NÚKIB

ZPRÁVA O STAVU

KYBERNETICKÉ BEZPEČNOSTI

ZA ROK 2017

OBSAH

ÚVOD

Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky (dále „ČR“) a zároveň práva jedinců na informační sebeurčení.

V roce 2018 lze očekávat další nárůst kybernetických hrozeb zejména další phishingové útoky nové generace, útoky na tržiště, peněženky a směnárny kryptoměn, bezsouborové varianty ransomware, využívání umělé inteligence ke kybernetickým útokům, útoky na data v Cloudových řešeních, útoky na internet věcí, průmyslové systémy atd. Očekává se, že se zvýší podíl státních nebo státem podporovaných aktérů kybernetických útoků, že bude i nadále docházet k masivním únikům osobních dat, hesel a přístupových údajů. Proto je nezbytné budovat kybernetickou bezpečnost informačních a komunikačních systémů důležitých pro chod státu a jeho kritické infrastruktury.

Rok 2017 byl pro ČR v oblasti kybernetické bezpečnosti jedním ze zásadních milníků v jejím pokračujícím rozvoji, a to nejen na úrovni budování kybernetických bezpečnostních kapacit, obsazení první příčky v mezinárodním cvičení Locked Shields 2017, ale taktéž ve formátu institucionálním a právním. Přelomovou událostí v tomto ohledu bylo vytvoření Národního úřadu pro kybernetickou a informační bezpečnost (dále „NÚKIB“; „Úřad“) oddělením Národního centra kybernetické bezpečnosti (dále „NCKB“) ze struktur Národního bezpečnostního úřadu (dále „NBÚ“) k 1. srpnu 2017. V roce 2017 pokračovalo ukotvení NÚKIB jakožto gestora kybernetické bezpečnosti díky novele zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), (dále „ZKB“) a navazování mezinárodní spolupráce nejenom na úrovni bilaterálních, ale i multilaterálních dohod.

Zpráva o stavu kybernetické bezpečnosti ČR 2017 (dále „Zpráva“) je předkládána na základě usnesení vlády ze dne 16. února 2015 č. 105 k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020. Zpráva předává přehled plnění cílů v budování kybernetické bezpečnosti ČR za rok 2017 v následujících kapitolách:

- Budování NÚKIB.
- Činnost Vládního CERT (GovCERT.cz) a sledování současných trendů v ČR.
- Vývoj legislativy v oblasti kybernetické bezpečnosti za rok 2017.
- Národní spolupráce.
- Informační a komunikační technologie důležité pro stát.
- Ochrana voleb 2017.
- Mezinárodní spolupráce.
- Cvičení kybernetické bezpečnosti.
- Vzdělávání a osvěta.

Cílem této Zprávy je poskytnout ucelené informace o aktivitách státu při zajišťování kybernetické bezpečnosti ČR v roce 2017.

1. BUDOVÁNÍ NÚKIB

K 1. srpnu 2017 byl vytvořen NÚKIB a základní komponentu nově vzniklého úřadu tvoří NCKB, které se vyčlenilo ze struktur NBÚ společně s těmito částmi: ochrana utajovaných informací v informačních a komunikačních systémech, kryptografická ochrana a neveřejná služba v rámci družicového systému Galileo. NÚKIB je ústředním orgánem státní správy v čele s ředitelem jmenovaným vládou. Úřad nyní tvoří: sekce provozně právní, sekce technická a sekce NCKB.

Sekce provozně právní plní personální, ekonomické, právní a legislativní úkoly a zastává logistickou podporu pro celý úřad. Sekce technická zajišťuje certifikaci informačních a komunikačních systémů nakládajících s utajovanými informacemi, kryptografickou ochranu a šifrovou službu a rovněž ochranu utajovaných informací v informačních a komunikačních technologiích (dále „ICT“) proti kompromitujícímu vyzařování, vykonává obranné prohlídky proti odposlechům a sledovacím zařízením. V této souvislosti došlo i k úpravě zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Sekce NCKB se dělí na odbor Vládní CERT (GovCERT.CZ) a odbor kybernetických bezpečnostních politik (dále jen „OKBP“). Vládní CERT se zabývá technickým řešením kybernetických bezpečnostních incidentů, provádí penetrační testy, analýzu malware a zajišťuje sdílení informací o incidentech a nových trendech. V této oblasti spolupracuje jak s odbornou komunitou, tak s veřejností. OKBP se soustředí na netechnické aspekty kybernetické bezpečnosti, zvláště na tvorbu a implementaci kybernetické bezpečnostní politiky ČR, regulaci, kontrolu a metodickou podporu správců informačních a komunikačních systémů v působnosti ZKB. Dále se zaměřuje na mezinárodní spolupráci, analýzu strategických informací, osvětu a vzdělávání nebo publikační činnost.

Oficiální zahájení činnosti NÚKIB proběhlo 1. srpna 2017 slavnostním představením nového úřadu Ing. Dušanem Navrátilem, ředitelem NÚKIB, ve staronovém sídle v prostorech NCKB v Brně.

2. ČINNOST VLÁDNÍHO CERT A SLEDOVÁNÍ SOUČASNÝCH TRENDŮ V ČR

V roce 2017 Vládní CERT úspěšně pokračoval v rozšiřování kapacit, aby pokryl nároky na něj kladené zejména po stránce odborné a také dostupnosti technických prostředků pro úspěšné plnění přidělených úkolů. Vládní CERT provozuje dvě laboratoře. Laboratoř pro zkoumání ICS/SCADA systémů, která byla založena v roce 2015, a forenzní laboratoř, jejíž budování započalo během roku 2016. Obě laboratoře jsou plně funkční a nadále probíhá jejich další rozvoj, aby bylo možné reagovat na nejnovější vývoj v těchto oblastech. Další informace k laboratořím jsou uvedeny v kapitolách 2.2 a 2.3, které jsou jim věnovány.

Vládní CERT nadále pokračuje s poskytováním formalizovaných penetračních testů orgánům státní správy. V roce 2017 výrazně vzrostl zájem o penetrační testy díky rozšířenému povědomí o této stále ještě nové službě a také díky tomu, že si subjekty v ČR uvědomují rizika spojená s kyberprostorem. S tím souvisí i rozvoj schopností detekce kybernetických útoků ve státní správě. Hlavní část tvoří Systém detekce kybernetických bezpečnostních událostí ve vybraných Informačních systémech státní správy (dále „ISVS“). Další část tvoří zpracování různých zdrojů dat. Vládní CERT nadále buduje své kapacity v této oblasti a zaměřuje se zejména na zdroje technického charakteru jako IoC (Indicator of Compromise) a další. Hlavní nástroj pro zpracování takto získaných informací je Botnet Feed. Aktivita vládního CERT v této oblasti doplňuje práci oddělení strategických informací a analýz v rámci OKBP. Vládní CERT disponuje mechanismy pro zpracování zdrojů, ale možnosti prezentace a doručení získaných informací postiženým subjektům jsou závislé na dokončení neveřejného části webového portálu. Tento portál umožní sdílet informace ve větší míře a formou, která je více vhodná k jejich dalšímu zpracování.

Součástí rozšiřování kapacit vládního CERT je i prohlubování technických znalostí jednotlivých specialistů. Zaměstnanci úspěšně absolvovali odborná školení včetně příslušných certifikačních zkoušek a tyto technické znalosti jsou uplatňovány jak při řešení kybernetických incidentů, tak při účasti na mezinárodních cvičeních.

2.1 Penetrační testování

Oddělení bezpečnostního testování a vývoje se v roce 2017 zaměřilo na poskytování externích penetračních testů. Rozsah prováděných testů se lišil v závislosti na požadavcích objednavatelů. Jednalo se o testování webových aplikací, zranitelností operačních systému a služeb dostupných z internetu. Testy probíhaly v režimu „black box“ nebo „grey box“. Tedy objednavatel neposkytl týmu provádějícímu penetrační test žádnou nebo pouze elementární znalost testovaných systémů. Po ukončení testování byla vždy vyhotovena závěrečná zpráva se zjištěnými zranitelnostmi a doporučeními pro jejich opravu a bezpečnější chod dané organizace. Většina testů probíhala po dobu jednoho měsíce s dodatečným časem pro tvorbu závěrečné zprávy.

Tuto službu, kterou Vládní CERT poskytuje zdarma, využili významné instituce ze státního i veřejného sektoru a zájem o penetrační testy byl oproti loňskému roku velmi poptávaným artiklem. Tato skutečnost ukazuje na to, že si subjekty v rámci ČR více uvědomují rizika spojená s kyberprostorem.

Kvalita zabezpečení subjektů se diametrálně lišila. Některé testy byly ukončeny se zjištěnými zranitelnostmi malé závažnosti, jiné s kritickými zranitelnostmi, které byly doporučeny k okamžité nápravě.

2.2 Forenzní laboratoř

Činnost laboratoře zahrnuje forenzní analýzu digitálních stop zajištěných v souvislosti s řešením kybernetických bezpečnostních incidentů. Služby forenzní laboratoře jsou využívány i v rámci dalších úkolů vykonávaných vládním CERT týmem, například projekt *Ochrana voleb 2017* (viz kapitola 9). Pracovníci laboratoře se zaměřují na analýzu počítačových systémů a jiných elektronických zařízení.

Provoz laboratoře byl po dlouhých přípravách zahájen na začátku roku 2017 a její budování a zdokonalování bude nadále pokračovat. V tomto roce byly také podniknuty první kroky k vytvoření znaleckého pracoviště v oboru kybernetické bezpečnosti a certifikaci samotné laboratoře.

2.3 ICS/SCADA laboratoř

Pracovníci SCADA laboratoře se soustavně vzdělávají v problematice bezpečnosti průmyslových automatizačních technologií a v navazujících oblastech. Pravidelně se zapojují do tuzemských i zahraničních kybernetických cvičení, v roce 2017 výrazně přispěli k vyřešení SCADA scénáře u cvičení Locked Shields. Současně je poskytována konzultace pro tvorbu technických ICS scénářů pro další zahraniční, ale i tuzemská cvičení.

Taktéž pokračuje systémové budování SCADA laboratoře a rozšiřování o další vybrané technologie. Pracovníci připravují osvětové prezentace a rozbory kybernetických útoků na automatizační technologie, se kterými se partnerské organizace a další zájemci mohou seznamovat v rámci návštěv SCADA laboratoře v budově NÚKIB nebo například na Úřadem pořádaných konferencích, jako byl CyberCon Brno 2017.

Pracovníci se v oblasti bezpečnosti SCADA systémů zapojují do diskusí s ostatními státními složkami a odborníky, např. kulatý stůl SCADA pořádaný při konferenci Future Forces 2017. V rámci proaktivních činností je plánována příprava systému pro zpracovávání dat, z veřejně dostupných zdrojů (např. Shodan.io), týkajících se připojených automatizačních technologií do sítě internet. Z uvedených důvodů rozšiřování činností a rozmanitosti technologií je plánováno i personální posílení SCADA týmu.

2.4 Systém detekce kybernetických bezpečnostních událostí ve vybraných ISVS

Cílem tohoto projektu je nasazení síťových sond do sítí klíčových orgánů státu. Síťové sondy získávají a uchovávají popisná data o provozu a poskytují tak data pro analýzu a vyšetřování incidentů. Zároveň dovolují rozsáhlou automatizaci a rozpoznávání škodlivých a nebezpečných aktivit. Pro samotné správce sítí znamenají možnost řešit provozní problémy z pohledu sítě daleko efektivněji. Správci těchto sítí tak budou mít přehled o dění ve své síti.

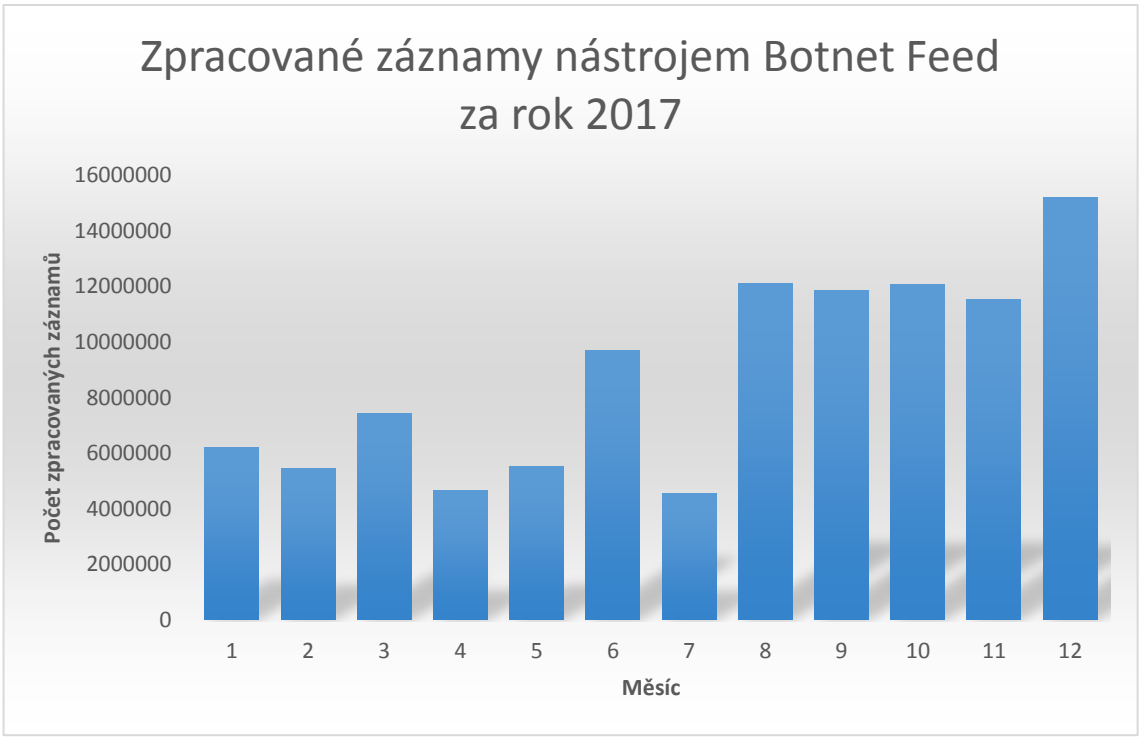
Přidanou hodnotou je předávání informací z perimetru sítí do centrálního vyhodnocovacího nástroje. Ten operátoři Vládního CERT budou používat k proaktivní činnosti s cílem informovat ostatní ještě před případným zasažením. Realizace tohoto projektu je očekávána v roce 2018.

