CSIRT.SK
WWW.CSIRT.GOV.SK
CSIRT.SK
REPORT 2016

CSIRT.SK REPORT 2016

Vydavateľ:

CSIRT.SK

DataCentrum

Cintorínska 5, 814 88 Bratislava

Tel. +421 2 592 78 542, email: info@csirt.gov.sk

https://www.csirt.gov.sk

Textácie a Editor:

CSIRT.SK

Grafika a Dizajn:

CSIRT.SK

©2017 CSIRT.SK Autorské práva vyhradené

OBSAH

ZHRNUTIE	3
ÚVOD	5
1 CSIRT.SK	7
2 INCIDENTY A ZRANITEĽNOSTI	13
3 PROJEKTY	29
4 VZDELÁVANIE	35
5 BUDOVANIE DÔVERY A SPOLUPRÁCA	43
ÚSPECHY, REFERENCIE A MÉDIÁ	51
TERMÍNY A SKRATKY	57

ZHRNUTIE

Tento dokument reprezentuje súhrn udalostí, incidentov a aktivít, ktorým sa venoval špecializovaný útvar na riešenie počítačových bezpečnostných incidentov CSIRT.SK v roku 2016.

CSIRT.SK sa zaoberal predovšetkým riešením bezpečnostných počítačových incidentov v národnej informačnej a komunikačnej infraštruktúre, odstraňovaním ich dôsledkov a následnou asistenciou pri obnove informačných systémov v Slovenskej republike. V roku 2016 bolo zaznamenaných a riešených 346 počítačových incidentov, ktoré boli nahlásené klientelou CSIRT.SK, zahraničnými partnermi, subjektmi SR alebo boli zistené naším tímom počas priebežného monitoringu. Jednalo sa predovšetkým o škodlivé aktivity typu phishing, sociálne inžinierstvo, zraniteľnosti, rôzne typy škodlivého kódu, defacementy, spam, ale aj o výskyt botnetov a s tým súvisiace DDoS útoky a v neposlednom rade prieniky do systémov a úniky informácií.

Na webovom portáli CSIRT.SK bolo publikovaných 12 oznámení, 12 mesačných prehľadov kritických zraniteľností a kontaktným osobám inštitúcií verejnej správy a partnerom bolo zaslaných 20 varovaní pred konkrétnymi hrozbami s možným dopadom na informačné systémy a elektronické služby. CSIRT.SK v roku 2016 priebežne dopĺňal a aktualizoval sekciu Bezpečnostná študovňa študijnými materiálmi, okrem iného aj materiálmi zo série vzdelávacích aktivít Ministerstva financií, publikoval správu o svojej činnosti za rok 2015 a v spolupráci s Úradom podpredsedu vlády SR pre investície a informatizáciu vypracoval Metodiku pre zabezpečenie organizácií v rámci OPII.

CSIRT.SK v roku 2016 spolupracoval v oblasti riešenia bezpečnostných incidentov a zdieľania informácií o aktuálnych hrozbách a trendoch na národnej úrovni predovšetkým s bezpečnostnými útvarmi Ministerstva obrany SR, Ministerstva vnútra SR, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu, Národnej agentúry pre sieťové a elektronické služby a Slovenskej informačnej služby. DataCentrum, ako materská organizácia CSIRT.SK, má ku koncu roka 2016 uzavretých 11 zmlúv o spolupráci v oblasti informačnej bezpečnosti so subjektmi štátnej správy, akademického sektora, bankového sektora, poskytovateľmi služieb internetu a ďalšími.

K preventívnym službám, ktoré CSIRT.SK vykonával, patrí analýza zraniteľností, technologický dohľad a vykonávanie penetračných testov, vrátane testov zraniteľností pre subjekty verejnej správy. V roku 2016 bolo vykonaných 56 interných a externých penetračných testov, z toho 22 penetračných testov bolo opakovaných. CSIRT.SK vykonal viacero školení na zvyšovanie bezpečnostného povedomia. Z dôvodu predsedníctva SR v Rade EÚ boli v prvej polovici roka 2016 tieto školenia zamerané na zvyšovanie bezpečnostného povedomia, úrovne bezpečnosti a budovanie spôsobilosti na zvládanie bezpečnostných incidentov. Okrem týchto aktivít CSIRT.SK vykonal aj množstvo osvetových a technických školení pre inštitúcie verejnej správy, ale aj študentov stredných a vysokých škôl.

Na medzinárodnej úrovni reprezentoval Slovenskú republiku v oblasti informačnej bezpečnosti CSIRT.SK a aktívne spolupracoval na formovaní a tvorbe pravidiel fungovania európskej Siete jednotiek CSIRT, ktorá vznikla na základe Smernice NIS. Spolupracoval tiež s Európskou agentúrou pre informačnú a sieťovú bezpečnosť (ENISA), zahraničnými CSIRT/CERT® tímami Českej republiky, Rakúska, Nemecka, Maďarska, Poľska, Španielska, USA, Holandska a ďalších krajín a aktívne sa zapájal do medzinárodných projektov (napr. CS Danube). CSIRT.SK je členom Stredoeurópskej platformy pre spoluprácu krajín V4 a Rakúska (CECSP) v oblasti kybernetickej bezpečnosti. CSIRT.SK spolupracuje s inštitúciou CERT-EU a združeniami CSIRT/CERT® tímov TF-CSIRT a FIRST.

Počas uplynulého roka sa CSIRT.SK zúčastnil cvičení zameraných na riešenie incidentov v oblasti informačnej bezpečnosti. Išlo o cvičenia Crossed Swords, Locked Shields, Cyber Coalition a Cyber Europe, a zaznamenal na nich viaceré úspechy. Najväčším prínosom účasti na cvičeniach je však možnosť precvičenia si technických, ale aj operatívnych schopností počas riešenia kybernetických incidentov.

ÚVOD

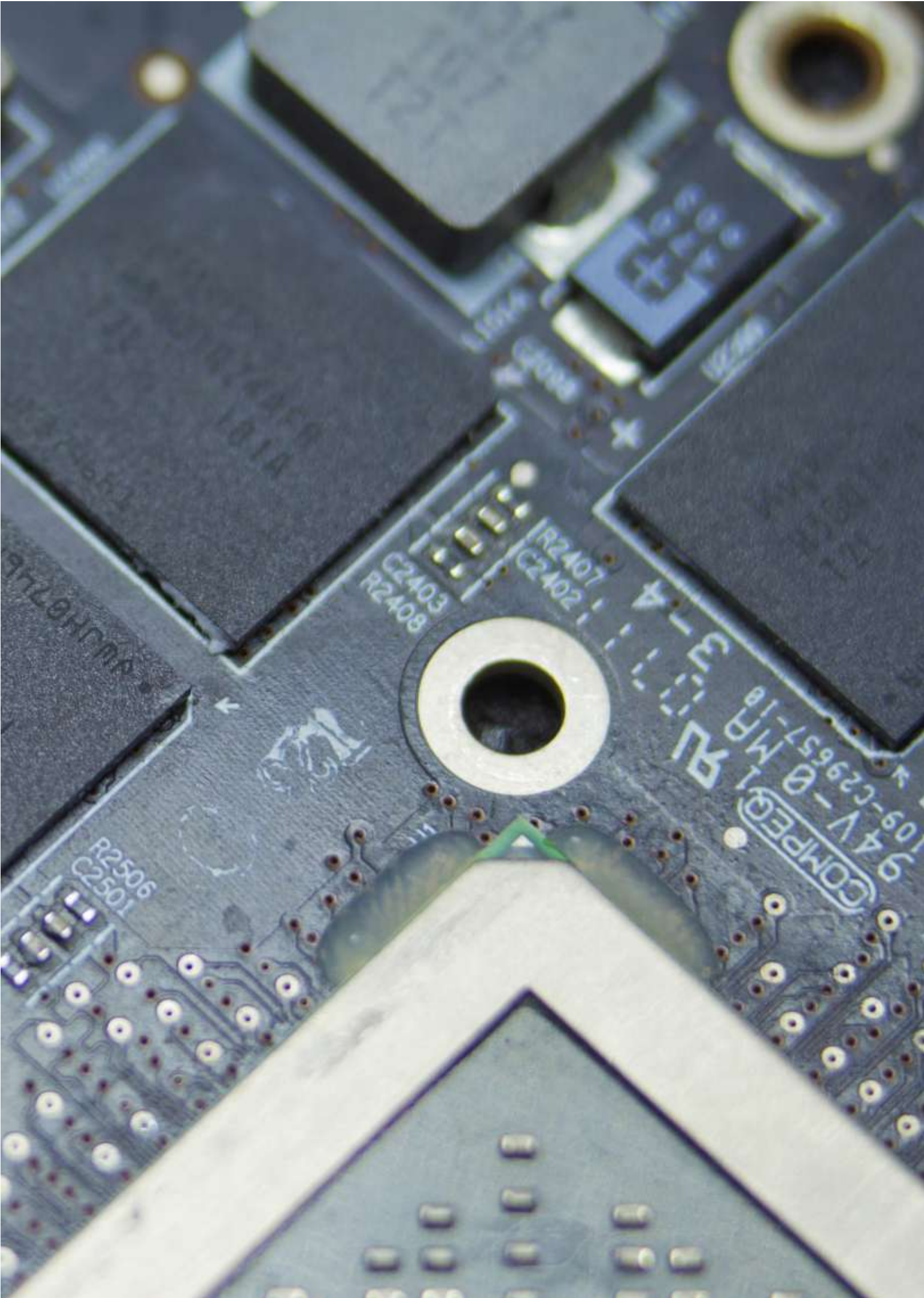
Rok 2016 bol z pohľadu informačnej bezpečnosti rokom veľmi bohatým na udalosti. V auguste 2016 vošla do platnosti Smernica NIS. Išlo o udalosť, ktorá v blízkej budúcnosti najviac ovplyvní bezpečnosť informačných systémov a sietí všetkých členských štátov EÚ.

Členské štáty majú 21 mesiacov na jej transpozíciu do svojej národnej legislatívy. V Slovenskej republike bol touto úlohou poverený Národný bezpečnostný úrad. Rok 2016 bol ale aj rokom nárastu výskytu škodlivého kódu, predovšetkým ransomvéru. Kybernetickým kriminálnikom sa tento typ škodlivej aktivity veľmi vypláca, pretože väčšina ľudí podceňuje zálohovanie svojich dát a nemá vybudované bezpečnostné návyky pri používaní Internetu. Tento typ „podnikania“ je v dnešnej dobe vysoko sofistikovaný a v mnohých prípadoch poskytuje aj služby callcentra pre používateľov, ktorí majú problémy so zaplatením výkupného za svoje zašifrované súbory. Útočníci používateľa prevedú celým procesom platby v bitcoinoch a obeť má po úspešnom vykonaní platby dokonca možnosť ohodnotiť kvalitu poskytovaných „služieb“. Ďalším významným znakom roku 2016 boli zraniteľné zariadenia Internetu vecí (IoT) a ich použitie na masívne DDoS útoky. Ešte pred niekoľkými rokmi by sa človek možno pousmial nad predstavou, že kybernetické útoky v blízkej budúcnosti budú vykonávať „múdre“ chladničky, termostaty alebo žiarovky. Použitie botnetu Mirai na DDoS útoky však tieto predstavy zhmotnilo a útočníkom sa vďaka nemu podarilo zneprístupniť napríklad služby Airbnb, Spotify, Twitteru, eBayu, Redditu či stránku New York Times.

Tak ako každý rok, aj v roku 2016 nastalo množstvo únikov dát. Napríklad v apríli nastal prienik do databázy filipínskej volebnej komisie, ktorý viedol k jednému z najzávažnejších únikov dát z vládnej inštitúcie vôbec. Kompromitované boli osobné údaje každého voliča na Filipínach, čo je približne 55 miliónov osôb. Zaujímavý bol aj únik dát 50 miliónov občanov Turecka, o ktorom sa informovalo v apríli , a obsahoval aj osobné údaje prezidenta Erdogana či premiéra Davutoglu. V decembri spoločnosť Yahoo! oznámila únik dát z roku 2013, ktorý mal kompromitovať 1 miliardu Yahoo účtov, čo z neho robí najväčší únik dát v histórii. Predpokladáme, že v roku 2017 budú kybernetické útoky pribúdať, preto je potrebné sa vopred na túto možnosť pripraviť. Organizáciám štátnej správy odporúčame, aby implementovali hĺbkovú ochranu (defense in depth) svojich informačných aktív a zintenzívnili aktivity na zvyšovanie povedomia o kybernetických hrozbách u svojich zamestnancov. Ako inšpirácia im môže poslúžiť naša Metodika pre zabezpečenie organizácií v rámci OPII, či phishingový test na našej stránke pre otestovanie zamestnancov na schopnosť rozpoznávať phishingové emaily.

