NÚKIB

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Shrnutí ředitele NÚKIB

Ing. Dušan Navrátil

ředitel NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost (dále „NÚKIB“ nebo také „Úřad“) předkládá za rok 2018 novou podobu zprávy o stavu kybernetické bezpečnosti České republiky. Hodnotíme v ní to, jak si v současné době stojí kybernetická bezpečnost v naší zemi, ohlížíme se do nedávné minulosti, upozorňujeme na největší hrozby a na cíle, které jsou v hledáčku útočníků, a také na dopady, které úspěšné kybernetické útoky mohou mít.

Kybernetická bezpečnost je dnes celospolečenskou problematikou, a proto se na tvorbě této zprávy nově podílela široká škála příslušných subjektů. Vedle NÚKIB k jejímu vzniku přispěly některé orgány veřejné správy, správci kritické infrastruktury, akademická sféra, bezpečnostní experti nebo významné soukromé společnosti z oblasti kybernetické bezpečnosti. Tímto všem za jejich pomoc děkuji. Na základě jejich podkladů, komentářů a postřehů je obrázek o stavu kybernetické bezpečnosti přesnější, což nám umožní se v ochraně kybernetického prostoru posunout zase o kousek dál. Zpráva byla vypracována s použitím tří hlavních zdrojů – informací, které má k dispozici GovCERT.CZ provozovaný NÚKIB, informací získaných od parterů Úřadu a na základě otevřených zdrojů.

Množství kybernetických hrozeb, kterým Česká republika čelí, se průběžně navyšuje. Počet kybernetických útoků a jejich důmyslnost roste, útočníci přicházejí s novými metodami útoků a současně se neustále rozšiřuje možné útočné pole, do kterého přibyla například tzv. zařízení internetu věcí (Internet of Things, IoT), která se pomalu stávají běžnou součástí našeho života.

Nejvýznamnějším aktérem kybernetických hrozeb jsou z hlediska státu vzhledem k dostupným lidským, finančním a časovým prostředkům **státní aktéři**.Jejich snahou je povětšinou získat strategické informace cestou špionážních operací v kyberprostoru a následně je využít ve svůj prospěch. V případě České republiky jsou to podle informací, které má NÚKIB k dispozici, konkrétně operace aktérů napojených na Ruskou federaci a Čínskou lidovou republiku. Druhým nejvýznamnějším aktérem hrozeb v kyberprostoru

jsou osoby a organizace podílející se na kriminální činnosti. Jelikož je **kyberzločin** výnosný a je stále jednodušší se do něj zapojit, bude představovat hrozbu pro organizace a jednotlivce i v následujících letech.

Pokud jde o způsoby útoků, došlo v roce 2018 jak ve světě, tak v České republice k ústupu vyděračských útoků (ransomware), které nahradila **těžba kryptoměn skrze malware**. Tento trend naznačuje, že se pravděpodobně jedná o efektivnější nástroj generování finančního zisku než v případě ransomwarových útoků. Přes dopady na výpočetní výkon infrastruktury napadených subjektů je nelegitimní těžba kryptoměn z pohledu ochrany ICT méně závažnou hrozbou. Na rozdíl od ransomwarových útoků nemá destruktivní charakter a neohrožuje dostupnost důležitých dat.

Dalším trendem bylo **rostoucí množství a sofistikovanost cílených spear-phishingových útoků**, u kterých je zřejmé, že pachatelé často disponují vynikající znalostí prostředí a investují množství času do jejich přípravy. Častým cílem spear-phishingových útoků jsou v České republice finanční instituce a jejich klienti, v posledních letech se však zvedl i podíl útoků proti českým univerzitám. Hlavní motivací útočníků je přímý finanční zisk, ale výjimkou nejsou ani snahy o krádež duševního vlastnictví. Kybernetické útoky na vzdělávací a výzkumné instituce přitom nelze podceňovat. V případě kompromitace univerzitních sítí může dojít k **úniku duševního vlastnictví** a dosud nepublikovaných výsledků výzkumu. Pokud by útočníci v sítích českých univerzit působili nepozorovaně delší dobu, mohlo by to pro Českou republiku ve výsledku znamenat **významné oslabení konkurenceschopnosti české ekonomiky**.

Významnými sektory, pro něž je otázka kybernetické bezpečnosti zcela klíčová, je energetika a bankovnictví. Trendem, který v energetickém sektoru stojí za pozornost, je nasazování chytrých elektroměrů, tzv. **SMART meterů**. Ty představují jak způsob optimalizace toku energie, tak případné slabé místo využitelné útočníky k přerušení dodávek proudu. Výrobci nasazovaných IoT technologií by tak měli dbát na jejich adekvátní zabezpečení, aby bylo riziko kybernetického útoku co nejmenší. Pokud jde o bankovnictví, objevují se především **útoky na mobilní aplikace internetového bankovnictví**. Stále více lidí využívá mobilní aplikace ke spravování svých financí a hackeři se tomu rychle přizpůsobili. V roce 2018 byla příkladem tohoto trendu upravená aplikace QRecorder, která poškodila klienty českých bank.

Významným problémem, který jde napříč státní správou i soukromým sektorem, je **nedostatek expertů** na kybernetickou bezpečnost. Ze 42 institucí, které NÚKIB poskytly informace pro potřeby této zprávy, to uvedlo 40 % respondentů. Důsledkem může být to, že jsou upozaďovány některé základní bezpečnostní procesy, případně že zaměstnanci, na kterých je kybernetická bezpečnost dané instituce postavena, jsou přetíženi. Specifickým rizikovým faktorem je v podmínkách České republiky **aplikace zákona o zadávání veřejných zakázek**, kdy převládají zadávací řízení s cenou jako hlavním či jediným kritériem. Do strategicky významných systémů se tak na základě nabídky nejnižší ceny mohou dostat potenciálně rizikové komponenty. Zákon přitom v současné podobě umožňuje zohlednit jiná kritéria než jen cenu. Využití těchto kritérií však v nemalém počtu případů vyžaduje větší kapacity ze strany zadavatele a navyšuje riziko možného přezkumu, který může zadávací řízení neúměrně prodloužit.

Jedním ze způsobů, jak může NÚKIB reagovat na hrozby v oblasti kybernetické bezpečnosti, je vydávání **varování**. NÚKIB taková varování vydává ve chvíli, kdy se dozví o kybernetické hrozbě, na kterou je nutné bezprostředně reagovat. Dne 17. prosince 2018 NÚKIB varoval před používáním technických a programových prostředků společností Huawei Technologies Co. Ltd. a ZTE Corporation. K jeho vydání vedla kombinace poznatků a zjištění získaných při výkonu působnosti Úřadu. NÚKIB k tomuto varování vydal i podpůrnou metodiku, která konkretizuje opatření, jež mohou správci informačních a komunikačních systémů spadajících pod zákon o kybernetické bezpečnosti přijmout.

Mezi průběžné způsoby navyšování kybernetické bezpečnosti patří **cvičení kybernetické bezpečnosti**. Jejich výsledky dlouhodobě ukazují, že neznalost fungování kyberprostoru, možných rizik a zásad digitální hygieny často vede ke snižování kybernetické bezpečnosti. Je proto nezbytné navyšovat povědomí o kybernetické bezpečnosti mezi zaměstnanci včetně středního a vyššího managementu. Důsledkem tohoto stavu mimo jiné je, že nejčastějším vstupním bodem pro získání informací a dat, jež jsou dostupné v interních sítích organizací, je už několik let **uživatel**. Útočníci na něj jako na nejslabší článek kybernetické bezpečnosti cílí pomocí technik sociálního inženýrství, jejichž podstata se nemění, ale narůstá počet i sofistikovanost takových útoků.

V České republice je mnoho osvětových projektů, ale **navýšení digitální gramotnosti** a odolnosti vůči hrozbám napříč společností je dlouhodobý proces, na kterém bude potřeba neustále pracovat. NÚKIB se proto angažuje v pracovních skupinách, které připravují revize rámcových vzdělávacích programů. Úřad usiluje především o významnější začlenění problematiky kybernetické bezpečnosti do školní výuky. Toto úsilí přineslo nezanedbatelné výsledky a kybernetická bezpečnost proniká do výuky jako nedílná složka digitální gramotnosti.

Prioritou je i vzdělávání osob pracujících pro státní a veřejnou správu, neboť právě ty přicházejí při výkonu své profese do kontaktu s řadou citlivých údajů. NÚKIB proto spustil dva **on-line kurzy pro veřejnou správu**, kterými do konce roku 2018 úspěšně prošlo více než 21 500 úředníků státní správy.

Aby Česká republika měla lepší povědomí o škodlivých aktivitách ve strategických sítích státu, realizoval NÚKIB projekt zaměřený na systém detekce kybernetických bezpečnostních událostí v informačních systémech veřejné správy. Jeho cílem je pomocí **rozmístění síťových sond** umožnit lepší ochranu klíčových státních sítí. Díky sdílení dat s partnery bude Úřad schopen dohledat i bezpečnostní incidenty, které by v rámci jednoho rezortu nebyly detekovány, případně by nebyly vyhodnoceny jako nebezpečné, a informovat o nich další organizace ještě před jejich případným zasažením. Na konci roku 2018 byly síťové sondy nasazeny u 20 partnerů z řad státní správy.

Kybernetická bezpečnost je často vnímána jako fenomén, se kterým se mohou vypořádat výhradně techničtí experti. Pro její efektivní zajištění je potřeba se od takového chápání oprostit. **Kybernetická bezpečnost prolíná celým veřejným, pracovním a zčásti i soukromým životem** – je součástí národní bezpečnosti, zahraniční politiky, ekonomiky, vzdělání a našeho každodenního života. Zainteresovaný management ve všech institucích státní správy je nezbytný pro navýšení kybernetické bezpečnosti v zemi a zvládnutí krizových situací.

Neočekáváme, že kybernetické hrozby budou v příštích letech ustávat. Útočníci budou hledat nové způsoby, jak prolomit ochranu a je na nás všech se jim postavit a nereagovat jen na útoky, které již proběhly, ale předvídat je a být na ně připraveni dříve, než nastanou. Kybernetická bezpečnost naší země nikdy nebude absolutní, ale je naší povinností se k tomu stavu co nejvíce přiblížit.

Obsah

2018

Kybernetická bezpečnost ČR v číslech

164

NAHLÁŠENÝCH KYBERNETICKÝCH INCIDENTŮ GOVCERT.CZ

54

Z NAHLÁŠENÝCH KYBERNETICKÝCH INCIDENTŮ VYŘEŠENO NA GOVCERT.CZ

1 079

BEZPEČNOSTNÍCH INCIDENTŮ ŘEŠENÝCH CSIRT.CZ – NÁRODNÍM BEZPEČNOSTNÍM TÝMEM ČR

6 815

TRESTNÝCH ČINŮ V OBLASTI KYBERNETICKÉ KRIMINALITY A KRIMINALITY PÁCHANÉ NA INTERNETU

518

NAHLÁŠENÝCH PHISHINGOVÝCH ÚTOKŮ CSIRT.CZ

10

UNIVERZIT VYSTAVENO VLNĚ PHISHINGOVÝCH ÚTOKŮ

11

CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI PROVEDENÝCH NÚKIB

77

ZEMÍ, KTERÉ SE CVIČENÍ ÚČASTNILY

320

ÚČASTNÍKŮ CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI USPOŘÁDANÝCH NÚKIB

21 443

PROŠKOLENÝCH ÚŘEDNÍKŮ STÁTNÍ SPRÁVY

178

VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMŮ

30

PROVOZOVATELŮ ZÁKLADNÍ SLUŽBY

45

SUBJEKTŮ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY

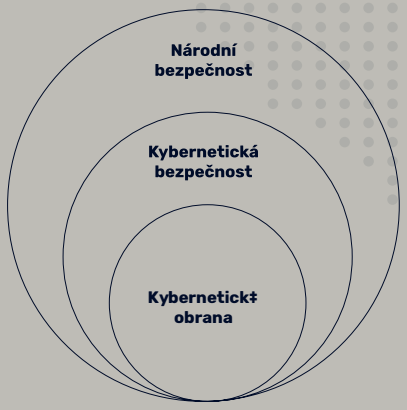
Co je kybernetická bezpečnost a jak se v ČR řeší její zajištění?[i]

Tři kategorie, které definují kybernetickou bezpečnost:

A	B	C
Prevence	**Lidé**	**Důvernost**
Detekce	**Procesy**	**Integrita**
Reakce	**Technologie**	**Dostupnost**

Česká republika

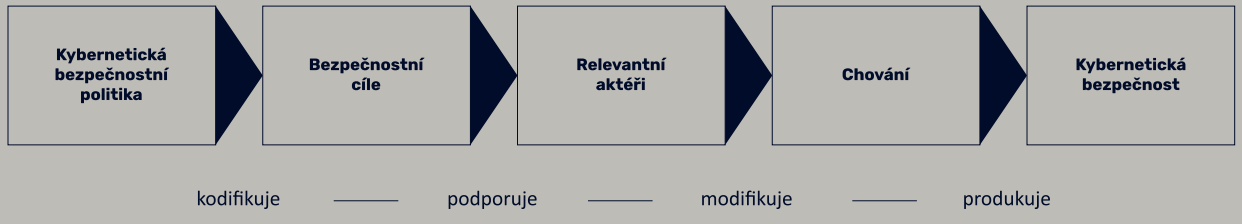
Gestorem v oblasti kybernetické bezpečnosti České republiky je Národní úřad pro kybernetickou a informační bezpečnost, který je ústředním správním orgánem pro kybernetickou bezpečnost, včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galleo. NÚKIB vznikl 1. srpna 2017 na základě zákona č. 2015/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., a kybernetické bezpečnosti a o změně souvisejících zákonů. Jeho součástí se stalo Národní centrum kybernetické bezpečnosti, které před tím působilo pod Národním bezpečnostním úřadem (NBÚ).



Role státu v zajištění kybernetické bezpečnosti

- Kybernetická obrana
- Ochrana kritické informační infrastruktury
- Kybernetická kriminalita
- Působení zpravodajských služeb

Tenze mezi požadavkem na funkcionalitu a požadavky na bezpečnost je reflektována skrze kybernetickou bezpečnostní politiku.



Aktéři

V kyberprostoru operuje celá řada aktérů s odlišnými zájmy. Jsou mezi nimi státy a jimi sponzorované hackerské skupiny, kyberzločinci, teroristé, hacktivisté, hackeři využívající své schopnosti ve svůj vlastní prospěch (black hats) nebo nezkušení jedinci (script kiddies). Na druhé straně stojí etičtí hackeři, kteří se snaží objevovat a upozorňovat na zranitelnosti ve snaze zabránit jejich zneužití.

Dále je možné rozlišovat externí útočníky a tzv. insidery. Insider může být nespokojený zaměstnanec, který například vynese citlivou či utajovanou informaci, ať už s motivací předat ji aktérům cizí moci, prodat nebo zveřejnit, aby poškodil svého zaměstnavatele.

Podle informací dostupných NÚKIB jsou aktéry, kteří ohrožují **Českou republiku** nejvíce, cizí mocnosti a kyberzločinci. V této Zprávě se ale pro úplnost objevují odkazy i na další skupiny.

Státní aktéři a státem sponzorované skupiny:

Z hlediska státu představují státní aktéři dlouhodobě nejvýznamnější hrozbu. Obecně mají k dispozici lidské, finanční a časové prostředky, díky kterým jsou jejich operace v kyberprostoru technicky sofistikované a perzistentní. Jejich hlavní motivací bývají strategicky a politicky důležité informace a získání vojenských výhod pro případné budoucí konflikty. Pro **Českou republiku** v současné době představují hrozbu zejména operace aktérů napojených na Ruskou federaci a Čínskou lidovou republiku.

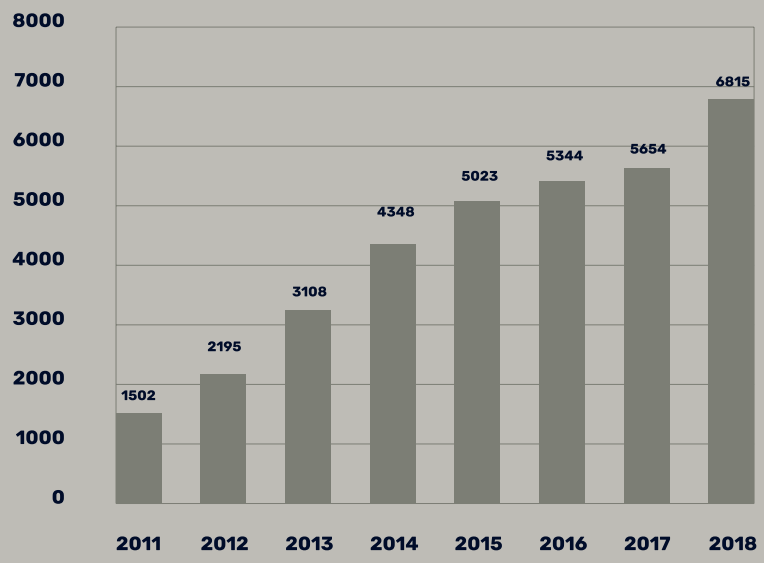
Kyberzločinci:

Hlavní motivací kyberzločinců je obecně finanční zisk, čemuž odpovídají i techniky, které používají. V jejich arzenálu se často nalézají různé typy ransomware, využívání sociálního inženýrství k proniknutí do bankovních účtů svých obětí nebo podvodných e-mailů ve snaze z lidí vylákat peníze. Zatímco před několika lety byl kyberzločin převážně v rukou technicky zdatných hackerů, v dnešním kybernetickém prostředí si potřebné hackerské nástroje může pořídit kdokoliv, kdo je schopen zaplatit. Hackování na zakázku– tzv. „Malware-as-a-Service“ – se stalo jednou z často vyhledávaných komodit na darknetu[1] a neustále přibývá útoků, které byly provedeny pomocí nástrojů koupených právě tam. Jelikož je kyberzločin výnosný a je stále jednodušší se do něj zapojit, bude představovat hrozbu pro organizace a jednotlivce i v následujících letech.

Jak ukazují statistiky Policie ČR, je kybernetická kriminalita a kriminalita páchaná na internetu v **České republice** na vzestupu a jejich případů každoročně přibývá.[ii]

Graf 1:

Vyšetřované kyberkriminální případy v ČR mezi roky 2011 a 2018



Zdroj: policie.cz

[1] *Darknet je skrytá část internetu, do které se lze dostat pomocí speciálního softwaru.*

Teroristé:

Teroristé v současné době nejsou pro kybernetickou bezpečnost **České republiky** zásadní hrozbou. Islámský stát si získal mnoho pozornosti svými aktivitami na internetu, ať už to byl způsob, jakým rekrutoval nové bojovníky, šířil propagandu nebo používal šifrované aplikace pro komunikaci. Nicméně v otázce kyberterorismu pravděpodobně nepředstavuje aktuální hrozbu. Audit národní bezpečnosti z roku 2016 definuje kyberterorismus jako kybernetický útok, který „ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy". Takový útok by vyžadoval vyspělé kybernetické kapacity, které teroristické skupiny v současné chvíli pravděpodobně nemají, a investici jak lidských, tak finančních prostředků. Konvenční útoky jsou pro teroristické skupiny stále efektivnější a prozatím přinášejí více pozornosti za menšího úsilí a nákladů.