2.5 Botnet Feed

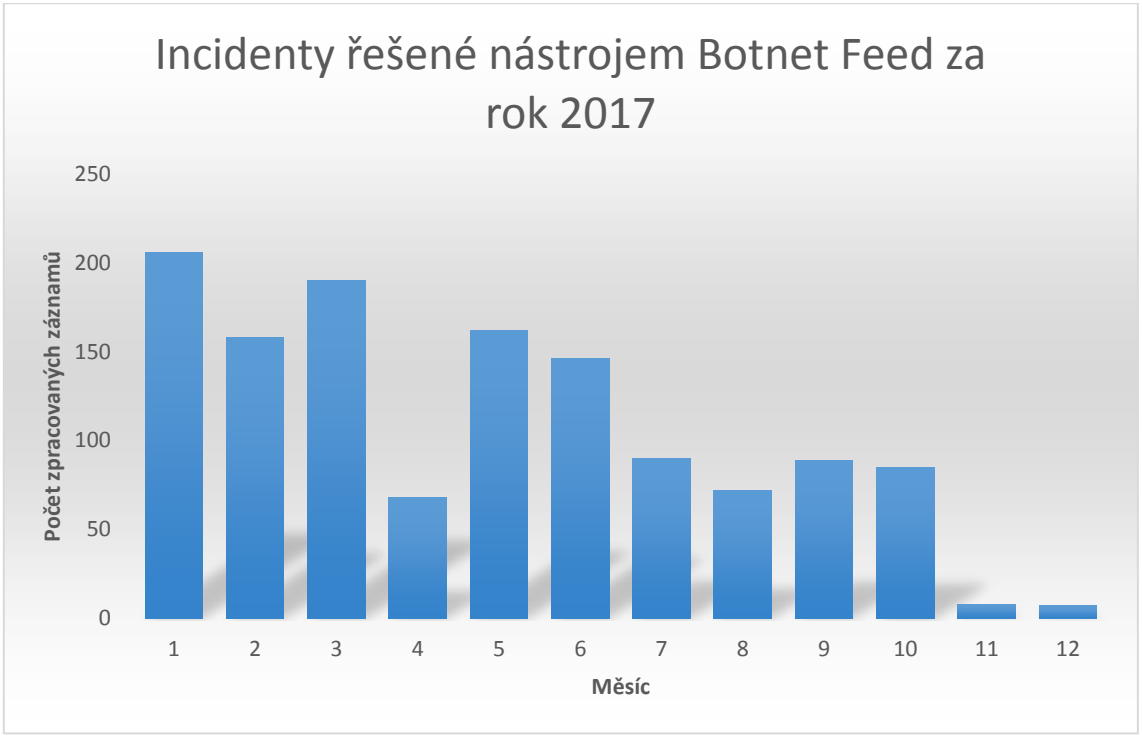
V rámci svých proaktivních činností GovCERT.CZ pomocí několika nástrojů analyzuje data z uzavřených i veřejně dostupných zdrojů, jež obsahují indikátory o kompromitaci systémů. Nejdůležitějším nástrojem je Botnet Feed, který je vyvíjen týmem GovCERT.CZ za účelem sběru a zpracování dat o koncových stanicích zapojených do sítí botnetů. Data jsou získávána ze zajištěných řídících serverů (C&C). Původcem dat je společnost Microsoft[1].

Převážná část reportů je určena komerční sféře (ISP/poskytovatelé hostingových služeb). Denně je exportováno přibližně 15 MB reportů ve strojově čitelném formátu. Od ledna do prosince roku 2017 bylo zpracováno a vyhodnoceno přibližně 106 365 418 záznamů o potenciálních bezpečnostních hrozbách v ČR. Celkem bylo partnerům a institucím spadajících do působnosti GovCERT.CZ odesláno 1 281 reportů.

[1] GovCERT.CZ doposud odebírá data týkající se 14 botnetů, mezi kterými jsou např. Bamital, Citadel, Conficker, Kelihos, Zeus, Simda, Ramnit, Dorkbot a další.



Graf 1 - počet zpracovaných záznamů za rok 2017



Graf 2 - počet incidentů za rok 2017 s rozdělením po měsících

2.6 Neveřejný web

V rámci reorganizace a vzniku NÚKIB došlo i k obsahovým změnám ve veřejné části webových stránek, které slouží jako informační portál pro širokou veřejnost. Z technických i personálních důvodů byl však pozdržen proces dokončení jejich neveřejné části a termín jejího spuštění je plánován během roku 2018. V současnosti prochází systém poslední fází testování a je věnován důraz na maximální zabezpečení. Kromě kontroly přístupu k jednotlivým informacím, bude možné snadněji sdílet užitečné informace a specifická technická data se správci systémů kritické informační infrastruktury (dále „KII“), provozovatelů základních služeb, významných informačních systémů (dále „VIS“) a dalšími spolupracujícími subjekty. Platforma umožní sdílet zkušenosti a „lessons learned“ i mezi jednotlivými uživateli. Jednat se bude zejména o neutajované informace, které ale není možné sdílet zcela veřejně, aby k nim nezískal přístup potenciální útočník.

3. NEJVÝZNAMNĚJŠÍ BEZPEČNOSTNÍ UDÁLOSTI

Cílem této podkapitoly je představení nejvýznamnějších událostí, které v roce 2017 ovlivnily nejenom českou kybernetickou bezpečností komunitu.

3.1 EternalRocks

Jedná se o nový kmen škodlivého kódu (malwaru), který ke svému šíření zneužívá chyb v protokolu SMB pro sdílení souborů v operačním systému Windows. Větší nebezpečí spočívá i v tom, že na rozdíl od ransomwaru WannaCry, který používá pouze dva uniklé nástroje NSA (EternalBlue a DoublePulsar), jich tento síťový červ nazvaný EternalRocks využívá všech sedm. Navíc nelze malware jednoduše vypnout tak, jak tomu bylo u ransomwaru WannaCry. EternalRocks se maskuje jako WannaCry, aby oklamal bezpečnostní výzkumníky. Místo toho, aby se pak projevil jako klasický ransomware, umožní útočníkům převzít kontrolu nad postiženým počítačem pro další možné kybernetické útoky. Do této doby nám žádný subjekt z VIS nebo KII nenahlásil napadení systému červem EternalRocks.

3.2 WannaCry

Ransomware WannaCry, který využíval pro své šíření kromě phishingu i unikátní metodu pomocí zneužití zranitelnosti protokolu SMB v operačním systému Microsoft Windows, se začal šířit v polovině května 2017 a ve

více než 150 zemích dokázal velmi rychle infikovat více než 230 tisíc počítačů. Útok postihl širokou škálu organizací a institucí. Mezi nejvíce postižené systémy patřil britský systém veřejného zdravotnictví National Helth Service (NHS), ruské ministerstvo vnitra, ruská státní železnice, ruský mobilní operátor Megafon a španělský telekomunikační operátor Telefónica. Mezi napadené sektory patřil i automobilový průmysl. V rámci ČR se podle vyjádření antivirových společností jednalo několik set nákaz. Vládní bezpečnostní tým (GovCERT.CZ) však neobdržel ani jedno hlášení týkající se WannaCry ransomwaru od správců KII nebo VIS, naopak zaslal těmto subjektům varování včetně souboru technických doporučení.

3.3 Petya/NotPetya/Neytya/Goldeneye

Podle dostupných informací se Petya začal šířit koncem června 2017 po hackerském útoku na ukrajinskou softwarovou společnost MeDoc, kde došlo k pozměnění aktualizačního balíčku účetního softwaru. Pro další šíření Petya využíval stejné zranitelnosti v operačním systému Windows, jako tomu bylo v případě ransomwaru WannaCry z května 2017. Mezi napadené cíle patřilo zejména široké spektrum cílů z Ukrajiny, včetně centrální banky, mezinárodního letiště Borispol, kyjevského metra, jaderné elektrárny Černobyl či energetické společnosti Ukrenergo a dále významné společnosti z Ruska, Dánska či Španělska. ČR byla zasažena pouze okrajově a GovCERT.CZ neevidoval žádné hlášení o napadení systémů KII nebo VIS.

3.4 CCleaner

V září bylo objeveno, že produkt CCleaner (jedná se o oblíbený čistící nástroj) od společnosti Avast obsahuje skrytý kód (backdoor). Analýza dat prokázala, že se jedná o APT (Advanced Persistent Threat) útok, který je vytvořen tak, aby vybraným uživatelům, kteří si tento produkt stáhli, doručil druhou fázi útoku. Druhá část útoku zajišťuje zakořenění škodlivého kódu v systému. Útočníci cílili především na velké technologické a telekomunikační společnosti v Japonsku, na Tchaj-wanu, ve Velké Británii, Německu a v USA. Jednalo se o tzv. watering-hole attack, typ útoku, kdy je napaden oficiální distribuční server důvěryhodného poskytovatele software a zneužit pro distribuci malware. Všechna fakta a použité techniky ukazují, že šlo o vysoce sofistikovaný útok, který se připisuje čínské skupině APT17. Avast kontaktoval všechny subjekty, na které se útočníci zaměřili, proto pokud by se obětí útoku stal subjekt spadající do naší působnosti, tímto způsobem by se o tom dozvěděl. NÚKIB neobdržel žádné hlášení o popisovaném útoku, a tak lze předpokládat, že nebyl zasažen žádný subjekt z oblasti jeho působnosti.

3.5 Bad Rabbit

Nový typ ransomwaru nazvaný Bad Rabbit se ke konci října postupně rozšiřoval zejména v Rusku a na Ukrajině. Případy nakažení se ale objevily také v Bulharsku a Turecku. Malware zasáhl například několik ruských webových stránek, ukrajinské letiště Odessa, ukrajinské Ministerstvo dopravy a metro v Kyjevě. V ČR byly zaznamenány jen jednotky případů napadení tímto ransomwarem. Ve známých případech nakažení požadoval

za odemknutí výkupné v hodnotě 0,05 bitcoinu. Firma Eset uvedla, že se malware šíří prostřednictvím falešných aktualizací Adobe Flash. Dle dostupných informací se Bad Rabbit šíří skrze protokol SMB (port 445).

3.6 ROCA

Jedná se o zranitelnost v procesu generování RSA klíčů, který se odehrává v softwarové knihovně implementované například v kryptografických čipových kartách, bezpečnostních tokenech a dalších hardwarových čipech vyrobených společností Infineon Technologies AG. Chyba byla zveřejněna na přelomu října a listopadu 2017 na konferenci ACM CCS. Zranitelnost umožňuje praktický faktorizační útok, při kterém útočník dokáže vypočítat soukromou část RSA klíče. Zranitelnost se objevuje v čipech vyrobených již v roce 2012, které jsou v současnosti běžně využívané, a to například i v KII a VIS. Vzdálený útočník může z hodnoty veřejného klíče spočítat privátní RSA klíč. Soukromý klíč může být zneužit k podvržení identity legitimního vlastníka, dešifrování citlivých zpráv, padělání podpisů (například pro vydávání softwaru), podvržení přístupových karet a další související útoky. Zranitelnost ROCA měla přímý dopad i na Českou republiku a dotýká se mnoha oblastí, kde se využívají asymetrické kryptografické klíče RSA.

3.7 KRACK

Útok nazvaný KRACKs (Key Reinstallation Attacks) týkající se vážné zranitelnosti protokolu WPA2. Podle zveřejněných informací byla zranitelná zařízení všech výrobců. O chybě byla v předstihu několika týdnů informována zhruba stovka organizací, především výrobci Wi-Fi routerů a dalších zařízení. Detaily zranitelnosti byly pečlivě střeženy, aby měli výrobci šanci vydat záplaty. Zranitelnosti KRACK byla dotčena všechna zařízení používající Wi-Fi připojení s ověřením pomocí protokolu WPA2. Většina výrobců vydala pro svoje zařízení updaty.

3.8 Intel Meltdown, Specter

Meltdown a Specter využívají kritické zranitelnosti v moderních procesorech. Pomocí této zranitelnosti umožňují programům ukrást data, která jsou aktuálně zpracovávána v počítači. Získají přístup k datům, která jsou uložena v paměti. Může se jednat například o hesla uložená ve správci hesel, osobní fotografie, emaily, pracovní dokumenty apod. Zatímco zranitelnost Meltdown je záležitostí čistě procesorů Intel. U zranitelnost Specter se jedná o problém většiny dnešních moderních procesorů. Jako obranou proti tomuto druhu útoku je nutné updatovat operační systémy, firmwary/BIOSy, virtualizační platformy, hypervisory. Opravné balíčky jsou v současné době již dostupné anebo jsou výrobci postupně dodávány. Z pohledu ČR se jedná o problém plošný, v současné době probíhá postupný update většiny velkých datacenter. O této události se hovoří jako o restartu internetu.

3.9 Nejvýznamnější úniky dat

- Cloudflare security flaw – chyba, která umožňovala přístup k datům zákazníků.
- TSA leak – únik dokumentů na letišti v New Yorku Deloitte – průnik do systému Deloite, přístup k e-mailům.
- Vault 7 – únik dokumentů CIA.
- Shadow Brokers – únik nástrojů NSA skupinou Shadow Brokers.
- Equifax – 140 milionů účtů, osobní data.

4. VÝVOJ LEGISLATIVY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI ZA ROK 2017

V průběhu roku 2017 došlo v otázce legislativy pro oblast kybernetické bezpečnosti k výrazným změnám. Nejen z důvodu povinnosti transponovat směrnici Evropského parlamentu a Rady Evropské unie (dále „EU“) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále „směrnice NIS“) došlo k přijetí dvou novelizací ZKB, kterými byl zákon ve značném rozsahu pozměněn. Vedle změny zákona došlo také k vytvoření nové vyhlášky o kritériích pro určení provozovatele základní služby a také byla připravována nová vyhláška nahrazující vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále „vyhláška o kybernetické bezpečnosti“).