1 CSIRT.SK

V roku 2016 CSIRT.SK pokračoval v poskytovaní služieb potrebných na zvládnutie bezpečnostných počítačových incidentov v národnej informačnej a komunikačnej infraštruktúre, na odstránenie ich následkov a na následnú obnovu informačných systémov v Slovenskej republike. Okrem týchto základných služieb jednotka poskytovala aj služby preventívneho a vzdelávacieho charakteru a zabezpečovala spoluprácu pri riešení bezpečnostných incidentov na medzinárodnej úrovni.


R2407
C2402
C2403
R2408
R2506
C2501
COMPEQ
94V-0
UL

1.1 Aktívne služby

V roku 2016 bolo riešených 346 počítačových incidentov, ktoré boli nahlásené klientelou CSIRT.SK, zahraničnými partnermi, subjektmi SR alebo boli zistené priebežným monitoringom nášho tímu. Incidenty boli riešené v spolupráci s vlastníkmi a prevádzkovateľmi informačných systémov verejnej správy, vybraných prvkov kritickej informačnej infraštruktúry a prevádzkovateľmi národnej informačnej a komunikačnej infraštruktúry SR. Počas riešenia incidentov CSIRT.SK spolupracoval aj s telekomunikačnými operátormi a poskytovateľmi internetových služieb, a s CSIRT/CERT® tímami v SR a zahraničí a ďalšími štátnymi orgánmi.

Počet jednotlivých typov závažných incidentov riešených CSIRT.SK v období 1.1. - 31.12.2016 je uvedený v nasledovnej tabuľke.

TYP ŠKODLIVEJ AKTIVITY	POČET
Získavanie informácií – (phishing, sociálne inžinierstvo, ...)	88
Výskyt závažnej zraniteľnosti	79
Škodlivý kód	50
Nežiaduci obsah (defacement, spam, ...)	48
Botnet	31
Nedostupnosť (DoS, DDoS, ...)	23
Prienik do systému	10
Neoprávnený prístup k informáciám/únik informácií	7
Ostatné	5
Pokus o prienik	4
Podvod	1
Neoprávnená modifikácia informácií	0
CELKOM	**346**

V roku 2016 bolo riešených 346 počítačových incidentov, ktoré boli nahlásené klientelou CSIRT.SK, zahraničnými partnermi, subjektmi SR alebo boli zistené priebežným monitoringom nášho tímu. Incidenty boli riešené v spolupráci s vlastníkmi a prevádzkovateľmi informačných systémov verejnej správy, vybraných prvkov kritickej informačnej infraštruktúry a prevádzkovateľmi národnej informačnej a komunikačnej infraštruktúry SR. Počas riešenia incidentov CSIRT.SK spolupracoval aj s telekomunikačnými operátormi a poskytovateľmi internetových služieb, a s CSIRT/CERT® tímami v SR a zahraničí a ďalšími štátnymi orgánmi.

Počet jednotlivých typov závažných incidentov riešených CSIRT.SK v období 1.1. - 31.12.2016 je uvedený v nasledovnej tabuľke.

TYP BEZPEČNOSTNEJ UDALOSTI	POČET
Botnet	720 241
Výskyt zraniteľnosti	544 855
Škodlivý kód	184 821
Nedostupnosť (DoS, DDoS, ...)	158 760
Nežiaduci obsah (defacement, spam, ...)	4 039
Získavanie informácií – (phishing, social engineering, ...)	372
Pokus o prienik	68
CELKOM	**1 613 156**

1.2 Proaktívne služby

VAROVANIA

V rámci služieb varovania pred hrozbami bezpečnosti IKT bolo v hodnotenom období na webovom portáli www.csirt.gov.sk publikovaných 12 oznámení. Informácie o zraniteľnostiach a hrozbách v oblasti informačnej bezpečnosti boli systematicky publikované v mesačných prehľadoch na web stránke CSIRT.SK. Okrem týchto aktivít bolo kontaktným osobám inštitúcií verejnej správy a partnerom zaslaných 20 varovaní pred konkrétnymi hrozbami s možným dopadom na informačné systémy a elektronické služby.

PREVENTÍVNE SLUŽBY

Tím CSIRT.SK poskytoval preventívne služby aj prostredníctvom svojho Informačného systému včasného varovania, zdieľania informácií a reakcie na kybernetické hrozby. Medzi preventívne služby patrí aj analýza škodlivého kódu a vykonávanie penetračných testov, vrátane testov zraniteľností pre subjekty verejnej správy. V roku 2016 bolo vykonaných 56 interných a externých penetračných testov, z toho 22 opakovaných penetračných testov.

PREDSEDNÍCTVO V RADE EÚ

V prvej polovici roka 2016 sa CSIRT.SK zameral na zvyšovanie povedomia, úrovne bezpečnosti a budovanie spôsobilosti na zvládanie bezpečnostných incidentov z dôvodu predsedníctva SR v Rade EÚ od 1.7.2016. V tomto období bola v rámci prevencie systematicky vykonávaná analytická a konzultačná činnosť pre predchádzanie bezpečnostných incidentov. V rámci prípravy na predsedníctvo prebehlo 8 penetračných testov, z toho 4 boli interné.

SPOLUPRÁCA NA NÁRODNEJ A MEDZINÁRODNEJ ÚROVNI

V roku 2016 špecializovaný útvar CSIRT.SK v oblasti riešenia bezpečnostných incidentov a zdieľania informácií o aktuálnych hrozbách a trendoch spolupracoval na národnej úrovni predovšetkým s bezpečnostnými útvarmi Ministerstva obrany SR, Ministerstva vnútra SR, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu, Národnej agentúry pre sieťové a elektronické služby a Slovenskej informačnej služby. CSIRT.SK v rámci poskytovania preventívnych služieb spolupracoval s ďalšími inštitúciami verejnej správy, prvkami kritickej infraštruktúry, akademickým a súkromným sektorom v rozsahu vecnej problematiky s dôrazom na ochranu informačných systémov verejnej správy a kritickej infraštruktúry. K 31.12.2016 má DataCentrum uzavretých 11 zmlúv o spolupráci v oblasti informačnej bezpečnosti so subjektmi štátnej správy, akademického sektora, bankového sektora, poskytovateľmi služieb internetu a ďalšími. Na medzinárodnej úrovni CSIRT.SK reprezentoval Slovenskú republiku a aktívne spolupracoval s Európskou agentúrou pre informačnú a sieťovú bezpečnosť (ENISA), zahraničnými CSIRT/CERT® tímami Českej republiky, Rakúska, Nemecka, Maďarska, Poľska, Španielska, USA, Holandska a ďalších krajín a aktívne sa zapájal do medzinárodných projektov (napr. CS Danube). CSIRT.SK je členom Stredoeurópskej platformy pre spoluprácu krajín V4 a Rakúska (CECSP) v oblasti kybernetickej bezpečnosti. CSIRT.SK spolupracuje s inštitúciou CERT-EU a združeniami CSIRT/CERT® tímov TF-CSIRT a FIRST.

1.3 Udalosti

19.01.2016	Návšteva NCKB v Brne
25.-27.01.2016	FIRTS/TF-CSIRT Technical Colloquium
27.01.2016	Pracovná skupina CSIRT.CZ
09.-11.02.2015	Cvičenie Crossed Swords 2016
17.-18.02.2015	The 25th Workshop on pan European Cyber Exercises, Lisabon
17.02.2016	Konferencia Security 2016
14.-15.03.2016	CS Danube
16.03.2016	ENISA Training
17.03.2016	Vydaná správa o činnosti CSIRT.SK za rok 2015
05.04.2016	1st informal CSIRTs Network meeting, Hague
12.04.2016	QuBit Conference
18.-22.04.2016	Cvičenie Locked Shields 2016
10.05.2016	2nd informal CSIRTs Network meeting, Riga
10.-11.05.2016	Annual National and Governmental CSIRTs Workshop – CSIRTs in Europe
12.-13.05.2016	48th TF-CSIRT meeting
18.-19.05.2016	CECSP Meeting Warsaw
13.-17.06.2016	CE2016 Final Planning Conference

06.07.2016	Schválená Smernica NIS
12.07.2017	Antall József Summer School 2016
08.08.2016	Smernica NIS vchádza do platnosti
13.–15. 09.2016	Letná škola kyberkriminality
20.-21.09.2016	49th TF-CSIRT meeting
06.-07.10.2016	5th Annual ENISA-EC3 Cyber Crime Workshop
11.10.2016	Meeting of the Informal Working Group regarding CBMs, OBSE
13.-14.10.2016	Cvičenie Cyber Europe 2016
22.-23.10.2016	OSS víkend 2016 Košice
24.10.2016	Zraniteľnosti v implementáciách SSL/TLS protokolov, prednáška na Bezadis, PF UPJŠ Košice
24.10.2016	Prednáška na zvýšenie bezpečnostného povedomia, Gymnázium Poštová, Košice
27.-28.10.2016	CECSP Meeting Warsaw
09.11.2016	3rd informal CSIRTs Network meeting, Hague
11.11.2016	Vydaná Metodika pre zabezpečenie organizácií v rámci OPII
28.11.-02.12.2016	Cvičenie Cyber Coalition 2016

2 INCIDENTY

V roku 2016 CSIRT.SK pokračoval v poskytovaní služieb potrebných na zvládnutie bezpečnostných počítačových incidentov v národnej informačnej a komunikačnej infraštruktúre, na odstránenie ich následkov a na následnú obnovu informačných systémov v Slovenskej republike. Okrem týchto základných služieb jednotka poskytovala aj služby preventívneho a vzdelávacieho charakteru a zabezpečovala spoluprácu pri riešení bezpečnostných incidentov na medzinárodnej úrovni.

A ZRANITEĽNOSTI

2.1 Vybrané incidenty

PHISHINGOVÁ STRÁNKA CIELENÁ NA POUŽÍVATEĽOV SLUŽBY PAYPAL

Tímu CSIRT.SK bola zahraničnými partnermi nahlásená phishingová stránka vydávajúca sa za prihlasovacie rozhranie do služby PayPal. Podvodná stránka bola na slovenskú doménu nahraná prostredníctvom zneužitia zraniteľnosti redakčného systému legitímneho webového sídla. CSIRT.SK v spolupráci s prevádzkovateľom webového sídla túto webstránku odstránil a získal prístup ku jej zdrojovým kódom a log záznamom, ktoré následne analyzoval. Analýza zdrojových kódov odhalila možnosti konfigurácie tejto phishingovej stránky (vrátane možnosti online overovania CVV kódov a rôznych možností zberu a odosielania zachytených údajov). Dôveryhodne vyzerajúca phishingová stránka si po zadaní údajov v nasledujúcom kroku vypýtala od obeti ďalšie (citlivejšie) údaje. Analyzovaná phishingová stránka bola vytvorená ako produkt, ktorý bolo možné ďalej predávať a konfigurovať („phishing ako služba“). Analýza logov odhalila vyše 15 tisíc prístupov na uvedenú stránku, z ktorých však len necelá tretina odoslala prihlasovací formulár. Skutočných prihlasovacích údajov do služby PayPal však bolo menej ako 100, boli však zachytené aj fakturačné údaje a údaje o niekoľkých platobných kartách. V rámci riešenia tohto incidentu boli kontaktované dotknuté platobné spoločnosti aj vydavatelia platobných kariet.

ÚTOK POČAS VOLIEB DO NÁRODNEJ RADY SR

CSIRT.SK analyzoval príčiny nedostupnosti stránky Štatistického úradu SR počas volebnej noci. Analýzou bola zistená prítomnosť DDoS útoku. Na základe zistení boli Štatistickému úradu navrhnuté odporúčania s cieľom eliminovať následky kybernetických útokov v budúcnosti.

IDENTIFIKÁCIA A ANALÝZA 0-DAY ZRANITEĽNOSTI V ADOBE FLASH PLAYER

Analytici CSIRT.SK počas analýzy vzorky škodlivého softvéru identifikovali 0-day zraniteľnosť v prehrávači Adobe Flash Player, ktorá už bola zneužívaná tvorcami malvéru. Viac sa o tomto prípade dočítate v časti Úspechy a referencie.