Hacktivisté:

Jsou političtí aktivisté, kteří s cílem politické, ideologické nebo sociální změny narušují dostupnost, důvěrnost nebo integritu informací. Často se jedná o DDoS, defacement, nabourávání se do účtů na sociálních sítích nebo zveřejňování osobních údajů. V **České republice** jsou hacktivistické útoky na ústupu. Jednou z posledních výraznějších aktivit byla operace Blokáda české odnože Anonymous, která proběhla v roce 2016. Byla namířena proti českým politikům a vládním institucím v reakci na schválení zákona o hazardních hrách. V tomto případě provedla Národní centrála proti organizovanému zločinu úspěšnou operaci, kdy obvinila šest osob z trestné činnosti.

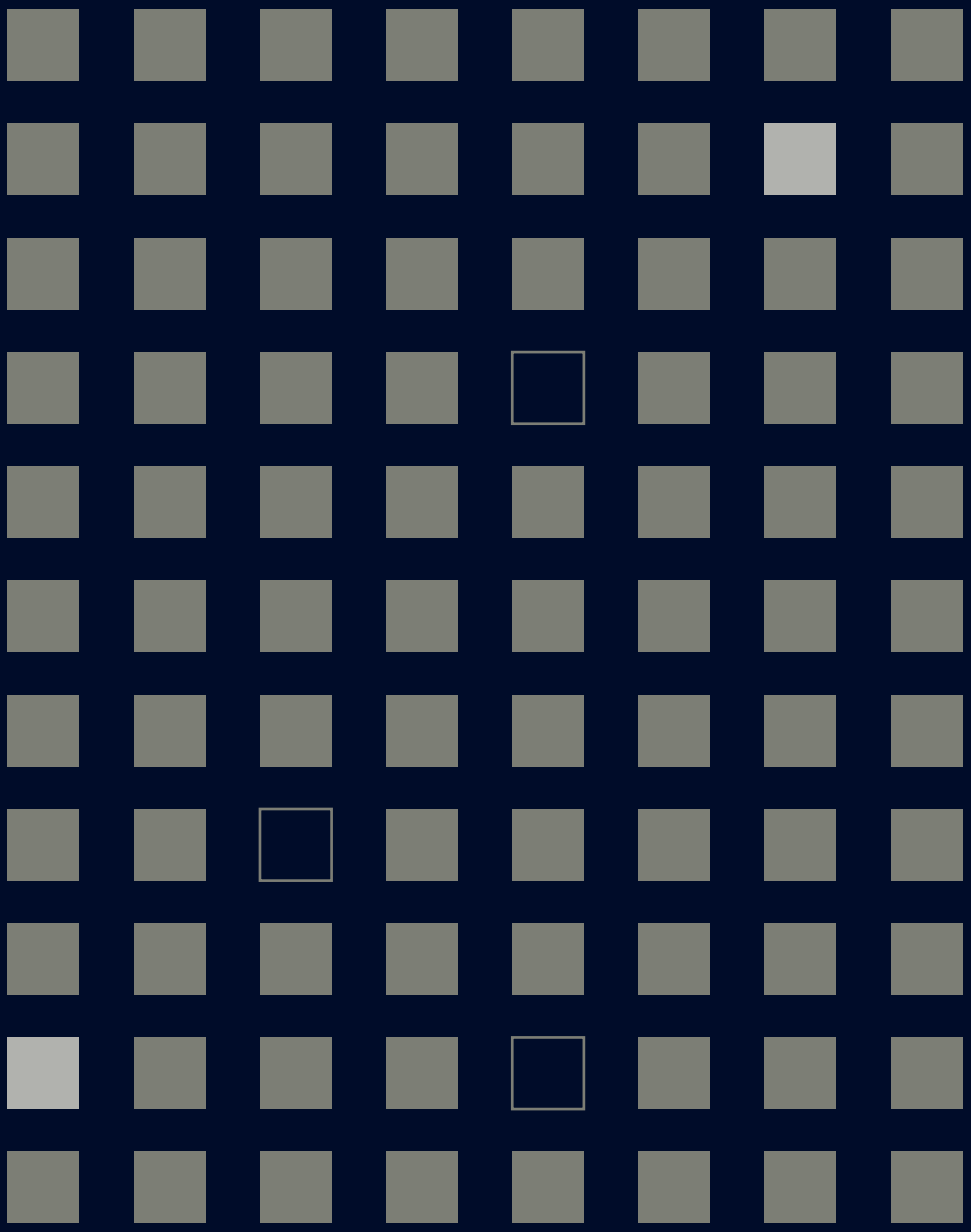
Black hats:

V **České republice** i ve světě jsou aktivními aktéry tzv. black hats. Jsou to hackeři, kteří nepracují pro žádnou zájmovou skupinu, ale svými útoky spíše sledují vlastní zájem, například získání uznání v hackerské komunitě nebo finanční prospěch.

Script kiddies:

Další skupinu v **České republice** i v zahraniční představují script kiddies, což je slangové označení pro amatéry, kteří pro své útoky používají nástroje vyvinuté jinými útočníky.

Kybernetické hrozby



Kybernetická špionáž: Státní aktéři v českých sítích

Dopady	ztráta dat, kompromitace citlivých a utajovaných informací, ztráta obchodních tajemství vedoucí ke ztrátě konkurenceschopnosti
Útočník	státní aktéři, státem sponzorované skupiny
Metody	zranitelnosti nultého dne, pokročilé spear-phishingové kampaně, útoky typu watering hole[2] a další

Kybernetickou špionáží se rozumí celá škála škodlivých aktivit v kyberprostoru, jejichž cílem je přístup k citlivým nebo utajovaným informacím a následné využití těchto informací ve prospěch útočníka. Nejčastějšími aktéry na poli kybernetické špionáže jsou tzv. skupiny Advanced Persistent Threat (APT).

U kybernetické špionáže platí, že nejčastějším vektorem útoku vedoucím k prvotnímu prolomení systému jsou metody sociálního inženýrství, z nichž nejčastější je tzv. spear-phishing (bližší informace ke spear-phishingu na straně 24).

Úspěšná kybernetická špionáž představuje závažný bezpečnostní incident, který může mít významné důsledky:

Únik citlivých informací:

Mezi takové informace mohou patřit informace strategicky důležité pro stát, přihlašovací údaje zaměstnanců organizace nebo patenty a know-how výzkumných a soukromých společností;

Příprava na závažnější útoky a operace:

Informace odcizené při kyberšpionáži mohou být zneužity k dalším útokům. Pokud má útočník vazby na státního aktéra, je možné, že získaná data využije k přípravě dalších zpravodajských operací, a to jak v rovině cílených kybernetických útoků, jako je spear-phishing, tak v rovině

APT skupiny

Pokročilost APT skupin není primárně v metodách útoku, ale ve schopnosti zůstat nepozorován v systému oběti po období v řádech měsíců až několika let.

Nejčastěji se jedná o státní aktéry snažící se získat utajované informace jiných států či obchodní tajemství, ale jsou známé i případy APT skupin bez napojení na stát, které mohou jednat v zájmu konkrétních soukromých společností či krást technologie s cílem prodat je komukoliv, kdo zaplatí nejvíc. V takovém případě se spíše jedná o průmyslovou špionáž, která má blíže ke kybernetické kriminalitě než k běžnému chápání klasické špionáže.

[2] Při útoku typu watering hole si útočník vytipuje webovou stránku, kterou jeho oběť často navštěvuje, a v případě využitelné zranitelnosti ji nakazí. V okamžiku, kdy oběť nakaženou infikovanou stránku navštíví, se jí do počítače nainstaluje malware.

zpravodajských operací využívajících lidské zdroje (HUMINT);

Rozesílání infikovaného obsahu dalším institucím:

Pokud se útočníkovi v rámci jeho kyberšpionážních aktivit podaří získat přístup do e-mailové schránky oběti, může ho zneužít k útokům na partnerské instituce, ať už doma nebo v zahraničí, a to prostřednictvím spearphishingu. Útočník může těžit z použití legitimní e-mailové adresy, která vzbuzuje u příjemce důvěru. Pokud přijde e-mail z adresy důvěryhodné organizace, pravděpodobnost, že příjemci škodlivý obsah otevřou a vpustí útočníka i do svých systémů, se zvyšuje;

Přístup do dalších systémů organizace:

Odcizené přihlašovací údaje mohou útočníka dostat do dalších systémů instituce, systémů státní správy nebo mezinárodních organizací;

Základ pro dezinformační kampaně:

Získání mnohdy neformální osobní e-mailové komunikace vrcholných, politicky činných představitelů státu může představovat účinný nástroj k jejich diskreditaci.

Tyto důsledky ilustruje úspěšné prolomení systému COREU (komunikační síť používaná Radou EU, Evropskou službou pro vnější činnost, ministerstvy zahraničních věcí členských států a stálými zástupci při EU a Evropskou komisí), ke kterému došlo v roce 2018. Útočníkům se podařilo za dobu tří let, kdy v COREU působili nepozorovaně, odcizit tisíce dokumentů. Podle informací médií celý případ začal na Kypru. Útočníci se pomocí phishingu na jednoho ze zaměstnanců dostali do systému kyperské vládní organizace, kde získali přihlašovací údaje do celého systému COREU, a odtamtud kradli dokumenty relevantní pro všech 28 zemí EU.[iii]

Kybernetická špionáž se nevyhýbá ani České republice.

NÚKIB v roce 2018 pokračoval ve zkoumání rozsáhlého útoku na strategicky významnou českou vládní instituci. V rámci zkoumání byla provedena analýza dostupných technických dat a dalších relevantních informací (charakter oběti, trvání útoku, povaha odcizených informací, nakládání s odcizenými informacemi atd.), jejímž závěrem bylo, že původcem útoku je téměř jistě (90–100 %)) státní aktér nebo na něj napojená skupina. Dle informací dostupných NÚKIB je pravděpodobné (55–70 %), že útok byl veden ze strany čínského aktéra.

Úniky dat: Nespočet možností pro další zneužití

Dopady	odcizení osobních údajů, jejich možné zneužití k následným spear-phishingovým útokům, krádežím identit či tzv. credential stuffingu (viz níže v kapitole)
Útočník	státní aktéři, státem sponzorované skupiny, kyberzločinci, script kiddies, teroristé
Metody	útoky hrubou silou, SQL injection [3] a další

Rok 2018 se vyznačoval častými úniky osobních dat ve světě. V průběhu celého roku se objevovaly zprávy o nových únicích a počty zasažených lidí, jejichž osobní informace byly odcizeny, se vyšplhaly do desítek až stovek milionů.

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

- Následné spear-phishingové kampani a zvýšení pravděpodobnosti, že oběť na odkaz klikne nebo si nakaženou přílohu stáhne;
- Krádeži identity oběti;
- Credential stuffingu, kdy útočníci zkoušejí uniklá hesla uživatelů použít pro přístup do jejich dalších účtů. Pokud uživatelé používají jedno heslo pro více služeb, útočníkům usnadní práci;[4]
- Vybudování vlastní databáze hesel specifické pro daný region, kterou útočníci mohou používat pro tzv. slovníkové útoky;
- Sestavení tzv. kill listů, ve kterých teroristické skupiny volají po zabití lidí na jejich seznamech;
- Sestavení tzv. black listů, na kterých extremisté publikují své nepřátele;
- Krádeži financí z elektronických peněženek. Útočníci hledají v e-mailech obětí informace o jejich elektronických peněženkách, ze kterých si převedou peníze na své účty. [vi]
- Rozesílání spamů a nevyžádané reklamy.

[3] SQL injection je technika běžně užívaná pro napadení databází. Pokud se útočníkovi podaří do dotazu směřovaného na databázi vsunout svůj vlastní příkaz, může s databázemi dělat téměř cokoliv – zkopírovat, pozměnit nebo je zcela smazat.

[4] Jak zjistil bezpečnostní expert Troy Hunt, některé ze seznamů využívaných při credential stuffingu obsahují i více než 100 milionů e-mailových adres.

Český příklad zneužití uniklých dat: Zkombinování uniklých hesel se spear-phishingem

Na podzim roku 2018 se **Českou republikou** šířily vyděračské e-maily, ve kterých se útočníci snažili uživatele přesvědčit o tom, že byli natočeni při sledování pornografie. Hrozili, že pokud uživatelé nezaplatí stanovenou částku v bitcoinech, bude nahrávka zveřejněna. Aby zvýšili pravděpodobnost, že lidé požadovanou částku uhradí, zneužili již uniklých dat. Prostřednictvím e-mailů zacílili na konkrétní uživatele a do textu přidali jejich odcizené osobní informace a hesla, čímž se snažili své oběti přesvědčit, že jejich počítač byl skutečně kompromitován a vyvolat v nich tak pocit urgentnosti danou částku zaplatit. Podle veřejně dostupných údajů o dané peněžence útočníci tímto způsobem získali téměř 6 000 dolarů, v přepočtu 130 000 korun.

Útoky skrze slabá místa v dodavatelském řetězci: Oklikou ke skutečnému cíli

Dopady	ztráta dat, kompromitace strategických informací, ohrožení konkurenceschopnosti, sabotáž
Útočník	státní aktéři, státem sponzorované skupiny
Metody	phishing a spear-phishing na zaměstnance dodavatelských společností

Útoky skrze slabá místa v dodavatelském řetězci jsou v posledních letech na vzestupu a ukázalo se, že útočníci jsou s jejich pomocí schopni napáchat značné škody.[5] Dodavatelský řetězec může být útočníky zneužit k získání přístupu ke státním institucím, ale také k průmyslovým nebo dalším subjektům. Důvody mohou být různé – od snahy získat data až po přístup do systému se záměrem sabotáže (způsobení materiálních škod).

Dodavatelský řetězec je zranitelný na softwarové i hardwarové úrovni. Na softwarové úrovni se jedná o kybernetické útoky zaměřující se na slabý článek řetězce s cílem získat privilegovaný přístup a ten využít pro kompromitaci systému na konci dodavatelského řetězce.

Široce diskutovaným tématem v roce 2018 byly útoky na poskytovatele tzv. spravovaných služeb (managed service providers, MSP), mezi které patří například poskytovatelé služeb založených na principu cloud computingu. Útoky skrze MSP jsou pro cílovou organizaci, která dané služby využívá, obtížně zjistitelné, protože útočník zneužívá privilegovaný přístup dodavatele.

Bezpečnost dodavatelského řetězce a využívání poskytovatelů spravovaných služeb (MSP) je relevantním tématem i v **České republice**. Příkladem jsou státní a soukromé instituce, které jsou subjekty zákona o kybernetické bezpečnosti [zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále „ZKB")] a využívají nebo se chystají využívat MSP. Řešením není zcela vyloučit dodavatele služeb, ale subjekty jsou dle ZKB povinny vzít při řízení rizik v potaz, že ochrana jejich systémů začíná již na úrovni zabezpečení systémů jejich dodavatelů. Z tohoto důvodu je třeba uvažovat zabezpečení poskytovatele služeb v míře, která odpovídá zabezpečení vlastního systému a zahrnout dodavatele do analýzy rizik.

V **České republice** je potenciálně rizikovým faktorem, který souvisí s dodavatelským řetězcem, současný způsob aplikace zákona o zadávání veřejných zakázek [zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále „ZZVZ")], kdy převládají zadávací řízení s cenou jako hlavním či jediným kritériem. Oslovené organizace dle zaslaných dotazníků tuto praxi vnímají jako omezení kybernetické bezpečnosti v jejich organizacích. Do systémů povinných osob dle ZKB se na základě nabídky nejnižší ceny mohou dostat potenciálně rizikové komponenty. ZZVZ v současné podobě ovšem umožňuje zohlednit jiná kritéria než jen cenu, využití těchto kritérií však v nemalém počtu případů vyžaduje větší kapacity ze strany zadavatele a navyšuje riziko možného přezkumu, který může zadávací řízení neúměrně prodloužit.

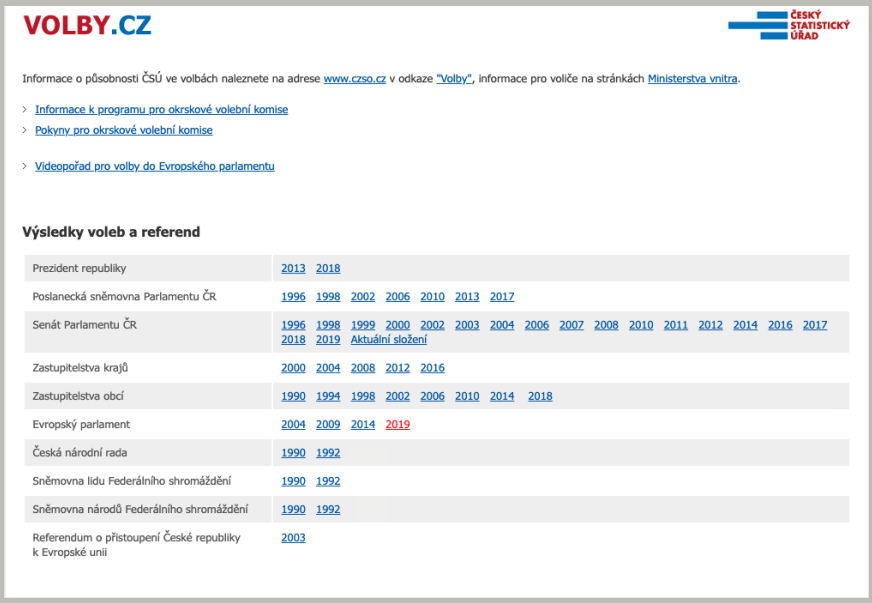
[5] *Příkladem je třeba malware NotPetya, který se šířil skrze aktualizaci účetního programu.*

Kybernetické útoky na volební proces: Útoky na základní pilíř demokracie

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

Události posledních tří let změnily pohled mnoha západních zemí na bezpečnost volebního procesu. Kybernetické útoky na americkou Demokratickou stranu v roce 2016 či na volební štáb francouzského prezidenta Macrona o rok později se v tomto ohledu staly předěly. Z obou volebních štábů 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.

Česká republika má s kybernetickými útoky na volby také své zkušenosti. Při parlamentních volbách na podzim 2017 a při komunálních volbách o rok později došlo k DDoS útokům na veřejné adresy Českého statistického úřadu (ČSÚ), který zpracovává výsledky voleb a informuje o nich. V roce 2017 DDoS útok vyřadil na několik desítek minut z provozu volební weby volby.cz a volbyhned.cz. Policie, která vedla ve věci prověřování, ho pro nedostatek zdrojových dat byla nucena odložit. [vii] O rok později byl neznámým pachatelem během komunálních voleb proveden DDoS útok na oficiální stránky ČSÚ www.czso.cz . Díky DDoS ochraně se po-



Webové stránky, na které byl proveden DDoS útok v říjnu 2017. Zdroj: volby.cz

dařilo nedostupnosti stránek zamezit. Ani jeden z útoků neovlivnil přenos výsledků voleb z přebíracích míst do centrály, a tudíž nedošlo ani k ovlivnění nezávislého zpracování dat. Jejich načasování nicméně naznačuje záměr pachatele narušit hladký proces zveřejnění výsledků.