4.1 Směrnice NIS a její implementace do českého právního řádu

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 vstoupila v platnost 9. srpna 2016. Směrnice NIS reflektuje úsilí EU o zavedení minimálních bezpečnostních standardů pro důležité informační a komunikační systémy napříč členskými státy EU a zajištění lepší úrovně koordinace mezi příslušnými subjekty zajišťujícími kybernetickou bezpečnost v těchto státech. Za tímto účelem zavedla povinnost členským státům určit vnitrostátní orgány, které budou příslušné v oblasti bezpečnosti sítí a informačních systémů. Dále směrnice zavedla povinnost určit jednotné vnitrostátní kontaktní místo pro oblast bezpečnosti sítí a informačních systémů. Obě tyto povinnosti plní v České republice NÚKIB. Povinnost členského státu zřídit

bezpečnostní tým typu CSIRT pro subjekty regulované směrnicí plní jak Vládní CERT (pro provozovatele základních služeb, viz níže), tak národní CERT (ve vztahu k poskytovatelům digitálních služeb, viz níže). Vedle těchto povinností byla směrnicí NIS zřízena na evropské úrovni také Skupina pro spolupráci a síť bezpečnostních týmů typu CSIRT (dále „Síť CSIRT“), a to s cílem podporovat spolupráci mezi členskými státy. Jak Skupina pro spolupráci, tak i Síť CSIRT začaly plnit své povinnosti.

Směrnice NIS ukládá členským státům povinnost upravit dvě obecné kategorie subjektů, kterými jsou tzv. provozovatel základních služeb (dále „PZS“) a poskytovatel digitálních služeb (dále „PDS“). Na tyto subjekty se budou poté vztahovat bezpečnostní opatření a povinnost hlásit bezpečnostní incidenty způsobilé narušit klíčové společenské a ekonomické činnosti zajišťované jimi provozovanými systémy. Transpoziční lhůta pro zavedení vnitrostátní právní úpravy zajišťující soulad právního řádu členského státu se směrnicí NIS končí 9. května 2018.

4.2 Změny zákona o kybernetické bezpečnosti

V průběhu roku 2017 byl ZKB celkem dvakrát novelizován:

- První novelizace proběhla cestou zákona č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB), a některé další zákony. V rámci této novelizace byla do zákona především zavedena nová povinná osoba, a to osoba provozovatele informačního nebo komunikačního systému KII nebo VIS. Tato novelizace zákona nabyla účinnosti k 1. červenci 2017.

- Druhá, podstatně rozsáhlejší, novelizace proběhla cestou zákona č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB), ve znění zákona č. 104/2017 Sb., a některé další zákony. Tato novelizace je transpozicí směrnice NIS a přináší řadu změn. Především zavádí do zákona nové povinné osoby: PZS, správce a provozovatele informačního systému základní služby a PDS, kterým ukládá nové povinnosti a upravuje další otázky s nimi související. Dále také zřizuje NÚKIB jako ústřední orgán státní správy pro oblast kybernetické bezpečnosti a vybrané otázky v oblasti ochrany utajovaných informací. Tato novelizace zákona nabyla účinnosti k 1. srpnu 2017.

4.3 Nová vyhláška o kritériích pro určení provozovatele základní služby[2]

Nová vyhláška č. 437/2017 Sb., o kritériích pro určení PZS je prováděcím právním předpisem souvisejícím s novelou ZKB, která transponovala směrnici NIS a zavedla do tohoto zákona jako jednu z povinných osob také PZS. Zákon stanovuje osm odvětví, v rámci kterých budou provozovatelé základních služeb určováni. Tato vyhláška pak obsahuje odvětvová a dopadová kritéria, podle kterých bude NÚKIB rozhodnutím určovat PZS. Na základě směrnice NIS mají členské státy povinnost určit PZS do 9. listopadu 2018. Vzhledem k účinnosti vyhlášky k 1. únoru 2018 lze očekávat, že bude tento požadavek naplněn. Od počátku byla vyhláška koncipována tak, aby byla čitelná i pro techniky a osoby, které spravují systémy, které mohou spadat do působnosti ZKB. Vyhláška má tedy pouze dva věcné paragrafy. První se zabývá předmětem úpravy, druhý popisuje odvětvová a dopadová kritéria a vztah mezi nimi. Stěžejní částí vyhlášky o kritériích pro určení PZS je její příloha. Přílohu tvoří série tabulek, jež jsou každá rozdělena do čtyř sloupců. V prvních třech sloupcích jsou odvětvová kritéria a ve čtvrtém sloupci jsou dopadová kritéria. Řádky jsou tvořeny kritérii, která v souhrnu určují jednotlivé budoucí základní služby, jež byly definovány dle směrnice NIS. NÚKIB k této problematice vydává množství podpůrných materiálů, které průběžně uveřejňuje na svém webu.

[2] Vyhláška byla rozeslána stejnopisem částky Sbírky zákonu ČR č. 157/2017 dne 15. prosince 2017. Tato částka Sbírky zákonů ČR je dostupná na adrese: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=437/2017&typeLaw=zakon&what=Cislo_zakona_smlouvy.

4.4 Příprava nové vyhlášky o kybernetické bezpečnosti

Vyhláška č. 316/2014 Sb. je prováděcím právním předpisem ZKB. Vzhledem k novele ZKB je nutné novelizovat také tuto vyhlášku. NÚKIB od června 2017 připravuje nové znění, které si klade za cíl soulad se ZKB. Dalším cílem je také odstranění některých nedokonalostí, úprava části stávajících povinností a soulad s „best practices“ v oblasti kybernetické bezpečnosti. NÚKIB plánuje vydat tuto vyhlášku zcela novou, která nahradí její původní znění.

Na tvorbě prvního pracovního znění se podílel zejména tzv. „expertní tým“ složený ze zaměstnanců NÚKIB a skupiny odborníků z řad odborné veřejnosti, regulovaných subjektů a spolupracujících institucí. Expertní tým absolvoval celkem jedenáct několikahodinových workshopů, na jejichž základě byl vytvořen již zmíněný návrh. Na začátku října byl návrh nové vyhlášky, prozatím bez jazykové a legislativně technické korekce, zveřejněn na webu NÚKIB společně s výzvou pro odbornou veřejnost. Výzva spočívala v možnosti vyjádřit se ke znění draftu vyhlášky, a to před samotným zařazením vyhlášky do legislativního procesu. Tento krok se poměrně vyplatil, neboť díky výzvě dorazila cca stovka připomínek, z nichž většina byla zapracována.

Počátkem roku 2018 bude návrh vyhlášky rozeslán do meziresortního připomínkového řízení. Nabytí účinnosti nové vyhlášky o kybernetické bezpečnosti se předpokládá na jaře roku 2018.

PODĚKOVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost tímto děkuje všem členům expertního týmu a všem zástupcům odborné veřejnosti za pomoc při tvorbě nové vyhlášky o kybernetické bezpečnosti.

4.5 Plán legislativních prací pro rok 2018

V rámci plánu legislativních prací pro rok 2018 je potřeba nadále pokračovat v plnění povinností uložených ZKB a tedy na základě zmocnění daného tímto zákonem vydat i zbývající právní předpisy.

Jedním z nových předpisů, které je potřeba vypracovat, je i nová vyhláška, která stanoví obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu. Ta by měla vycházet ze základů vyhlášky o kybernetické bezpečnosti a zohledňovat zejména výsledky práce jednotlivých pracovních skupin vzniklých pod Ministerstvem vnitra (dále „MV“) v rámci přípravy eGov Cloud (eGC) projektu.

Dalším z plánovaných právních předpisů je vyhláška, která stanoví způsob likvidace kopií dat a provozních údajů a náležitosti protokolu o průběhu likvidace kopií dat a provozních údajů. K vypracování této vyhlášky byl NÚKIB zmocněn na základě novelizace zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Nový předpis bude obsahovat úpravu způsobu likvidace kopií dat a provozních údajů, stejně tak jako náležitosti protokolu o průběhu této likvidace.

Posledním bodem je plánovaná novelizace vyhlášky č. 317/2014 Sb., o VIS a jejich určujících kritériích. Rozsah této novelizace bude vyplývat z projednání materiálu Metodická podpora v oblasti kybernetické bezpečnosti pro rok 2018, který NÚKIB zpracoval a do 31. března 2018 jej předloží vládě ČR.

5. NÁRODNÍ SPOLUPRÁCE

Široká spolupráce na národní úrovni je nezbytná pro zajištění kybernetické bezpečnosti ČR. NÚKIB jako národní gestor dané oblasti aktivně spolupracuje s ostatními subjekty státní správy a snaží se tak udržovat jednotný postoj ČR směrem do zahraničí. Spolu s akademickou sférou se podílí na přípravě budoucích odborníků a na navyšování povědomí o kybernetické bezpečnosti. S bezpečnostními týmy CSIRT sdílí informace a zkušenosti se zranitelnostmi a podílí se na vývoji nových technických nástrojů.

5.1 Výbor pro kybernetickou bezpečnost

Vláda ČR ustavila usnesením č. 360 ze dne 10. května 2017 Výbor pro kybernetickou bezpečnost. Jedná se o nový stálý pracovní orgán Bezpečnostní rady státu (dále „BRS“) pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti ČR. Tento výbor v rámci své působnosti zejména:

- zabezpečuje meziresortní spolupráci, projednává záměry plánovacích a koncepčních materiálů z oblasti kybernetické bezpečnosti předkládaných ministerstvy a jinými ústředními správními úřady a doporučuje jejich projednání v BRS,
- zabezpečuje mezirezortní koordinaci plánovacích a přípravných aktivit v oblasti zajišťování kybernetické bezpečnosti, důležitých pro stabilitu a bezpečnost ČR s důrazem na ochranu KII,
- posuzuje a projednává požadavky státních orgánů uplatňované v rámci zajišťování kybernetické bezpečnosti,
- posuzuje a projednává dokumenty na základě usnesení BRS,
- zpracovává a projednává vlastní materiály,
- projednává vyhodnocení meziresortních připomínkových řízení k materiálům vztahujícím se k působnosti výboru a doporučuje jejich projednání v BRS,
- posuzuje, projednává a koordinuje základní zaměření činnosti zástupců ČR v orgánech EU, Severoatlantické aliance (dále „NATO“) a dalších mezinárodních organizacích, navazuje, rozvíjí spolupráci s mezinárodními subjekty a přispívá k formování jednotného postoje v oblasti kybernetické bezpečnosti ČR směrem do zahraničí.

5.2 Národní strategie kybernetické bezpečnosti 2015 – 2020 a Akční plán

Informace o plnění Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020, respektive jejího Akčního plánu je zpracovaná na základě vstupů jednotlivých subjektů v příloze č. 5.

5.3 Spolupráce s CSIRT.CZ a rozvoj Národního CERT

V roce 2017 CSIRT.CZ navázal na úspěšnou spolupráci s Národním CERT, který je provozovaný na základě veřejnoprávní smlouvy se sdružením CZ.NIC z. s. p. o. Na operativní úrovni jde o téměř každodenní spolupráci při sdílení informací o zranitelnostech nebo žádostí o pomoc při koordinaci řešení incidentů.

Spolupráce však probíhá i na dalších úrovních. Jednou z nich jsou kybernetická cvičení, kde například při cvičení Cyber Czech 2016 (viz kapitola 6.1) vyslal tým CSIRT.CZ vlastní tým odborníků.

Tým CSIRT.CZ se v roce 2017 nadále věnoval rozvoji projektu *Predikce a ochrana před kybernetickými incidenty* (PROKI) a zaslaným reportům od operátorů na abuse kontakt v databázi RIPE NCC, dále začal jednou týdně zasílat souhrnné zprávy o počtu incidentů pocházejících z jejich sítě. Zároveň byl týmu schválen projekt v rámci výzvy CEF (Connecting Europe Facility). Cílem projektu je například další expertní vzdělávaní členů týmů či pokračování Pracovních skupin CSIRT.CZ. Tyto pracovní skupiny se pořádají již několik let a propojují odborníky na bezpečnost z veřejné a soukromé sféry. Další projekt, který sdružení řeší ve spolupráci se sdružením CESNET je *Vybudování a ověřovací provoz systému Cyber Threat Intelligence* pro potřeby Vládního CERT. Daný projekt je realizovaný v rámci Bezpečnostního výzkumu pro potřeby státu v letech 2016 – 2021 a v první fázi projektu bude rozděleno několik set routerů Turris Omnia mezi subjekty státní správy.

Národní CERT také v roce 2017 uskutečnil jednu ze svých doposud největších osvětových kampaní na problematiku zranitelných redakčních systémů. Držitelé 50 000 domén byli upozorněni na rizika spojená s provozováním webu na zastaralých a zranitelných redakčních systémech. Nadále se také pokračovalo v osvětových přednáškách pro základní školy a různé vzdělávací instituce. Celkově se, i díky zapojení do projektu Safer Internet, podařilo proškolit přes 900 žáků a učitelů v základech fungování Internetu včetně hrozeb, kterým mohou v jeho prostředí čelit.

6. INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE DŮLEŽITÉ PRO STÁT

Důležitost některých ICT pro fungování státu, ekonomiky a poskytování nezbytných služeb občanům je nezpochybnitelná. Ochrana a bezpečnost takových systémů je stále více aktuální a tato problematika začíná být řešena nejen na úrovni jednotlivých států, ale také na úrovni mezinárodní. V ČR jsou systémy důležité pro bezpečnost státu, zajištění základních životních potřeb obyvatel, zdraví občanů a ekonomiku určovány jako KII a systémy mající vliv na výkon státní správy pak jako VIS. V návaznosti na transpozici směrnice NIS se okruh takových důležitých systémů rozšířil o systémy základních služeb, které budou popsány níže. Tyto systémy musejí být odpovídajícím způsobem chráněny.

6.1 Systémy nově regulované podle ZKB

Předpokládané systémy, které budou nově regulovány podle novely ZKB, je nutné rozdělit do dvou skupin.

- První skupinou jsou již zmíněné PDS. Do této kategorie budou spadat on-line tržiště, internetové vyhledávače a cloud computing. Subjekt se povinnou osobou podle ZKB stane, pokud naplňuje zákonnou definici uvedenou v ZKB. Definice těchto digitálních služeb v ZKB vychází přímo ze směrnice NIS. To znamená, že v případě, kdy subjekt naplní definici, stává se tento subjekt povinnou osobou dle ZKB. Regulace v této skupině se netýká malých a mikro podniků a funguje zde princip sebeposouzení.

- Druhou skupinou, která bude nově spadat pod ZKB, jsou taktéž zmínění PZS, u kterých budou určeny informační systémy základních služeb (ISZS). Tato skupina cílí na subjekty, které v následujících odvětvích zabezpečují společenské a ekonomické činnosti, přičemž tyto činnosti jsou závislé na sítích elektronických komunikací nebo informačních systémech: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura a chemický průmysl. Předpokládané systémy, které budou zahrnuty v této kategorii, jsou například systémy, které řídí dodávky tepla, elektřiny, ropy a plynu. Dalšími příklady mohou být systémy, které jsou využívány pro provoz letišť a leteckou dopravu, mají vliv na provoz drážní dopravy, provoz inteligentních dopravních systémů, poskytování zdravotních služeb, výrobu dodávku nebo distribuci pitné vody, výkon úvěrových institucí, propojování technicky soběstačných sítí, správu nebo provoz registru internetových domén nejvyšší úrovně. Jak je patrné z jednotlivých odvětví, dochází zde k překryvu s KII. To znamená, že nárůst počtu systémů, které budou nově spadat pod ZKB, nebude extrémně vysoký, protože zejména v energetice, dopravě, bankovnictví již některé systémy pod ZKB spadají jako KII.