ÚNIKY CITLIVÝCH ÚDAJOV A ANALÝZA VEREJNE DOSTUPNÝCH ZDROJOV

V roku 2016 bolo na Internete zverejnených viacero informačných zdrojov, vrátane databáz obsahujúcich citlivé údaje a online trhovísk ponúkajúcich prístup ku kompromitovaným serverom. Taktiež boli zachytené a analyzované informácie o pripravovaných kampaniach skupiny Anonymous. CSIRT.SK bližšie preskúmal viaceré zdroje a dotknutým stranám vo svojej konštituencii zaslal varovania.

FORENZNÉ ANALÝZY KOMPROMITOVANÝCH SERVEROV

V priebehu roka CSIRT.SK riešil viacero podozrení na kompromitáciu zariadení vo svojej konštituencii. Analytický tím vykonal viacero forenzných analýz serverov aj pracovných staníc, často sprevádzaných aj analýzou nájdených vzoriek potenciálne škodlivého softvéru. Následne CSIRT.SK navrhol dotknutým stranám odporúčania s cieľom zmierniť následky incidentu, zvýšiť zabezpečenie ich systémov a predchádzať útokom v budúcnosti.

ANALÝZA ŠKODLIVÉHO KÓDU A PHISHINGOVÝCH KAMPANÍ

CSIRT.SK v priebehu roka analyzoval viaceré phishingové kampane a ďalšie incidenty, v ktorých sa vyskytoval škodlivý kód. V priebehu riešenia týchto incidentov boli vykonané analýzy exploit kitu Blackhole, viacerých škodlivých kódov typu spyware a ransomware a taktiež rôzne škodlivé skripty.

VÝSKYT ŠKODLIVÉHO KÓDU A BOTNETOV

Pre lepšie využitie infikovaných zariadení útočníci do škodlivého kódu (malvéru) často dopĺňajú funkcionalitu, vďaka ktorej je zariadenie schopné pripojiť sa do tzv. botnet siete a vykonávať v nej útočníkom zamýšľanú aktivitu. Napadnuté zariadenia, tzv. „zombie“, sú potom ovládané prostredníctvom serverov C&C (Command and Control), ktoré kontroluje útočník. Pri akciách zameraných na znefunkčnenie botnetov je odchytávaná práve riadiaca komunikácia medzi C&C a klientmi, na základe ktorej sú následne identifikované samotné infikované zariadenia. V roku 2016 CSIRT.SK od svojich zahraničných partnerov prijímal hlásenia o výskyte rôznych druhov škodlivého kódu a informoval o tom príslušných správcov systémov a zariadení.

ICS/SCADA SYSTÉMY DOSTUPNÉ Z INTERNETU (JANUÁR)

V januári a vo februári CSIRT.SK prijal hlásenia o dohľadových systémoch ICS/SCADA v IP adresnom priestore SR, ktoré sú voľne dostupné z Internetu a upozornili na túto skutočnosť ich prevádzkovateľov. Tieto systémy sa používajú na monitorovanie priemyselných a výrobných procesov a nezriedka sú v prevádzke aj niekoľko rokov bez aktualizácií ich softvéru. Neaktualizované systémy môžu obsahovať bezpečnostné zraniteľnosti a preto je vhodné obmedziť prístup týchto zariadení do siete Internet. Z minulosti je známy napríklad útok na energetické systémy v Ukrajine v decembri 2015, v ktorom bol použitý škodlivý kód BlackEnergy.

EBURY (FEBRUÁR)

„Ebury“ je rootkit/backdoor trojan pre Linux/Unix operačné systémy, ktorý získava SSH prihlasovacie údaje (meno/heslo) z SSH spojení a odosiela ich pomocou DNS dotazov na "dropzone" server útočníka. Na nakazených strojoch tiež inštaluje backdoor, pomocou ktorého získa útočník plný prístup k OS. Zaujímavou vlastnosťou je, že spojenia uskutočnené cez backdoor sa nenachádzajú v žiadnych logoch. Kompromitované stanice môžu byť taktiež zneužívané na vykonávanie ďalšej škodlivej aktivity.

RAMNIT (FEBRUÁR – DECEMBER)

Od februára až do konca roka CSIRT.SK pravidelne informoval o výskyte škodlivého kódu s označením “Ramnit”. Ramnit sa zameriava na zariadenia s OS Windows. Šíri sa viacerými spôsobmi, zvyčajne pomocou spam e-mailov s odkazmi na kompromitované stránky a sociálne siete, pomocou verejných FTP serverov, prípadne pri inštalácii softvérových balíkov z nedôveryhodných zdrojov. Tento škodlivý kód umožňuje útočníkom získavať citlivé informácie z napadnutých zariadení. Môže ísť o bankové údaje, cookies z prehliadača pre ukradnutie identity alebo heslá uložené na disku. Útočníkom tiež sprostredkúva vzdialený prístup do počítača obete, ktorý umožňuje ovládanie zariadenia a prístup k súborom obete na diaľku. Okrem toho môžu byť infikované zariadenia zapojené do siete "botnet" a môžu vykonávať ďalšie nekalé aktivity (DDoS útoky, SPAM a pod.).

ZRANITEĽNOSŤ SSL/TLS DROWN (MAREC)

V marci bola publikovaná zraniteľnosť SSL/TLS protokolu „Drown“, ktorá umožňovala útočníkovi dešifrovať zachytenú komunikáciu zabezpečenú pomocou SSL/TLS protokolu. Útočník mohol následne odpočúvať komunikáciu medzi klientom a serverom a mohol tak získať prístup k prenášaným údajom - používateľské mená a heslá, obsah emailov, osobné a finančné údaje. Na základe dát od bezpečnostných výskumníkov CSIRT.SK kontaktoval zasiahnuté inštitúcie štátnej správy, verejnej správy a ISP a odporučil im kroky na odstránenie zraniteľnosti.

MUMBLEHARD

Od apríla až do konca roka CSIRT.SK na základe hlásení od partnerov informoval o výskyte škodlivého kódu „Mumblehard“. Zameriava sa na OS Linux/BSD, kde slúži ako backdoor na poskytnutie prístupu k infikovanému systému, resp. zariadeniu. Na komunikáciu využíva HTTP GET požiadavky, ktoré sú odosielané v pravidelných intervaloch pomocou naplánovanej CRON úlohy.

VOĽNE DOSTUPNÉ ROZHRANIA IPMI (MÁJ)

V máji CSIRT.SK zaznamenal u viacerých organizácií voľne dostupné prihlasovacie rozhrania z prostredia Internetu. Konkrétne išlo o manažovacie rozhrania IPMI (Intelligent Platform Management Interface). Rozhrania na správu serverov používajúce štandard IPMI, napríklad HP iLO alebo Dell iDRAC, môžu obsahovať viaceré zraniteľnosti, ktoré umožňujú obídenie alebo prelomenie autentifikácie. Vzhľadom na skutočnosť, že IPMI poskytuje prístup k hardvéru, je možné zraniteľnosti zneužiť na získanie kontroly nad daným zariadením. CSIRT.SK sa preto rozhodol informovať o možných rizikách správcov týchto systémov.

XDEDIC MARKETPLACE (JÚN)

Spoločnosť Kaspersky v júni zverejnila analýzu xDedic Marketplace, kde bolo možné zakúpiť prístupy ku kompromitovaným serverom po celom svete, vrátane Slovenskej republiky. Táto služba bola ponúkaná už od r. 2014 a v čase publikácie analýzy boli v „ponuke“ prístupy k viac ako 70 000 kompromitovaným serverom spolu s doplňujúcimi údajmi - OS servera, rýchlosť pripojenia, prítomnosť antivírusového softvéru a ďalšie. Po analýze CSIRT.SK kontaktoval zodpovedné osoby a odporučil im preveriť dotknuté servery na prítomnosť indikátorov kompromitácie zverejnených v dokumente od Kaspersky.

EXPLOIT KIT NEUTRINO (SEPTEMBER)

V septembri CSIRT.SK prijal oznámenie od zahraničného partnera o prítomnosti exploit kitu s názvom Neutrino hostovanom na Slovensku. Exploit kity sa využívajú pri útokoch typu Drive-by-Download s cieľom stiahnuť škodlivý kód pri navštívení webovej stránky a následne kompromitovať klienta. Jedná sa o pokročilé nástroje útočníkov, ktoré dokážu rozlíšiť verzie a typy systémov obetí pristupujúcich na kompromitované stránky a na základe nich použiť najvhodnejší exploit na infikovanie počítača obete. Škodlivý obsah sa po komunikácii s ISP podarilo úspešne odstrániť.

JAVASCRIPT SKIMMING (OKTÓBER)

V októbri bol bezpečnostným expertom publikovaný článok o tzv. „online skimmingu“ platobných kariet. Podobne ako v prípade fyzického skimmingu ide o získavanie údajov o kartách a ich odosielanie útočníkom, avšak v tomto prípade sa jedná o inštaláciu škodlivého javascript kódu na stránky zraniteľných e-shopov. Tento kód následne odosielal získané údaje na servery útočníkov. Krátko po zverejnení CSIRT.SK prijal hlásenie o výskyte zraniteľných e-shopov na Slovensku a dotknutých prevádzkovateľov o tejto hrozbe informoval.

AVALANCHE

Koncom novembra sa podarilo znefunkčniť rozsiahly botnet Avalanche, ktorý slúžil ako platforma pre rôzne kriminálne aktivity. Botnet bol využívaný viacerými rodinami malvéru ako napríklad Andromeda, Bolek, Nymaim, Tinba a ďalšie. Na základe informácií zo sinkhole serverov, monitorujúcich požiadavky na C&C servery tohto botnetu, ktoré CSIRT.SK prijal v decembri, mohli byť identifikované a následne notifikované obete (botov) na Slovensku.

ÚTOKY DOS A DDOS

Útoky DoS a DDoS sú medzi útočníkmi stále populárne najmä kvôli ich jednoduchosti a významnému dopadu na cieľ útoku. Hlásenia o zapojení sa IP adries zo Slovenska do DDoS útokov sa vyskytovali takmer každý mesiac a ich vlastníkov CSIRT.SK priebežne o tejto nežiaducej aktivite informoval. Najčastejší typ útoku bol DNS amplification, ktorý zneužíva verejné DNS resolvery odpovedajúce na rekurzívne požiadavky (tzv. „open-resolvery“). Tiež boli zaznamenané amplifikačné a záplavové „flood“ útoky pomocou iných služieb, napríklad NTP a UPnP. Okrem bežných DDoS útokov CSIRT.SK riešil tiež zriedkavejšie prípady ako napríklad TTL Expiry alebo Wordpress Pingback DDoS. Napríklad Wordpress Pingback DDoS zneužíva funkciu Pingback štandardne zapnutú vo Wordpress inštaláciách. Prehľad dominantných typov DoS a DDoS útokov v jednotlivých mesiacoch:

OBDOBIE:	HLÁSENIE OD:	TYP:
február – marec	CERTSI	DNS amplification DDoS
marec	CCIRC	DNS reflection
apríl	GCCMaster	DNS amplification
apríl, maj	CERT.BG	TTL Expiry Attack
jún	CCIRC	NTP amplification
jún	CSIRT.CZ	upnp port udp/1900
august	CCIRC	Wordpress pingback
december	CSIRT.CZ	DDoS UDP flood from port 53

PHISHING

Z incidentov riešených počas roka 2016 boli phishingové útoky a kampane jedny z najpočetnejších. Vo väčšine prípadov sa jednalo o podvodné stránky s cieľom vylákať od neskúsených používateľov prihlasovacie údaje k rôznym službám a bankovým účtom. Keďže mnohé organizácie neobmedzujú komunikáciu z vnútra siete, je tento typ útokov veľmi efektívny a používaný aj pri pokročilých kampaniach a APT útokoch ako vektor prvotnej infekcie. Phishingové emaily často obsahujú škodlivú prílohu alebo odkazy na stiahnutie škodlivého kódu.