Kybernetické útoky na volby jsou útokem na základní pilíř demokracie a mohou mít dalekosáhlé následky. Mohou znevěrohodnit proces zpracování výsledků voleb, podrýt legitimitu zvolených představitelů a v krajním případě zasít nedůvěru voličů v demokratický systém.

Česká republika si je hrozby, kterou kybernetické útoky na volby představují, vědoma a přijímá opatření k navýšení bezpečnosti českého volebního procesu. Bližší informace o opatřeních jsou k dispozici na straně 49.

DDoS: Exponenciální nárůst síly útoků

Dopady	narušení dostupnosti služeb, finanční ztráty, odlákání pozornosti od jiného útoku, poškození konkurence
Útočník	kyberzločinci, státní aktéři, státem sponzorované skupiny, hacktivisté, script kiddies, teroristé
Metody	botnety, DNS amplification, SYNFlood[7]

Základem kybernetické bezpečnosti je zabezpečení dostupnosti, integrity a důvěryhodnosti informací. DoS (denial of service) a DDoS (distributed denial of service) útoky omezují první zásadu kybernetické bezpečnosti – dostupnost služeb a s nimi spojených informací. (D)DoS 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. Provedení DoS a DDoS útoku je navíc poměrně jednoduché. Pokud útočníci nemají dostatečné schopnosti útok připravit sami, mohou si v současné době botnet [7] pronajmout jako službu.

DDoS v roce 2018

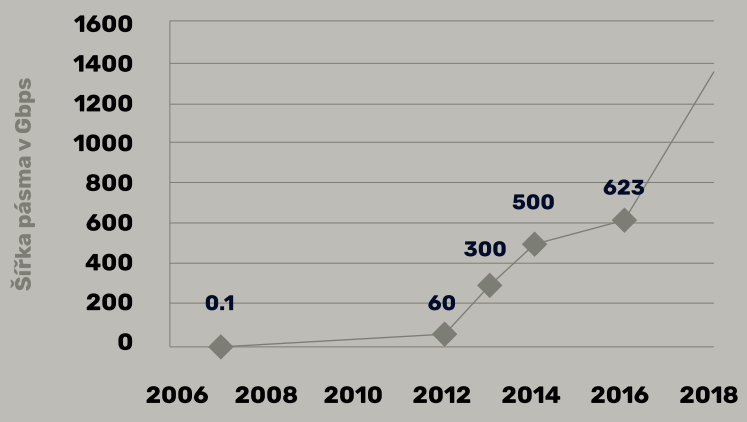
Rok 2018 přinesl významný předěl v DDoS útocích a jejich síle. Koncem února došlo k desetiminutovému výpadku platformy Github, když ji zasáhl DDoS útok o síle až 1,35 Tb/s. DDoS útok v historii. Byl veden novou metodou, která využívá špatného nastavení serverového protokolu Memcached.

S tím, jak narůstá síla DDoS útoků (viz graf níže), narůstají také nároky na ochranu proti nim. DDoS útok, který přesahuje velikost 1 TB/s, by v **České republice** pravděpodobně nenarušil pouze dostupnost napadených webových stránek, ale ovlivnil by také páteřní linku a s ní související infrastrukturu.

Jaký je rozdíl mezi DoS a DDoS útokem?

Útoky DoS (denial of service) a DDoS (distributed denial of service) útoky se liší v počtu zdrojů, které je generují. Při DoS útoku se k přehlcení systému oběti požadavky většinou používá jeden počítač a jedno připojení. DDoS k přehlcení využívá více počítačů spojených do tzv. botnetu.

Vývoj síly DDoS útoků



[6] SYNFlood je forma DoS útoku, při které útočník pošle vlnu SYN paketů, které se používají k navázání komunikace mezi dvěma systémy. Oběť je tímto způsobem zahlcena.

[7] Síť infikovaných počítačů, které ovládá jediný hacker, jenž tak má přístup k výpočetnímu výkonu mnoha tisíců strojů současně.

Jak fungjí Memcached DDoS útoky?

Memcached je veřejně dostupný nástroj, který je využíván pro efektivnější komunikaci serverů v rámci jedné organizace. Pokud ale administrátoři nedbají správného nastavení a službu provozují na protokolu UDP a její port nechají otevřený do internetu, mohou toho využít útočníci pro silné DDoS útoky. Proskenují internet, najdou nezabezpečené servery Memcached a na ně pošlou požadavek s podvrženou IP adresou oběti. Systém Memcached dokáže velikost tohoto požadavku znásobit až 51 000krát a odpověď, kterou odešle oběti, je tak mnohonásobně větší než požadavek samotný. Zahltit server oběti tímto způsobem je poměrně snadné, zejména jsou-li k útoku zneužity tisíce nezabezpečených serverů Memcached.

1

Útočník

Požadavek na nezabezpečené Memcached porty

Cílový port: UDP 11211
Velikost: X bytů
Zdroj požadavku: podvržená IP adresa oběti
Cíl požadavku: servery s nezabezpečenými Memcached porty

2

Servery s nezabezpečenými Memcached porty

Memcached systém odpoví na požadavek

Zdroj odpovědí: Servery s Memcached
Cíl požadavku: IP adresa oběti
Velikost: n x X bytů (n = násobitel velikostí)

3

Oběť

DDoS v České republice

Útoky, které zasáhly českou infrastrukturu v roce 2018, nedosahovaly takové síly jako v zahraničí. Jednalo se převážně o menší útoky v desítkách GB/s, které buď napadené webové stránky na několik minut vyřadily z provozu, nebo je ochrana proti DDoS útokům zastavila úplně. I tak ale zůstává DDoS častým způsobem útoku. Přesně polovina respondentů v dotaznících k této Zprávě odpověděla, že v roce 2018 zaznamenala DDoS útoky na své sítě.

Pozornost si v roce 2018 vyžádalo několik případů

A

DDoS útok na webové stránky Českého statistického úřadu, který je blíže popsán na straně 16;

B

DDoS útok na stránky jednoho z českých konzulátů. Výpadek trval několik desítek minut;

C

Série DDoS útoků na české poskytovatele internetového připojení, včetně největších mobilních operátorů. Ti byli na přelomu roku 2018 a 2019 vystaveni vlně útoků, která mířila jak na jejich zákazníky, tak na ně samotné. Útoky se od běžných lišily v tom, že necílily na konkrétní provozovanou službu, ale spíše na různé adresy a subjekty. Mohlo se tak jednat o test ochranných kapacit v **České republice**. [viii]

Malware na nelegální těžbu kryptoměn: Růst na úkor ransomwaru

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

Malware na těžbu kryptoměn (též kryptomining) je nastupující 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 navržentak, aby zůstal před uživateli zcela skrytý.“,

CoinMiner v České republice

Škodlivá aplikace CoinMiner v roce 2018 představovala velmi častou internetovou hrozbu. Dle vyjádření některých antivirových společností patřila aplikace CoinMiner na počátku roku dokonce mezi nejčastější internetové hrozby v rámci České republiky. CoinMiner existuje ve dvou verzích. První verze běží na webové stránce a využívá počítač návštěvníka stránek pro těžbu kryptoměn, provedení druhé verze této aplikace je však zajímavější z toho důvodu, že využívá exploit EternalBlue, pomocí kterého infikuje zranitelné počítače. Po úspěšném nakažení počítače proběhne spuštění WMI skriptů. WMI skripty běží pouze v paměti nakaženého počítače a jsou tudíž obtížnější na detekci. S využitím těchto skriptů je na oběť stažen dodatečný škodlivý kód. Proti exploitu EternalBlue byla již v minulosti vydána záplata, nicméně vzhledem k dopadu aplikace CoinMiner je zjevné, že stále existují počítače, které nebyly aktualizovány.

U kryptominingu je možné rozlišovat tři základní způsoby nakažení:

1

Nakažená je webová stránka a kryptoměnu těží oběti přes prohlížeč při návštěvě nakažené stránky. V některých případech oběť dočasně těží i po tom, co odejde z nakaženého webu.

2

Útočník použije již existující botnet a na dříve nakažené počítače nainstaluje modul pro kryptomining.

3

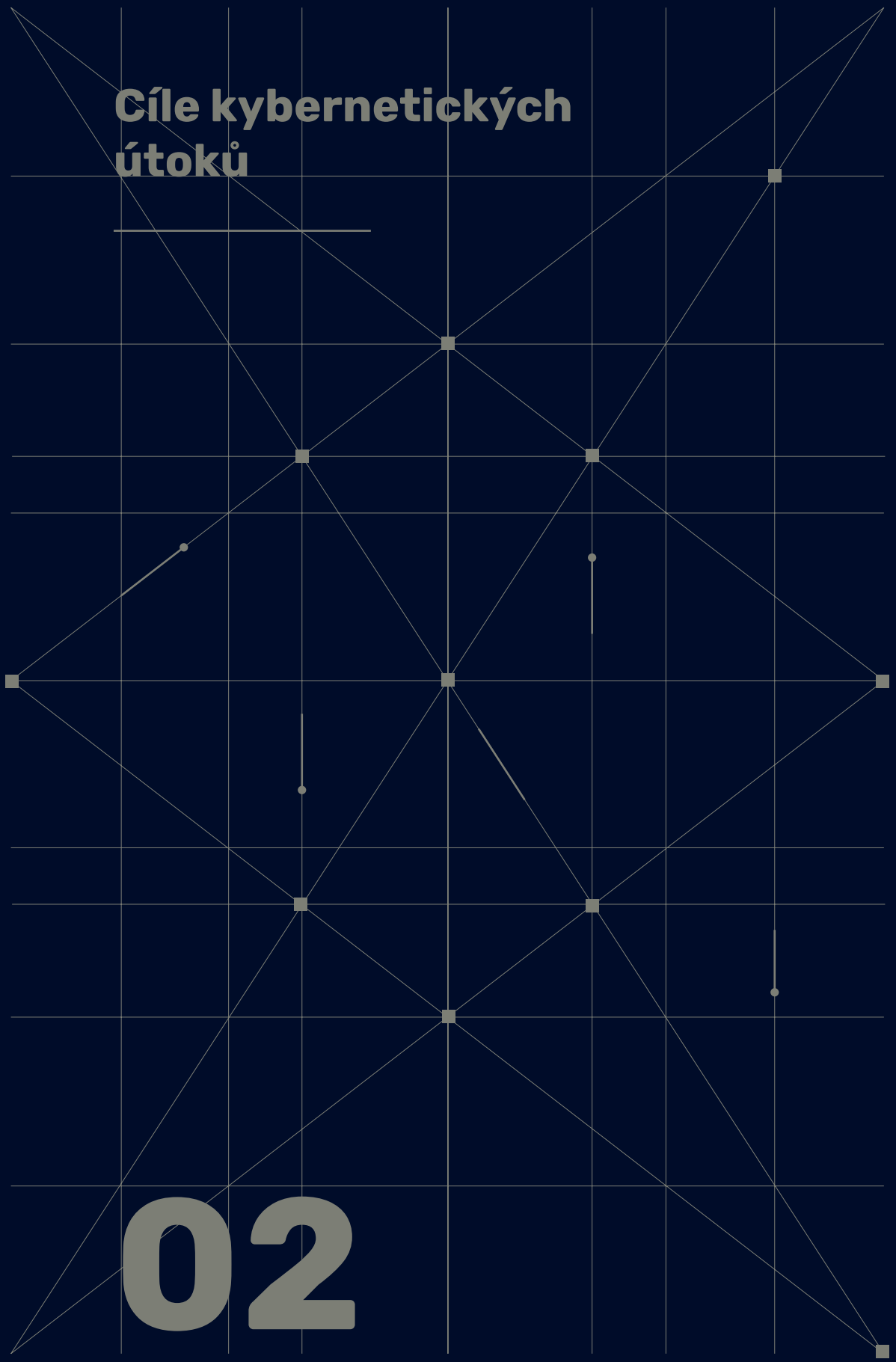
Malware, který využívá k šíření po síti zranitelnost apod.

Kryptomining vs. ransomware

Těžba kryptoměn skrze malware nevyžaduje na rozdíl od ransomwarových útoků po útočníkovi komunikaci s napadeným subjektem (například dokazování schopnosti dešifrovat napadená data) ani žádné konkrétní kroky na straně napadeného, včetně ochoty zaplatit výkupné. Na rozdíl od ransomwarových útoků útočníci méně riskují z trestně-právního pohledu, když součástí kryptominerových útoků není vydírání a velmi malá je i pravděpodobnost, že v krajním případě budou ohroženy lidské životy. Trend nástupu kryptominerů naznačuje, že by se celkově mohlo jednat o efektivnější nástroj generování finančního zisku a pro útočníky atraktivnější volbu než ransomware. Přes dopady na výpočetní výkon infrastruktury napadených subjektů jsou tyto útoky z pohledu ochrany ICT méně závažné. Na rozdíl od ransomwarových útoků nemají destruktivní charakter a neohrožují dostupnost důležitých dat. Zájmem útočníků je, aby kryptominer bral natolik malou část výkonu, že jej oběť vůbec nezaznamená.

Nákaza kryptominery je **narůstajícím trendem, který je zaznamenáván napříč většinou odvětví i v rámci České republiky.**

Cíle kybernetických útoků



02

Uživatelé: Brána do sítí organizací

Dopady	poskytnutí přístupu do sítí organizace útočníkům
Útočník	státní aktéři, státem sponzorované skupiny, kyberzločinci
Metody	phishing, spear-phishing, watering hole

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

Útočníci proti uživatelům většinou využívají sociálního 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 (například heslo) nebo uživatele přesvědčit ke stažení přílohy obsahující malware. Mezi nejvíce užívané techniky sociálního inženýrství v kybernetickém prostoru patří phishing a spear-phishing.

Phishing:

Tento typ sociálního inženýrství má podobu e-mailu, SMS nebo zprávy na sociální síti, ve které se útočník snaží přesvědčit oběť, aby mu prozradila citlivou informaci, otevřela odkaz vedoucí na škodlivou stránku nebo otevřela přiložený soubor obsahující škodlivý kód. Na rozdíl od spear- phishingu není personalizovaný a zpravidla je odesílán velkému množství lidí najednou.

Spear-phishing:

Jde o personalizovanou formu phishingu, která cílí na konkrétní osoby. Útok vyžaduje rozsáhlejší přípravu, v rámci niž útočník musí například identifikovat konkrétní osobu v organizaci, které pošle phishingový e-mail. Útočník musí mít zároveň dostatečné znalosti k tomu, aby dokázal vytvořit takový e-mail, který bude působit hodnověrně a nevzbudí u oběti pochybnosti. Spear-phishing je jednou z primárních technik, kterou APT skupiny využívají k získání přístupu do cílové sítě, ať už za účelem špionáže nebo způsobení škod.

Fyzickou formou spear-phishingu (metoda, které se také říká „Baiting“) může být i pohozený USB disk v blízkosti vytipovaného cíle, například na parkovišti pracoviště zaměstnance. Útočník spoléhá na zvědavost zaměstnanců, kteří disk najdou a na to, že disk připojí do pracovního počítače připojeného k cílové síti. Disk může obsahovat například škodlivý kód, který útočníkovi umožní přístup do sítě.

V **České republice** byl v roce 2018 patrný trend rostoucí sofistikovanosti cílených phishingových útoků. I když je stále nejrozšířenější phishing skrze e-maily psanými lámanou češtinou, roste počet spear-phishingových útoků, u kterých je zřejmé, že pachatelé disponují vynikající znalostí prostředí a investovali množství času do přípravy útoků (například tvorba podvržených stránek, které jsou identické s těmi legitimními). Častým cílem phishingových útoků jsou v České republice finanční instituce a jejich klienti, ale v posledních letech se zvedl i podíl útoků proti českým univerzitám (podrobnosti k phishingovým útokům na české univerzity na straně 38). Hlavní motivací útočníků je finanční zisk, ale výjimkou nejsou ani snahy o krádež duševního vlastnictví. Příkladem nepříliš sofistikovaného phishingu byly v roce 2018 výhružné e-maily, ve kterých útočníci sdělují oběti, že přes webovou kameru získali choulostivé záběry a vyhrožují jejich zveřejněním. Aby tomu oběť zabránila, měla by poslat určitou částku v bitcoinech. [ix]

Nejde však čistě o problém samotných uživatelů. V řadě soukromých firem, veřejných institucí i neziskových organizací není kybernetické bezpečnosti věnována dostatečná pozornost a zaměstnanci postrádají potřebná školení o základech digitální hygieny, která by jim měl zaměstnavatel poskytnout.

Veřejný sektor: Pomalu se adaptující prostředí

Dopady	ztráta dat, kompromitace citlivých a utajovaných informací
Útočník	státní aktéři, státem sponzorované skupiny
Metody	phishing, spear-phishing, DDoS a další

Častým cílem kybernetických útoků je veřejný sektor, především v podobě institucí státní správy, které jsou pro útočníky zdrojem zpravodajsky, vojensky, politicky i ekonomicky významných informací. Kybernetické špionážní operace usilující o získání podobných informací jsou dlouhodobého charakteru a vyžadují po útočnících pokročilé schopnosti dlouhodobě se vyhýbat odhalení a nepozorovaně z napadeného systému získat data. Takovou úrovní know-how disponují zejména státní aktéři nebo jimi sponzorované skupiny, což se do budoucna velmi pravděpodobně nezmění, stejně jako jejich zvýšený zájem o státní instituce.

V českém veřejném sektoru se vyskytuje řada specifických vlivů, které jej odlišují od principů běžných v soukromém sektoru. Tyto faktory se promítají do principů běžného fungování jednotlivých státních institucí a přímo či nepřímo ovlivňují úroveň kybernetické bezpečnosti v nich. Jedná se o:

Nejistotu z nedaleké budoucnosti:

Změny v důsledku volebních výsledků mnohdy znamenají zastavení aktuálně probíhajících činností a čekání na nové vedení, postupy a přístupy i v rámci provozu ICT či zajišťování kybernetické bezpečnosti;

Upřednostňování krátkodobých cílů před dlouhodobými:

Převažuje tendence provádět to, co je vidět hned. Strategické projekty, které se projeví za dlouhou dobu (vzhledem k předešlému bodu), jsou obtížněji realizovatelné;

Tabulkové platy a nedostatečné osobní ohodnocení či odměny:

Platy odborníků ve veřejném sektoru zpravidla nejsou schopné konkurovat platům v soukromém sektoru.