6.2 Kontrolní činnost a analýzy kybernetické bezpečnosti v roce 2017

Plnění plánu kontrolní činnosti v roce 2017 bylo v důsledku mnoha zásadních událostí pozastaveno v první polovině února těsně před zahájením prvních plánovaných kontrol. Hlavním důvodem bylo přijetí usnesení vlády ČR ze dne 8. února 2017 č. 104, které, v reakci na kybernetický útok na Ministerstvu zahraničních věcí (dále „MZV"), dalo NCKB za úkol provést analýzu stavu kybernetické bezpečnosti a poskytnout metodickou podporu u jednotlivých ministerstev, Úřadu vlády ČR a tento postup doporučilo také vedoucím Kanceláře Poslanecké sněmovny a Kanceláře Senátu Parlamentu ČR a Kanceláře prezidenta republiky.

V roce 2018 se předpokládá zahájení kontrolní činnosti od druhého čtvrtletí. Plánovanou novinkou v oblasti analýz kybernetické bezpečnosti je pravidelné každoroční provádění takových analýz všech ministerstev ze strany NÚKIB. Na základě těchto analýz má být Vládě ČR poskytnuto i celkové srovnání stavu kybernetické bezpečnosti ministerstev.

6.3 Technická bezpečnost systémů KII/VIS

V roce 2017 pokračoval NÚKIB spolu s partnery z Ministerstva financí (dále „MF"), Ministerstva práce a sociálních věcí (dále „MPSV") a Ministerstva spravedlnosti (dále „MSp") v realizaci projektu *Systém detekce kybernetických bezpečnostních událostí*, jehož cílem je pomocí analýzy síťového provozu zvýšit kybernetickou bezpečnost strategických sítí státu.

Systém bude po spuštění mimo jiné schopen identifikovat datový provoz na IP adresy se špatnou reputací a také anomální datové přenosy, tj. data proudící v nezvyklý čas, nezvyklém formátu či objemech.

V tomto roce provedl NÚKIB výběr hlavních technologických dodavatelů řešení a započal přípravné práce pro instalaci do partnerských rezortů. Po spuštění systému v roce 2018 hodlá NÚKIB okruh zapojených institucí dále rozšiřovat.

7. OCHRANA VOLEB 2017

NCKB se v únoru 2017 začalo věnovat hodnocení bezpečnosti volebního procesu v gesci Českého statistického úřadu (ČSÚ). Spolupráce byla započata v rámci pracovní skupiny MV na ochranu voleb. V první fázi se za pomoci partnerů z ČSÚ věnovala pozornost důkladnému zmapování a pochopení elektronické části sčítání hlasů a prezentace volebních výsledků. NCKB analyzovalo tři hlavní rozměry voleb:

- **procesní** – tedy pracovní postupy zaměstnanců ČSÚ, volebních komisí a dalších osob podílejících se na průběhu voleb,
- **datový** – tedy toky dat z volebních komisí přes regionální přebírací místa až po centrální databázi ČSÚ a dále k veřejnosti, v jakém jsou data formátu, jak jsou zabezpečena a šifrována,
- **infrastrukturní** – tedy po jakých linkách data tečou, jak jsou tyto linky zabezpečeny, kdo vlastní počítače a další hardware, na kterém jsou sčítány výsledky atd.

Teprve po této úvodní fázi předalo NCKB partnerům první výstup – netechnickou analýzu zranitelností s několika doporučeními ke zlepšení, určenou především pro vedení ČSÚ. Po vzájemné dohodě následovaly penetrační testy webu www.volby.cz a penetrační testy notebooků a programového vybavení používaného na přebíracích místech ČSÚ, kam jsou sváženy výsledky z jednotlivých volebních okrsků. Výsledkem byly další dva výstupy – technicky laděné zprávy z penetračního testování určené zejména pro IT odborníky ČSÚ, opět obsahující doporučená opatření vedoucí k minimalizaci nalezených rizik.

V rámci zlepšení ochrany volebního procesu proběhlo také školení zaměstnanců ČSÚ vedené odborníky z Úřadu. Cílem školení bylo zvýšit povědomí o rizicích elektronické komunikace, hrozbě sociálního inženýrství a podobně. Pracovníci ČSÚ byli také seznámeni s průběhem kampaní na ovlivnění voleb, které proběhly v zahraničí v nedávné minulosti.

Úřad se dále aktivně podílel na školeních pořádaných MV pro volební štáby. V červenci proběhlo školení kybernetické bezpečnosti pro volební týmy před parlamentními volbami. V prosinci poté seminář kybernetické bezpečnosti pro volební týmy prezidentských kandidátů. Šlo o první školení na toto téma určené pro politické strany a prezidentské kandidáty. NÚKIB byl jedinou veřejnou institucí, která na školeních aktivně vystupovala. Pracovníci NÚKIB během obou akcí vedli dva přednáškové bloky. První se věnoval případům kybernetických útoků ze zahraničí. S pomocí nich došlo k představení možné podoby útoků, jejich cílů a rovněž potenciálních vektorů. To vše na příkladech skutečných útoků. Druhý blok se zaměřil na kybernetickou bezpečnost na uživatelské úrovni. Pracovník NÚKIB se soustředil na základní pravidla, která by měla být na uživatelské úrovni dodržována a vynucována. Součástí tohoto bloku byly i živé ukázky možných technik využitelných útočníky, kam typicky spadá například spear phishing. Součástí školení před prezidentskými volbami byly i základní doporučení pro mediální komunikaci, kterými by se volební štáby měly řídit a které vycházely ze zkušeností Úřadu. Právě živé ukázky, konkrétní doporučení a příklady skutečných, doložených útoků byly účastníky nejvíce oceňovány.

8. MEZINÁRODNÍ SPOLUPRÁCE

Mnoho rozhodnutí podstatných pro vývoj kybernetické bezpečnosti v ČR je tvořeno nikoli pouze na vnitrostátní, ale také na mezinárodní úrovni. NÚKIB se proto snaží aktivně a efektivně zastupovat zájmy ČR v klíčových mezinárodních organizacích, zejména pak v EU, NATO, ale i Organizaci pro bezpečnost a spolupráci v Evropě (dále „OBSE"). V roce 2017 se pak práce Úřadu soustředila zejména na jednání s členskými státy i institucemi EU, a to především pokud jde o agendu směrnice NIS, jakož i nového souboru legislativních i nelegislativních aktů o kybernetické bezpečnosti, tzv. kybernetického balíčku, jenž byl Evropskou komisí představen v září a o kterém je konkrétněji pojednáno níže.

8.1 Evropská unie

Aktivity NÚKIB ve vztahu k EU se soustředily na implementaci směrnice NIS schválené v červenci 2016 a spolupráci v rámci Rady EU.

V kontextu směrnice NIS se kromě transpozice do vnitrostátní legislativy (viz výše) jednalo o aktivní účast na jednáních pracovních orgánů zřízených směrnicí, a to Skupiny pro spolupráci a Sítě CSIRT. Obě uskupení se v roce 2017 zaměřila na sdílení zkušeností s transpozicí směrnice se zaměřením na oblasti identifikace provozovatelů základních služeb a stanovení bezpečnostních a notifikačních požadavků na ně kladených. Důležitou součástí bylo rovněž nastavení mechanismů spolupráce a komunikace při incidentech postihujících více členských států. Pozitivně byla hodnocena prezentace českého přístupu k identifikaci subjektů regulovaných směrnicí NIS zástupci NÚKIB na jednání Skupiny pro spolupráci v září 2017 v Tallinnu.

V Radě EU je NÚKIB reprezentován vlastním zástupcem v Horizontální pracovní skupině pro kybernetické otázky (dále „HWPCI"), která se zabývá bezpečnostně politickými aspekty spolupráce v kybernetické bezpečnosti v EU. Hlavním tématem první poloviny roku 2017 byl rámec pro společnou diplomatickou odpověď na škodlivé aktivity v kyberprostoru, tzv. Cyber Diplomacy Toolbox, který představuje sadu diplomatických nástrojů, jež by členské státy a EU mohly využít pro reakci na kybernetické incidenty a nežádoucí aktivity v kyberprostoru. HWPCI vypracovala k rámci závěry Rady, schválené Radou pro zahraniční věci dne 19. června 2017, a následně příslušné vodítko, přijaté na úrovni Politicko-bezpečnostního výboru dne 11. října 2017.

V září roku 2017 Evropská komise představila soubor aktů legislativní i nelegislativní povahy, pracovně nazvaný „kybernetický balíček". Ten má jednak doplňovat směrnici NIS, jednak rozvíjet strategii kybernetické bezpečnosti EU z r. 2013. V jeho rámci byl předložen k projednání návrh nařízení zakotvujícího stálý a posílený mandát Evropské agentury pro bezpečnost sítí a informací (dále „ENISA") a vytvářejícího rámec pro jednotnou bezpečnostní certifikaci ICT produktů a služeb na území EU. Balíček také obsahuje tzv. Cooperation Blueprint, což je procesní dokument o zvládání přeshraničních kybernetických hrozeb. NÚKIB se aktivně účastní jednání v HWPCI, která byla pověřena zpracováním jak závěrů Rady ke kybernetickému balíčku (schváleny Radou pro obecné záležitosti dne 20. listopadu 2017), tak projednáním souvisejících legislativních návrhů.

NÚKIB v této skupině vytrvale prosazoval zájmy ČR, především pokud šlo o postoj ke společné certifikaci, ke spolupráci ve vzdělávání či k otázkám mezinárodního práva v kybernetickém prostoru.

Mezi další aktivity s EU dimenzí patřila též spolupráce NÚKIB s Úřadem vlády na digitální agendě, například ohledně volného toku dat či v přípravě na Digitální summit, který proběhl v září 2017 v Tallinnu.

V rámci ENISA se ČR i v roce 2017 účastnila výročního a dalších mimořádných jednání správní rady ENISA. Dva zástupci NÚKIB zde působí jako řádný člen a alternát, kde hájí zájmy ČR, sdílejí pohled ČR na vybraná témata kybernetické bezpečnosti a již tradičně se podílejí na schvalování programu, plánu prací a rozpočtu ENISA. V ČR slouží i tzv. National Liaison Officer (pracovník NÚKIB), který v každé členské zemi EU vykonává funkci referenčního bodu v specifických otázkách kybernetické bezpečnosti, zprostředkovatele spolupráce a podporovatele aktivit ENISA. ČR se v roce 2017 zúčastnila i veřejné konzultace k revizi mandátu ENISA, která vedla mimo jiné k výše zmíněnému požadavku na posílení mandátu ENISA. ENISA hraje dlouhodobě klíčovou roli v kybernetické bezpečnosti na úrovni EU. V souvislosti zejména s přijetím směrnice NIS pak ENISA získala další úkoly, jejichž efektivní plnění by současná podoba jejího mandátu omezovala.

8.2 Severoatlantická aliance

ČR pokračovala v plnění svých závazků v rámci NATO. Na Varšavském summitu v roce 2016 se v tzv. Cyber Defence Pledge spolu s ostatními spojenci zavázala posilovat bezpečnost svých národních sítí a neustále navyšovat odolnost proti kybernetickým útokům. Pro NATO proto počátkem roku připravila v úzké spolupráci NCKB a Ministerstvo obrany (dále „MO“) první zprávu o stavu svých kybernetických schopností. Dílčí části této zprávy byly vyzdvihnuty jako příklady dobré praxe i v souhrnném hodnocení spojenců, které zpracovala Emerging Security Challenges Division a které bylo předloženo Severoatlantické radě a následně na summit hlav států a vlád dne 25. května 2017. Aby ČR prokázala, že své závazky plní a kybernetické kapacity průběžně navyšuje, předloží toto hodnocení i v následujícím roce pro potřeby zpracování zprávy pro summit NATO, který se koná v červenci 2018.

Na půdě NATO ČR pokračovala i ve své účasti na NATO Smart Defence projektu Multinational Cyber Defence Education and Training (MN CD ET), jehož cílem je vyplnit mezery ve vzdělávání a školení v oblasti kybernetické bezpečnosti a obrany. Prohloubilo se zapojení v pracovní skupině, která připravuje vznik nového mezinárodního magisterského programu se zaměřením na právo v kybernetickém prostoru. ČR se ve spolupráci s portugalskou stranou ujala vedení skupiny a přípravy celého programu. Ústav práva a technologií na Masarykově univerzitě v Brně, kde by se NATO magisterský program měl primárně vyučovat, v těchto přípravách hraje zásadní roli.

8.3 Organizace pro bezpečnost a spolupráci v Evropě a další mezinárodní organizace a platformy

V roce 2017 pokračovala práce neformální pracovní skupiny OBSE zřízené rozhodnutím Stálé rady č. 1039, která se zabývá vytvářením a implementací opatření pro budování důvěry v oblasti kybernetické bezpečnosti (cyber CBMs). Účastnické státy projednávaly zejména návrhy na operacionalizaci CBM 3, směřujícího k vytvoření konzultačního mechanismu pro kybernetické incidenty a krize, a CBM 10, upravujícího komunikační kanály pro výměnu informací, proběhlo rovněž komunikační cvičení na procvičení CBM 8.

V činnosti pokračovala i Středoevropská platforma kybernetické bezpečnosti (Central European Cyber Security Platform, dále „CECSP"), která se ve formátu V4 + Rakousko schází od r. 2014, letos pod předsednictvím Slovenska. Diskutovány byly zejména možnosti větší koordinace v pracovních orgánech EU, NÚKIB v květnu 2017 zorganizoval cvičení kybernetické bezpečnosti Cyber Czech pro zástupce členů platformy (viz níže). V roce 2018 se ČR ujme předsednictví platformy.