DEFACEMENTY

Rok 2016 bol bohatý aj na kompromitované webové stránky patriace do IP adresného priestoru Slovenskej republiky. Útočníci sa zväčša snažili upozorniť administrátorov na nízku úroveň zabezpečenia ich webových stránok, prípadne serverov, umiestnením informácie o ovládnutí stránky na domovskú stránku daného webu. Išlo zvyčajne o formuláciu s textom „Hacked by ...“. V sledovanom období sa zvýšil počet útokov s cieľom propagovať politické a náboženské postoje útočníkov. Niektorí útočníci plne využívajú multimediálne možnosti, ktoré im dnešné technológie umožňujú. Typický „defacement“ dnes pozostáva z pútavého obrázku na pozadí stránky, posolstva útočníka a hudobnou vložkou, prehrávanou tiež na pozadí. Webové stránky poskytujúce služby online objednávania a platby za tovary alebo služby, tzv. e-shop služby, predstavujú zaujímavú kategóriu pre útočníkov. CSIRT.SK totiž zaznamenal útoky, v ktorých sa útočník snažil pomocou defacementu odvrátiť pozornosť od skutočnosti, že na stránku umiestnil škodlivý script, ktorý zachytával citlivé informácie zadávané používateľom a odosielal ich naspäť útočníkovi. Išlo napríklad o prihlasovacie údaje a informácie o platobnej karte.

2.2 Varovania

21.01.2016	Exploit na zraniteľnosť v Linuxovom jadre
08.02.2016	Informácie CSIRT.SK ku TeslaCrypt RansomWare
23.02.2016	Kritická zraniteľnosť v knižnici GNU C Library
04.03.2016	Kritická zraniteľnosť zabezpečenia komunikácie prostredníctvom SSL/TLS protokolu
02.05.2016	Zraniteľnosť v Adobe Acrobat and Reader (DLL hijacking)
13.05.2016	0-day zraniteľnosť v Adobe Flash Player umožňujúcu spustenie škodlivého kódu
24.05.2016	Škodlivá aktivita z IP adresy
25.05.2016	C&C servery malvéru Qakbot
25.05.2016	Podozrivá doména - finacnasprava.sk
27.05.2016	IoC kampane podvodu SWIFT
09.06.2016	Cyber Security Brief
16.06.2016	Overenie kontaktov pre varovania
27.07.2016	Zraniteľnosti routerov Ubee EVW3226
05.08.2016	Súhrn indikátorov kompromitácie za rok 2016
10.08.2016	Informácia o novej hrozbe - útok Flip Feng Shui
12.08.2016	Varovanie pre používateľov WiFi smerovača Ubee EVW3226
17.08.2016	Varovanie - zraniteľnosti Microsoft Office Word
05.09.2016	Varovanie - Verejne dostupné exploity na zraniteľnosti sieťových prvkov
12.09.2016	Varovanie pred hrozbou APT
07.10.2016	Threat Landscape Report 2016
20.10.2016	Cyber Security Brief
21.10.2016	Verejne dostupný exploit na zraniteľnosť Dirty COW v Linuxovom jadre
31.10.2016	Varovanie pred útokom DDoS
03.11.2016	Indikátory phishingovej kampane Sofacy
16.11.2016	Indikátory phishingovej kampane
01.12.2016	Zraniteľnosť Mozilla Firefox
28.12.2016	Informácia o skene zraniteľností webov domény gov.sk

2.3 Mesačný prehľad

Špecializovaný útvar CSIRT.SK na svojej webovej stránke každý mesiac uverejňuje prehľad kritických zraniteľností spolu s odporúčaniami na ich odstránenie. Popis zraniteľností pozostáva z jej opisu jej funkcionalít, určenia zraniteľných systémov a odporúčaní. Na nasledujúcich stranách uvádzame výber najzaujímavejších zraniteľností z mesačných prehľadov od CSIRT.SK.

JANUÁR

- Koniec podpory starších verzií prehliadača Internet Explorer.
- Verejne známy exploit na zraniteľnosť CVE-2016-0728 v Linuxovom jadre umožňujúci zvýšenie oprávnení.

FEBRUÁR

- Zraniteľnosť CVE-2015-7547 v knižnici GNU C Library umožňujúca spôsobiť pád aplikácie alebo vzdialené spustenie škodlivého kódu prostredníctvom DNS odpovede.

MAREC

- Zneužívanie zraniteľnosti CVE-2016-1010 v programe Adobe Flash Player na vzdialené spustenie škodlivého kódu v cielených útokoch.
- DROWN útok umožňujúci dešifrovať zachytenú komunikáciu zabezpečenú pomocou SSL/TLS protokolu.

APRÍL

- Zneužívanie zraniteľností CVE-2016-0165 a CVE-2016-0167 v OS Windows na zvýšenie oprávnení a prevzatie kontroly nad zariadením.
- Zneužívanie zraniteľnosti CVE-2016-1019 v programe Adobe Flash Player na vzdialené spustenie škodlivého kódu.
- Zraniteľnosť Badlock v OS Windows (CVE-2016-0128) aj v Samba (CVE-2016-2118) umožňujúca spôsobiť zamietnutie služby (DoS) alebo eskaláciu práv.

MÁJ

- Zneužívanie zraniteľností CVE-2016-0184 v OS Windows na vzdialené spustenie škodlivého kódu a prevzatie kontroly nad zariadením po navštívení webovej stránky alebo otvorení infikovaného dokumentu.
- Zneužívanie zraniteľností CVE-2016-0189 v prehliadači Microsoft Internet Explorer na vzdialené spustenie škodlivého kódu po navštívení webovej stránky alebo otvorení infikovaného dokumentu.
- Zneužívanie zraniteľnosti CVE-2016-4116 a CVE-2016-4117 v programe Adobe Flash Player na vzdialené spustenie škodlivého kódu a zvýšenie oprávnení. Zraniteľnosť CVE-2016-4116 bola identifikovaná tímom CSIRT.SK.
- Zraniteľnosť CVE-2016-1090 v programe Adobe Reader umožňujúca spustenie škodlivého kódu a zvýšenie oprávnení bola identifikovaná tímom CSIRT.SK.

JÚN

- Zneužívanie zraniteľnosti CVE-2016-4171 v programe Adobe Flash Player na vzdialené spustenie škodlivého kódu v cielených útokoch.
- Verejne známy exploit na zraniteľnosť v jadre OS Linux umožňujúci zvýšenie oprávnení.
- Zraniteľnosti v Network Time Protocol daemon (ntpd) umožňujúce spôsobiť pád servera a rozsynchronizovanie lokálnych hodín.

JÚL

- Zraniteľnosti CVE-2016-3280, CVE-2016-3281, CVE-2016-3282 v Microsoft Office umožňujúce vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru alebo zobrazení jeho náhľadu v emaile.

AUGUST

- Publikované exploity a nástroje používané skupinou Equation Group na kompromitáciu sieťových prvkov.
- Zraniteľnosti v domácich smerovačoch Ubee EVW3226 používaných spoločnosťou UPC BROADBAND SLOVAKIA.

SEPTEMBER

- Zraniteľnosti v databázach MySQL umožňujúce zápis do konfiguračných súborov a následné spustenie škodlivého kódu.

OKTÓBER

- Zneužívanie 0-day zraniteľnosti CVE-2016-7255 v OS Windows na zvýšenie oprávnení.
- Zneužívanie zraniteľnosti CVE-2016-3393 v OS Windows a Microsoft Office na vzdialené spustenie škodlivého kódu a prevzatie kontroly nad zariadením.
- Zneužívanie zraniteľnosti CVE-2016-3298 v prehliadači Microsoft Internet Explorer na testovanie prítomnosti súborov na disku.
- Zneužívanie zraniteľnosti CVE-2016-7855 v programe Adobe Flash Player na vzdialené spustenie škodlivého kódu v cielených útokoch.
- Verejne dostupný exploit na zraniteľnosť Dirty COW v jadre OS Linux umožňujúci zvýšenie oprávnení.

NOVEMBER

- Zneužívanie zraniteľnosti CVE-2016-7256 v OS Windows na vzdialené spustenie škodlivého kódu a prevzatie kontroly nad zariadením.
- Zneužívanie zraniteľnosti CVE-2016-9079 v prehliadačoch Mozilla Firefox.

DECEMBER

- Zneužívanie zraniteľnosti CVE-2016-7892 v programe Adobe Flash Player na vzdialené spustenie škodlivého kódu v cielených útokoch.

2.4 Závažné úniky dát

Tak ako každý rok, aj v roku 2016 nastalo množstvo únikov dát. Napríklad v apríli nastal prienik do databázy filipínskej volebnej komisie, ktorý viedol k jednému z najzávažnejších únikov dát z vládnej inštitúcie vôbec. Zaujímavý bol aj únik dát 50 miliónov občanov Turecka, o ktorom sa informovalo v apríli, a obsahoval aj osobné údaje prezidenta Erdogana či premiéra Davutoglu. V decembri spoločnosť Yahoo! oznámila únik dát z roku 2013, ktorý mal kompromitovať 1 miliardu Yahoo účtov, čo z neho robí najväčší únik dát v histórii

U.S. DEPARTMENT OF JUSTICE

9. február 2016 – Útočníci v reakcii na vývoj vzťahov medzi USA a Izraelom narušili databázu amerického Ministerstva spravodlivosti. CNN upozornilo na to, že útočníci zverejnili dáta o 10 000 zamestnancoch amerického Ministerstva vnútornej bezpečnosti a na druhý deň dáta o 20 000 zamestnancoch FBI. Ukradnuté dáta obsahovali mená, tituly, telefónne čísla a emailové adresy. Útočníci tvrdia, že Ministerstvu spravodlivosti trvalo týždeň, kým si všimli, že ich systémy boli kompromitované.

DAŇOVÁ SPRÁVA USA (IRS)

29. február 2016 – daňová správa USA (Internal Revenue Service - IRS) oznámila, že únik dát, ktorý zaznamenala v máji 2015 je oveľa rozsiahlejší ako sa pôvodne myslelo. Pôvodne išlo o kompromitáciu osobných údajov niečo vyše 100 000 daňových poplatníkov. Vo februári 2016 sa však zistený počet daňových poplatníkov, ktorých dáta unikli, zvýšil na 700 000. IRS za pravdepodobného útočníka označila sofistikovaných ruských kriminálnikov, ktorí majú za cieľ podať podvodné daňové priznania v budúcnosti.

VERIZON ENTERPRISE SOLUTIONS

25. marec 2016 – divízia spoločnosti Verizon poskytujúca IT a asistenčné služby pri riešení únikov dát po celom svete, sa stala obeťou útočníkov, ktorí odcudzili informácie o približne 1,5 milióne zákazníkov. Tieto dáta boli objavené bezpečnostným špecialistom Brianom Krebsom na predaj na čiernom trhu. Verizon sa vyjadril, že bezpečnostnú chybu našli a dotknutých zákazníkov kontaktovali.

OBČANIA TURECKA

4. apríl 2016 – zverejnenie osobných údajov 50 miliónov občanov Turecka bol jedným z najhorších únikov dát z vládnej inštitúcie vôbec. Dáta obsahovali mená, ID čísla, pohlavie, dátum a miesto narodenia, celú adresu, mesto a oblasť registrácie ID a mená otca a matky. Nie je jasné, odkiaľ tieto dáta unikli, minister spravodlivosti Bekir Bozdag však povedal, že počet dotknutých občanov je porovnateľný s počtom zapísaných voličov.

FILIPÍNSKA VOLEBNÁ KOMISIA

11. apríl 2016 – prienik do databázy filipínskej volebnej komisie spôsobil ešte rozsiahlejší únik dát z vládnej inštitúcie ako v Turecku. Kompromitované boli osobné údaje každého voliča vo Filipínach, čo je približne 55 miliónov. K útoku sa prihlásila hacktivistická skupina Anonymous Philippines, aby prinútila volebnú komisiu k zvýšeniu bezpečnosti na zariadeniach zabezpečujúcich sčítavanie hlasov pred národnými voľbami, ktoré sa mali uskutočniť 9. mája 2016. Uniknutú databázu o pár dní neskôr publikovala skupina LulzSec Pilipinas.

VIACERO VEĽKÝCH POSKYTOVATEĽOV FREEMAILU

5. máj 2016 – spoločnosť Hold Security, zaoberajúca sa poskytovaním bezpečnostných služieb, objavila viac ako 270 miliónov prihlasovacích mien a hesiel do najväčších freemailových služieb, ktoré boli zdarma dostupné v ruskom kriminálnom podsvetí. Nie je známe akým spôsobom tieto údaje unikli, išlo však približne o 57 miliónov účtov do Mail.ru, 40 miliónov účtov Yahoo, 33 miliónov účtov do Hotmailu a 24 miliónov účtov Gmailu. Identifikované boli aj stovky tisíc nemeckých a čínskych mien a hesiel, ktoré pravdepodobne patria zamestnancom najväčších bankových, výrobných a maloobchodných spoločností.