Mezi nejčastější zranitelnosti českého veřejného sektoru patří:

Nedostatek odborníků na kybernetickou bezpečnost způsobený především nekonkurenceschopností veřejného sektoru v nabídce finančního ohodnocení a benefitů pracovníků.

- **Příklad:** Platy v soukromém sektoru jsou zpravidla v oblasti kybernetické bezpečnosti vyšší.
- **Riziko:** Přetížení jednotlivců, na kterých kybernetická bezpečnost dané instituce stojí.

Nedostatečné prohlubování znalostí pracovníků zajišťujících provoz, správu nebo bezpečnost ICT prostředků, které je způsobeno nízkým rozpočtem na školení těchto pracovníků.

- **Příklad:** Předpoklad top managementu, že cena školení základních administrativních dovedností pro úředníky a specializovaných školení pro ICT odborníky ve veřejné správě je srovnatelná. Běžné školení pro úředníky obvykle stojí v řádu jednotek tisíc korun, školení na ICT provoz a bezpečnost se zpravidla pohybují v řádu desítek tisíc korun. Top management pak takto drahá školení nepovoluje, případně je povoluje pouze sporadicky.
- **Riziko:** Odborníci na ICT neznají aktuální trendy v oblasti kybernetické bezpečnosti, čímž může být práce pro potencionálního útočníka usnadněna.

Organizační střet zájmů v odpovědnostech za správu ICT a bezpečnost ICT

- **Příklad:** Osoba spravující bezpečnostní opatření současně kontroluje i bezpečnost takového opatření.
- **Riziko:** Neexistence adekvátní kontroly, zda dané opatření opravdu správně slouží svému účelu a je dostatečně efektivní.

Délka prosazování a schvalování bezpečnostních záměrů

- **Příklad:** Schválení nové bezpečnostní politiky/směrnice v řadě institucí trvá rok a déle.
- **Riziko:** Tím, že není taková politika/směrnice schválena a účinná, není ani vymahatelná a zaměstnanci se jí nemusí řídit.

Jiná pravidla pro top management

Příklad: V některých institucích má top management kvůli svému pohodlí nastavena administrátorská práva a oprávnění pro využívání ICT zařízení. Jedná se například o možnost instalace spustitelných souborů.

Riziko: Top management neověřuje, že jím instalovaný spustitelný soubor neobsahuje škodlivý kód. Instalací takového softwaru může dojít k narušení provozu celé interní sítě instituce.

Využívání slabých autentizačních (přihlašovacích) mechanismů

Příklad: Přihlašování uživatelů do informačních systémů je prováděno pouze na základě uvedení jména a hesla i u zásadních systémů.

Riziko: Dnes již překonaný autentizační mechanismus, který má mnoho slabin, jako je například uživatel, který si napíše heslo na papír vedle monitoru nebo zvolí slabé heslo, které je možné během chvíle uhádnout provedením tzv. slovníkového útoku či samotný přenos a uložení hesla.

Kritická infrastruktura: Útoky na hladké fungování státu

Dopady	narušení důvěrnosti, dostupnosti nebo integrity informací v sítích důležitých pro chod státu
Útočník	státní aktéři, státem sponzorované skupiny
Metody	phishing, spear-phishing, watering hole, zranitelnosti nultého dne

Kritickou informační infrastrukturou (KII) je dle § 2 ZKB[x] prvek nebo systém prvků kritické infrastruktury (KI) v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti. Kritická infrastruktura (KI) samotná je dle § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)[xi] , definována jako prvek nebo systém prvků, jejichž narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Informační systémy kritické infrastruktury dlouhodobě patří mezi oblíbené cíle útočníků v kyberprostoru. Útoky na takové cíle vyžadují vysokou míru sofistikovanosti, časově náročnou přípravu i rozsáhlé prostředky, a proto zůstávají doménou spíše národních států nebo jimi sponzorovaných skupin. KI je pro útočníky lákavým cílem. Ochromení jednoho či více prvků může cílovému státu způsobit vážné škody, které pro útočníky mohou být strategicky výhodné. Mezi tradiční prvky KI patří elektrárny, přehrady, letiště nebo telekomunikační sítě. Vyřazení některého z těchto prvků může ochromit schopnost státu poskytovat služby (elektřina, teplo, voda) nebo se bránit proti konvenčnímu útoku. Podle informací dostupných NÚKIB v **České republice** zatím neproběhl žádný sofistikovaný a soustředěný kybernetický útok, který by cílil na KII, ale to stejné nelze říci o jiných státech. I když nedošlo k žádným vážným útokům, které by měly dramatické dopady jako v minulosti,[8] vydaly instituce zodpovědné za kybernetickou bezpečnost v průběhu roku 2018 řadu varování před probíhajícími útoky, jako například:

- V dubnu 2018 vydaly Ministerstvo vnitřní bezpečnosti USA, FBI a britské Národní centrum pro kybernetickou bezpečnost společné technické varování před útoky na správce jejich kritické informační infrastruktury a poskytovatele internetových služeb. Předmětem varování byla především síťová zařízení (routery), která představují ideální cíle díky kombinaci relativně slabé ochrany a rozsáhlého přístupu k síti. Podle varování pocházely útoky od skupin sponzorovaných Ruskou federací.[xii]

[8] Jako například útok z prosince 2015 na Ukrajině, kde se následkem kybernetického útoku bez proudu ocitlo přes dvě stě tisíc lidí.

- V prosinci roku 2018 vydaly Austrálie, Japonsko, Kanada, Nový Zéland a Velká Británie varování před probíhajícími kybernetickými útoky na subjekty z oblasti zdravotnictví, obranného průmyslu, energetiky či telekomunikací. Podle varování stojí za útoky skupina APT 10 mající vazby na ČLR.[xiii]

Vzhledem k důležitosti kritické infrastruktury a existujícím zájmům různých aktérů nelze podobné útoky vyloučit ani v budoucnu. Soustředěné útoky na KII mají zpravidla několik charakteristických znaků. Útočníci se do systémů oběti dostanou nejčastěji pomocí metod sociálního inženýrství (phishing, spear-phishing, watering hole), v systému za účelem sběru potřebných informací působí dlouhou dobu a jejich konečným cílem bývá získání citlivých dat nebo ovládnutí řídicích průmyslových systémů v jednotlivých prvcích KI.

Právě skrze nakažení řídicích systémů škodlivým kódem mohou útočníci kontrolovat napadený prvek KI, vyřadit ho z provozu nebo v krajním případě způsobit materiální škody a ztráty na životech. Dalším cílem útoku na prvek KI mohou být průmyslové bezpečnostní systémy. Na ty cílí například malware Triton (také Trisis, Hatman), který byl v roce 2017 nalezen v petrochemickém zařízení v Saúdské Arábii. V roce 2018 byl kyberbezpečnostní společností FireEye jeho původ vystopován do Ruské federace.

Malware Triton/Trisis cílící na průmyslové bezpečnostní systémy

Triton byl poprvé objeven na konci roku 2017 v bezpečnostním přístrojovém systému[9] Triconex od Schneider Electric v saúdskoarabském petrochemickém zařízení. Jde o první malware svého druhu, který se nezaměřuje na programovatelné logické automaty[10] , ale útočí na bezpečnostní systémy. Bezpečnostní systémy mají za úkol detekovat bezprostřední hrozbu havárie a pomocí vhodných protiakcí provádějí nezbytná opatření k vrácení procesu do bezpečného stavu. Bezpečnostní systém nakažený malwarem by krizovou situaci (přetlak, přehřátí) nemusel vyhodnotit jako nebezpečí a mohlo by tak dojít k havárii a následně materiálním škodám nebo ztrátám na životech. V případě útoku na petrochemické zařízení v Saúdské Arábii byl malware kvůli chybě v kódu odhalen a nepodařilo se mu napáchat žádné škody. Původ malwaru byl odborníky společnosti FireEye v roce 2018 vystopován do ruské vědecké instituce s vazbami na ministerstvo obrany, Ústředního naučně-výzkumného ústavu chemie a mechaniky. [xiv]

Zařízení Triconex od společnosti Schneider Electric

[9] Také Safety Instrumented System (SIS)
[10] Také Programmable Logic Controller (PLC)

Energetický sektor: Útočné pole se rozšiřuje[11]

Dopady	výpadek dodávek elektřiny nebo plynu, únik informací
Útočník	státní aktéři, státem sponzorované skupiny
Metody	phishing, spear-phishing, watering hole, zranitelnosti nultého dne

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

I přesto počet a sofistikovanost útoků na energetický sektor narůstá (viz časovou osu vedle). Zejména pro státní aktéry je lákavá možnost kontroly nad dodávkami elektrické energie v rozvodné síti protivníka.

Prostředí energetiky je natolik specifické, že zde mohou vznikat kombinace určitých zranitelností, které útočník může zneužít.

Zastaralé komponenty

První z nich je spojena se samotnými průmyslovými řídicími technologiemi. Jedná se o speciální elektrotechnická zařízení, jejichž životní cyklus může být plánován na mnoho let dopředu (i více než deset let). Systém tak může z pohledu kybernetické bezpečnosti obsahovat zastaralé komponenty;

Aktualizace

Se zastarávajícími řídicími zařízeními se pojí problematika aktualizací firmwaru. Aktualizace nebývají vydávány výrobci zařízení v takové četnosti jako v oblasti IT, a když vydány jsou, může nastat problém s jejich instalací, neboť obdobně jako v IT by aktualizace měla být zprvu testována v neprodukčním prostředí. Kromě plánovaných odstávek se systémy v elektrárnách nevypínají, aby nedošlo k výpadkům elektřiny, a aktualizace tak mohou být instalovány se zpožděním;

Útoky na dodavatelský řetězec

Dodavatelský řetězec může představovat zranitelnost i v energetickém sektoru. V některých případech zůstávají průmyslové řídicí systémy připojeny do sítí dodavatelů. Dodavatelům to umožňuje získat data z reálně instalovaných zařízení například pro potřebu jejich diagnostiky (zjištění stavu zařízení, jeho vytížení, opotřebení apod.). Tyto vstupy ale vytváří příležitost pro útočníky, kteří takto získají možnost přistupovat do sítí energetické společnosti skrze dodavatelské sítě.[xv]

[11] Zpráva o stavu kybernetické bezpečnosti se každý rok zaměřuje na ty sektory kritické informační infrastruktury, o kterých se objevují nové poznatky.

Čínská kybernetická špionáž dodavatelů do energetického průmyslu

Výrobci průmyslových řídicích zařízení jsou také lákavým cílem pro kybernetickou špionáž. Americké ministerstvo spravedlnosti v roce 2017 obvinilo tři občany Čínské lidové republiky z kybernetické špionáže proti společnosti Siemens, která do energetického sektoru dodává průmyslová řídicí zařízení. Žaloba specificky uvedla, že energetická divize společnosti byla jedním z cílů útočníků. Jednalo se pravděpodobně o kybernetickou špionáž, ale není možné vyloučit, že útočníci informace sbírali k přípravě útoků s destruktivním charakterem.

V českém energetickém sektoru přichází nový trend SMART technologií, které distribuční společnosti začínají nasazovat napříč zemí. Chytré elektroměry, tzv. SMART metery, dokážou zaznamenávat spotřebu energie (nebo vody a plynu) a data automaticky odesílat na centrálu ke zpracování. Pro distributora to bude představovat možnost optimalizovat tok energie, pro hackera možnost rozšíření útočného pole o nové cíle útoků. V případě, že budou mít SMART metery funkcionalitu, díky které bude možné neplatiče odpojit na dálku, bude možné zneužít případného nedostatečného zabezpečení k plošným výpadkům elektřiny nebo plynu. Výrobci SMART meterů by tak měli dbát na jejich adekvátní zabezpečení, aby bylo riziko kybernetického útoku co nejmenší.

Malware cílící na průmyslové řídicí systémy v energetickém sektoru

2014

Havex (Evropa a USA)

Společnosti, které malware Havex napadl, se zabývaly systémy pro vzdálenou správu ICS systémů, což značí, že útočníci v jejich sítích hledali informace, které by mohli použít k dalším útokům na energetický sektor. Nejsou zprávy o tom, že by malware způsobil fyzické škody.[xvi]

2015

BlackEnergy (Ukrajina)

Útok, který se stal den před Vánoci, je považován za první úspěšný kybernetický útok, který způsobil výpadek elektrické energie. Útočníkům se podařilo kompromitovat sítě tří ukrajinských distribučních společností a tím způsobit dočasný výpadek elektrické energie, který zasáhl více než 200 000 lidí.[xvii]

GreyEnergy (Polsko)

Společnost ESET zaznamenala malware GreyEnergy, nástupce BlackEnergy. Jeho prvním cílem byla blíže nespecifikovaná energetická společnost v Polsku.[xviii]

2016

Industroyer (Ukrajina)

Ukrajina se stala rovněž obětí malwaru Industroyer (známý také jako Crashoverride), jehož následkem se pětina Kyjeva ocitla bez elektřiny. Jedná se o důmyslný malware, který útočníkům umožnil skrze průmyslové komunikační protokoly ovládat distribuci elektřiny. Podle expertů se jednalo o test, ve kterém si útočníci zkoušeli své kapacity.[xix]

2017

Kybernetické útoky na americké a německé energetické společnosti (USA a Německo)

Americké a německé energetické společnosti čelily v roce 2017 soustavným pokusům o kompromitaci jejich sítí. Počátečními oběťmi byli dodavatelé, kteří byli vystaveni vlně spear-phishingových útoků a útokům pomocí metody watering hole. Přes ně hackeři útočili na své primární cíle – energetické distribuční společnosti a další subjekty tamní kritické infrastruktury. Jejich cílem byl nejen sběr informací, ale i narušení průmyslových řídicích procesů.[xx]

TRITON (Saúdská Arábie)

Více o malwaru TRITON na straně 29.

2018

GreyEnergy (Polsko a Ukrajina)

Útoky GreyEnergy se vrátily a jejich cíli se staly energetické a přepravní společnosti na Ukrajině a v Polsku.

Bankovní sektor: Zabezpečený, přesto velmi lákavý cíl

Dopady	finanční ztráty, ztráta reputace banky, narušení kontinuity činnosti, ztráta nebo neoprávněná změna dat
Útočník	kyberzločinci
Metody	phishing, spear-phishing, trojanizace legitimních mobilních aplikací

Česká národní banka provádí pravidelné kontroly kybernetické bezpečnosti v bankovním sektoru. Vzhledem k absenci vážnějších incidentů lze vyvodit, že **český bankovní sektor** je poměrně dobře zabezpečený. Stále ale existují rozdíly ve vyspělosti jednotlivých finančních institucí především ve smyslu ochrany proti pokročilým kybernetickým hrozbám a vnitřnímu útočníkovi (například v bezpečnostním monitoringu a penetračním testování). Obecně se ale banky snaží kybernetickou bezpečnost nepodceňovat, protože kompromitace jejich informačních systémů by mohla mít dalekosáhlé finanční i reputační následky.

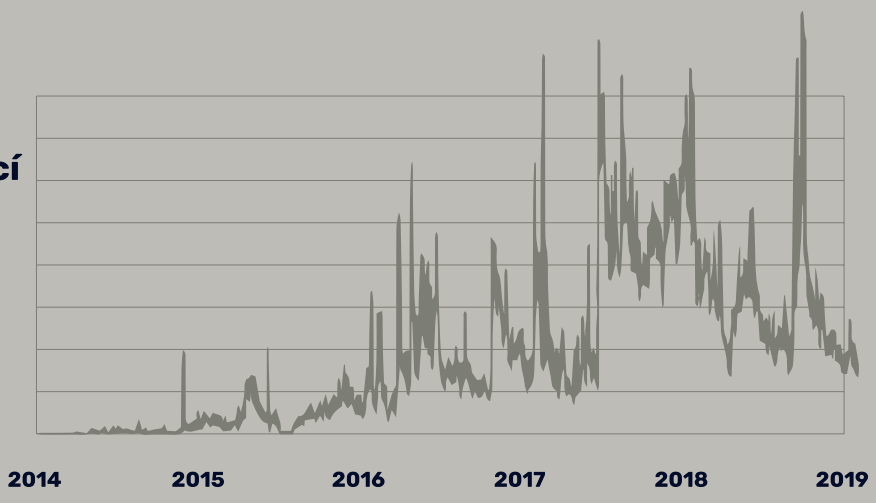
Největší zranitelností v bankovním sektoru byli v roce 2018 uživatelé samotní. Útočníci tohoto dlouhodobě slabého článku často využívali a banky tak v roce 2018 zaznamenaly nárůst počtu i důmyslnosti phishingových a spear-phishingových útoků na své klienty.

Dalším slabým místem jsou v některých případech nedostatky v účinnosti a rychlosti reakce na kybernetické incidenty (útoky) ve smyslu koordinace a kapacit bankovních CERTů a přípravy dostatečně otestovaných plánů pro zvládání incidentů.

Novým trendem začínají být **útoky na mobilní internetové bankovnictví.** Stále více lidí využívá mobilní aplikace ke spravování svých financí a hackeři se tomu rychle přizpůsobili. Telemetrická data společnosti ESET jasně ukazují, že přibývá malwaru zaměřeného na bankovní aplikace pro OS Android.

Graf 3:

Nárůst malwaru bankovních aplikací na OS Androidv ČR i ve světě [xxi]



Zdroj: https://www.welivesecurity.com/wp-content/uploads/2019/02/ESET_Android_Banking_Malware.pdf

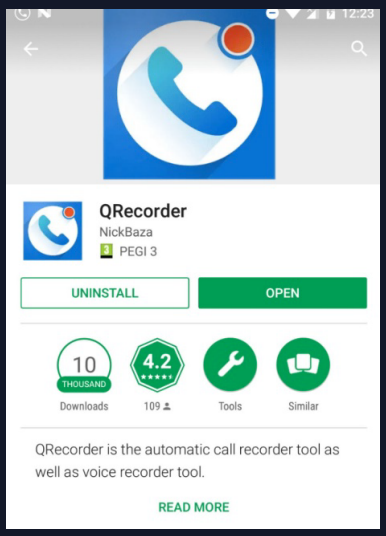
V roce 2018 byla příkladem tohoto trendu aplikace QRecorder, která poškodila klienty českých bank. Aplikace dostupná v oficiálním obchodě Google Play sloužila k nahrávání hovorů. Po jedné z aktualizací byla aplikace QRecorder upravena tak, aby se chovala jako trojský kůň. „Trojanizace“ legitimních aplikací je potenciálně velmi vážným problémem. Do obchodu Google Play vkládá aplikace velké množství nezávislých vývojářů, kteří prodávají práva k aplikacím. V případě aplikace QRecorder zaplatili útočníci za zdrojový kód aplikace 29 dolarů (asi 650 Kč). Jedná se tedy o relativně nízké výdaje, které umožňují kyberkriminálním aktérům zneužít legitimní aplikace k šíření malwaru.