Na půdě OSN pokračovalo v roce 2017 páté kolo jednání skupiny vládních expertů (UN GGE[3]) zabývající se současnými a novými hrozbami v oblasti kybernetické bezpečnosti, normami, pravidly a principy zodpovědného chování států v kyberprostoru, budováním opatření k posílení důvěry a mezinárodní spoluprací v oblasti ICT. Jednání skončilo v červnu 2017 nedohodou. Na podzim 2017 byla odstartována reflexe toho, jak dále postupovat. ČR nebyla členem UN GGE, nicméně vývoj pozorně monitorovala a v případě, že bude rozhodnuto o určité formě pokračování procesu, má zájem se jej aktivně účastnit.

8.4 Bilaterální a další spolupráce

V roce 2017 uskutečnila ČR řadu bilaterálních konzultací a jednání. ČR pokračovala ve spolupráci se strategickými partnery, tj. se Spojenými státy (USA), Izraelem a Jižní Koreou. V této souvislosti se dne 12. prosince 2017 v Soulu uskutečnilo druhé kolo strategických konzultací mezi ČR a Jižní Koreou. V rámci spolupráce s USA ČR absolvovala setkání s čelními představiteli, kteří se zabývají kybernetickou problematikou, například na úrovni kongresu Spojených států, NSA či FBI.

Ve spolupráci s Velkou Británií byl spuštěn projekt, který na základě grantu z Foreign & Commonwealth Office umožnil čerpat prostředky na specifická školení pro oblast kybernetické bezpečnosti pro českou bezpečnostní komunitu. V následujícím roce bude tato spolupráce pokračovat.

Jedním ze strategických zájmů ČR je také pomoc v oblasti budování kybernetických bezpečnostních kapacit. Tento zájem je rozvíjen například na Ukrajině, kde v této oblasti proběhlo několik školení. Další bilaterální spolupráce proběhla také s Marokem a Libanonem. Obě zmíněné země v roce 2018 plánují vyslání zástupců ze svých domácích CERT týmů do ČR.

[3] Plným jménem „Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security".

8.5 GÉANT/TF-CSIRT/Trusted introducer

Tým GovCERT.CZ je aktivním členem platformy TF-CSIRT, která sdružuje CERT týmy působící zejména v Evropě, a také je zapsán jako akreditovaný tým v adresáři Trusted Introducer. Platforma TF-CSIRT i adresář CERT týmů Trusted Introducer jsou zaštítěny evropskou organizací GÉANT.

Členství v této platformě umožňuje GovCERT.CZ účastnit se pravidelných setkání. Zde jsou diskutovány výzvy a problémy, jakým čelí CERT týmy, představovány nové projekty nebo výsledky výzkumů. V rámci této komunity si také na neveřejných jednáních nebo prostřednictvím uzavřeného zabezpečeného mailing listu týmy předávají informace týkající se kybernetických bezpečnostních incidentů a pozorovaných hrozeb.

Trusted Introducer poskytuje CERT týmům adresář ověřených kontaktů. Jedná se o službu, která je placena z příspěvků týmů se statutem „Accredited“ a vyšším, uvedení v adresáři se statutem „Listed“ pro tým nepřináší žádné náklady. V roce 2017 byl identifikován problém, který souvisí s českým Projektem FÉNIX. Tento projekt má jako jeden z požadavků na vstup podmínku provozování CERT/CSIRT týmu se statutem „Listed“ v Trusted Introducer. Tento požadavek vede k tomu, že adresář Trusted Introducer aktuálně obsahuje 30 týmů z ČR (nejvíce ze všech zemí společně s Francií). „Listed“ status týmu nikdy nebyl zamýšlen k podobnému využití a v kombinaci s tím, že k dosažení tohoto statutu v adresáři nejsou týmům ukládány žádné povinnosti a může se tedy o členství přihlásit libovolný tým, je pravděpodobné, že se v adresáři objeví zastaralé nebo neaktuální informace, případně již neaktivní týmy. To by mohlo mít negativní dopad na důvěryhodnost ČR v komunitě CERT/CSIRT týmů, čemuž se Vládní CERT spolu s Národním CERT týmem snaží aktivně předcházet a čelit.

8.6 The Honeynet Project

Dva členové GovCERT.CZ jsou od roku 2015 součástí výzkumné organizace „Honeynet Project“ (Honeynet.org), kde se společně s kolegy převážně z univerzitního prostředí podílejí na vývoji nových a úpravách stávajících open-source nástrojů využitelných pro boj s kybernetickými hrozbami.

Pracovníci GovCERT.CZ se pravidelně každý rok účastní Honeynet Project workshopu, který má za cíl setkání členů organizace z celého světa a současně uspořádání konference pro veřejnost. V rámci této události mají pracovníci možnost navazovat kontakty s lidmi z jiných států a organizací, kteří se věnují problematice honeypotů a bezpečnosti informačních technologií obecně. Získané kontakty umožňují konzultovat řešené problémy i s dalšími světovými odborníky.

V souvislosti s řešením problematiky honeypotů byly na Masarykově univerzitě v Brně vypsány jedna bakalářská práce a jedna diplomová práce. Výsledky obou prací byly zveřejněny v rámci organizace Honeynet a jsou také přístupné on-line na platformě GitHub.

V rámci bakalářské práce byl vytvořen rámec pro automatizované analýzy webů s využitím klientského honeypotu emulujícího webový prohlížeč. Diplomová práce se zaměřila na implementaci hlavních myšlenek staršího a neudržovaného honeypotu do nového honeypotu. Vzniklý honeypot je implementován v jazyce

Python, který využívá většina aktuálních honeypotů s cílem umožnit jeho snadnější udržování a rozšiřování o další funkcionalitu.

V průběhu roku pokračovali zaměstnanci GovCERT.CZ v přípravě virtuální image s honeypoty pro distribuci do míst nasazení. S tím souvisí i příprava centrálního sběrného místa, do kterého se budou zasílat události zaznamenané jednotlivými honeypoty.

Ministerstvo vnitra v rámci provozování dohledového pracoviště eGovernmentu vybudovalo systém Honey Net, který bude nadále testován v rámci spolupráce mezi NÚKIB a MVČR.“

9. CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI

I v roce 2017 byl Úřad zapojen do cvičení v oblasti kybernetické bezpečnosti. Technické cvičení Cyber Czech 2016 bylo v roce 2017 pořádáno NÚKIB, ve spolupráci s Ústavem výpočetní techniky Masarykovy univerzity (dále „ÚVT MU"), ve třech opakováních. NÚKIB, přesněji oddělení vzdělávání a cvičení, rovněž uspořádal mobilní table-top cvičení pro národní a mezinárodní partnery, totéž cvičení bylo uskutečněno i během konference CyberCon Brno 2017. ČR je do cvičení kybernetické bezpečnosti zapojená taktéž aktivně například v rámci cvičení Cyber Coalition 2017 nebo mezinárodním technickém cvičení Locked Shields, kde v roce 2017 obsadila první příčku.

9.1 Technické cvičení Cyber Czech 2017

9.1.1 Cyber Czech 2016 #2

Na přelomu ledna a února 2017 proběhl druhý běh cvičení Cyber Czech, které se poprvé uskutečnilo v říjnu roku 2016. Cvičení pořádané v té době ještě za působení NCKB v rámci struktur NBÚ ve spolupráci s ÚVT MU v Brně mělo za cíl ověřit praktické znalosti zvládání kybernetických incidentů v souvislosti s ochranou prvků KII včetně komunikace s médii při zvládání nastalé krize. Cvičení bylo opět provedeno ve speciálně upravené infrastruktuře kybernetického polygonu ÚVT MU.

Cvičení bylo zasazeno do scénáře obrany informační infrastruktury fiktivní železniční stanice a zabránění vykolejení vlaku s radioaktivním odpadem. Tentokrát se cvičení v roli obránců, tzv. modrých týmů, zúčastnili zástupci především z úřadů krajů ČR, ale i soukromých subjektů jako bank, či mobilních operátorů. Na informační systémy útočil tým hackerů, tzv. červený tým, složený ze zaměstnanců Vládního CERT týmu a Masarykovy univerzity. V letošním roce zde byla role medií zastávána reálnými novináři, kteří dotvářeli realističnost scénáře svými dotazy na jednotlivé týmy a následnými články, které publikovali na fiktivním zpravodajském portále.

Cvičení zasazené do tohoto kontextu mělo v roce 2017 ještě dvě opakování (viz níže).

9.1.2 Cyber Czech 2016 #3

Třetí běh cvičení Cyber Czech, avšak vůbec první běh v anglickém jazyce pro zahraniční partnery, se uskutečnil na přelomu února a března 2017. Cvičení se účastnili zástupci balkánských států, a to Albánie, Bosny a Herzegoviny, Černé Hory, Kosova, Makedonie a Srbska. Státy byly pozvány v rámci projektu TAIEX, zaštítěného a financovaného Evropskou komisí. Účastníci byli vysláni především ze státních institucí těchto států.

Na předchozí běhy cvičení navazoval vždy evaluační workshop, na kterém byly prezentovány provedené útoky a reakce jednotlivých týmů na ně společně s doporučeními do budoucna. Účastníci mohli rovněž vést diskuzi se zástupcem útočícího týmu a své kroky tak interaktivně debatovat.

Cvičení přispělo k budování vztahů a důvěry mezi jednotlivými státy a šíření povědomí o kybernetických útocích, potažmo incidentech a jejich řešení. Dále byla propagována důležitost takových cvičení a jejich význam pro vzdělávání bezpečnostních expertů v této oblasti. Výše uvedené bylo šířeno i mezi pozorovateli, kteří byli na cvičení přizváni, a to konkrétně zástupci Cooperative Cyber Defence Centre of Excellence (dále „CCD CoE“) včetně jeho tehdejšího ředitele Svena Sakkova, USA či Izraele.

9.1.3 Cyber Czech 2016 #4

Poslední běh cvičení Cyber Czech a v pořadí druhý v anglickém jazyce byl uspořádán v květnu 2017. Cvičení bylo organizováno pro zahraniční partnery a mělo opět regionální charakter. Účastnili se jej zástupci států tzv. Středoevropské platformy pro kybernetickou bezpečnost, tj. ČR, Maďarska, Rakouska a Slovenska, konkrétně pak pracovníci CERT týmů, či národních bezpečnostních úřadů. Polsko se zúčastnilo v roli pozorovatele.

ČR byla zastoupena dvěma týmy. První tým byl složený ze zástupců CZ.NIC, správce Národního CSIRT, a druhý tým tvořili experti z GovCERT.CZ, kteří si vůbec poprvé cvičení vyzkoušeli ze strany bránícího, modrého týmu. V minulých cvičeních stáli na straně útočícího týmu. Jejich zapojení umožnilo získat další zpětnou vazbu, která bude prospěšná při plánování budoucích cvičení. Setkání zástupců států CECSP dále jen utužilo spolupráci v rámci této platformy. Cvičení bylo, kromě již zmiňovaného Polska, navštíveno rovněž pozorovateli z Francie, Rakouska či Slovenska.

9.2 Mobilní table-top cvičení

NÚKIB organizuje také mobilní netechnická table-top cvičení. Ta jsou připravována na míru pro národní i mezinárodní partnery. Těmi bývají například univerzity nebo organizace zajišťující kybernetickou bezpečnost v partnerských zemích. Letos poprvé proběhlo cvičení také jako součást Úřadem pořádané konference CyberCon Brno 2017. Takováto cvičení mohou plnit rozličné účely:

- **Sdílení získaného know-how** s našimi zahraničními partnery. ČR se snaží držet na předních příčkách, pokud jde o kvalitu a míru zkušenosti s netechnickými cvičeními. V rámci reciprocity je tedy tento produkt nabízen blízkým zahraničním partnerům.
- **Vzdělávání státních zaměstnanců** na vedoucích pozicích, obsahem jejichž agendy je i kybernetická bezpečnost nebo jsou touto problematikou přímo ovlivňováni. S tím, jak se informační a komunikační technologie stále hlouběji integrují do procesu výkonu státní správy, narůstá také cílová skupina netechnických cvičení. Úřad aktivně nabízí přípravu cvičení na míru relevantním státním institucím.
- **Pomoc při vzdělávání studentů**, kteří získají jedinečnou zkušenost z oblasti kybernetické bezpečnosti. Cvičení také pomůže cílovému publiku porozumět problematice a přilákat talentované studenty do tohoto oboru.

V roce 2017 organizoval úřad mobilní cvičení v rámci následujících akcí:

- **NATO Summer School**. Úřad v rámci letní školy vedl přednášku na téma hybridní války se zaměřením na kybernetický aspekt, po níž následovalo cvičení, kterého se zúčastnila dvacítka studentů pocházejících z různých evropských zemí. Letní školu organizoval Prague Security Studies Institute.

- **Konference CyberCon Brno 2017**. Součástí úřadem organizované konference bylo krátké cvičení nabízené účastníkům v podobě workshopu.

- **Předmět Kybernetická bezpečnost v rámci magisterského programu Bezpečnostní a strategická studia na Masarykové univerzitě**. Součástí předmětu, na jehož obsahu se významnou měrou úřad podílí, je i cvičení, které dává studentům možnost projít si krizovou situací a vžít se do role rozhodovacích orgánů.

- **Program on Cyber Security Studies**. Jedná se o prestižní kurz pořádaný George C. Marshall European Center for Security Studies. Úřad byl jeho organizátory osloven s žádostí o uspořádání cvičení, které by sloužilo jako modelový příklad pro účastníky kurzu, který je určen pro vedoucí pracovníky v oblasti kybernetické bezpečnosti. Cvičení proběhlo dne 19. prosince pro více než 90 účastníků z 52 zemí světa. Tito účastníci si prošli dvouhodinovým eskalujícím scénářem, odehrávajícím se ve stresovém prostředí. Domů si odvezli nejen celý obsah cvičení, které mohou dále upravovat a používat na národní úrovni, ale rovněž příručku, jak takováto cvičení sami tvořit a vést. Šlo o unikátní příležitost, která NÚKIB umožnila sdílet svoje know-how a navázat kontakty s experty na poli kybernetické bezpečnosti z celého světa.

9.3 Crisis Management Exercise 2017

V roce 2017 proběhl další ročník pravidelného cvičení orgánů krizového řízení Crisis Management Exercise (CMX), a to v datech 4. až 11. října. Jedná se o akci pořádanou NATO, zaměřenou na strategickou úroveň rozhodování. Během cvičení nedochází k reálnému rozvinutí vojenských jednotek. Cvičení je velmi komplexní, kybernetická bezpečnost je tedy pouze jednou z jeho komponent a rovin. Právě svojí komplexitou je cvičení výjimečné a tvoří velkou část přidané hodnoty.