LINKEDIN

17. máj 2016 – únik dát z roku 2012, pri ktorom bolo útočníckmi ukradnutých približne 117 miliónov kombinácií emailu a hesla, vyvrcholil v roku 2016, keď bola táto databáza publikovaná online. Dotknutí používatelia LinkedInu boli v roku 2012 vyzvaní na zmenu hesla. Tým, čo tak neurobili, LinkedIn heslá promptne zneplatnil. Zatiaľ nie je známe, kto je za únik zodpovedný, LinkedIn však poskytol súčinnosť pri vyšetrovaní prípadu orgánom činným v trestnom konaní.

YAHOO!

22. september 2016 – spoločnosť Yahoo! oznámila, že v roku 2014 sa útočník, ktorý pravdepodobne pracoval pre zahraničnú vládu, zmocnil informácii o 500 miliónoch používateľských účtoch. Podarilo sa mu získať emailové adresy, heslá, celé mená, dátumy narodenia, telefónne čísla a v niektorých prípadoch aj bezpečnostné otázky a odpovede. Yahoo! v tomto prípade spolupracuje s orgánmi činnými v trestnom konaní a FBI.

DROPBOX

30. august 2016 – v auguste bol zverejnený únik dát zo služby Dropbox, ktorý obsahoval údaje o vyše 68 mil. používateľských účtov. V októbri CSIRT.SK získal údaje o účtoch, ktoré boli zaregistrované na e-mailové adresy zo slovenských domén a následne kontaktoval príslušných správcov. Vzhľadom na skutočnosť, že išlo o únik dát z roku 2012, nebol dopad až taký vážny. Bezpečnosť cloudových služieb je v súčasnosti veľmi diskutovaná téma. Z hľadiska bezpečnosti firemného prostredia odporúčame zakázať registrovanie cloudových účtov na pracovné e-mailové adresy a používanie verejných cloudových služieb na pracovné účely.

CISCO

3. november 2016 – nesprávne bezpečnostné nastavenie v mobilnej verzii webovej stránky spoločnosti Cisco „Professional Careers“ vytvorilo bezpečnostnú zraniteľnosť umožňujúcu prístup k osobným údajom uchádzačov o zamestnanie. Dáta boli prístupné medzi augustom a septembrom 2015 a medzi júlom a augustom 2016. Tieto dáta obsahovali mená, adresy, emailové adresy, telefónne čísla, používateľské mená, heslá, odpovede na bezpečnostné otázky, životopisy, motivačné listy a voliteľné údaje ako napr. pohlavie, rasa, veteránsky status či postihnutie. K údajom pravdepodobne pristúpil len bezpečnostný výskumník, ktorý zraniteľnosť nahlásil, spoločnosť Cisco však vynútila zmenu hesla u všetkých používateľov.

ADULTFRIENDFINDER.COM

13. november 2016 – táto zoznamka pre dospelých sa stalo obeťou hackerského útoku už druhýkrát za dva roky. Tento krát bol však objem uniknutých dát značný, až 412 miliónov používateľov prišlo o svoje osobné údaje, ktoré boli následne umiestnené na online čierny trh. Uniknuté dáta obsahovali emailové adresy, heslá, členský status, informácie o prehliadači, poslednú IP adresu, z ktorej bolo vykonané prihlásenie sa a nákupy používateľov.

AGENTÚRA MESTSKEJ DOPRAVY SAN FRANCISCO (MUNICIPAL TRANSPORTATION AGENCY)

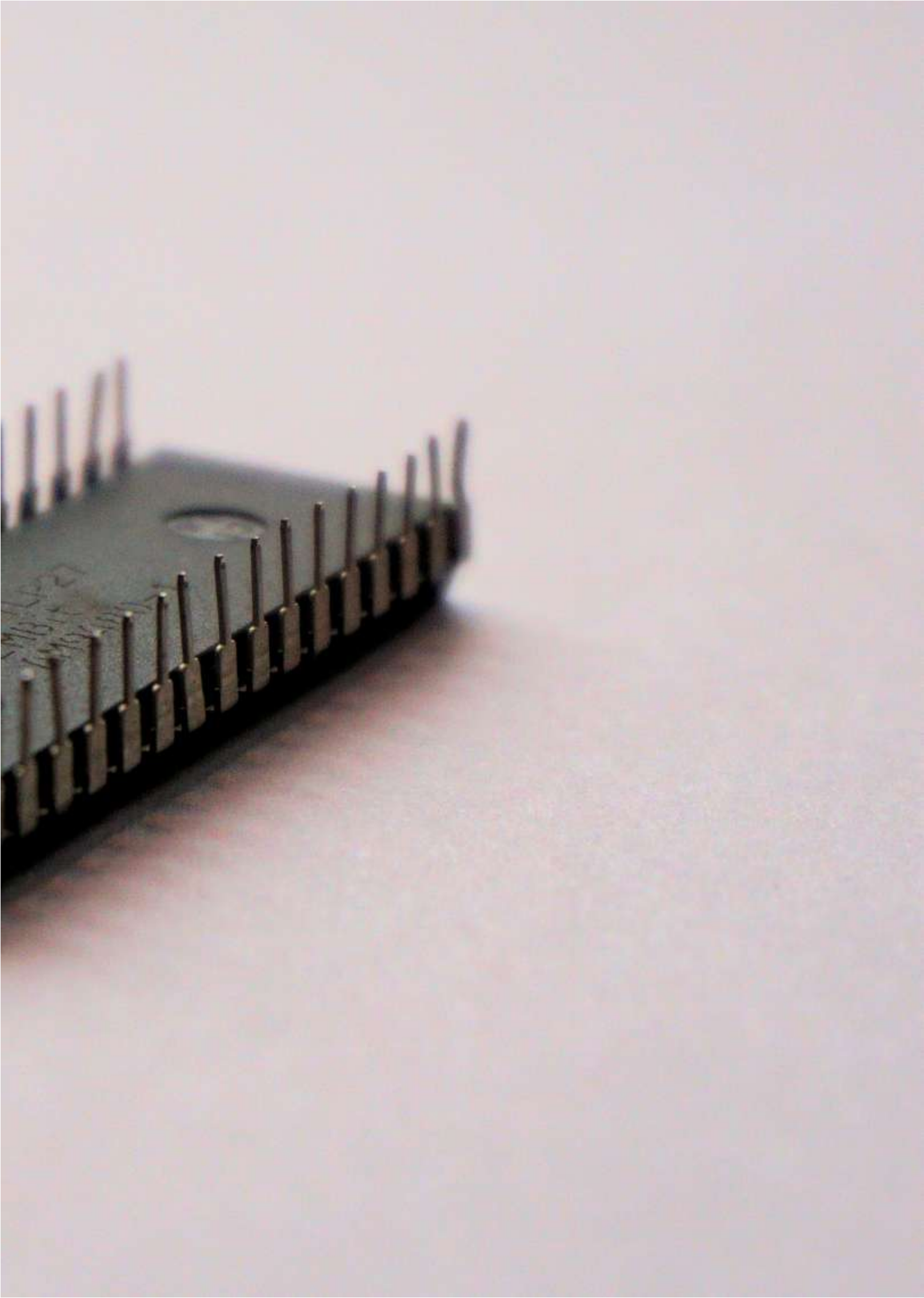
25. november 2016 – verejný železničný systém San Francisca, známy ako Muni, bol infikovaný škodlivým kódom počas víkendu Dňa vďakyvzdania. Výsledkom boli zamknuté kiosky a počítače a dva dni bezplatných jázd pre všetkých cestujúcich až do nedele 27. novembra, kedy boli všetky systémy opäť v plnej prevádzke. Útočníci tvrdia, že útok nebol cielený, ale že išlo o automatizovaný útok typu „spray and pay“. Získali 30GB dát, vrátane osobných údajov zamestnancov a cestujúcich a požadovali zaplatenie výkupného v hodnote 100BTC (v súčasnosti približne 100 000 EUR), v opačnom prípade hrozili zverejnením všetkých osobných údajov. Dopravná agentúra výkupné nezaplatila.

YAHOO!

14. december 2016 – spoločnosť Yahoo! po menej ako troch mesiacoch od ohlásenia úniku dát z roku 2014 oznámila ešte väčší únik z roku 2013. V tomto prípade mala byť kompromitovaná až 1 miliarda Yahoo účtov. Týmto sa tento únik dát dostal na čelo rebríčka ako najväčší únik dát v histórii.

3 PROJEKTY

CSIRT.SK aj v roku 2016 pokračoval v práci na projektoch zameraných zlepšovanie informačnej bezpečnosti v SR. Patrí k nim informačný systém Athena, laboratórium na analýzu malvéru, informačný systém MRM, nástroj na detekciu indikátorov kompromitácie IoC Checker a ďalšie.



3.1 Athena

Systém Athena je vyvinutý a prevádzkovaný špecializovaným útvarom CSIRT.SK za účelom bezpečnej komunikácie a zdieľania a výmeny informácií medzi zapojenými subjektmi. Bezpečná komunikácia v systéme Athena prebieha na základe správ, ktoré sú rozdelené do 4 kategórií:

- Bezpečnostné incidenty. Informácie o bezpečnostných incidentoch, ktoré má pôvodca záujem zdieľať s vybranými inštitúciami, CSIRT.SK, alebo skupinami inštitúcií. V prípade prebiehajúcich incidentov existuje priamo v prostredí systému Athena možnosť požiadať o súčinnosť CSIRT.SK. V tomto prípade je informácia automatizovaným spôsobom zaslaná do tiketovacieho systému CSIRT.SK.
- Varovania. Informácie o prebiehajúcich incidentoch, aktuálnych vektoroch útokov, zneužívaných zraniteľnostiach a indikátoroch kompromitácie (IoC).
- Odporúčané postupy. Informácie o odporúčaných postupoch pre zabezpečenie infraštruktúr a informačných systémov. V tejto sekcii zverejňujeme aj príručky pre hardening operačných systémov a aplikácií, odporúčané nastavenia a informácie na predchádzanie útokom.
- Zraniteľnosti. Informácie o aktuálnych zraniteľnostiach a postupoch ich ošetrenia, prípadne postupov na zníženie dopadov alebo pravdepodobnosti zneužitia zraniteľnosti (tzv. workaround).

Správy v systéme Athena sú klasifikované na základe TLP (Traffic Light protokolu) z hľadiska dôvernosti a každá správa je klasifikovaná na základe závažnosti na stupnici od 1 do 10. Do systému sa môže zapojiť každá inštitúcia verejnej správy a významné organizácie súkromného sektora z nasledujúcich oblastí, pričom prednostne sú zapájaní prevádzkovatelia prvkov kritickej infraštruktúry:

- energetický sektor,
- finančný sektor,
- ISP a správca domény a
- zdravotníctvo.

Pre zapojenie organizácie do systému Athena je potrebné zaslať žiadosť na adresu DataCentra.

3.2 MalwareLab

CSIRT.SK v roku 2016 pokračoval v budovaní laboratória určeného na analýzu vzoriek škodlivého kódu. V rámci zvyšovania kapacít a schopností tímu analytikov škodlivého kódu sa analytici zoznámili s ďalšími rozšírenými technológiami, ktoré sa zneužívajú pri vytváraní škodlivých vzoriek. Analytický tím poskytuje službu analyzovania vzorky nájdenej a extrahovanej zo siete svojej konštituencie, čím pomáha zmierňovať následky infekcie. Správa z analýzy malvéru obsahuje popis funkconality vzorky, indikátory kompromitácie a odporúčania ako postupovať pri odstraňovaní následkov infekcie, ale aj ako predchádzať prípadnej infekcii. Ukážka takéhoto reportu je dostupná na webovej stránke CSIRT.SK. V rámci zvyšovania bezpečnostného povedomia analytický tím pripravil pre verejnosť aj niekoľko prednášok a školení o základoch analýzy škodlivého kódu.

V tomto laboratóriu sa taktiež priebežne analyzujú aktuálne šírené vzorky škodlivého kódu, vďaka čomu si CSIRT.SK vytvára stále lepší obraz o hrozbách, ktorým čelia koncoví používatelia a administrátori inštitúcií a umožňuje mu držať krok s aktuálnymi trendmi v evolúcii malvéru.

Analytický tím v priebehu roka 2016 analyzoval napr. niektoré druhy ransomware, spyware, škodlivé skripty a súčasti exploit kitov. Zároveň v spolupráci s inými inštitúciami verejnej správy pomáhal minimalizovať následky bezpečnostných incidentov.

