a spolehlivosti. Citlivější data chráníme dostatečně silným heslem nebo jinými metodami (otisk prstu, PIN, velmi účinnou metodou je zašifrování samotného obsahu). Heslo neodvozujeme od osobních údajů a pro různé přístupy volíme různá hesla. Své přístupové údaje nikomu nesdělujeme. Svá digitální zařízení chráníme ověřeným antivirovým programem. Uvědomuje si, že ostatní uživatelé nemusí sdílet svoji pravou totožnost (udání jiného pohlaví, nepravdivý věk apod.), a tudíž sami nesdělujeme svoje důvěrné údaje neznámým osobám nebo uživatelům na sociálních sítích. Data, o která nechceme přijít, si pravidelně zálohujeme.

Antivirový program (zkráceně antivirus)
Program vyvinutý pro detekci a odstranění počítačových virů chránící digitální přístroje před hrozbou napadení. Tyto programy fungují na bázi porovnávání segmentů nalezených v počítači s databází virů, nebo s nebezpečným chováním určitých webů či instalovaných programů. Mezi přední antivirové programy patří např. Avast, ESET či AVG.