Letošní ročník se zaměřoval na využití článku 4 a 5 Severoatlantické smlouvy během krizové situace, dále také zohlednil rozhodnutí přijatá na summitu NATO ve Varšavě. Scénář byl zasažen do fiktivní geopolitické situace a jeho součástí byla hybridní kampaň vedená protivníkem. V rámci cvičení došlo i ke koordinaci a synchronizaci krizových procedur s EU.

NÚKIB se na cvičení podílí jak během přípravné, tak také prováděcí fáze, a to především v rámci části scénáře věnujícího se kybernetické bezpečnosti. Primárním koordinátorem cvičení na národní úrovni je MO.

9.4 Cyber Coalition 2017

Na přelomu listopadu a prosince 2017 se ČR v zastoupení MO ČR a NÚKIB již po sedmé zúčastnila mezinárodního aliančního cvičení kybernetické bezpečnosti Cyber Coalition. Primárním cílem cvičení bylo procvičit technickou i netechnickou koordinaci při řešení kybernetických bezpečnostních incidentů a zlepšit vzájemnou informovanost o stávajících obranných schopnostech. Letos bylo do cvičení zapojeno více než 900 techniků a IT odborníků, vládních zaměstnanců a expertů na kybernetickou bezpečnost z více než 28 členských a partnerských zemí, včetně EU a pozorovatelů.

Cvičení je zasazeno do fiktivního geopolitického kontextu, ve kterém došlo k několika incidentům, které se sebou mohou, ale nemusí, být propojeny. Úkolem národních koordinátorů cvičení je incidenty zasadit do národního kontextu a cvičení tak udělat pro cvičící více realistické. To bylo i letos úkolem MO ČR a NÚKIB. Cvičení se účastnily tzv. společné týmy složené ze zástupců několika subjektů. Mezi ně patřili zástupci státní správy (MO, NÚKIB, Úřad pro zahraniční styky a informace, Bezpečnostní informační služba, Vojenské zpravodajství, Ministerstvo zahraničních věcí, Policie ČR, Jihomoravský kraj), soukromého sektoru (CSIRT.CZ, Avast) a akademické sféry (CSIRT-MU, Univerzita Tomáše Bati ve Zlíně). Experti byli dle svého odborného zaměření rozděleni do dílčích skupin. Paralelně tak řešili incidenty na SCADA systémech, exfiltraci a šifrování dat, ke kterému docházelo v síti českého kontraktora, který dodával komponenty do vojenské mise, kompromitaci Android zařízení či kybernetickou špionáž probíhající prostřednictvím zařízení s bezdrátovým připojením. Jelikož integrální součástí řešení kybernetických incidentů je také posuzování právních aspektů, byly technické týmy nuceny konzultovat své kroky s právníky.

Oproti cvičení Locked Shields nejsou výstupy jednotlivých týmů bodovány. I přesto organizátoři cvičení velmi ocenili postup českých odborníků při řešení scénáře na Cyber Range. Jejich analýza se stala součástí doporučeného řešení distribuovaného všem zapojeným státům. Češi si vedli výborně i v ostatních scénářích, o čemž svědčí také rychlost, se kterou se jim podařilo všechny úkoly vyřešit. Vzhledem k tomu, že se experti z GovCERT.CZ zúčastnili cvičení poprvé od oddělení od NBÚ v srpnu 2017, bylo cvičení přínosné i pro procvičení procesů, které byly migrovány.

9.5 Locked Shields 2017

Od 24. do 27. dubna 2017 se uskutečnil již 8. ročník největšího mezinárodního technického cvičení kybernetické bezpečnosti Locked Shields (LS17). Cvičení je pořádáno prostřednictvím NATO CCDCoE v Tallinnu v Estonsku. Zapojilo se do něj přes 900 odborníků z 25 zemí včetně ČR. V této konkurenci se podařilo ČR obsadit první příčku. Na druhém místě skončil tým z Estonska a na třetím tým NCIRC NATO. Vítězný český tým byl složen ze zástupců GovCERT.CZ a dalších subjektů bezpečnostní komunity ze státní, soukromé i akademické sféry. Kromě modrého týmu měla ČR své zástupce v týmu organizátorů a poprvé rovněž také v týmu útočníků. Účast v plánovacích týmech představuje pro pracovníky NÚKIB jedinečnou zkušenost, jelikož nabité znalosti a dovednosti mohou dále uplatňovat při vývoji národních cvičení.

Locked Shields je simulací útoků tzv. červeného týmu na systémy a sítě tzv. modrých týmů, složených z expertů, kteří v reálném světě IT systémy chrání každodenně. Pro autentičnost je cvičení založeno na scénáři, který pro účastníky zasazuje v reálném čase probíhající útoky do geopolitického kontextu. V průběhu letošního cvičení bylo mimo jiných úkolem modrého týmu zachování funkčnosti služeb a udržení chodu sítí vojenské letecké základny ve fiktivní zemi. Kromě toho byl tým pod tlakem také díky četným dotazům fiktivních médií a řešením právních úkolů.

Novinkou letošního ročníku byla vedle technické části paralelně probíhající strategická hra. Jejím cílem bylo upozornit na rozdílnost technického řešení incidentu a rozhodovacího procesu při jeho eskalaci. Jelikož se jednalo o pilotní projekt, nebyla strategická část bodována.

10. VZDĚLÁVÁNÍ A OSVĚTA

Jednou z úloh NÚKIB je také osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti, což představuje stálou spolupráci s vysokými, středními, ale i základními školami. V letošním roce probíhala například intenzivní spolupráce s Univerzitou obrany v Brně, se Střední školou informatiky, poštovnictví a finančnictví v Brně či ověřování pilotní fáze výukového modulu *Digitální stopa* na základních školách. Během roku 2017 byl taktéž vytvořen nový e-learningový výukový program pro zaměstnance veřejné správy ve spolupráci s odborem kybernetické bezpečnosti a koordinace ICT Ministerstva vnitra ČR.

10.1 Spolupráce s vysokými, středními a základními školami

10.1.1 Výuka vlastního předmětu „Kybernetická bezpečnost“

Již třetím rokem NÚKIB pokračuje ve výuce jednosemestrálního předmětu s názvem *Kybernetická bezpečnost* na Fakultě sociálních studií Masarykovy univerzity v Brně a na Přírodovědecké fakultě Univerzity Palackého v Olomouci. Předmět zahrnuje témata, jako jsou konceptuální, historické aspekty, role bezpečnostních CERT/CSIRT týmů a jejich constituency, politicky motivované a destruktivní útoky, propaganda a informační válka, komparace přístupů k zajišťování kybernetické bezpečnosti hlavních světových aktérů či kyberkriminalita. Dílčí přednášky vybraných zástupců úřadu jsou pořádány i na CEVRO institutu a Prague Security Studies Institute.

10.1.2 Vedení vlastního kurzu „Analýza otevřených zdrojů“ na FSS MU

V roce 2017 byla zahájena vlastní výuka předmětu *Analýza otevřených zdrojů*, jehož cílem je předat studentům prakticky orientované dovednosti v této aktuální oblasti. Studenti jsou v rámci kurzu seznámeni se základními technikami analýzy bezpečnostních otázek a po jeho absolvování budou schopni bezpečně vyhledávat informace v otevřených zdrojích, aktivně aplikovat nástroje analýzy bezpečnostních otázek na relevantní problémy ČR, EU nebo NATO, identifikovat implikace pro zákazníka a navrhnout doporučení.

10.1.3 Spolupráce s Univerzitou obrany v Brně

Na základě již dříve uzavřené dohody o spolupráci v současnosti probíhá spolupráce na sestavení nového pětiletého studijního programu *Kybernetická bezpečnost* s Univerzitou obrany v Brně. Tento obor má zahrnovat ucelený blok odborných přednášek a cvičení pro studenty Fakulty vojenských technologií. Komplexně se má zabývat tématy kybernetické bezpečnosti a IT. V rámci spolupráce je dále připravován jednosemestrální kurz *Kybernetická bezpečnost*, který bude pokrývat jak technická témata a praktické přípravy z činnosti CERT, tak témata bezpečnostně strategického a právního charakteru z gesce OKBP. Realizace kurzu je plánovaná na červen roku 2018.

10.1.4 Spolupráce se Střední školou informatiky, poštovnictví a finančnictví, Brno

V září 2017 byla zahájena pilotní výuka nového oboru *Kybernetická bezpečnost*. V souvislosti s touto výukou byla uspořádána exkurze pro vyučující na pracoviště NÚKIB včetně podrobného představení jeho činnosti. Úřad byl také touto školou osloven, aby se podílel na tvorbě vznikajícího Školního vzdělávacího

programu (ŠVP), kde uplatnil své připomínky. Nyní je v přípravě rámcová smlouva o spolupráci, kde budou konkretizovány oblasti spolupráce.

Pilotáž nového oboru *Kybernetická bezpečnost* byla zahájena také na Smíchovské střední průmyslové škole v Praze, kde je plánované též bližší navázání kontaktů, sdílení informací a případné navázání spolupráce.

V uplynulém roce bylo v rámci uskutečněného mapování navázaná spolupráce i s dalšími středními školami, konkrétně se Střední školou informatiky a služeb ve Dvoře Králové a Střední školou technickou a ekonomickou v Brně. Obě zmíněné školy se v rámci oboru ICT hodlají blíže věnovat též kybernetické bezpečnosti. Dá se předpokládat, že zájem o tento obor bude v nejbližší době značně narůstat i u dalších středních škol. NÚKIB je proto připraven poskytnout metodickou a obsahovou podporu dalším školám.

10.1.5 Pásmo přednášek pro Integrovanou střední školu automobilní v Brně

Na základě přání tamního metodika prevence zástupci NÚKIB uspořádali celé pásmo přednášek týkajících se kybernetické bezpečnosti a její důležitosti coby prevence různých druhů rizikového chování. Cílovou skupinou byli žáci různých oborů i ročníků. V příspěvcích bylo primárně cíleno na digitální stopu, její význam a co vše z ní lze vyčíst. Žáci se tak mohli například dozvědět a prakticky zjistit, co jde zjistit a použít například z facebookového archivu. Některé přednášky probíhaly ve spolupráci se zástupcem Krajského ředitelství Policie ČR Jihomoravského kraje. Přítomný policista tak příspěvek doplňoval svými postřehy a zkušenostmi z praxe při vyšetřování kybernetické trestné činnosti.

S žádostí o obdobné vystoupení byli zástupci oddělení vzdělávání a osvěty z NÚKIB pozváni i do Amerického centra při Velvyslanectví USA v Praze. Zde se v souvislosti s digitální stopou podrobně věnovali důležitosti ochrany osobních a citlivých údajů, problematice kyberšikany v ČR (nejen žáků, ale též například učitelů), hate crime, potažmo nenávistným projevům a jejich šíření. Zmíněna byla i nezbytnost kritického myšlení a sebevzdělávání vzhledem k mnoha druhům současných zdrojů informací, které je třeba pečlivě zhodnocovat.

10.1.6 Spolupráce se základními školami

Na úrovni základního školství a víceletých gymnázií pokračuje pilotní ověřování interaktivní vzdělávací aktivity s názvem *Digitální stopa*, která se zabývá problematikou rizikového chování v prostředí Internetu a sociálních síti s důrazem na patologické jevy jako např. kyberšikana či sexting. Ukončení pilotní fáze je plánováno s dosažením počtu dvaceti testovaných škol. NÚKIB poté aktivitu bezplatně poskytne i dalším školám skrze krajské manažery prevence kriminality.

10.2 E-learning pro veřejnou správu

Během roku 2017 byl vytvořen nový e-learningový výukový program pro zaměstnance veřejné správy. Tento úkol vycházel jednak z Akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020, a také z Akčního plánu pro společnost 4.0, vypracovaného Úřadem vlády.

NÚKIB zpracoval celý obsah, zajistil jeho import do platformy Moodle a rovněž vytvořil grafický design a doplnil jej vlastními obrazovými materiály. Výukový program Moodle navíc umožňuje vložit do kurzu také audiovizuální materiály, praktické příklady a evaluační nástroje pro zpětnou vazbu. Celkově je prostředí kurzu nastaveno interaktivně a uživatelsky přívětivě.

Obsahově se e-learning skládá ze dvou výukových modulů (A a B). Modul A – Základní kurz kybernetické bezpečnosti je určen všem běžným uživatelům, kde se věnuje zásadám bezpečného chování na Internetu s ICT prostředky v kontextu širší kybernetické bezpečnosti. Jedná se o základní povinné pensum znalostí a dovedností, které by měli mít a využívat zaměstnanci veřejné správy při práci i v soukromí. Modul B – Kurz kybernetické bezpečnosti dle ZKB je zaměřený na zaměstnance zastávající role podle ZKB. V říjnu 2017 byl spuštěn modul A, modul B byl následně spuštěn v lednu 2018.

10.2.1 Školení pro uživatele z řad veřejné správy

V dubnu 2017 bylo na základě žádosti vedení Ministerstva pro místní rozvoj (MMR) uspořádáno podrobné školení pro běžné uživatele. Školení zahrnovalo celou škálu bezpečnostních zásad a pravidel práce s ICT a každá z nich byla doplněna praktickým případem, potažmo kazuistikou. Zaměstnanci tak získali nejen ucelený přehled o současných hrozbách v kyberprostoru, ale i rad, jak nejrůznější rizika eliminovat. Školení bylo pojato plošně pro všechny zaměstnance, kde jsme proškolili cca 800 osob. Obdobné školení bylo v říjnu 2017 uspořádáno také pro zaměstnance Nejvyššího soudu v Brně.

10.2.2 Spolupráce s odborem bezpečnostní politiky a prevence kriminality na MV

V tomto roce NÚKIB taktéž navázal na spolupráci s MV v oblasti prevence kriminality. Kybernetická bezpečnost vs. kybernetická kriminalita se stává stále aktuálnějším tématem nejrůznějších cílových skupin zejména široké veřejnosti. V této věci byla ustavena pracovní skupina a pravidelná setkání krajských manažerů prevence kriminality, kam byl NÚKIB tento rok nově přizván. Zde Úřad na úvod představil svou činnost a prezentoval své projekty a aktivity. Krajští manažeři prevence kriminality jsou zde považováni za velmi důležité styčné body k distribuci aktivit Úřadu.