MalwareLab poskytuje dva typy služieb:

- Proaktívne analyzovanie "mass-targeted" malvéru šíriaceho sa v rámci slovenského adresného priestoru. Na základe analýz následne CSIRT.SK podniká kroky k odstraňovaniu identifikovaných Command & Control serverov, varovaniu dotknutých inštitúcií a zdieľaniu informácií s partnermi a verejnosťou.
- Analýza (potenciálne) škodlivej vzorky zachytenej našou konštituenciou alebo identifikovanej počas forenznej analýzy. Cieľom tejto analýzy je poskytnúť inštitúcii informácie o funkcionalite vzorky, možnom dopade na infraštruktúru a činnosť inštitúcie a odporúčania ako postupovať pri odstraňovaní následkov a šírenia infekcie.

3.3 MRM

Informačný systém Malicious Resource Manager (MRM) CSIRT.SK používa už od roku 2012 a denne spracováva približne 284 000 hlásení bezpečnostných udalostí. Okrem toho v sebe integruje zoznam kontaktov pre klientelu CSIRT.SK a poskytovateľov Internetových služieb, umožňuje priame nahlasovanie škodlivých a phishingových URL odkazov na analýzu a obsahuje rôzne generátory dát a pohľadov, napr. generátor incidentov súvisiacich s vybranou organizáciu, poskytovateľom internetového pripojenia (ISP) alebo konkrétnou IP adresou.
V zmysle úlohy 3.3 vládou schváleného Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, predmetom ktorej bolo navrhnúť metodiku pre spoločné postupy a podporu (hotline) za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív kritickej infraštruktúry, špecializovaný útvar CSIRT.SK vedie v informačnom systéme MRM vlastnú evidenciu týchto subjektov. Z tohto dôvodu CSIRT.SK priebežne rozširuje vlastnú verziu informačného systému MRM, aby napĺňal požiadavky v zmysle úloh.

3.4 CS Danube

CSIRT.SK, ako partner projektu CS Danube, sa aktívne zúčastnil na záverečnej konferencii, ktorá sa v rámci tohto projektu konala v marci 2016 v Prahe. Na konferencii boli prezentované štatistiky, zaujímavé incidenty za rok 2015 a metodika rozoznávania podvodných phishingových e-mailov. Projekt bol organizovaný v rámci medzinárodného programu spolupráce Danube v podunajskom regióne a bol realizovaný od apríla 2015 do marca 2016. Veľkým prínosom pre CSIRT.SK bolo získanie kontaktov na ostatné bezpečnostné tímy v podunajskom regióne a zdieľanie cenného know-how pri riešení bezpečnostných incidentov.

3.5 IoC Checker

CSIRT.SK spolupracoval s Fakultou matematiky, fyziky a informatiky UK v Bratislave na vývoji nástroja na detekciu indikátorov kompromitácie (IoC) v operačných systémoch Windows. Nástroj slúži na odhaľovanie prítomnosti IoC na základe výskytov súborov určených názvom alebo hashom, kontroluje spustené procesy a mutexy prítomné v systéme, obsahy registrov, DNS záznamy v cache, nadviazané sieťové spojenia, prípadne kombinácie predchádzajúcich. Súčasťou je aj serverová časť slúžiaca na správu a distribúciu IoC a prezeranie výsledkov kontroly.
IoC Checker vznikol na základe dvoch bakalárských prác a v súčasnosti je vo fáze neverejnej testovacej prevádzky.

3.6 Penetračné testy

Cieľom penetračného testovania a ohodnotenia zraniteľností je overenie úrovne zabezpečenia informačných systémov pred počítačovými útokmi, identifikovanie zraniteľností a navrhnutie bezpečnostných opatrení. CSIRT.SK je schopný vykonávať interné aj externé penetračné testy.

V prípade externých penetračných testov sú simulované aktivity útočníka z externého prostredia (najčastejšie siete Internet alebo Govnet). Týmto typom testu sa preveruje bezpečnosť webových stránok inštitúcií alebo celých verejne dostupných IP rozsahov. Takýto test je vhodné vykonať pre všetky novo nasadzované verejné portály alebo služby a systémy, ktoré boli zásadným spôsobom menené alebo neboli testované za posledné dva roky.

V prípade Interných penetračných testov sú simulované aktivity útočníka z internej siete. Ide o analógiu k situácii, keď je pracovná stanica v internej sieti inštitúcie kompromitovaná napríklad škodlivým kódom. Tento typ testu sa vykonáva najmä pre inštitúcie prevádzkujúce kritické informačné systémy verejnej správy, ústredné orgány štátnej správy a prevádzkovateľov prvkov kritickej infraštruktúry. Hĺbkový test je potrebné vykonať aj pre infraštruktúry, v ktorých prebehli závažné bezpečnostné incidenty. Takýto typ testu je nutné opakovať minimálne raz za dva až tri roky, ideálne však raz ročne. V prípade, že pri poslednom penetračnom teste bola kompromitovaná väčšia časť infraštruktúry, je potrebné vykonať penetračný test ihneď po odstránení nájdených zraniteľností.

CSIRT.SK začal vykonávať penetračné testy v roku 2013. Počas prvého roka bolo vykonaných 10 penetračných testov a 5 ohodnotení zraniteľností informačných systémov a sietí. V roku 2014 bolo vykonaných 9 testov a 1 ohodnotenie zraniteľností. Od roku 2015 sa počet testov rapídne zvýšil na 29 a 9 ohodnotení zraniteľností informačných systémov a sietí. Dôvodom bolo najmä systematické testovanie informačných systémov vytváraných v rámci Operačného programu Informatizácia Spoločnosti (OPIS).

Počas roka 2016 bolo vykonaných 56 penetračných testov (34 nových testov a 22 opakovaných testov) a jedno ohodnotenie zraniteľností. Vo viacerých prípadoch išlo o retesty projektov, ktoré boli testované už v roku 2015. Vykonaných bolo 5 interných penetračných testov priamo v priestoroch inštitúcií verejnej správy. V roku 2016 uskutočnil CSIRT.SK aj prvé lokálne bezpečnostné ohodnotenie WiFi sietí. V porovnaní s rokom 2015 bolo celkovo vykonaných viac externých penetračných testov, zároveň sa zvýšil počet testovaní internej infraštruktúry významných inštitúcií SR. Nezanedbateľná časť penetračných testov bola vykonaná na overenie účinnosti opatrení na zvýšenie bezpečnosti projektov financovaných z OPIS.

Po vykonaní penetračných testov CSIRT.SK poskytuje konzultácie a súčinnosť pri odstraňovaní odhalených nedostatkov. Po ich oprave sa vykoná opakovaný test za účelom overenia úplnosti nápravy zistených bezpečnostných zraniteľností.

4 VZDELÁVA-

V rámci zvyšovania povedomia v oblasti informačnej bezpečnosti a zvyšovania odborných spôsobilostí zamestnancov verejnej správy CSIRT.SK spolupracoval pri zabezpečovaní školení v inštitúciách verejnej správy ako napr. NBS, NBÚ, KP SR, MZVaEZ, a PZ SR.

Poskytnuté školenia boli zamerané na forenznú analýzu, riešenie a predchádzanie bezpečnostným incidentom, zvyšovanie povedomia v oblasti informačnej bezpečnosti a zabezpečenie systémov a sietí.

NIE

4.1 Kontrolný zoznam pre bezpečnosť webových aplikácií

CSIRT.SK počas vykonávania penetračných testov pozoroval časté opakovanie sa niektorých zraniteľností. Na základe týchto zistení a štandardných odporúčaných postupov vypracoval kontrolný zoznam bezpečnostných opatrení, ktoré by mali byť overené pred nasadením webového portálu do produkčného prostredia.

Podobne ako všetky nové technológie aj webové aplikácie so sebou priniesli nové zraniteľnosti a možnosti kompromitácie organizácie. Existuje celá škála útokov, ktoré môže útočník využiť na získanie prístupu k citlivým informáciám alebo prístupu do systémov, na ktorých sú webové aplikácie prevádzkované. Okrem implementácie opatrení na zaistenie bezpečnosti webových aplikácií je potrebné myslieť aj na zabezpečenie a hardening ich podporných systémov. Tento kontrolný zoznam stručne sumarizuje najdôležitejšie bezpečnostné aspekty pri vývoji a prevádzke webových portálov a je možné ho využiť pri vykonávaní interného auditu bezpečnosti webových aplikácií a webových stránok.

4.2 Bezpečnostná študovňa

Bezpečnostná študovňa je novovytvorená vzdelávacia sekcia na našom webovom sídle s cieľom koncentrovať informácie, články, návody a odporúčania z rôznych oblastí informačnej bezpečnosti. V súčasnosti študovňa obsahuje články, ktoré sa venujú jednak štandardom, organizačnej a personálnej bezpečnosti, outsourcingu IT, bezdrôtovým sieťam, vývoju informačných systémov, kontinuite činností, bezpečnosti mobilných a webových aplikácií, ale aj sociálnemu inžinierstvu a hrozbe v podobe útočníka z vnútra organizácie.

Obsah študovne postupne aktualizujeme a pridávame nové študijné materiály. V roku 2016 okrem iného pribudol archív študijných materiálov zo série vzdelávacích aktivít Ministerstva financií, ktoré prebehli v rokoch 2013 a 2014. Archív obsahuje učebnice informačnej bezpečnosti pre laikov, informatikov – ne-špecialistov v informačnej bezpečnosti, špecialistov v informačnej bezpečnosti, učiteľov a vedúcich zamestnancov. Materiály zahŕňajú aj prezentácie, ktoré boli v rámci tejto aktivity odprednášané.

4.3 Metodika pre zabezpečenie organizácií v rámci OPII

CSIRT.SK v spolupráci s Úradom podpredsedu vlády SR pre investície a informatizáciu vypracoval metodiku pre zabezpečenie organizácií v rámci OPII. Táto metodika obsahuje požiadavky na organizáciu rozdelené do oblastí:

- Administratívna a organizačná bezpečnosť,
- Vývoj a nasadenie informačného systému,
- Zabezpečenie externe dostupnej infraštruktúry,
- Zabezpečenie externe dostupných služieb – webové služby,
- Zabezpečenie internej infraštruktúry,
- Zabezpečenie pracovných staníc.

Metodika bola pôvodne vypracovaná pre potreby zaistenia bezpečnosti projektov OPII, je však dobre použiteľná pre organizácie, informačné systémy, webové aplikácie a koncové stanice všetkých typov, pre organizácie verejnej správy či súkromného sektora. Dodržaním odporúčaných postupov možno docieliť úroveň bezpečnosti zodpovedajúcu požiadavkám danej organizácie.

Motiváciou pre vznik tohto dokumentu bola snaha vytvoriť ucelený podklad pre organizácie verejnej správy pre systematické zabezpečenie informačnej bezpečnosti v organizácii, ktorý by bral do úvahy aktuálne využívané technológie s dôrazom na nasadzovanie projektov implementovaných v rámci OPII. Inšpiráciou pre vznik tohto dokumentu boli, podobne ako pri kontrolnom zozname pre bezpečnosť webových aplikácií, často opakujúce sa výsledky a pozorovania pri vykonávaní penetračných testov a riešených incidentov.

Požiadavky uvedené v dokumente boli vybrané tak, aby po ich splnení organizácia mala zabezpečenú základnú úroveň bezpečnosti (baseline), ktorá pokrýva štandardné bezpečnostné hrozby pre organizáciu.

4.4 Pracovná skupina CSIRT.CZ

Predmetom stretnutia pracovnej skupiny v januári 2016 bolo prezentovanie príspevkov o aktuálnych hrozbách v oblasti IT bezpečnosti, predstavenie nových nástrojov aj ukážky pracovných postupov. Pracovník CSIRT.SK vystúpil s prednáškou o analýze malvéru. Súčasťou stretnutia bola aj diskusia v rámci uzavretej skupiny pracovníkov CSIRT/CERT® tímov. CSIRT.SK s tímom CSIRT.CZ úzko spolupracuje. Na pravidelnej báze prebieha výmena osvedčených postupov pre analýzu bezpečnostných incidentov a zmiernenie ich dopadov.