QRecorder pod drobnohledem

Bezpečnostní analytici zjistili, že po jedné z aktualizací byla aplikace QRecorder upravena tak, aby se chovala jako trojský kůň. Pomocí této modifikace mohli útočníci vzdáleně přistupovat do chytrého telefonu, ve kterém byla aplikace nainstalovaná. Mimo to měli také možnost snímat zadané přihlašovací údaje a číst SMS pro získání obou potřebných faktorů pro autentizaci k různým službám, například mobilního bankovnictví.

V první fázi malware zjistil, zda jsou v telefonu aplikace, které mohou být pro útočníky zpeněžitelné, tedy například bankovní aplikace. Následně byl do telefonu stažen modul, který vytvořil neviditelnou vrstvu nad cílovou aplikací, například internetovým bankovnictvím, a zachytil přihlašovací údaje uživatele.

Způsob, jakým se doposud legitimní aplikace QRecorder proměnila v bezpečnostní riziko je mimořádně zákeřný. Útočníci legálně koupili zdrojový kód od developera původní aplikace a na obchod Google Play následně umístili téměř identickou aplikaci se stejným jménem. Vložení škodlivého kódu prostřednictvím aktualizace pak učinili tak, že to nebudilo podezření.



eHealth: Útoky na nejcitlivější osobní data s potenciálem ohrozit život

Dopady	nedostupnost kritických dat s možnými dopady na efektivitu zdravotnických zařízení a zdraví pacientů; u útoků na důvěrnost dat možnost vydírání a v případě zveřejnění dat zásah do osobního života pacientů
Útočník	kyberzločinci, pravděpodobně i státní aktéři
Metody	phishing, spear-phishing, neautorizované využívání přístupových údajů, ransomware

Vzhledem k citlivosti dat a možným dopadům útoků v oblasti eHealth na zdraví a osobní život pacientů jsou rizika vyplývající z ohrožení informačních systémů využívaných ve zdravotnictví relativně vyšší než u jiných systémů zpracovávajících osobní údaje. Mezi největší hrozby patří pozměnění, odcizení či ztráta citlivých osobních údajů pacientů společně s častějším výskytem vyděračských útoků (ransomware) způsobujících nedostupnost důležitých informací. Výzvou se také stává zabezpečení medicínských IoT zařízení a možnosti jejich zneužití. Pozměnění či znepřístupnění narůstajícího množství digitalizovaných zdravotnických informací může pacienta přímo ohrozit na životě. Únik a zneužití, v krajním případě pak zveřejnění zdravotních informací o pacientovi, je považováno za silný zásah do pacientovy osobní sféry. Může jedince poškodit v osobním i veřejném životě. Mnoho subjektů, které spravují zdravotní informační systémy, zejména pak poskytovatelé zdravotních služeb, často nemá dostatečné finanční a personální kapacity k adekvátnímu zabezpečení spravovaných dat. Kombinace těchto skutečností způsobuje, že **kybernetické útoky proti zdravotním systémům mohou při nízkých nákladech a malém vynaloženém úsilí přinést relativně velké zisky.**

V **českém zdravotnictví** existuje několik rizik a zranitelností, které jsou pro tento sektor charakteristické a kterých mohou útočníci zneužít. Patří k nim:

Chybějící standardy kybernetické bezpečnosti

V České republice dosud není dostatečně řešen problém kybernetických bezpečnostních standardů jednotlivých poskytovatelů zdravotních služeb. V září 2017 byl Ministerstvem zdravotnictví vydán metodický materiál ke kybernetické bezpečnosti v oblasti zdravotnictví, který se tuto mezeru snaží překonat. Vzhledem k absenci jeho závaznosti lze očekávat pouze omezený dopad. Od 1. srpna 2017 vstoupila v účinnost novela ZKB, která pod rozsah zákona zahrnula nemocnice s kapacitou nad 800 akutních lůžek nebo statusem centra vysoce specializované traumatologické péče, jejichž informační systémy zároveň naplní předem stanovené dopady; zbytek ovšem zůstává neregulován.

Zastaralost softwaru

Společným znakem nemalého počtu informačních systémů využívaných v nemocnicích je zastaralý software.

Riziko odcizení dat

V rámci procesu zdravotní péče přistupuje k citlivým datům o pacientech velké množství osob jak ze strany zaměstnanců, tak dodavatelů. U poskytovatelů zdravotních služeb, u nichž není zavedeno řádné řízení a kontrola přístupů k informacím, se zvyšuje riziko možného odcizení dat a jejich dalšího zpeněžení na černém trhu.

Mezi nejčastější typy útoků **v českém zdravotnickém sektoru** patří i ve zdravotnickém sektoru phishingové a spear-phishingové útoky, které podle oslovených subjektů představují až 90 % evidovaných útoků. Přijímaná technická opatření snižují počty zejména phishingových útoků, na druhou stranu stoupá sofistikovanost spear-phishingových útoků, jejichž častým cílem jsou i u zdravotnických zařízení ekonomická oddělení zodpovědná za finanční prostředky organizací.

České zdravotnictví zaznamenalo i ransomwarový útok, když Léčebnu tuberkulózy a respiračních nemocí v Janově na Rokycansku zasáhl koncem června 2018 vyděračský útok. Personál ztratil přístup do informačních systémů léčebny. Pro dešifrování souborů byla požadována platba v kryptoměně.

Akademický svět: Rostoucí zájem útočníků

Dopady	únik duševního vlastnictví, ekonomické ztráty či nedostupnost vědeckých přístrojů kvůli vyřazení serverů z provozu
Útočník	kyberzločinci, státem sponzorované skupiny
Metody	phishing, spear-phishing, podvodné e-maily, DDoS

Český akademický svět je atraktivním cílem pro kybernetické aktéry, kteří mají zájem o intelektuální vlastnictví z několika důvodů:

- Na univerzitách se často provádí špičkový výzkum, akumuluje se tam know-how a shromažďují přední vědci z daných oborů;
- Zabezpečení českých univerzit se různí. V České republice neexistují jednotná bezpečnostní pravidla, která by všechny univerzity dodržovaly. Sdružení CESNET dává rady a návody (best practices), jejich implementace ale záleží na prozíravosti, finanční situaci dané instituce a také na ochotě dotčených pracovníků;
- Vzhledem k vysokému počtu uživatelů představují pro bezpečnostní týmy univerzitní sítě specifickou výzvu. Počty studentů na českých univerzitách se pohybují v tisících a ve většině postrádají povědomí o kybernetických hrozbách a způsobech, jak se jim bránit. Jejich účtů lze zneužít stejně jako účtů zaměstnanců univerzit a hackeři tak mají široké pole pro pokusy o kompromitaci.

cesnet

Je sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní digitální infrastrukturu pro vědu, výzkum a vzdělávání zahrnující počítačovou síť, výpočetní gridy, datová úložiště, prostředí pro spolupráci a nabízející širokou škálu služeb.

Rok 2018 jasně ukázal, že hackeři mají o český akademický svět zájem. Deset **českých univerzit** nahlásilo, že bylo vystaveno vlně phishingových a spear-phishingových útoků.

U phishingových útoků z roku 2018 je patrný nárůst sofistikovanosti, kdy útočník namísto generického e-mailu psaného špatnou češtinou prokazuje detailní znalost prostředí českých univerzit. Útočníci vystupují jako reální zaměstnanci univerzit a podvodné stránky, na které phishingové a spear-phishingové e-maily odkazují, přesně kopírují vizuální styl jednotlivých pracovišť.

V **českém školství** je mnoho citlivých informací, které mohou uniknout i bez zapříčinění útočníka. V roce 2018 nedostatečná správa osobních údajů zapříčinila, že se skrze aplikaci České školní inspekce InspIS bylo možné dostat k důvěrným informacím až 140 000 žáků druhého stupně základních škol. Mezi informace, které bylo možné vyhledat v databázi České školní inspekce, patří jméno, příjmení, třída a informace o zdravotním znevýhodnění (bez údajů o konkrétním postižení). Za únikem dat stála pravděpodobně technická chyba v aplikaci InspIS. Podle informací z médií přispělo k úniku také to, že autoři aplikace ji rok neaktualizovali.[xxii]

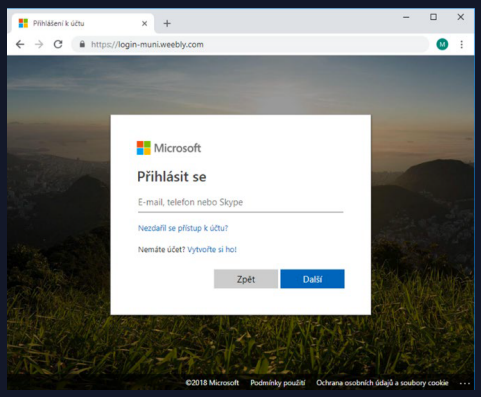
Kybernetické útoky na vzdělávací a výzkumné instituce nelze podceňovat. V případě kompromitace univerzitních sítí může dojít k úniku duševního vlastnictví a dosud nepublikovaných výsledků výzkumu. Pokud by útočníci v sítích českých univerzit působili nepozorovaně delší dobu, mohlo by to pro Českou republiku ve výsledku znamenat oslabení její konkurenceschopnosti.

Phishing na českých univerzitách

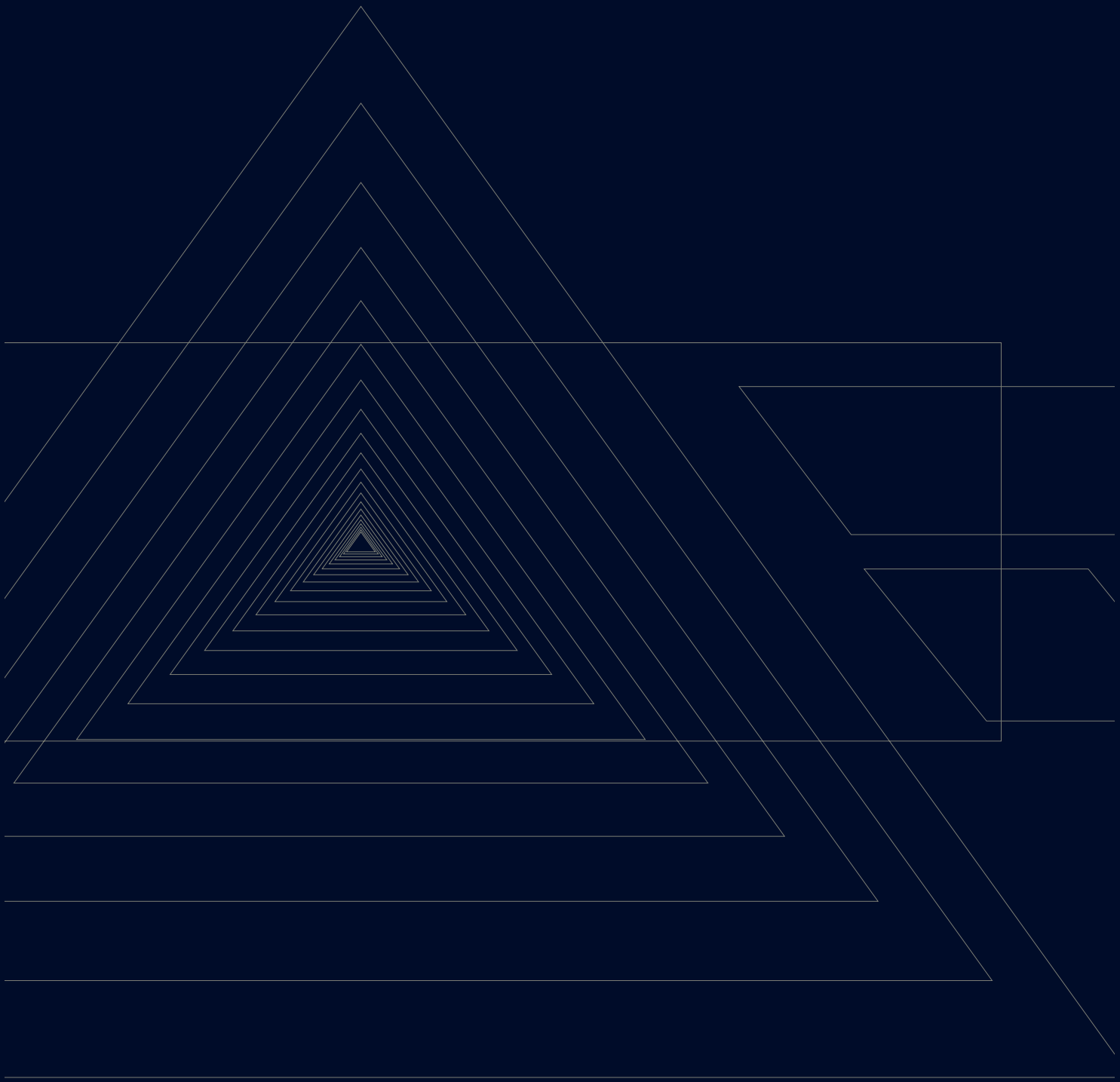
Bezpečnostní tým Masarykovy univerzity (CSIRT MU) v září 2018 varoval před phishingovou kampaní, která postihla několik českých univerzit a jejímž cílem byla krádež výzkumných dat, nepublikovaných výsledků nebo know-how výzkumných skupin. Jejich zájmem byla data z různých oborů, jako například z lékařství, technických oborů nebo humanitních věd.

Jednalo se o dobře připravené útoky, při nichž útočníci prokázali znalost prostředí českých univerzit. Text phishingového e-mailu sice nebyl psán dobrou češtinou a obsahoval velké množství chyb, zaštiťoval se ale reálným IT oddělením univerzity a zneužíval jméno reálného správce včetně jeho fotografie, čímž vytvářel dojem věrohodnosti.

Útočníci po svých obětech požadovali aktivaci jejich účtů v aplikaci Office 365, které byly údajně z důvodů probíhajících phishingových útoků dočasně zrušeny. K aktivaci měli použít odkaz v e-mailu. Ten byl ale ve skutečnosti odkazem na podvržené stránky, které svým vzhledem kopírovaly reálné stránky pro přihlášení do systému Office 365. Pokud by oběť své přihlašovací údaje do podvržené stránky zadala, získali by je i útočníci, kterým by tím byl otevřen vstup do sítí univerzity. Podle dostupných informací ke kompromitaci nedošlo.



Zdroj: https://csirt.muni.cz/about-us/news/phish_sci



03 Opatření

Legislativní ukotvení kybernetické a informační bezpečnosti: Nastavení základních pravidel pro důležité subjekty

Ochrana kybernetického prostoru je do značné míry závislá na legislativě, kterou jsou povinny se příslušné subjekty řídit. Z hlediska zákona o kybernetické bezpečnosti se jedná o subjekty, jejichž informační systémy jsou důležité pro fungování státu. Tyto subjekty se dělí do následujících čtyř kategorií:

A	B	C	D
Kritická informační infrastruktura	**Základní služba**	**Významný informační systém**	**Poskytovatel digitální služby**

Každá z těchto čtyř kategorií je přiblížena v příloze č. 3.

Právní úprava vztahující se k těmto subjektům:

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS)
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby
- Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018

Určování informačních systémů, které spadají do působnosti ZKB, stále probíhá a počty povinných subjektů narůstají. Na konci roku 2018 byla čísla následující:

Počet určených subjektů ke konci roku 2018:

Subjekty kritické informační infrastruktury:

45

subjektů

Prvky kritické informační infrastruktury:

114

informačních systémů

Významné informační systémy:

178

informačních systémů

Provozovatelé základní služby:

30

subjektů

Informační systémy základní služby:

30

informačních systémů

Metodická podpora NÚKIB na webu

NÚKIB pravidelně zveřejňuje na svých internetových stránkách podpůrné materiály nebo schémata týkající se výkladu zákona o kybernetické bezpečnosti, jejichž cílem je zjednodušit odborné i široké veřejnosti problematiku spojenou s kybernetickou bezpečností.

Varování NÚKIB: Opatření proti bezprostředním hrozbám

Jeden z úkolů NÚKIB je vydávání varování o hrozbách v oblasti kybernetické bezpečnosti. NÚKIB taková varování vydává ve chvíli, kdy se dozví zejména z vlastní činnosti, z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o kybernetické hrozbě, na kterou je nutné bezprostředně reagovat.

Takovým varováním bylo varování ze dne 17. prosince 2018 před používáním technických a programových prostředků společností Huawei Technologies Co. Ltd. a ZTE Corporation. K jeho vydání vedla kombinace poznatků a zjištění, které jsou blíže popsány na stránkách NÚKIB.

NÚKIB vydal k tomuto varování podpůrnou metodiku, která konkretizuje opatření, jež mohou správci informačních a komunikačních systémů spadajících pod ZKB přijmout. Jedno z opatření se týká i ZZVZ, který organizace často aplikují s cenou jako hlavním kritériem. ZZVZ v současné podobě ovšem umožňuje zohlednit i jiná kritéria než jen cenu, využití těchto kritérií ale v nemalém počtu případů vyžaduje větší kapacity ze strany zadavatele a navyšuje riziko možného přezkumu, který může zadávací řízení neúměrně prodloužit. NÚKIB v roce 2017 publikoval podpůrný materiál k zadávání VZ pro ICT, kde jsou některá bezpečnostní opatření v rámci ZZVZ diskutována.

Celé znění Varování a související metodické podpory je k dispozici zde:

https://nukib.cz/cs/informacni-servis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/

https://nukib.cz/cs/informacni-servis/aktuality/1320-metodika-k-varovani-ze-dne-17-prosince-2018/

Vedle varování podle ZKB, kterým bylo zmíněné varování před technologiemi společností Huawei Technologies Co. Ltd. a ZTE Corporation, Úřad na svých webových stránkách pravidelně informuje veřejnost o aktuálních kybernetických hrozbách.

Cvičení kybernetické bezpečnosti: Příprava na krizové situace

Přístup whole-of-government

Označuje přístup, při kterém instituce napříč státní správou spolupracují, aby dosáhly společného cíle a jednotného řešení konkrétní otázky.

Cvičení hrají nezastupitelnou roli při zajišťování kybernetické bezpečnosti České republiky. Umožňují věrně simulovat rozličné typy krizových situací a slouží jak technickému personálu, tak pracovníkům na nejvyšší úrovni a pracovníkům s rozhodovacími pravomocemi.

Při jejich tvorbě a provedení je zásadní úzká kooperace s dalšími partnery v rámci tzv. přístupu whole-of- government. NÚKIB jako národní autorita za cvičení kybernetické bezpečnosti zodpovídá, ale na jejich přípravě spolupracuje s celou řadou partnerů. Vedle edukativního prvku pomáhají cvičení budovat důvěru a utužovat vzájemné vztahy nebo identifikovat bílá místa v procesech zajišťování kybernetické bezpečnosti.