10.2.3 Spolupráce s Národním ústavem pro vzdělávání

V rámci této spolupráce jsou zástupci NÚKIB součástí pracovní skupiny, která má za úkol revidovat Rámcový vzdělávací program (RVP) pro obor *Informační a komunikační technologie* s cílem začlenit kybernetickou bezpečnost do osnov výše uvedeného tématu. Z pozice národní autority kybernetické bezpečnosti v ČR Úřad cílí na pevné zasazení výuky této oblasti do konkrétních předmětů a jejího rozšíření do co nejširšího spektra základních a středních škol.

PŘÍLOHY

11. Příloha č. 1 – Nejvýznamnější incidenty šetřené GovCERT.cz za rok 2017

V průběhu roku 2017 obdrželi pracovníci GovCERT.CZ od českých i zahraničních partnerů v souhrnu 248 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 50 kybernetických bezpečnostních incidentů spadajících do oblasti působnosti Vládního CERT, tedy KII, VIS a veřejné správy.

V rámci řešení incidentů byl vždy kladen důraz na rychlé kontaktování zodpovědných osob dotčených institucí a subjektů, případně dohledání dalších možných potenciálních obětí a jejich informování o možném riziku. Na základě zpětné vazby od dotčených subjektů víme, že díky varováním zaslaným vládním CERT týmem došlo k zabránění kybernetickému útoku. Pokud by Vládní CERT dostával zpětnou vazbu od všech subjektů, kterým varování posílá, byl by schopen dopad svých činností vyhodnotit lépe.

V prvním měsíci nového roku byl nahlášen incident, kdy začalo docházet k zamykání poštovních schránek zaměstnanců vrcholné instituce státní správy. Během analýzy probíhajícího incidentu se objevily nové skutečnosti, které nakonec vedly ke vzniku nového incidentu. Tento incident lze považovat za nejvážnější incident, který tým GovCERT.CZ řešil v měsíci lednu. Došlo ke kompromitaci administrátorského účtu k databázi Lotus Notes. Útočník měl přístup k emailovým schránkám pracovníků dané instituce a svého oprávnění opakovaně využíval ke sledování několika poštovních schránek, včetně vrcholových představitelů. Útočník pravidelně stahoval velký objem dat. Po spolupráci s Národním centrem kybernetické bezpečnosti přijali pracovníci dotčené instituce náležitá opatření.

Měsíc leden se taktéž vyznačoval početnými DDoS útoky. Na počátku měsíce byly uskutečněny dva DDoS útoky na státní instituci, i přestože se útok vyznačoval velkou silou, tak při těchto útocích nevznikla žádná škoda. Následující DDoS útok byl směřován na systém státní správy. Útok byl prováděn hlavně ze zahraničí a jeho velikost dosahovala ve špičkách masivních hodnot. Útok byl veden z velkého počtu zdrojových IP adres a využíval protokoly ICMP a UDP. Následující DDoS útok, byl mířen na systémy KII, VIS a probíhal v podstatě ze všech koutů světa, při útocích nevznikla žádná škoda. Útok byl realizován formou amplifikačního DNS DDoS útoku. K závěru měsíce se objevil další DDoS útok o menší síle, kdy nedošlo k žádným škodám.

Během února tým GovCERT.CZ řešil incident neznámého útočníka, který vytvořil kopii webových stránek státní instituce. Nicméně útočník nezůstal pouze u vytvoření této kopie, v dalším kroku si útočník zaregistroval doménu, která připomínala doménu dotčené instituce. Pod touto doménou rozesílal podvodné emailové zprávy, ve kterých nabádal ke vstupu na podvodné stránky prostřednictvím vloženého odkazu. Za tímto

odkazem se nacházel škodlivý soubor. Ke konci měsíce byl také nahlášen incident, který cílil na klienty bankovní instituce, útok spočíval v rozeslání podvodných zpráv a pokusu o vylákání přihlašovacích údajů.

V březnu pokračoval trend DDoS útoků, který jsme viděli na počátku roku. Terčem dvou DDoS útoků se stala státní instituce. V průběhu měsíce byl také nahlášen phishing mířený na představitele státní instituce, tento podvodný email obsahoval škodlivý soubor, na základě provedené analýzy tým GovCERT.CZ zjistil, že se jednalo o Hancitor malspam.

Počátek měsíce dubna pokračoval v nastoleném trendu z předchozího měsíce, NCKB obdrželo hlášení o dalším phishingovém útoku mířící na klienty bankovní instituce. Nejzávažnějším incidentem v měsíci dubnu byl uskutečněný ransomware útok, kdy došlo k zašifrování dat na uživatelské stanici poté, co uživatel otevřel škodlivý soubor, jenž obdržel jako přílohu emailové zprávy. Významný incident se odehrál ke konci měsíce, kdy došlo ke zneužití emailového účtu zaměstnance státní instituce. Kompromitovaný emailový účet poté rozesílal nevyžádané emailové zprávy ostatním uživatelům.

Začátkem května byl NCKB nahlášen masivní DDoS útok na médium veřejné služby, tento útok byl výjimečný svým rozsahem, neboť útok pocházel z celého světa. V průběhu května detekovala státní instituce skenování svých serverů, které jsou přístupné z internetu. Z provedené analýzy vyplynulo, že se jedná patrně o Mirai botnet. Závěrem května NCKB řešilo podezřelou komunikaci, která probíhala uvnitř státní instituce. Po analýze bylo zjištěno, že se jednalo o botnet síť, se kterou komunikovaly dvě pracovní stanice. Nejednalo se o prokázané napadení, pouze počítač ze sítě komunikoval se serverem, který byl uveden ve více reputačních databázích jako šiřitel ransomware.

V měsíci červnu detekovala sonda vrcholné státní instituce komunikaci koncových stanic s botnetem. Podle provedené analýzy se jednalo o útok typu typosquating. V tomto případě útočník spoléhal na to, že uživatel špatně zadá adresu webového serveru a jeho počítač poté přistoupí na škodlivou stránku.

Nevšední incident musel tým GovCERT.CZ řešit v červenci, kdy došlo k nahlášení úniku dat ze strany instituce státní správy. Rozsah úniku čítal tisíce dokumentů a tyto dokumenty byly vyneseny zaměstnancem, jemuž měla vypršet pracovní smlouva.

V srpnu byl NÚKIB nahlášen výskyt ransomwaru Lokitus. Malware postihl část systému, kterou se podařilo obnovit ze zálohy a větší dopady tak neměl. Rovněž bylo nahlášeno několik útoků typu DDoS. Jednalo se o útoky na služby DNS, z nichž se některé podařilo mitigovat.

Během měsíce září NCKB zaznamenalo několik významnějších hlášení týkajících se útoků DDoS. Útočníci v některých případech využívali státní organizace k amplifikačním útokům, kde útočník podvrhne zdrojovou adresu a nahradí ji za adresu oběti.

V prvním měsíci posledního kvartálu probíhaly volby do Poslanecké sněmovny. V minulosti již bylo mnohokrát prokázáno, že volební systém je velmi oblíbeným cílem hackerů, kteří mají v úmyslu jakkoliv narušit průběh voleb. ČR není výjimkou a NÚKIB byl na různé situace připraven. Volební systém byl během roku 2017 prověřen a ve spolupráci s ČSÚ se pracovalo na zvýšení bezpečnosti celého volebního procesu. Ačkoliv byl

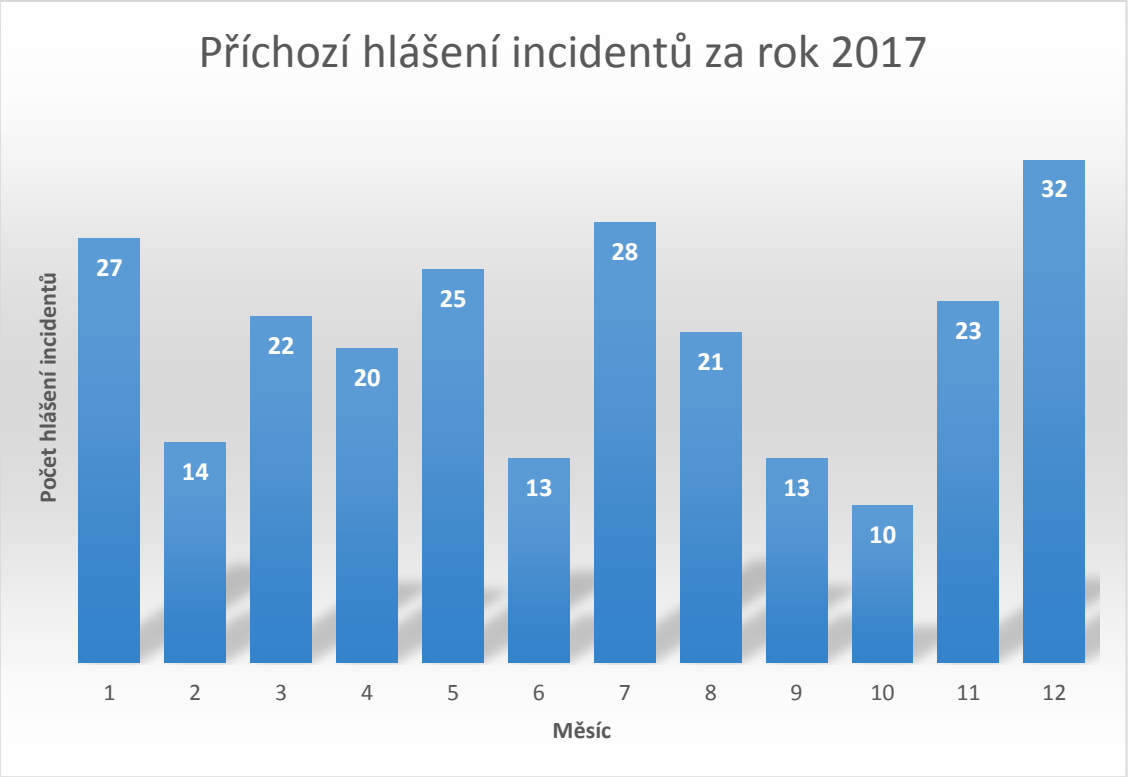
zaznamenán DDoS útok na webovou prezentaci ČSÚ, především servery volby.cz a volbyhned.cz, které médiím a občanům poskytují přehled o průběžných výsledcích sčítání, nedošlo k narušení samotného sčítání ani k manipulaci s výsledky voleb.

Během měsíce října dále NCKB zaznamenalo několik hlášení phishingových útoků. Některé z útoků byly sofistikovanější a zaměřovaly se na konkrétní organizace, kde docházelo k plošným útokům na zaměstnance za cílem získat přístupové údaje k jejich e-mailovým účtům.

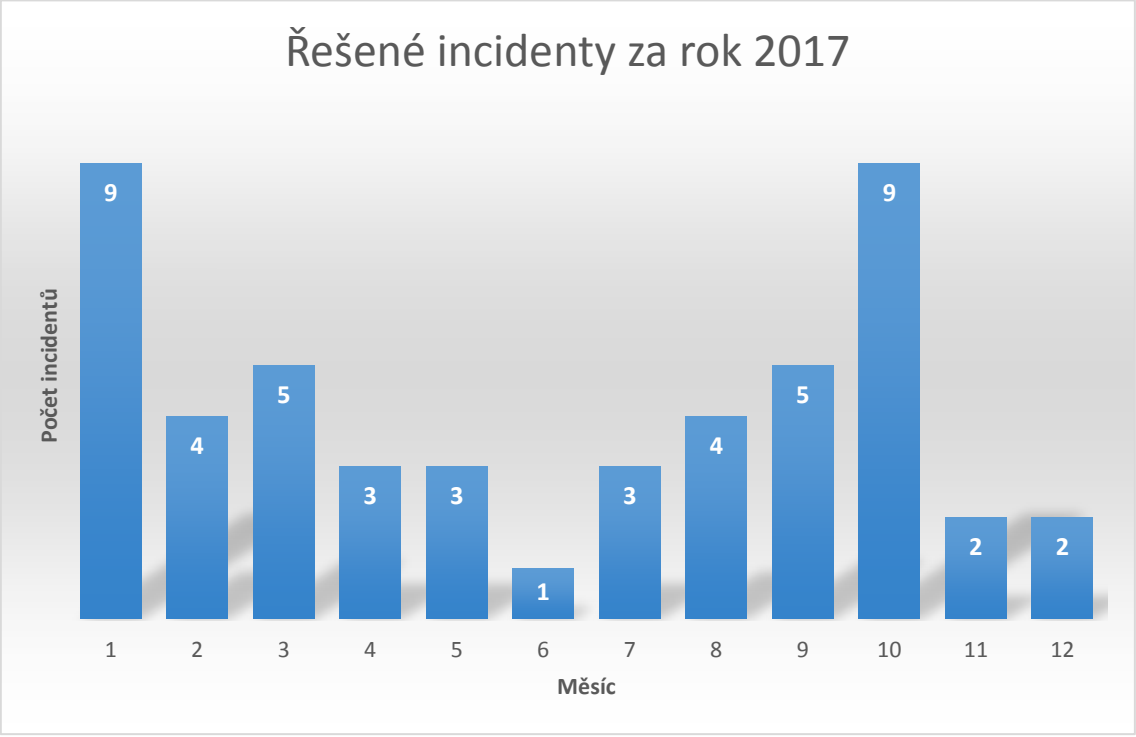
V posledním čtvrtletí tohoto roky byly řešeny vyděračské emaily, které po adresátech požadovaly zaplacení finančního obnosu ve virtuální měně bitcoin výměnou za neprovedení cíleného DDoS útoku, tato hrozba byly doprovázena demonstrativním útokem, tyto výhružky ukazují trend, který se opakuje každoročně.