4.5 ECSM

European Cyber Security Month (ECSM) je kampaň Európskej únie, ktorá má za cieľ propagáciu kybernetickej bezpečnosti medzi občanmi EÚ. Snaží sa o zmenu vnímania bezpečnostných hrozieb prostredníctvom propagácie informačnej bezpečnosti, vzdelávania, zdieľania dobrých praktík a súťaží.
CSIRT.SK pri príležitosti Európskeho mesiaca kyberbezpečnosti (ECSM) organizoval súťaž v analýze malvéru. Súťaž bola určená pre študentov a záujemcov z radov odbornej verejnosti, ktorí si chceli vyskúšať svoje schopnosti pri analýze vzorky neznámeho, potenciálne škodlivého, softvéru. Najlepší riešitelia získali od CSIRT.SK vecnú cenu. Taktiež bola zverejnená vzorová analýza súťažnej vzorky pre kontrolu a inšpiráciu samotných súťažiacich aj pre záujemcov, ktorí by si chceli dodatočne skúsiť analyzovať súťažnú vzorku po skončení súťaže.
Do ECSM sa CSIRT.SK zapojil aj prostredníctvom prednášok s bezpečnostnou tematikou pre širokú verejnosť na nasledovných podujatiach:
Na Open source víkende v Košiciach odznela prednáška o základoch analýzy malvéru, v rámci ktorej sa účastníci akcie dozvedeli, ako si pripraviť laboratórne prostredie s pomocou otvoreného softvéru, v ktorom je možné bezpečne spúšťať a analyzovať podozrivé súbory. Súčasťou prednášky boli aj ukážky analýzy vzorky potenciálne škodlivého softvéru.
Na Gymnáziu Poštová odznela prednáška o informačnej bezpečnosti zameraná na zvýšenie bezpečnostného povedomia. Prednáška bola určená pre študentov, učiteľov, aj verejnosť. Na prednáške boli prezentované základné atribúty informačnej bezpečnosti, najčastejšie hrozby a možnosti obrany jednotlivých používateľov pred bežnými útokmi.
Na Univerzite Pavla Jozefa Šafárika v rámci seminára Bezadis odznela prednáška o zraniteľnostiach v implementáciách SSL/TLS protokolov. Prednáška bola určená pre študentov a odbornú verejnosť. Účastníkom predstavila implementačné a konfiguračné chyby spolu s viacerými známymi zraniteľnosťami z posledných rokov, napr. SMACK, FREAK, DROWN, Logjam, ale aj Poodle a Heartbleed.
Viac o ECSM sa môžete dozvedieť aj z rozhovoru, ktorý CSIRT.SK poskytol portálu zoznam.sk.

4.6 Phishingový test

Phishing patrí k najčastejším spôsobom získavania osobných údajov na ich nekalé použitie. Email poskytuje jednoduchý spôsob ako nalákať obete. Legitímne vyzerajúci email od vašej banky, ktorá vás zdvorilo žiada o overenie totožnosti a iných údajov (napr. čísla kreditnej karty či prístupových kódov), je príkladom phishingu. Cieľom phishingu je získať citlivé osobné informácie (údaje o platobnej karte, meno a heslo k službe, ktorú používate, a pod.) alebo naviesť príjemcu správy na nainštalovanie nedôveryhodných aplikácií do počítača alebo mobilného telefónu, ktoré používateľa presmerujú na falošné webové stránky. Nevyžiadaná správa často obsahuje odkaz, prípadne súbor, obsahujúci skrytý malvér, ktorý sa nainštaluje do počítača alebo do mobilného telefónu, poškodzuje ostatné programy, mení nastavenia alebo odosiela rôzne údaje, a to bez vášho vedomia.
CSIRT.SK na základe zachytených podvodných elektronických správ vytvoril on-line phishingový test pre organizácie verejnej správy a širokú verejnosť. Poskytuje možnosť otestovať si svoju obozretnosť pri práci s elektronickou poštou a schopnosť odhaľovať falošné emaily, ktorých cieľom je získanie informácii a často aj spustenie škodlivého kódu na zariadení príjemcu.
Test pozostáva zo 17 testovacích otázok. Úlohou riešiteľa testu je rozhodnúť, či zobrazený email, ktorý prijal fiktívny používateľ Chuck Norris (chucknorris@gmail.sk), je legitímny alebo podvrhnutý útočníkom. Po skončení testu poskytujeme používateľovi správne odpovede aj s vysvetlením toho, čo si bolo potrebné všimnúť v jednotlivých otázkach testu.

4.7 Antall József Summer School

CSIRT.SK sa v júli 2016 zúčastnil letnej školy Józsefa Antalla v Budapešti s prednáškou „The Future of the Central European Cyber Security Platform. Is it an Effective Tool for the V4 Countries and Austria to Combat Cyber Threats?“. Letnej školy sa zúčastňujú študenti medzinárodných vzťahov. Prednáška bola zameraná na spoluprácu krajín strednej Európy v oblasti kybernetickej bezpečnosti, ale aj na zvýšenie bezpečnostného povedomia študentov, keďže sa jednalo o jedinú prednášku zameranú na túto oblasť. Študentom boli predstavené súčasné hrozby a významné bezpečnostné incidenty a spôsoby, ktorými sa EÚ prostredníctvom novej legislatívy snaží na tieto hrozby reagovať.

4.8 QuBit Conference

Zamestnanci CSIRT.SK sa v roku 2016 zúčastnili ako školitelia na konferencií QuBit 2016, kde sa podieľali na školení na tému Forenzná analýza Windows prostredníctvom Linuxu. Počas školenia boli účastníci oboznámení s najdôležitejšími príkazmi a postupmi počas forenznej analýzy a identifikácie dôkazov. Prednáška bola ďalej zameraná na file carving a data carving, vytváranie časovej línie pre analýzu udalostí v rámci kontextu a chronologické usporiadanie udalostí. Účastníkom boli tiež predstavene nástroje na forenznú analýzu, ktoré si potom mohli vyskúšať počas následných cvičení.

4.9 Letná škola kyberkriminality

V rámci vzdelávacích aktivít sa zástupca CSIRT.SK zúčastnil Letnej školy kyberkriminality organizovanej Univerzitou Pavla Jozefa Šafárika v septembri 2016. Cieľom Letnej školy bolo oboznámenie študentov Prírodovedeckej a Právnickej fakulty UPJŠ s rôznymi aspektmi počítačovej kriminality z pohľadu bezpečnostného analytika, súdneho znalca alebo vyšetrovateľa.
Zamestnanec CSIRT.SK v rámci Letnej školy kyberkriminality predstavil účastníkom prednášky a workshopy na témy týkajúce sa základov forenznej analýzy, základov analýzy škodlivého kódu, zvyšovania bezpečnostného povedomia, ako aj možnosti obrany proti útokom na webový server. Študenti informatiky aj práva si na týchto prednáškach a workshopoch vyskúšali technické aj právne úlohy súvisiace s riešením bezpečnostných incidentov a precvičili si komunikáciu v rámci medziodborovej spolupráce.

4.10 Cyber Crime Training

„Budovanie kapacít pre boj proti počítačovej kriminalite / Cyber Crime Training“, je názov projektu HOME/2013/ISEC/AG/INT/4000005300, v rámci cielenej výzvy na predkladanie návrhov projektov „Nezákonne používanie Internetu - INT“ z programu Európskej komisie „Predchádzanie a boj proti trestnej činnosti – ISEC“. Pod vedením Odboru počítačovej kriminality PZ SR na tomto projekte participoval aj CSIRT.SK poskytnutím školení forenznej analýzy. V rámci tohto projektu vzdelávania príslušníkov PZ SR v rámci budovania kapacít pre boj proti počítačovej kriminalite bolo vyškolených viac ako 250 príslušníkov PZ SR.

4.11 Zvyšovanie bezpečnostného povedomia

CSIRT.SK poskytuje pre inštitúcie štátnej správy školenia zamerané na zvýšenie bezpečnostného povedomia o rizikách, kybernetických útokoch a možnostiach ochrany pred nimi. V prípadoch, kedy sú informačné systémy organizácie z technického hľadiska zabezpečené, sa prípadnému útočníkovi viac oplatí pokúsiť sa zneužiť zraniteľnosť v podobe neuvedomelého používateľa. Účasť zamestnancov štátnej správy na tomto školení by mala napomôcť pri ich zorientovaní sa v oblasti informačnej bezpečnosti, naučiť ich odhaľovať potenciálny škodlivý kód, zvýšiť ich obozretnosť pri práci s Internetom a elektronickou poštou a zoznámiť ich s najzaujímavejšími kybernetickými incidentmi a ich príčinami v posledných rokoch. Školenie v trvaní do 4 hodín, vrátane diskusie a voľných kvízov, špecializovaný útvar CSIRT.SK pre inštitúcie štátnej správy SR zabezpečuje bezodplatne.

V rámci školenia je účastníkom ozrejmené, čo je to dôvernosť, integrita a dostupnosť a dôvody, prečo sú aj oni cieľom útočníkov, predstavia sa útoky sociálnym inžinierstvom, bežné formy škodlivého softvéru a v prípade záujmu je možné predviesť praktický útok na zraniteľnú webovú aplikáciu. V ďalšej časti prednášky sa poukazuje na časté chyby pri práci s informačnými a komunikačnými technológiami, účastníkom sa predstavia spôsoby zabezpečenia webových prehliadačov, bezpečné používanie emailu, sociálnych sietí, používanie šifrovania, riziká vzdialeného prístupu k IS, zabezpečenie WiFi spolu s praktickou ukážkou, bezpečné používanie mobilných zariadení, Internet of Things a organizačné aspekty bezpečnosti v organizácii. V závere prednášky sa účastníci dozvedia čo robiť v prípade vzniku bezpečnostného incidentu, sú im predstavené najzaujímavejšie incidenty v nedávnom období a odporúčania na záver.

4.12 Výučba na univerzitách

Pracovníci CSIRT.SK dlhodobo spolupracujú s Fakultou elektrotechniky a informatiky STU v Bratislave i Fakultou matematiky, fyziky a informatiky UK v Bratislave pri príprave prednášok z odborných predmetov, týkajúcich sa informačnej bezpečnosti. V letnom semestri odznela na FEI STU v rámci predmetu Počítačová kriminalita prednáška o penetračnom testovaní webových aplikácii. Na prednáške z Úvodu do informačnej bezpečnosti na FMFI UK sa pracovníci CSIRT.SK venovali okrem penetračných testov aj problematike sieťovej bezpečnosti a analýze malvéru. V zimnom semestri bola ďalším študentom FEI STU na predmete Spoločenské, morálne a právne súvislosti vývoja IS predstavená práca CSIRT.SK, s dôrazom na problematiku forenznej analýzy a penetračného testovania. V závere roka odzneli na predmete Manažment informačnej bezpečnosti FMFI UK dve prednášky predstaviteľov CSIRT.SK. Prvá bola zameraná na všeobecný pohľad na kyberkriminalitu, nasledujúca sa podrobnejšie venovala technikám a postupom forenznej analýzy.

CSIRT.SK má aj v roku 2017 záujem pokračovať v rozvoji spolupráce s univerzitami. V letnom semestri akademického roka 2016/2017 CSIRT.SK v spolupráci s Fakultou matematiky, fyziky a informatiky UK v Bratislave otvorí nový seminár nazvaný Vybrané kapitoly z informačnej bezpečnosti. Tento seminár budú viesť pracovníci CSIRT.SK, ktorí v rámci svojich špecializácií študentom predstavia jednotlivé úlohy a činnosti CSIRT tímov spolu s praktickými ukážkami a odporúčaniami pre ďalšie štúdium.

Absolventi seminára sa dozvedia o úlohách a spolupráci CSIRT/CERT® tímov, získajú základné informácie o bezpečnostných incidentoch, procese a postupe ich riešenia a využívaných podporných nástrojoch. Ďalej sa bude preberať penetračné testovanie a monitorovanie činnosti útočníkov, následne sa získané poznatky využijú pri zabezpečení a obrane prvkov infraštruktúry („hardening“). Ďalšie preberané témy sa budú venovať riešeniu incidentov na mieste, zaisťovaniu stôp a ich spracovaniu a vyhodnoteniu v rámci forenznej analýzy napadnutých pracovných staníc. Nevynecháme ani základy analýzy škodlivého kódu, ktorá je často pri riešení incidentov potrebná.

Absolventi seminára Vybrané kapitoly z informačnej bezpečnosti by mali byť pripravení na základné riešenie bezpečnostných incidentov a prácu v bezpečnostných tímoch.

5 BUDOVANIE

V oblasti spolupráce na národnej a medzinárodnej úrovni je dôležitá vzájomná dôvera. V roku 2016 boli Smernicou NIS vytvorené dve kooperatívne skupiny – Skupina pre spoluprácu a Sieť jednotiek CSIRT. Rovnako dôležitá je aj spolupráca na regionálnej úrovni v rámci platformy CECSP a v rámci cvičení zameraných na riešenie bezpečnostných incidentov, ako napríklad Cyber Europe, Cyber Coalition alebo Crossed Swords.