Mezi největší přínosy cvičení patří:

1

Cvičení dávají NÚKIB **možnost zjistit a upozornit na slabá místa** či nedostatky v oblasti kybernetické bezpečnosti. Metodou krizových scénářů umožňují lépe nastínit možné negativní dopady;

2

Na základě zjištěných nedostatků a slabých míst přispívají k návrhu, implementaci a zpětnému testování konkrétních nových či pozměněných řešení. Jinými slovy cvičení představují výborný **nástroj pro ověřování i revizi politik a procesů**, například v otázkách institucionálního a zákonného rámce, krizového řízení, mediální komunikace apod.;

3

S pomocí pravidelných cvičení může NÚKIB velice dobře **mapovat přístupy** a chápání různých otázek různými institucemi stejně jako jejich úroveň zajišťování kybernetické bezpečnosti ČR;

4

Cvičení jsou neocenitelným **zdrojem výměny nových znalostí, zkušeností a technických schopností;**

5

Učiněné poznatky a získané know-how jsou sdíleny s dalšími relevantními subjekty. Cvičení tak **pomáhají identifikovat, definovat či potvrzovat konkrétní trendy v oboru.** Sdílení také dále prohlubuje vzájemnou spolupráci a důvěru;

6

Výstupy ze cvičení představují cenné poznatky, které jsou dále využívány pro **přípravu dalších osvětových a edukativních aktivit**;

7

Díky žádanosti a ohlasu ze strany zahraničních partnerů, jakými jsou například Spojené státy americké, Jižní Korea nebo Tchaj-wan, se cvičení stala **významným produktem s potenciálem pro českou zahraniční politiku.**

Cvičení kybernetické bezpečnosti v roce 2018

Počet cvičení pořádaných NÚKIB:	Počet mezinárodních cvičení, kterých se NÚKIB účastnil:	Počet účastníků cvičení provedených NÚKIB:
11	**3**	**320 ze 77 zemí**

Poznatky ze cvičení, která proběhla v roce 2018:

1.

Je nutné soustavně a pravidelně zvyšovat povědomí o kybernetické bezpečnosti mezi zaměstnanci pracujícími v oblasti národní bezpečnosti, a to včetně středního a vyššího managementu. Zde je nutné podotknout, že s problémem nízkého povědomí v oblasti kybernetické bezpečnosti se potýkají téměř všechny státy, jejichž zástupci se cvičení pořádaných NÚKIB účastnili. Netechnická table-top cvičení opakovaně ukázala, že **pracovníci klíčových institucí zabývajících se bezpečností ČR mají často nízké povědomí o povaze krizových situací v kyberprostoru a kybernetické bezpečnosti jako takové.** Právě neznalost fungování kyberprostoru, možných rizik a hlubší podstaty digitální hygieny často vede k jejímu nedůslednému dodržování. K dobrému vyhodnocení hrozeb je potřeba i kritické myšlení. Právě kritické myšlení je klíčovým aspektem rozpoznávání například phishingových útoků či defacementů, které dnes mohou být velmi sofistikované a na první pohled mohou působit věrohodně. Cvičení pravidelně odhalují nízkou odolnost cílového publika vůči manipulacím a dezinformacím, které jsou s kybernetickou bezpečností neodmyslitelně spjaty.

2.

Během cvičení se pravidelně negativně projevuje absence systému strategické komunikace (také STRATCOM) státu. Propojenost kyberprostoru a jeho aktérů vyžaduje úzkou spolupráci a koordinaci. V případě kybernetického incidentu se stává často poškozeným nejen jeden subjekt, ale hned několik. V takové situaci je koordinace nejen vlastního řešení incidentu, ale i jeho komunikace směrem k veřejnosti (a potenciálním útočníkům) zásadní. Mediální aspekt, jenž je součástí téměř všech cvičení, však není jejich účastníky vnímán jednotně. Různě je nahlíženo jak na důležitost samotné externí komunikace, tak i na otázku, kdo by měl být na národní úrovni odpovědným koordinátorem. Pokud incident dopadá na soukromé i státní instituce, je otázka jednotné komunikační linky směrem ven o to složitější. Vhodná strategická komunikace, jakožto promyšlená a koordinovaná snaha veřejného sektoru jako celku, která proaktivně podporuje stanovené priority ČR, je přitom klíčovým prvkem mitigace následků incidentu skrze včasnou a srozumitelnou komunikaci klíčových informací. V případě absence koordinace a synergie však bude obtížné takovou strategickou komunikaci realizovat a dosáhnout vytyčených priorit.

3.

Kybernetická bezpečnost je stále často vnímána jako specifická oblast, kterou by měly pokrývat k tomu výlučně určené instituce. Pro zajišťování bezpečnosti ČR je nezbytné oprostit se od vnímání kybernetické bezpečnosti skrze čistě technickou dimenzi a tudíž problematiku, se kterou se mohou vypořádat pouze techničtí pracovníci či specializované instituce. Vzdělaný a zainteresovaný management napříč státní správou je nezbytný pro efektivní zajišťování kybernetické bezpečnosti a krizových situací s ní spojených.

Osvěta a vzdělání v ČR: Běh na dlouhou, ale nezbytnou trať

Obecně platí, že jsou to právě uživatelé, kteří svou neznalostí či neopatrností usnadňují práci útočníkům. Budování návyků pro bezpečné využívání digitálních technologií je jednou ze základních kompetencí digitální gramotnosti a zaslouží si patřičnou pozornost. Prostřednictvím důsledné osvěty a vzdělávání je možné vzniku těchto nežádoucích situací a jevů předcházet. Osvětové aktivity jsou v České republice poměrně pestré a zaměřují se na nejčastěji ohrožené skupiny populace, jimiž jsou především děti a senioři.

Mezi celorepublikové osvětové činnosti a vzdělávací aktivity z oblasti kybernetické bezpečnosti, které se uskutečnily v roce 2018, patří:

Projekt **E-bezpečí:**

V jeho rámci se v roce 2018 uskutečnilo 404 akcí. Pod záštitou tohoto projektu vedeného Univerzitou Palackého bylo proškoleno 8 362 dětí, 579 rodičů, 983 učitelů, 656 různých specialistů a 73 seniorů. On-line poradna projektu řešila 334 případů. [xxiii] Byly zde také realizovány dva celonárodní výzkumy a byla vydána odborná monografie. Tento projekt se stal vítězem národního kola Evropské ceny prevence kriminality;

Safer Internet Day:

Uskutečnil se 6. února 2018 a v jeho rámci se v Praze konala tisková konference Národního centra bezpečnějšího internetu. Propagace bezpečí se zúčastnila řada subjektů, mimo jiné se připojil i portál E-bezpečí a množství obcí a škol;

Say No!:

Mezinárodní kampaň Europolu proti zneužívání dětí on-line, která se uskutečnila na Zlínském mezinárodním filmovém festivalu pro děti a mládež. Kampaň je v ČR propagována prostřednictvím Policie České republiky – Národní centrály proti organizovanému zločinu.

Velmi důležitou proměnou v kybernetické bezpečnosti ČR je vzdělání. NÚKIB se proto angažuje v pracovních skupinách, které připravují revize rámcových vzdělávacích programů. Úřad usiloval především o významnější začlenění problematiky kybernetické bezpečnosti do školní výuky. Toto úsilí přineslo nezanedbatelné výsledky a kybernetická bezpečnost proniká do výuky jako nedílná složka digitální gramotnosti. [xxiv] Snaha prosazovat výuku kybernetické bezpečnosti na školách zatím převážně naráží na otázky, zda se jedná o informatické nebo průřezové téma a zda je výuka kybernetické bezpečnosti věcí pedagogů nebo rodičů. Školy namísto začlenění kybernetické bezpečnosti do výuky volí přednášky či besedy externích organizací (Policie ČR, neziskových organizací, NÚKIB a dalších) s ospravedlněním, že se v daném tématu necítí sebejistě nebo že jim chybí potřebné znalosti. Dále též zmiňují pocit, že v tomto ohledu nemají žákům co předat, neboť žáci se na internetu pohybují mnohem více než vyučující.

Podobná situace panuje i v oblasti mediální výchovy, jejímž smyslem je budovat u žáků schopnost odolávat dezinformacím a dalším podobným jevům. Rovněž schopnost pracovat s informacemi chápe NÚKIB jako důležitou kompetenci pro život v informační společnosti, která nepřímo

přispívá k budování bezpečnějšího kyberprostoru ze strany běžných uživatelů. Proto za zmínku stojí i průzkum „Stav výuky mediální výchovy na středních školách“, [xxv] ze kterého vyplývá například to, že podle 77 % dotazovaných vyučujících se jedná o důležitou oblast vzdělávání, ale i zde panuje obecná nejistota a neshoda v otázkách, jakým způsobem k výuce přistupovat a kdo by tato témata měl vyučovat.

Na základě výše zmíněných důvodů vytvořil NÚKIB rozcestníky pro učitele základních [xxvi] i středních škol[xxvii] , které mají za úkol pomoci učitelům orientovat se v této problematice a poskytnout jim oporu a metodické vedení. Česká pobočka AFCEA pak pořádá Středoškolské soutěže kybernetické bezpečnosti.

Zajímavé poznatky přinesla výzkumná zpráva s názvem Rodič a rodičovství v digitální éře, publikovaná Univerzitou Palackého v Olomouci a O2 Czech Republic v roce 2018. Zpráva připomíná, že nejen školy, ale také **rodiče hrají významnou roli ve výchově k bezpečnému používání digitálních technologií.** Pozitivním zjištěním je, že se více než polovina dotazovaných rodičů se svými dětmi baví o navazování vztahů na internetových seznamkách a celých 80 % rodičů zapojených do tohoto průzkumu diskutuje se svými dětmi o bezpečnosti internetové komunikace obecně. [xxviii] Nutnost podpory rodičů reflektuje také NÚKIB, který v loňském roce připravil i rozcestník pro rodiče [xxix] – materiál, který má za úkol usnadnit výchovu dětí v infomační společnosti.

V případě starší generace, tedy seniorů, stav kybernetické gramotnosti poodhaluje rozsáhlý průzkum **„Starci na netu“**, [xxx] na kterém se společně podílely Seznam.cz a Univerzita Palackého v Olomouci. Tento výzkum byl orientován na různé věkové skupiny seniorů a zabýval se jejich kybernetickou gramotností – například tím, nakolik jsou jejich hesla bezpečná. Jedním ze zjištění tohoto výzkumu bylo, že hesla více než 50 % dotazovaných nad 55 let nesplňují obecná doporučení a není možné na ně nahlížet jako na bezpečná. I pro tuto cílovou skupinu připravil NÚKIB patřičný rozcestník, [xxxi] který reflektuje některá výzkumná zjištění, slouží seniorům jako materiál pro sebevzdělávání a poskytuje rady, tipy i doporučení pro bezpečnější pohyb na internetu.

Vzdělávání osob pracujících pro **státní a veřejnou správu** je prioritou, neboť právě tyto osoby přicházejí při výkonu své profese do kontaktu s řadou citlivých údajů, s nimiž dále pracují. Nezbytným předpokladem pro bezpečné fungování státu je osvojení správného používání digitálních technologií a práce s daty. NÚKIB proto spustil dva **on-line kurzy pro veřejnou správu.**

První kurz

První z nich přibližuje této cílové skupině základní vhled do problematiky kybernetické bezpečnosti. Tímto kurzem dosud prošlo úspěšně **21 443 úředníků státní správy**. Z tohoto počtu bylo 7 493 úředníků pod zákoníkem práce a 13 950 úředníků pod služebním zákonem;

Druhý kurz

Druhý on-line kurz reflektuje zákon o kybernetické bezpečnosti. Je určen pro osoby pověřené výkonem některé z bezpečnostních rolí podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Tímto kurzem prošlo **111 úředníků**, z toho 57 pod zákoníkem práce a 54 pod služebním zákonem.

Síťové sondy v klíčových orgánech státu: Včasné varování před kybernetickými útoky

Kybernetické útoky jsou málokdy izolovaným incidentem. Útoky jednoho aktéra často cílí na více institucí zároveň. Aby Česká republika měla lepší povědomí o škodlivých aktivitách ve strategických sítích státu, realizoval NÚKIB projekt s názvem **„Systém detekce kybernetických bezpečnostních událostí ve vybraných ISVS“**[12]. Jeho cílem je pomocí rozmístění síťových sond usnadnit administrátorům těchto klíčových státních sítí nalezení případného útočníka a lépe tyto sítě chránit.[13]

Síťové sondy pomohou upozornit na podezřelá datová spojení, anomální objemy dat opouštějící konkrétní síť, rozpoznají „oťukávání“ sítě zvnějšku a budou sloužit i jako nástroj včasného varování před blížícími se útoky. Sondy mají také schopnost získávat a uchovávat popisná data o provozu a vytvořit tak auditní stopu pro pozdější zkoumání toho, k čemu na daném ministerstvu nebo úřadu došlo. Díky sdílení dat s partnery bude NÚKIB schopen dohledat i bezpečnostní incidenty, které by v rámci jednoho rezortu nebyly detekovány, případně by nebyly vyhodnoceny jako nebezpečné, a informovat o nich další organizace ještě před jejich případným zasažením.

Na konci roku 2018 byly síťové sondy nasazeny u 20 partnerů z řad státní správy. Místní správci byli patřičně proškoleni a začali s GovCERT sdílet kybernetické bezpečnostní události a vybraná data o síťovém provozu procházejícím přes perimetr sítě. GovCERT přijatá data ukládá a dále analyzuje. V současné době se pracuje na doladění systému a jeho napojení na interní databáze a aktualizační server pro publikování aktualizovaných seznamů hrozeb zpět do zařízení zapojených partnerů.

Do budoucna se bude projekt dále rozšiřovat o další subjekty disponující vlastními prostředky sledování síťového provozu. Čím více subjektů bude do projektu zapojeno, tím přesněji bude možné vykreslit obrázek škodlivých aktivit v českých institucích a tím včasnější bude varování proti nim.

[12] *Informační Systémy Veřejné Správy*
[13] *Projekt nesouvisí s plány rozmisťování sond v sítích elektronických komunikací ze strany Vojenského zpravodajství.*

Ochrana volebního procesu: České poznatky rezonují i v zahraničí

Ve světle zahraničních útoků začala Česká republika osm měsíců před parlamentními volbami v roce 2017 přezkoumávat kybernetickou odolnost svého volebního procesu. Byla ustanovena Pracovní skupina Ministerstva vnitra na ochranu voleb a Český statistický úřad započal úzkou spolupráci s NÚKIB. Výsledkem byla řada opatření od mapování volebního procesu a analyzování jeho slabých míst přes penetrační testování infrastruktury až po cvičení kybernetické bezpečnosti. Z celého procesu vzešlo několik doporučení, které ČSÚ implementoval. Kybernetické zabezpečení voleb ovšem není absolutní a na jeho navyšování je třeba pracovat neustále.

2017

01

02 **Únor 2017**

Ustanovení Pracovní skupiny Ministerstva vnitra na ochranu voleb a začátek bližší bilaterální spolupráce mezi NÚKIB a ČSÚ

03 **Březen 2017**

Začátek tříměsíčního mapování volebního procesu. Zkoumán byl celý řetězec zpracování výsledků voleb a na základě jeho analýzy byla identifikována potenciální slabá místa

04

05 **Květen 2017**

Penetrační testování infrastruktury používané ve volebním procesu

06 **Červen 2017**

Cvičení kybernetické bezpečnosti pořádané pro ČSÚ, které bylo postavené na případech napadení voleb v zahraničí

07 **Červenec–září 2017**

Vyhotovení doporučení pro navýšení kybernetické bezpečnosti volebního procesu

08

09

10 **Říjen 2017** (parlamentní volby):

DDoS na weby volby.cz a volbyhned.cz

2018

01 **Leden 2018**

Cvičení kybernetické bezpečnosti zaměřené na interaktivní rozehrávání krizových scénářů

02

03

04 **Duben 2018**

Setkání technických expertů ČSÚ a NÚKIB, na kterém byla vyhodnocena doposud přijatá opatření a další postup

05

Díky svým zkušenostem se zabezpečením volebního procesu vedla Česká republika spolu s Estonskem přípravu doporučení pro zabezpečení voleb do Evropského parlamentu. Výsledkem je volně dostupný dokument „Compendium on Cyber Security of Election Technology“, na jehož tvorbě se podílelo přes 20 členských států EU stejně jako Evropská komise, Evropská agentura pro bezpečnost sítí a informací (ENISA) a zástupci Evropského parlamentu.

Dokument Compendium on Cyber Security of Election Technology je k dispozici zde:

https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2624-doporuceni-k-zajisteni-kyberneticke-bezpecnosti-volebnich-procesu/

Doporučení, která z dokumentu vzešla, se dotkla řady důležitých oblastí pro bezpečné elektronické zpracování a vyhlášení volebních výsledků. Věnovala se například:

A

Významu dostatečně robustních anti-DDoS řešení, šifrování, dohledu nad sítí zpracovávající výsledky v reálném čase za pomocí nástrojů typu SIEM, významu segmentace sítě, zálohování a dalších technických opatření;

B

Problematice penetračního testování volebních systémů od tradičních přístupů ČR nebo Nizozemska až po Estonsko, které již několik let kompletně zveřejňuje zdrojový kód i dokumentaci svého volebního softwaru;

C

Fungování volebních bezpečnostních týmů IT tvořených organizací sčítající hlasy, úřadem zodpovědným za kybernetickou bezpečnost, případně i relevantními ministerstvy a tajnými službami;

D

Bezpečnému vývoji softwaru včetně bezpečnosti dodavatelského řetězce;

E

Hodnocení rizik a krizový management;

F

A dalším.

Jedním z doporučení byla i potřeba do školení o bezpečnosti voleb zahrnout politické strany a jejich představitele. Útoky ve Spojených státech (DNC Hack) a Francii (#MacronLeaks) jasně ukázaly, že kybernetické útoky jdou často ruku v ruce s **dezinformační kampaní**, která se snaží některého z kandidátů zdiskreditovat a ovlivnit tak výsledky voleb. Proto by nejvyšší političtí představitelé měli dbát na metody bezpečné komunikace, a to jak v osobním, tak pracovním životě.

Projekt FENIX: Společná ochrana proti DoS a DDoS

S tím, jak narůstá síla DDoS útoků, narůstají také nároky na ochranu proti nim. Česká republika si toho začala být plně vědoma v březnu roku 2013, kdy země byla vystavena čtyřdenní vlně DoS útoků, která ovlivnila média, banky i operátory a způsobila nedostupnost jejich webových stránek. Rozsahem a počtem cílů to byla do té doby největší kybernetická kampaň, které Česká republika čelila.

V reakci na tyto útoky vznikl **projekt FENIX**. Zaštiťuje ho sdružení NIX.CZ, které sdružuje poskytovatele internetového připojení a internetového obsahu, aby mohli vzájemně propojit své sítě a jejich zákazníci tak mohli rychle komunikovat.