12. Příloha č. 2 – Statistické údaje o incidentech

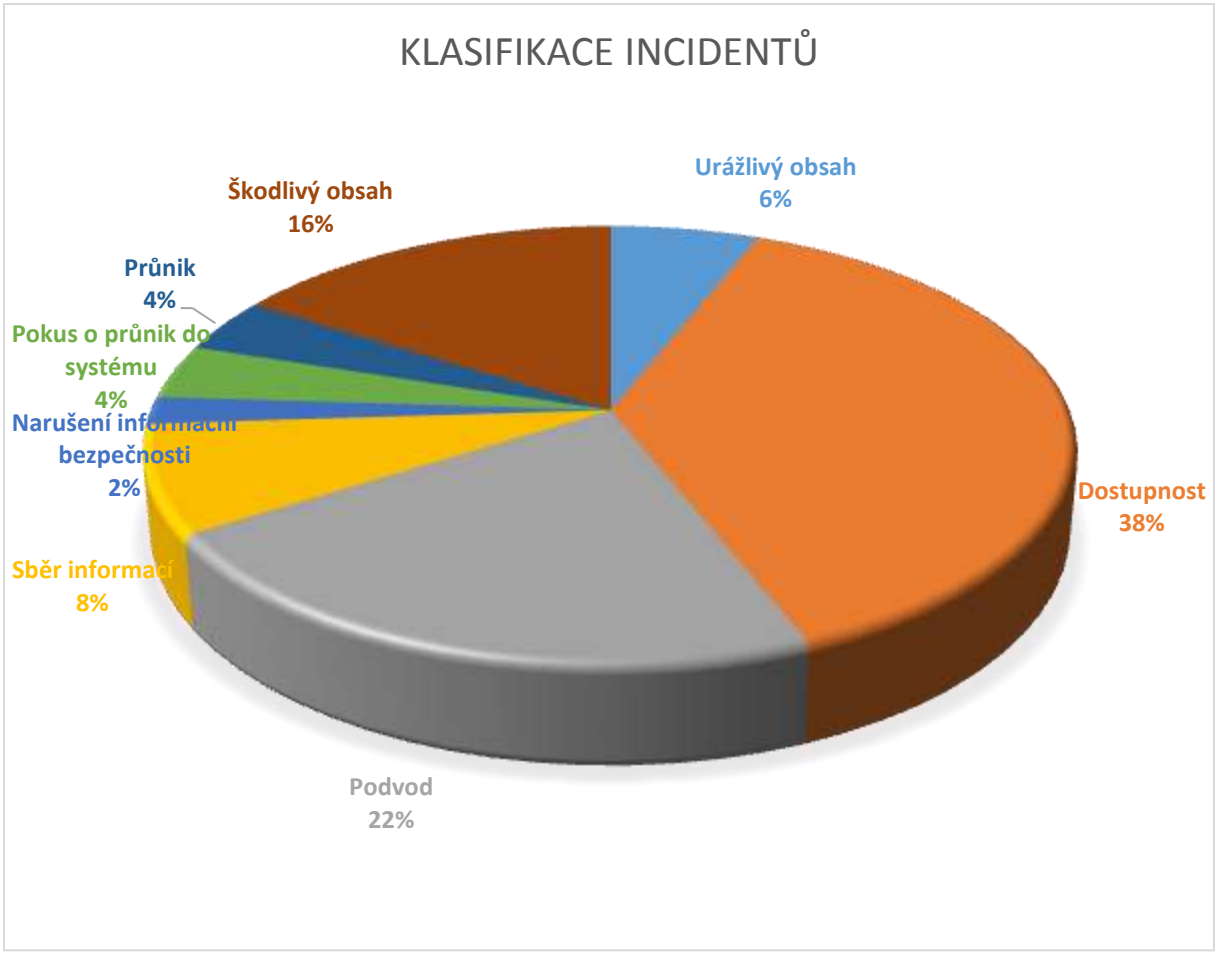
Grafy zachycují počty přijatých hlášení, řešených incidentů a jejich klasifikaci v roce 2017.



Graf 3 - počet příchozích hlášení o incidentech za jednotlivé měsíce v roce 2017



Graf 4 – počet řešených incidentů za jednotlivé měsíce v roce 2017



Graf 5 - klasifikace řešených incidentů za rok 2017

Popis kategorií vychází z formuláře pro hlášení incidentů[4]:

- Urážlivý obsah (např. spam, kyberšikana, nevhodný obsah)
- Škodlivý obsah (např. virus, červ, trojský kůň, dialer, spyware)
- Sběr informací (např. skenování, sniffing, sociální inženýrství)
- Pokus o průnik do systému (např. pokus zneužití zranitelnosti, kompromitace aktiva, "0-day" útok)
- Průnik (např. úspěšná kompromitace aplikace nebo uživatelského účtu)
- Dostupnost (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)

[4] K dispozici na: https://www.govcert.cz/cs/vladni-cert/hlaseni-incidentu/ .

- Narušení informační bezpečnosti (např. neautorizovaný přístup nebo neautorizovaná změna informace, atd.)
- Podvod (např. phishing, neoprávněné využití ICT - porušení licenčních práv, krádež identity, aj.)
- Administrativní = tato kategorie se liší od kybernetických incidentů. Příkladem může být soudní rozhodnutí o vypnutí systému, který je součástí KII / VIS

13. Příloha č. 3 – Další osvětová a přednášková činnost NÚKIB

Pracovníci všech oddělení se aktivně účastní konferencí, odborných diskusí, přednášek na vysokých školách a jiných vzdělávacích aktivit, jejichž výběr je popsán níže podle čtvrtletí, ve kterém probíhaly:

PRVNÍ ČTVRTLETÍ

- 15. březen: Přednáška na téma „aktéři kybernetické bezpečnosti“ v rámci Joint Command and General Staff Course, Baltic Defence College, Tartu, Estonsko.
- 22. – 23. březen: Příspěvek na téma: „Výstavba NCKB a jeho úloha v kybernetické bezpečnosti ČR“ v rámci odborná konference spojovacího vojska AČR, Praha
- 30. březen: „National security threats: Czech perspective“ na XIII. Brněnské politologické sympozium: (Ne)bezpečnost ve střední Evropě. FSS MUNI, Brno

DRUHÉ ČTVRTLETÍ

- 4. – 5. duben: Školení: Bezpečné používání ICT pro Ministerstvo pro místní rozvoj
- 10. duben: Přednáška: Zákon o kybernetické bezpečnosti v souvislostech
- 26. duben: Kurz: Zákon o kybernetické bezpečnosti v praxi I
- 27. duben: Přednáška na téma „kybernetická bezpečnost vs. kybernetická kriminalita“ Valašské Meziříčí
- 4. květen: Kurz: Zákon o kybernetické bezpečnosti v praxi II
- 17. květen: Přednáška na téma „digitální stopa“ ve spolupráci pro Integrovanou střední školu Automobilní s Krajským ředitelstvím Policie Jihomoravského kraje
- 18. květen: Audit bezpečnostních opatření a zákon o kybernetické bezpečnosti
- 18. květen: Přednáška na téma „bezpečné používání ICT"
- 25. květen: Přednášky na téma „digitální stopa" a „kyberkriminalita"
- 30. květen: Vystoupení na konferenci IS2, Praha
- 26. červen: Školení: Bezpečné používání ICT pro Český statistický úřad
- 27. červen: Přednáška na téma „aktuální a nastupující kybernetické hrozby“ v rámci Summer University for Young Professionals, STRATPOL, Liptovský Mikuláš

TŘETÍ ČTVRTLETÍ

- 9. srpen: Exkurze a prezentace pro studenty letní školy Brno Summer School on IT Law pořádanou studentskou organizací ELSA Brno na NÚKIB
- 19. září: Bezpečnost chytrých měst
- 20. – 21. září: Konference a seminář CyberCon Brno 2017 – třetí ročník pořádaný NÚKIB

ČTVRTÉ ČTVRTLETÍ

- Říjen: Měsíc kybernetické bezpečnosti; Kulatý stůl organizovaný Národním centrem bezpečnějšího Internetu. Diskuze nad otázkami kybernetické bezpečnosti ve školním prostředí a nedostatku technických odborníků. Dále nad problematikou obsahu a začlenění kybernetické bezpečnosti do RVP, a také rozdílné dovednosti absolventů v oblasti kybernetické bezpečnosti na všech stupních škol.
- Říjen: Pásmo přednášek na téma „digitální stopa“ pro Integrovanou střední školu Automobilní ve spolupráci s Krajským ředitelstvím Policie Jihomoravského kraje
- 4. říjen: Vystoupení na konferenci ICS Security při FP VUT v Brně
- 16. říjen: Školení: Bezpečné používání ICT pro Nejvyšší soud
- 19. – 20. říjen: Mezinárodní konference „Řešení elektronického násilí a kybernetické kriminality“ v Jihlavě, kterou pravidelně organizuje kraj Vysočina s Policií ČR. Na této akci byl prezentován příspěvek, který se věnoval průběžným výsledkům mapování vzdělávání v oblasti kybernetické bezpečnost na středních školách a gymnáziích.
- 25. říjen: „Evoluce kybernetických útoků a útočníků“ v rámci Bezpečnostního večeru na FSS MUNI, Brno
- 31. říjen: Přednáška na téma „digitální stopa“ pro Střední průmyslovou školu na Třebešíně
- Listopad: „Zajišťování kybernetické bezpečnosti ve Westeros“ Netbox store, Brno
- 1. listopad: Český institut interních auditorů – pravidelný kurz „Audit bezpečnostních opatření podle ZKB“
- 16. listopad: přednáška na téma „aktéři kybernetické bezpečnosti“ v rámci Model UN, FSS MU, Brno
- 20. listopad: Institut veřejné správy Praha – Bezpečnostní opatření podle ZKB

- 4. prosinec: Exkurze a přednáška pro studenty Právnické fakulty Univerzity Karlovy
- 5. prosinec: Seminář kybernetické bezpečnosti pro státní zástupce
- 13. prosinec: Přednáška na téma „digitální stopa“
- Říjen - prosinec: Výuka CŽV při FP VUT v Brně – „Kybernetická bezpečnost“ 5. prosinec: přednáška pro vedoucí státní zástupce a jejich náměstky, nevyššího státního zastupitelství a vrchní státní zastupitelství, krajské a městské zastupitelství v Praze, Justiční akademie, Kroměříž

14. Příloha č. 4 – Seznam použitých zkratek a pojmů

BRS – Bezpečnostní rada státu

CBMs – Confidence Building Measures (opatření pro zvyšování důvěry mezi státy)

CCDCoE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform (Středoevropská platforma pro kybernetickou bezpečnost)

CERT – Computer Emergency Response Team

CESNET – sdružení založené roku 1996 českými veřejnými vysokými školami a Akademií věd ČR

CIRC MO – Computer Incident Response Capability, středisko kybernetické ochrany resortu Ministerstva obrany

CMX – Crisis Management Exercise

CSIRT – Computer Security Incident Response Team

CSIRT-MU – bezpečnostní tým pro dohled nad sítí Masarykovy university v Brně

CZ.NIC –zájmové sdružení právnických osob založené v roce 1998 předními poskytovateli internetových služeb, jeho hlavní činností je provozování registru domén

ČR – Česká republika

ČSÚ – Český statistický úřad

DNS – distribuovaný hierarchický jmenný systém používaný v síti Internet

DoS/DDoS – Odmítnutí služby (Denial of Service) a distribuované odmítnutí služby (Distributed Denial of Service)

eGC – eGov. Cloud

ENISA – European Union Agency for Network and Information Security (Evropská agentura pro bezpečnost sítí a informací)

EU – Evropská unie

FBI – Federal Bureau of Investigation

FIRST – Forum for Incident Response and Security Teams

FSS MU – Fakulta sociálních studií Masarykovy univerzity v Brně

GovCERT.CZ – Vládní CERT sloužící jako koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty; je organizační složkou Národního úřadu pro kybernetickou a informační bezpečnost

HONEYPOT – návnada lákající útočníka. Po zachycení potenciálně nebezpečného software dochází k jeho automatizované analýze.

HWPCI – Horizontální pracovní skupině pro kybernetické otázky

ICS – Industrial Control System je systém pro řízení technologických celků; příkladem může být SCADA

ICT – Informační a komunikační technologie

IoC – Indicator of Compromise

IP adresa – Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol) slouží k rozlišení síťových rozhraní připojených k počítačové síti

ISVS – Informační systémy veřejné správy

ISZS – Informační systém základní služby

IT – Informační technologie

KII – kritická informační infrastruktura

KYBERKRIMINALITA – specifický druh kriminality páchaný prostřednictvím výpočetních a komunikačních technologií

MALWARE – počítačový program určený k proniknutí nebo poškození počítačového systému

MF – Ministerstvo financí

MMR – Ministerstvo pro místní rozvoj

MN CD ET - Multinational Cyber Defence Education and Training (NATO Smart Defence projekt)

MO – Ministerstvo obrany

MPO – Ministerstvo průmyslu a obchodu

MPSV – Ministerstvo práce a sociálních věcí

MSp – Ministerstvo spravedlnosti

MV – Ministerstvo vnitra

MZV – Ministerstvo zahraničních věcí

NATO – North Atlantic Treaty Organization (Severoatlantická aliance)

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

NIS - směrnice Evropského parlamentu a Rady Evropské unie 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

NSA – National Security Agency

NÚKIB/ÚŘAD – Národní úřad pro kybernetickou a informační bezpečnost

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OKBP – Odbor kybernetických bezpečnostních politik

PČR – Policie České republiky

PDS – poskytovatel digitálních služeb, povinná osoba podle ZKB nově zavedená v souvislosti s transpozicí evropské směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS)

PHISHING – podvodná metoda usilující o odcizení citlivých údajů uživatele za účelem jejich zneužití, většinou vytvořením podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží citlivé informace uživatelů vylákat; zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele

PZS – provozovatel základních služeb, povinná osoba podle ZKB nově zavedená v souvislosti s transpozicí evropské směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS)

RVP – Rámcový vzdělávací program

SCADA systém (Supervisory Control and Data Acquisition) – počítačový systém pro dispečerské řízení a sběr údajů; mohou to být průmyslové řídicí systémy nebo počítačové systémy monitorování a řízení procesů, procesy mohou být průmyslové (např. výrobě elektrické energie), infrastrukturní (např. rozvod pitné vody) nebo zařízení (např. železniční stanice)

SÍŤ CSIRT– Skupina pro spolupráci a síť bezpečnostních týmů typu CSIRT

ŠVP – Školský vzdělávací program

TABLE-TOP – cvičení navržené k testování teoretických schopností cvičících ve skupině reagovat na krizovou situaci; výhodu tohoto druhu cvičení představuje možnost vyzkoušet si jakoukoliv hypotetickou situaci bez rizika způsobení škody a dalších důsledků

UN GGE – skupina vládních expertů OSN pro vývoj na poli informačních technologií a telekomunikací v kontextu mezinárodní bezpečnosti (Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security), ustavená rezolucí Valného shromáždění OSN k posouzení otázek norem chování států v kyberprostoru včetně použití existujícího mezinárodního práva

ÚVT MU – Ústav výpočetní techniky Masarykovy univerzity

VIS – významný informační systém

ZKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů

15. Příloha č. 5 – Hlášení o stavu naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020[5]

Umístěno jako příloha v samostatném dokumentu.

[5] Toto hlášení reflektuje stav naplňování úkolů Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 s termínem do čtvrtého kvartálu 2017 a úkolů, které mají být plněny průběžně.