Smyslem celého projektu je v případě DoS a DDoS útoků zajistit dostupnost internetových služeb u subjektů, které jsou do projektu zapojeny. Projekt FENIX provozuje redundantní přípojky a v případě přetížení jednoho uzlu je jeho provoz automaticky přesměrován na ostatní přípojky a dostupnost je tak zachována. Vedle toho projekt zahrnuje i další bezpečnostní opatření, mezi něž patří například:

Monitoring neobvykle vytížených přípojek členů projektu

Detekce a likvidace tzv. amplification útoků (viz například Memecached na straně 22);

Provoz dohledového střediska, které reaguje do 30 minut

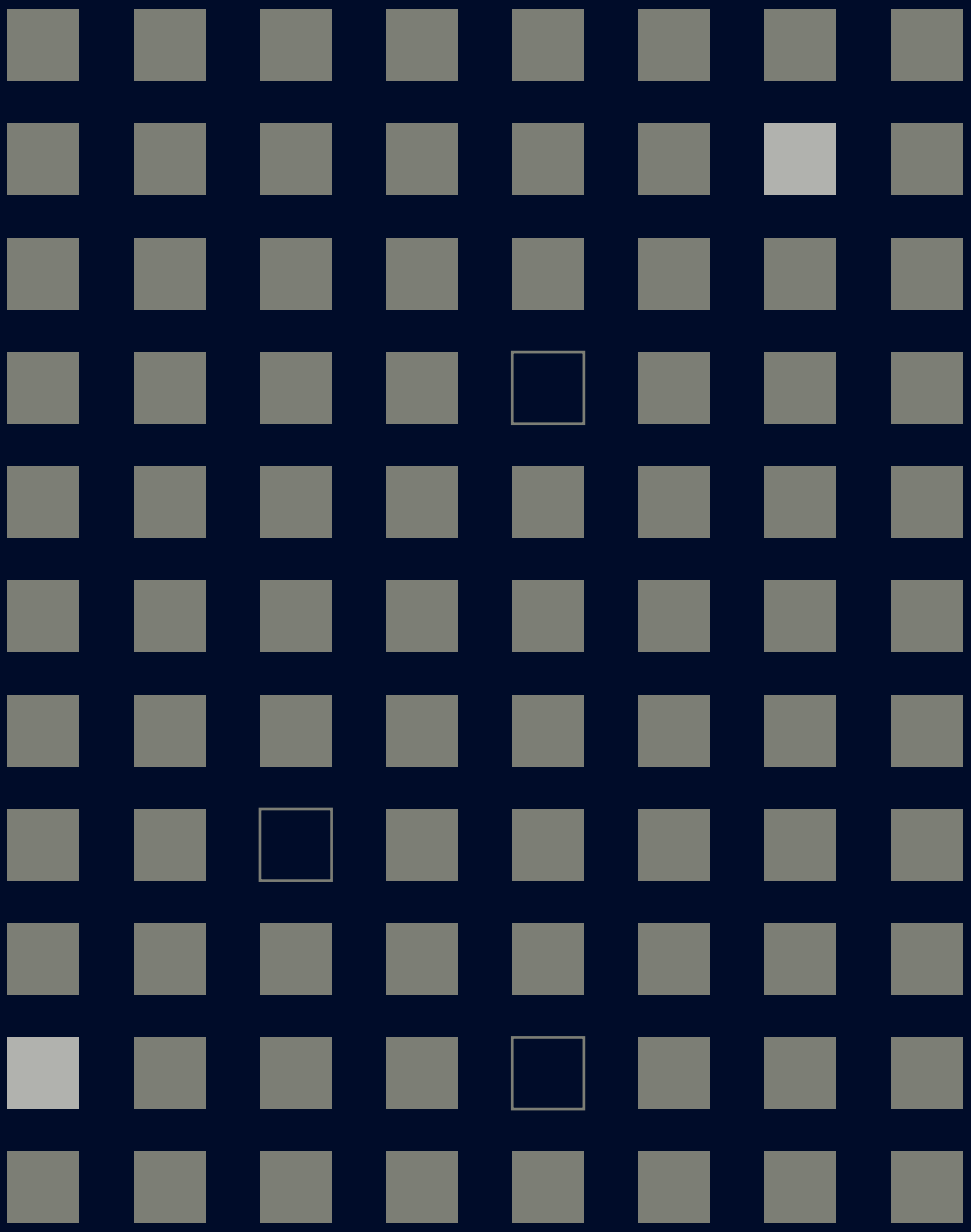
Platforma pro nouzovou komunikaci;

Smluvní zákaz spamů a útoků na zákazníky všech členů projektu

Zabránění podvrhování IP adres ve své části sítě (například pomocí BCP-38).

Členy projektu FENIX jsou společnosti, které poskytují připojení významným službám a potřebují zabezpečit svůj provoz i v těch nejkritičtějších situacích. Jsou v něm tak zastoupeni i největší čeští poskytovatelé internetového připojení.

Výhled na rok 2019



Hrozby

Kybernetická špionáž

Zájem cizích států o Českou republiku v následujícím roce velmi pravděpodobně neustane. Aktivity státních aktérů související s ČR se v kyberprostoru ponesou ve znamení zesílené potřeby získávat strategické informace o působení ČR v EU a NATO, bilaterální komunikaci ČR se spojenci a o oblast bilaterálních vztahů. Nelze vyloučit ani útoky s cílem odcizit obchodní tajemství či duševní vlastnictví českých firem a výzkumných institucí, zejména v oblasti vývoje a výzkumu nové generace polovodičů, telekomunikačních technologií, využití satelitních technologií, zpracování „big data“, umělé inteligence nebo deep learning.

DDoS

DDoS útoky budou pravděpodobně stále nabývat na síle. Počet nezabezpečených IoT zařízení se každým rokem navyšuje a tím se navyšuje i počet zařízení, která je možné napojit do botnetů. Útočníci budou pokračovat v hledání nových vektorů útoků a nových způsobů pro navýšení jejich efektivity. I přes to, že organizace jsou si hrozby DDoS útoků vědomy a neustále svou odolnost proti nim navyšují, není pravděpodobné, že útočníky zcela odradí.

Úniky dat

Jelikož databáze s osobními údaji nabízí mnoho možností pro jejich další zneužití, je pravděpodobné, že úniků bude nadále přibývat. Budou se objevovat jak nově uniklé databáze, tak již dříve zcizené osobní údaje recyklované v nově zveřejněných kompilátech. To se velmi pravděpodobně, stejně jako tomu bylo v uplynulých letech, nevyhne ani České republice.

Volby

Hrozba kybernetických útoků na volby bude pravděpodobně provázet i rok 2019. Na jaře čekají členské státy volby do Evropského parlamentu a bude na každém z nich, aby se na ně co nejlépe připravil. Pokud by následkem kybernetického útoku došlo ke zpochybnění výsledků byť v jedné zemi, nebylo by možné jejím zástupcům přiřadit křesla a celý volební proces by byl kompromitován. Schopnost Evropského parlamentu se scházet by byla narušena, čímž by bylo ovlivněno fungování celé Evropské unie. Pro státy, které se dlouhodobě snaží zasít nedůvěru v západní instituce, tak nadcházející evropské volby mohou představovat lákavý cíl.

Dodavatelé

Hrozba útoků skrze slabá místa v dodavatelském řetězci je v posledních letech na vzestupu a tento trend bude pokračovat i v roce 2019. Rovněž nelze vyloučit odhalení starších kampaní a následné přiřazení zodpovědnosti konkrétním skupinám aktérů včetně těch, které pracují pro různé státy. Trendem bude i snaha aktualizovat existující regulace, aby došlo ke snížení rizika kompromitace skrze dodavatelský řetězec.

Kryptomining

Vzhledem k větší účinnosti oproti jiným typům útoků a nižším rizikům na straně útočníka je velmi pravděpodobné, že útoky využívající kryptominery budou pokračovat i v roce 2019. Využívány pravděpodobně budou zejména existující sítě napadených počítačů (botnety).

Umělá inteligence a sítě 5G

Multiplikátorem schopností útočníků i obránců bude především výzkum a vývoj umělé inteligence a rozšíření sítí 5G. Zatímco umělá inteligence umožní aktérům automatizovat velkou řadu složitých úkonů, sítě páté generace budou představovat pro útočníky i obránce prostředek k masivnějším útokům i obranným kapacitám.

Cíle

Veřejný sektor:

Útoky na veřejný sektor ze strany cizích států a jimi podporovaných skupin budou velmi pravděpodobně pokračovat stejně jako snahy těchto aktérů působit v sítích veřejného sektoru nepozorovaně po co nejdelší dobu. Nicméně odolnost proti takovým útokům bude pravděpodobně i nadále negativně ovlivněna nedostatkem odborníků spojeným s nekonkurenceschopností veřejného sektoru v oblasti finančního ohodnocení.

Uživatelé:

Koncoví uživatelé velmi pravděpodobně zůstanou primárním vstupním bodem útočníků do sítí svých obětí. S přihlédnutím k trendům v zahraničí lze očekávat větší množství phishingových e-mailů, jejichž cílem bude získání přístupu do online rozhraní služby Office 365 (Microsoft) nebo G Suite (Google). Útočníci budou velmi pravděpodobně využívat falešné stránky připomínající legitimní přihlašovací rozhraní k získání přihlašovacích údajů. V zahraničí se také postupně rozšiřuje podíl phishingových zpráv poslaných skrze sociální sítě (Facebook Messenger nebo Instagram). Je proto pravděpodobné, že se s tímto trendem setkají i čeští uživatelé.

Energetický sektor:

Energetický sektor bude pravděpodobně v příštím roce vystaven větším kybernetickým hrozbám. Počet a sofistikovanost útoků budou dále narůstat, s nasazováním IoT zařízení se rozšíří prostor pro možné průniky do průmyslových řídicích systémů. Pokusy o útok skrze třetí strany, jejichž sítě nemusí být tak dobře zabezpečeny jako sítě distribučních společností a elektráren, budou na vzestupu.

eHealth:

Vzhledem k citlivosti dat a jejich atraktivitě zůstane pro útočníky oblast eHealth mimořádně zajímavou i v roce 2019. Je pravděpodobné, že vzhledem k celkově klesajícímu počtu ransomwarových útoků ve světě, dojde k poklesu i v oblasti eHealth. Na druhou stranu je možné předpokládat nárůst sofistikovaných, obtížně zjistitelných útoků na důvěrnost dat za využití stále sofistikovanějších technik zejména spear-phishingu.

Bankovní sektor:

V roce 2019 budou velmi pravděpodobně pokračovat útoky na uživatele elektronického bankovnictví, a to především ve formě útoků na neobezřetné uživatele mobilních telefonů.

Akademický svět:

Phishingové kampaně proti českým univerzitám z roku 2018 vykazují znepokojující trend – jejich počet i důmyslnost v minulém roce výrazně vzrostly. Je pravděpodobné, že je to teprve začátek a že v příštím roce český akademický sektor zůstane v hledáčku kybernetických aktérů a pokusy o krádež duševního vlastnictví budou pokračovat.

Přílohy

05

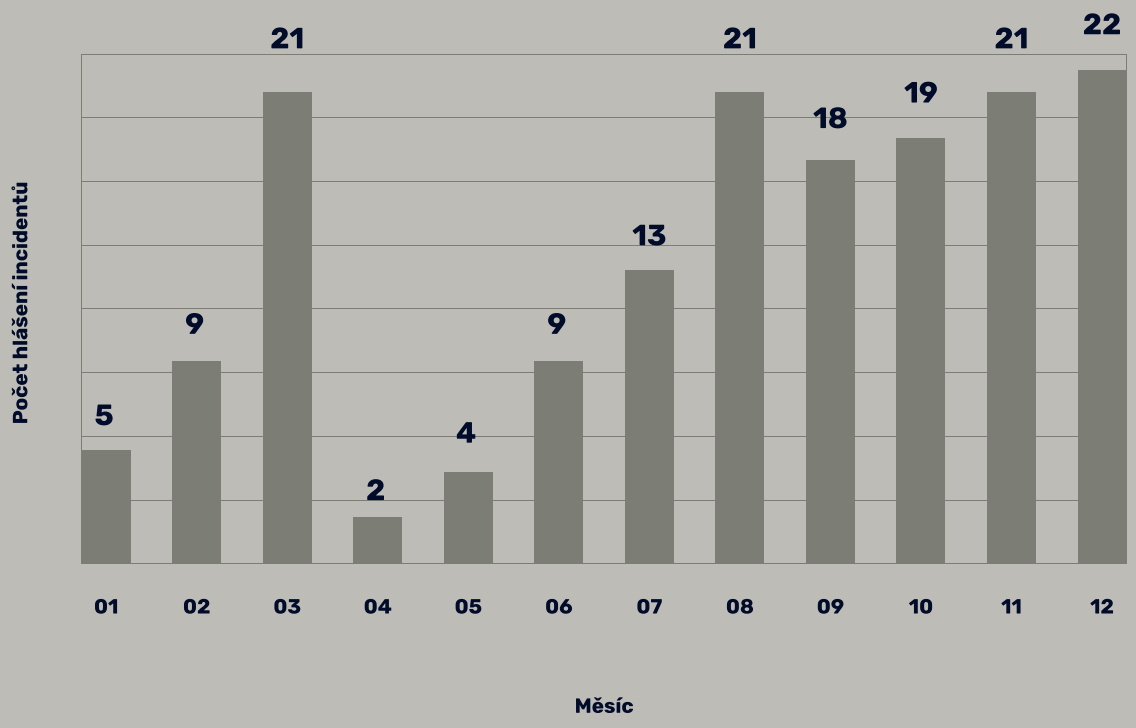
Příloha 1: Statistické údaje o incidentech řešených na GovCERT.CZ

V průběhu roku 2018 obdrželi pracovníci GovCERT.CZ od českých i zahraničních partnerů v souhrnu 164 relevantních hlášení o kybernetických bezpečnostních incidentech. Tato hlášení byla dále vyhodnocována ve vztahu k oblasti působnosti týmu GovCERT.cz a následně zpracována buď vlastními prostředky, nebo předána příslušným subjektům. Za uplynulý rok tak bylo z přijatých hlášení a z informací získaných vlastními prostředky vyhodnoceno, zpracováno a vyřešeno 54 kybernetických bezpečnostních incidentů spadajících do oblasti působnosti vládního CERT, tedy KII, VIS a veřejné správy.

Graf 1:

Počet příchozích hlášení na GovCERT.CZ o incidentech za jednotlivé měsíce v roce 2018

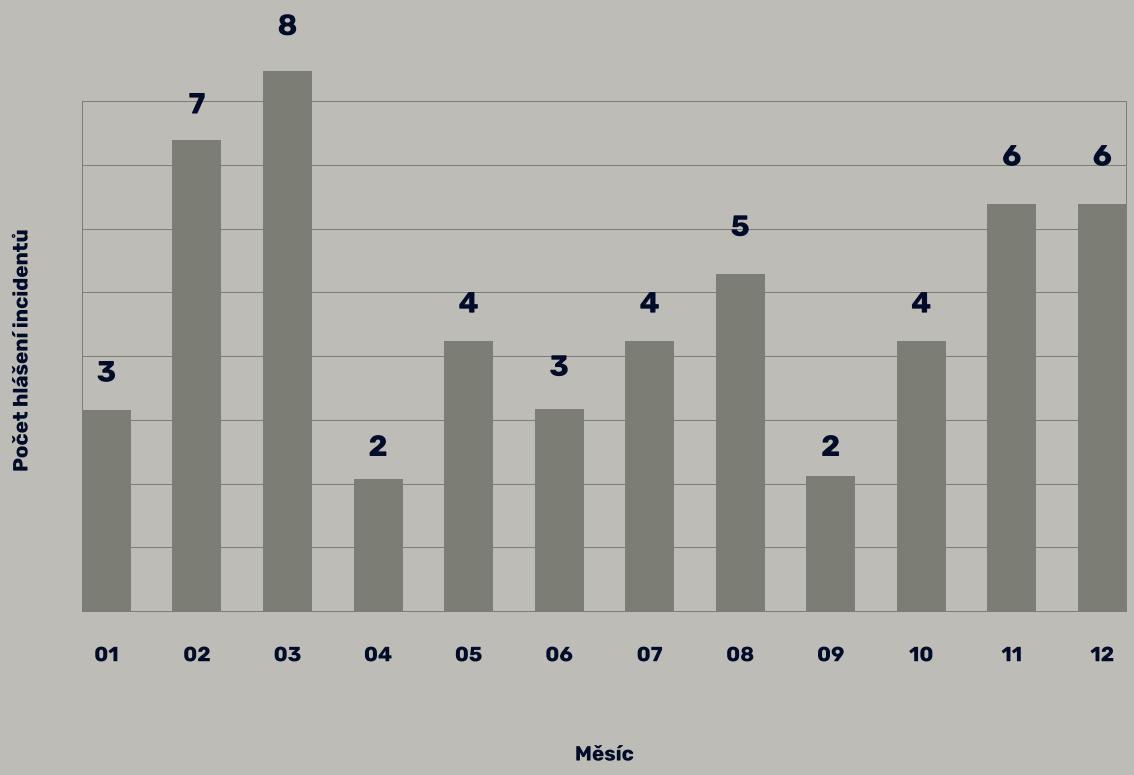
Graf 1:



Graf 2:

Počet řešených incidentů v GovCERT.CZ
za jednotlivé měsíce v roce 2018

Graf 2:

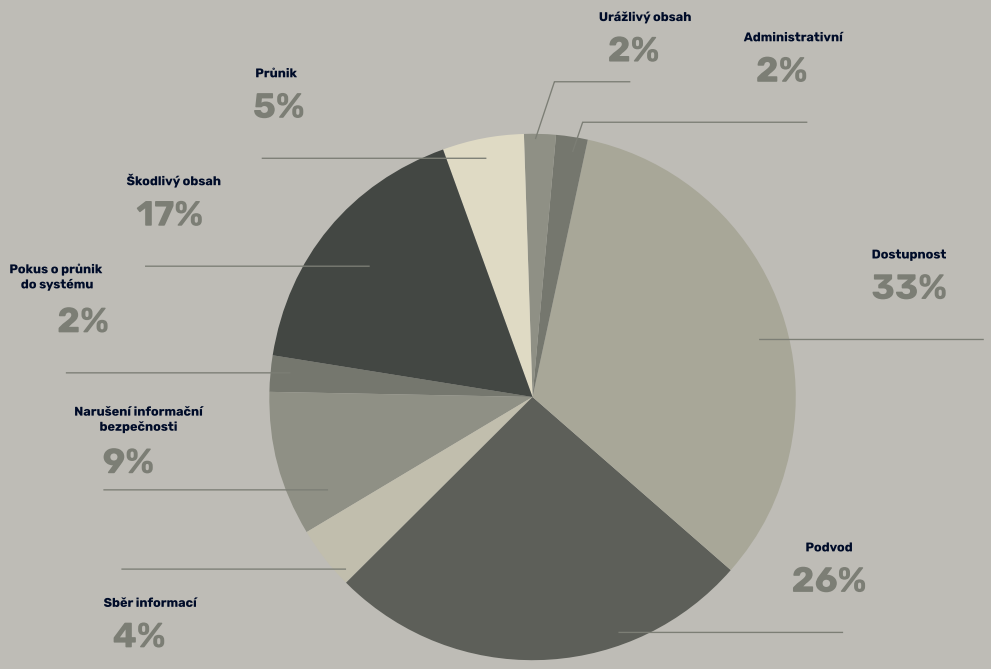


Graf 3:

klasifikace řešených incidentů v roce 2018

Graf 3:

Klasifikace incidentů za rok 2018



Popis kategorií vychází z formuláře pro hlášení incidentů:

Urážlivý obsah

(například spam, kyberšikana, nevhodný obsah)

Administrativní

(bezpečnostní incident způsobený administrativní chybou)

Škodlivý obsah

(například virus, červ, trojský kůň, dialer, spyware)

Sběr informací

(například skenování, sniffing, sociální inženýrství)

Pokus o průnik do systému

(například pokus o zneužití zranitelnosti, kompromitace aktiva, „0-day“ útok)

Průnik

(například úspěšná kompromitace aplikace nebo uživatelského účtu)

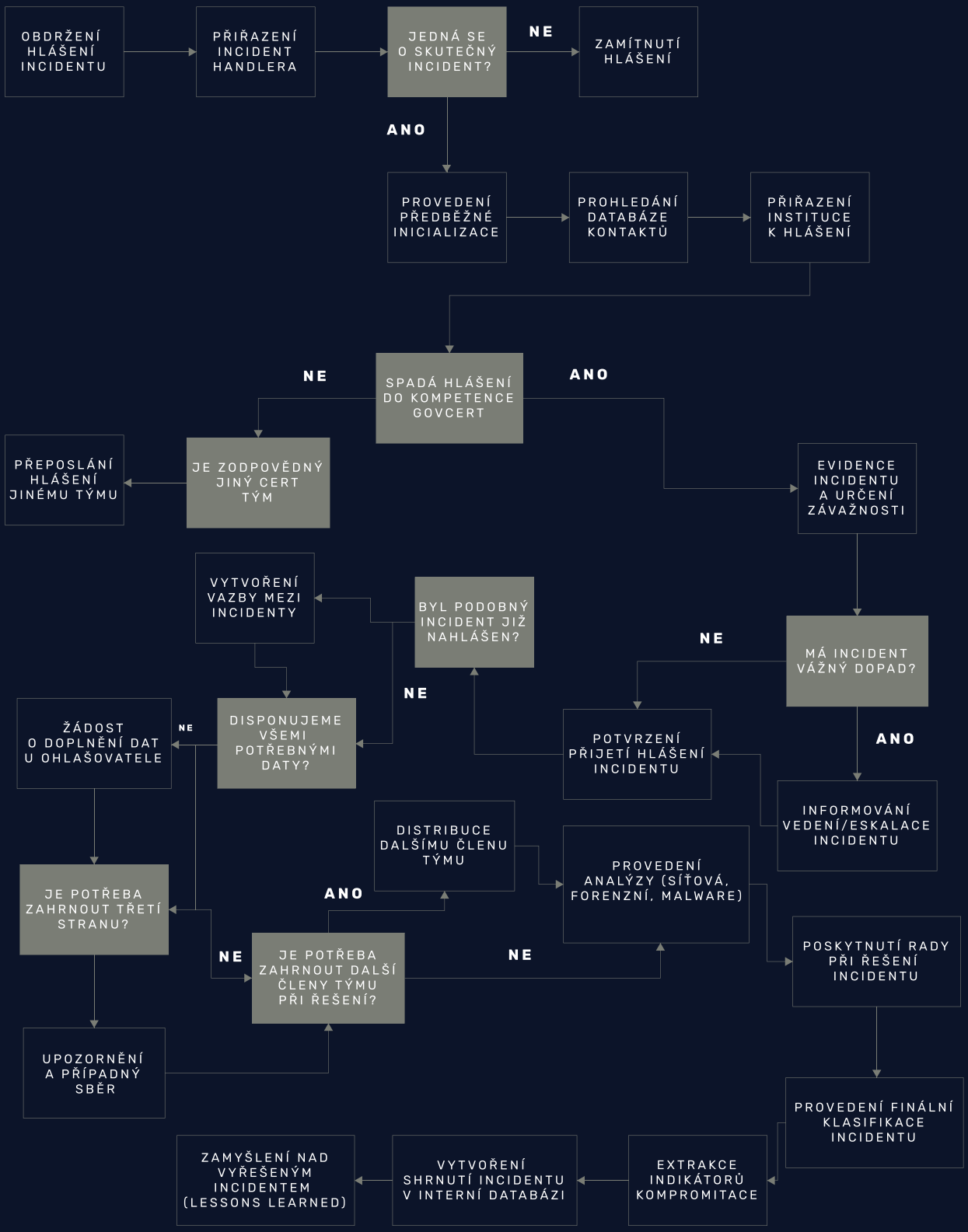
Dostupnost

(například narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)

Podvod

Narušení informační bezpečnosti

Příloha 2: Jak se řeší incident v GovCERT.CZ?



Příloha 3: Povinné subjekty dle zákona o kybernetické bezpečnost

Mezi subjekty, které jsou povinny se řídit zákonem o kybernetické bezpečnosti, patří následující:

a) Kritická informační infrastruktura

Ochrana kritické infrastruktury v kybernetickém prostoru (tzv. kritická informační infrastruktura) je v České republice na úrovni legislativy zajištěna souběhem krizového zákona a zákona o kybernetické bezpečnosti. Zákon o kybernetické bezpečnosti označil prvek nebo systém prvků v této oblasti jako tzv. kritickou informační infrastrukturu. Tím došlo k posunu od fyzických objektů k informačním a komunikačním systémům. Způsob zajištění těchto informačních a komunikačních systémů je dán komplexním systémem řízení bezpečnosti informací. Zavedení tohoto systému je ústřední povinností, kterou zákon o kybernetické bezpečnosti klade na povinné subjekty. Dalšími povinnostmi jsou například hlášení kontaktních údajů, hlášení kybernetických bezpečnostních incidentů nebo povinnost provádět opatření, která může NÚKIB vydat.

Povinné osoby:	Postup určení:	Prováděcí právní předpisy:
Správce a provozovatel informačního systému kritické informační infrastruktury Správce a provozovatel komunikačního systému kritické informační infrastruktury	Prvky kritické informační infrastruktury NÚKIB určí vydáním opatření obecné povahy nebo jsou pro organizační složky státu určeny usnesením vlády (NÚKIB zasílá Ministerstvu vnitra návrh těchto prvků)	Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

b) Základní služba

Institut základní služby a jejího provozovatele byl do zákona o kybernetické bezpečnosti zaveden na základě požadavků evropské legislativy. Od subjektů kritické informační infrastruktury se provozovatelé základní služby liší především tím, že v jejich případě jde výhradně o zabezpečení společenských nebo ekonomických činností, které tyto subjekty provozují. To vyplývá ze samotné definice základní služby, kdy se takovou rozumí služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít dopad na zabezpečení společenských nebo

ekonomických činností v některém ze zákonem uvedených odvětví. Tato odvětví se s odvětvími kritické informační infrastruktury překrývají v několika případech. Těmito odvětvími jsou energetika, doprava, bankovnictví, infrastrukturaké bezpečnosti klade na povinné subjekty. Dalšími povinnostmi jsou například hlášení kontaktních údajů, hlášení kybernetických bezpečnostních incidentů nebo povinnost provádět opatření, která může NÚKIB vydat. finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura a chemický průmysl. Způsob zajištění ochrany takových systémů je pak shodný s kritickou informační infrastrukturou.

Povinné osoby:	Postup určení:	Prováděcí právní předpisy:
Správce a provozovatel informačního systému základní služby Provozovatel základní služby	NÚKIB určí provozovatele základní služby a informační systém základní služby vydáním rozhodnutí	Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

c) Významný informační systém

Z definice je významným informačním systémem takový informační systém, který je spravován orgánem veřejné moci a zároveň by u něj narušení bezpečnosti informací mohlo omezit nebo výrazně ohrozit výkon působnosti tohoto orgánu. Jde tedy o skupinu, která se výhradně skládá z takových subjektů, jakými jsou ministerstva a také vyšší územní samosprávné celky nebo školy, zdravotní pojišťovny, profesní komory a podobně. Na rozdíl od systémů kritické informační infrastruktury nebo základní služby nejsou tyto v rámci významných informačních systémů určovány NÚKIB, ale je povinností každého orgánu veřejné moci posoudit naplnění daných kritérií a identifikované významné informační systémy nahlásit.

Povinné osoby:	Postup určení:	Prováděcí právní předpisy:
Správce a provozovatel významného informačního systému	Orgán veřejné moci sám posoudí naplnění kritérií dle vyhlášky č. 317/2014 Sb. a nahlásí se jako povinná osoba NÚKIB. Druhou možností je, že je informační systém zahrnut do přílohy č. 1 vyhlášky č. 317/2014 Sb.	Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

d) Poskytovatel digitální služby

Digitální službou je služba informační společnosti dle zákona č. 480/2004 Sb., o některých službách informační společnosti, která spočívá v provozování on-line tržiště, internetového vyhledávače nebo cloud computingu. Poskytovatelem digitální služby však není malý podnik nebo tzv. mikropodnik dle doporučení komise č. 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků.

Povinné osoby:	Postup určení:	Prováděcí právní předpisy:
Poskytovatel digitální služby	Subjekt sám posoudí naplnění zákonné definice a nahlásí se jako povinná osoba provozovateli národního CERT	Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018

Příloha 4: Hlášení o stavu naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020

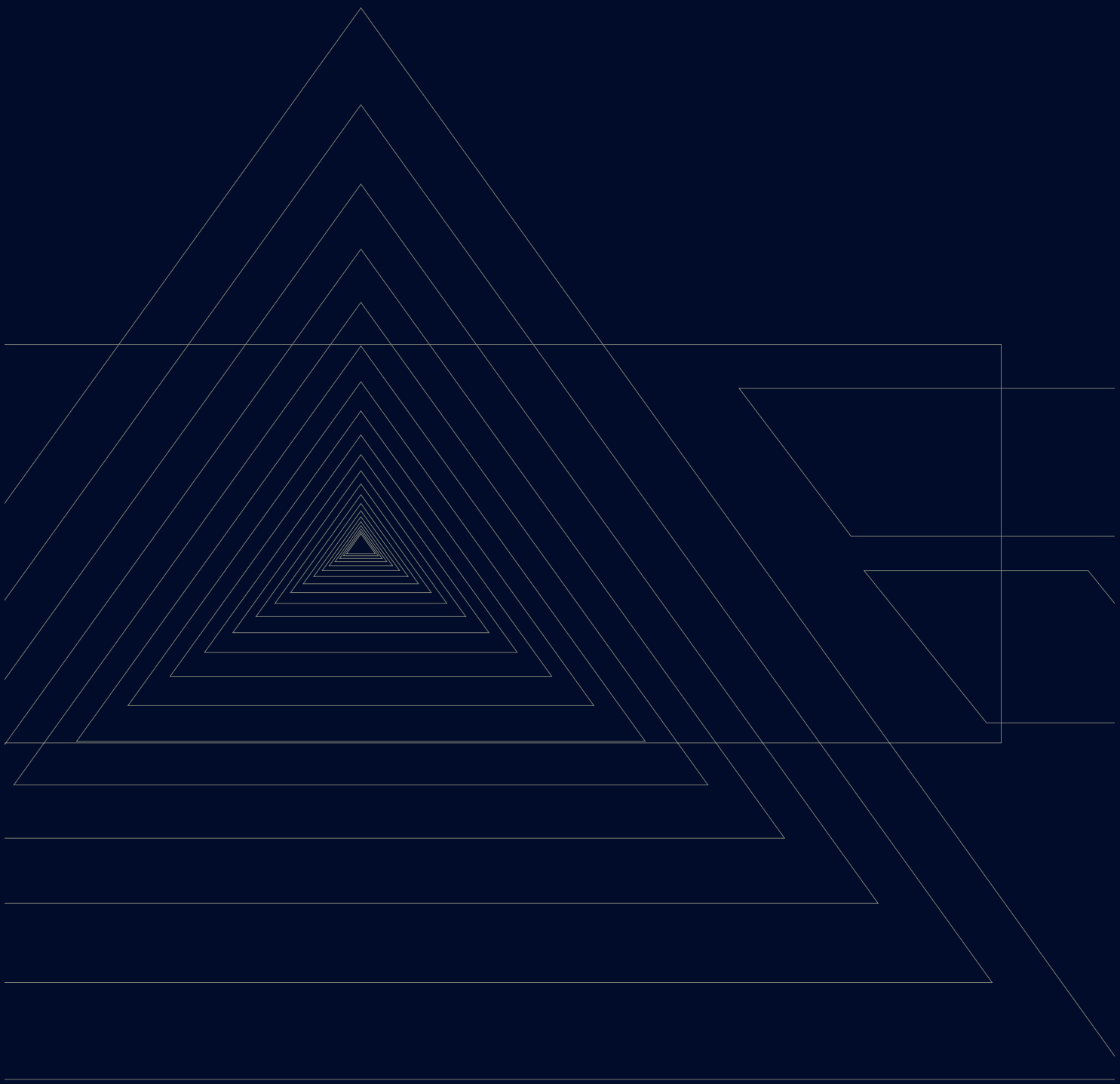
Toto hlášení je umístěno jako příloha v samostatném dokumentu.

Hlášení reflektuje stav naplňování úkolů Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 s termínem do roku 2019 a úkolů, které mají být plněny průběžně. Hlášení bude k dispozici na webových stránkách NÚKIB.

Pravděpodobnostní výrazy použité ve Zprávě o stavu kybernetické bezpečnosti za rok 2018

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot.

Výraz	Pravděpodobnost
Téměř jistě	90–100%
Velmi pravděpodobně	75–85%
Pravděpodobně	55–70%
Nelze vyloučit/Reálná možnost	25–50%
Nepravděpodobně	15–20%
Velmi nepravděpodobně	0–10%



06 Odkazy

i Pačka, Roman. 2015. Role státu v zajišťování kybernetické bezpečnosti. Bezpečnostní teorie a praxe, č. 3. str. 93–110.

ii Policie ČR. 2018. Kyberkriminalita. https://www.policie.cz/clanek/kyberkriminalita.aspx

iii Sanger, David. 2018. Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran. NY Times. https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html?smtyp=cur&smid=tw-nytimes

iv Avast. 2018. Top 10Biggest Data Breaches in 2018. https://blog.avast.com/biggest-data-breaches

v Bing, Chrisopher. 2018. Clues in Marriott hack implicate China – sources. Reuters. https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D

vi Hunt, Troy. 2018. Data Provided by the Estonian Central Criminal Police is Now Searchable on Have I Been Pwned. https://www.troyhunt.com/data-provided-by-the-estonian-central-criminal-police-is-now-searchable-on-have-i-been-pwned/

vii iRozhlas. 2018. Loňský útok hackerů při parlamentních volbách? Odloženo. Policie pachatele nevypátrala. https://www.irozhlas.cz/zpravy-domov/cesky-statisticky-urad-hackeri-hackersky-utok-parlamentni-volby-rijen-2017_1805110600_hm

viii Slížek, David. 2019. České ISP na přelomu roku potrápila vlna silných DDoS útoků. Lupa.cz. https://www.lupa.cz/aktuality/ceske-isp-na-prelomu-roku-potrapila-vlna-ddos-utoku/

ix Policie ČR. 2018. Upozornění na výhružné e-maily. https://www.policie.cz/clanek/upozorneni-na-vyhruzne-e-maily.aspx

x Národní centrum kybernetické bezpečnosti. 2018. Aktuální legislativa. https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

xi Český parlament. 2011. Zákon č. 118/2011 (krizový zákon). http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22968

xii V překl. National Cyber Security Centre. 2018. Additional information: Russia's malicious cyber activity. https://www.ncsc.gov.uk/content/files/protected_files/article_files/Russian%20State%20Sponsored%20Actor%20Advisory.pdf

xiii National Cyber Security Centre. 2018. APT10 continuing to target UK organisations. https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations

xiv FireEye Intelligence. 2018. TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

xv Department of Justice. 2017. U.S. Charges Three Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

xvi Národní centru kybernetické bezpečnosti. 2014. Malware Havex útočí na ICS/SCADA systémy. https://www.govcert.cz/cs/informacni-servis/hrozby/2294-malware-havex-utoci-na-icsscada-systemy/

xvii US Department of Homeland Security. 2016. Cyber Attacks Against Ukrainian Critical Infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

xviii Eset. 2018. GreyEnergy: Updated arsenal of one of the most dangerous threat actors. https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

xix Eset. 2017. Industroyer: Biggest threat to industrial control systems since Stuxnet. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

xx Bundesamt für Sicherheit in der Informationstechnik. 2018. The State of IT Security in Germany 2018. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf;jsessionid=91EF3BA2F7D18807A3DD05C6E290343E.2_cid351?__blob=publicationFile&v=3, pg. 12

xxi ESET. 2018. Banking Malware: Sophisticated Trojans vs. FakceBanking Apps. https://www.welivesecurity.com/wp-content/uploads/2019/02/ESET_Android_Banking_Malware.pdf

xxii Polesný, David. 2018. Díra v systému České školní inspekce. Osobní údaje 140 tisíc žáků si mohl kdokoliv stáhnout. Živě.cz. https://www.zive.cz/clanky/ceska-skolni-inspekce-ma-diru-v-systemu-osobni-udaje-140-tisic-zaku-si-muze-kdokoli-stahnout/sc-3-a-195817/default.aspx59

xxiii Centrum prevence rizikové virtuální komunikace PdF UP. 2019. E-Bezpečí v roce 2018. 2019. E-bezpečí. http://www.e-bezpeci.cz/index.php/z-nasi-kuchyne/1415-e-bezpeci-v-roce-2018

xxiv Národní ústav pro vzdělávání. 2019. Návrh revizí ICT. http://www.nuv.cz/file/3362/

xxv Jeden svět na školách. 2018. Stav výuky mediální výchovy na středních školách. https://www.jsns.cz/nove/projekty/medialni-vzdelavani/vyzkumy/6517086_ucitele_medialni_vychovy_celkova_zprava_v24jp.pdf

xxvi Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro učitele základní školy. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20u%C4%8Ditele%20z%C3%A1kladn%C3%AD%20%C5%A1koly.pdf

xxvii Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro učitele střední školy. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20u%C4%8Ditele%20st%C5%99edn%C3%AD%20%C5%A1koly.pdf

xxviii Kopecký, Kamil a Szotkowski, René. 2018. Rodič a rodičovství v digitální éře: Rizikové chování rodičů v on-line prostředí ve vztahu k dětem. E-Bezpečí. https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/107-rodic-a-rodicovstvi-v-digitalni-ere-2018/file

xxix Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro rodiče. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20rodi%C4%8De.pdf

xxx Kopecký, Kamil a Kožíšek, Martin a Szotkowski, René a Kasáčková, Jana. 2018. Starci na netu: Výzkumná zpráva 2018. E-Bezpečí. https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/102-starci-na-netu-2017-2018/file

xxxi Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro seniory. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20seniory.pdf