DÔVERY A SPOLUPRÁCA

5.1 Smernica NIS

Dňa 6. Júla 2016 bola Európskym parlamentom schválená Smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, tzv. smernica NIS, ktorá je prvým legislatívnym aktom riešiacim informačnú bezpečnosť v EÚ.

Jej cieľom je zaistiť vysokú úroveň sieťovej a informačnej bezpečnosti v Európe. Prostriedkom na splnenie tohto cieľa je súbor požiadaviek kladených na členské štáty, ku ktorým patrí predovšetkým zlepšenie pripravenosti a vzájomnej spolupráce a prijatie krokov pre riadenie bezpečnostných rizík a hlásenie závažných incidentov kompetentným národným autoritám. Členské štáty budú musieť vykonať identifikáciu prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, prijať národnú stratégiu v oblasti NIS, určiť jeden alebo viac vnútroštátne príslušných orgánov a jednotné kontaktné miesto pre bezpečnosť NIS, určiť jednu alebo viac jednotiek CSIRT a zabezpečiť ich spoluprácu na národnej úrovni. Smernica sa tiež zaoberá spoluprácou medzi členskými štátmi prostredníctvom skupiny pre spoluprácu a siete jednotiek CSIRT. Smernica prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb ukladá bezpečnostné požiadavky a povinnosť oznamovať incidenty.

Smernica nadobudla účinnosť v auguste 2016 a členské štáty majú od tohto času 21 mesiacov na to, aby ju transponovali do svojej národnej legislatívy. V SR ju touto úlohou poverený NBÚ, ktorý novým zákonom o kybernetickej bezpečnostní upraví kompetencie, činnosti, práva a povinnosti NBÚ, vecne príslušných autorít a jednotiek CSIRT, identifikuje prevádzkovateľov základných a digitálnych služieb a ustanoví ich povinnosti.

5.2 Sieť jednotiek CSIRT

Sieť jednotiek CSIRT (CSIRTs Network, ďalej len „sieť“) pozostáva z jednotiek CSIRT členských štátov a jednotky CERT-EU, ktorá je CSIRT tímom európskych inštitúcií. Cieľom tejto siete je výmena informácií na dobrovoľnej báze o službách, činnostiach, spôsobilostiach a incidentoch na základe vybudovanej dôvery medzi jednotlivými tímami. V prípade incidentu môže táto sieť vymieňať, sprístupňovať a prerokúvať informácie a prediskutovať a vykonať koordinovanú reakciu na incident či poskytnúť podporu pri jeho riešení.

Na neformálnych stretnutiach Siete jednotiek CSIRT Slovenskú republiku reprezentovali zástupcovia CSIRT.SK. Počas slovenského predsedníctva v Rade EÚ sa podieľali na rozvoji pravidiel a postupov fungovania tejto siete, tvorbe koncepčných materiálov a testovaní pilotného portálu pre túto sieť.

V roku 2016 sa uskutočnili tri neformálne stretnutia siete, z ktorých dve sa uskutočnili v Haagu a jedno, v poradí druhé stretnutie, sa konalo v Rige. Tieto stretnutia bývajú organizované popri významných konferenciách a workshopoch organizovaných agentúrou ENISA, združením TF-CSIRT, Europolom a inými organizáciami, aby sa redukoval čas a náklady spojené s cestovaním. Cieľom týchto stretnutí bolo pripraviť sa na formálne zahájenie fungovania tejto siete. Smernica NIS stanovuje, že si táto sieť nastaví vlastné pravidlá svojho fungovania. Z toho dôvodu boli hlavnou aktivitou počas stretnutí diskusie a workshopy s cieľom tieto pravidlá definovať, aby mohli byť na prvom formálnom stretnutí vo februári 2017 odsúhlasené. Ďalším dôležitým bodom agendy bola príprava plánu práce siete so zameraním na krátkodobé a strednodobé ciele. Rovnako dôležitým bodom agendy týchto stretnutí býva výmena informácií o riešených incidentoch, najlepších postupoch a projektoch, na ktorých jednotky CSIRT participovali.

Prvé formálne stretnutie siete jednotiek CSIRT sa uskutočnilo v dňoch 22. až 23. februára v meste Sliema na Malte. Na tomto stretnutí Slovenskú republiku reprezentovali zástupcovia CSIRT.SK a zástupca NBÚ. Počas tohto stretnutia boli tak ako sa predpokladalo jednohlasne odsúhlasené pravidlá fungovania siete. Tieto pravidlá, okrem iného, stanovujú, že každý členský štát menuje dvoch stálych zástupcov, ktorí sa budú zúčastňovať pravidelných stretnutí. V rámci zdieľania informácii sa aplikuje TLP protokol, zdieľanie utajovaných skutočností sa nevykonáva. Členovia siete sa dohodli, že primárnym rozhodovacím mechanizmom bude konsenzus, avšak o niektorých procedurálnych záležitostiach je možné rozhodnúť aj kvalifikovanou väčšinou. Každý člen siete jednotiek CSIRT je zodpovedný za informácie, ktoré sa rozhodne zdieľať. Sieť samotná nebude žiadať o prístup k externým zdrojom informácií, ani hradiť náklady spojené s prístupom k takýmto informáciám. Naopak sieť bude tam, kde je to možné používať znalosti a expertízu už existujúcich „sietí jednotiek CSIRT“ (napr. TF-CSIRT alebo FIRST). Predsedníctvo siete je založené na predsedníckom kalendári Rady EÚ a bude vykonávané tzv. predsedníckym triom – t.j. predseda, minulý predseda a budúci predseda. Aktuálnym predsedom je teda z Malty za asistencie delegátov zo Slovenska a Estónska. Agentúra ENISA bude pre sieť jednotiek CSIRT poskytovať sekretariát a podporovať jej fungovanie. Každých 18 mesiacov sieť pripraví správu o svojom fungovaní a predloží ju Skupine pre spoluprácu.

Komunita tímov CSIRT/CERT® v Európskej únii a ich spolupráca je založená na dôvere. V pravidlách fungovania siete sa uvádza, že zástupcom členského štátu v tejto sieti by mali byť ľudia, ktorí sú v tejto komunite známi, pravidelne sa stretávajú, spolupracujú, vzájomne si vymieňajú informácie a preto si dôverujú. Rovnako je dôležité, aby zástupcovia reprezentovali takú jednotku CSIRT, ktorá je medzinárodne uznávaná a akreditovaná združeniami ako napr. TF-CSIRT alebo FIRST a pravidelne dokazuje svoju pripravenosť riešiť incidenty kybernetickej bezpečnosti. Sieť jednotiek CSIRT je v úvodnom štádiu svojho fungovania a očakáva sa, že postupne naplní svoje ambície. Nimi sú byť úspešnou kooperatívnou skupinou na operatívnej úrovni a zvýšiť tak úroveň pripravenosti EÚ, ako aj čeliť závažným bezpečnostným incidentom.

5.3 CECSP

Stredoeurópska platforma kybernetickej bezpečnosti CECSP (Central European Cyber Security Platform) bola zriadená v roku 2013 z iniciatívy Českej republiky a Rakúska. Jej stálymi členmi sú zástupcovia národných, vládnych, vojenských jednotiek CSIRT, ako aj zástupcovia národných príslušných autorít s kompetenciami v danej oblasti zo Slovenska, Českej republiky, Poľska, Maďarska a Rakúska. Cieľom tejto platformy je intenzívna spolupráca týchto krajín v oblasti kybernetickej bezpečnosti, výmena informácií a zdieľanie skúseností o kybernetických útokoch a hrozbách. Spoločné úsilie o zvyšovanie úrovne kybernetickej bezpečnosti v strednej Európe prispieva k výmene získaného „know-how" a vzájomnej pomoci pri budovaní kapacít. V neposlednom rade táto forma spolupráce prispieva aj k upevneniu pozície stálych členov v európskom aj medzinárodnom prostredí.

V roku 2016 sa predstavitelia NBÚ a CSIRT.SK zúčastnili dvoch rokovaní CECSP, ktoré boli v rámci poľského predsedníctva v tejto platforme organizované vo Varšave. Okrem pravidelného informovania členov platformy o aktualitách a dôležitých udalostiach, ktoré sa od posledného stretnutia v jednotlivých členských štátoch udiali, bola počas nich prediskutovaná spoločná účasť členov platformy na cvičení Cyber Europe 2016, spoločné postoje k modelu fungovania vtedy formujúcej sa siete jednotiek CSIRT a skupiny pre spoluprácu podľa smernice NIS. Rovnako boli prezentované dôležité projekty, na ktorých sa tímy podieľali a bolo možné zúčastniť sa technického workshopu „Build your own botnet".

V roku 2017 je predsedajúcou krajinou tejto platformy Slovenská republika, ktorej predstavitelia poľského predsedníctva symbolicky odovzdali predsednícke kladivko. Najbližšie stretnutie CECSP sa uskutoční v Bratislave. Na rok 2017 je naplánované aj cvičenie kybernetickej bezpečnosti pre účastnícke štáty tejto platformy.

5.4 OBSE

V roku 2016 sa zástupca CSIRT.SK zúčastnil na stretnutí Neformálnej pracovnej skupiny ku kybernetickej bezpečnosti OBSE, ktorého cieľom, tak ako počas predchádzajúcich stretnutí, bolo zvýšiť transparentnosť, podporiť spoluprácu a dobrovoľné šírenie informácií a zefektívniť implementáciu opatrení na posilnenie dôvery (CBMs) v oblasti kybernetickej bezpečnosti. Účastnícke štáty OBSE boli vyzvané prediskutovať možnosti pre rozšírenie a zvýšenie aktivít na posilnenie a urýchlenie implementácie druhého súboru opatrení na budovanie dôvery v kybernetickej oblasti. Zástupca CSIRT.SK pracovnú skupinu informoval o pretrvávajúcich aktivitách v oblasti kybernetickej bezpečnosti SR a o podpore implementácie CBMs a pripravenosti participovať na vývoji a implementácii druhého súboru CBMs. Rovnako informoval o rôznych opatreniach na zvýšenie ochrany kritickej infraštruktúry a krízového manažmentu na národnej úrovni, o vytvorení Výboru pre kybernetickú bezpečnosť v rámci Bezpečnostnej rady SR v januári 2016, vytvorení pracovnej skupiny pre zosúladenie terminológie v oblasti kybernetickej bezpečnosti s medzinárodnými štandardmi a o prípravách SR na predsedníctvo v Rade EÚ a prioritách SR, ktoré sú v súlade s CMBs. Najvýznamnejším výstupom zasadania pracovnej skupiny bolo jednohlasné odsúhlasenie druhého súboru CBMs.

5.5 Cyber Europe

Cvičenie Cyber Europe sa postupom času stalo najväčším cvičením svojho druhu v Európe, ktoré je každé dva roky organizované Európskou agentúrou pre sieťovú a informačnú bezpečnosť. Tak, ako počas minulých rokov, aj v roku 2016 sa ho CSIRT.SK zúčastnil v roli hráča aj v roli národného plánovača. Plánovanie cvičenia zahŕňalo tri plánovacie konferencie a jeden „dry run“. Samotné cvičenie prebehlo v dňoch 13. – 14. októbra 2016 a bolo riadené z riadiaceho strediska v Aténach. Scenár cvičenia bol začlenený do prostredia IT, telekomunikácií a kybernetickej bezpečnosti a obsahoval rôzne typy bezpečnostných incidentov, s ktorými si hráči mali poradiť. Cvičenia sa okrem jednotky CSIRT.SK zúčastnili aj špecialisti informačnej bezpečnosti z NASES, VNET, SIS a NBÚ.

V prvej fáze cvičenia sa hráči vžili do role bezpečnostného analytika, ktorý dostával úlohy od svojho nadriadeného v priebehu niekoľkých mesiacov pred cvičením. Tieto úlohy pozostávali predovšetkým z forenznej analýzy, analýzy malvéru, ale riešené boli aj incidenty, ako napr. mobilné infekcie, kampane škodlivých reklám, OSINT alebo forenzná analýza bezpilotného lietadla (UAV, drone). Všetky incidenty, riešené v prvej fáze cvičenia, boli zdanlivo nesúvisiace a mali za úlohu postupne eskalovať situáciu do krízy na rôznych úrovniach: lokálnej, organizačnej, národnej a európskej.

V druhej fáze cvičenia následne jednotlivé tímy spolupracovali na vyriešení incidentov, vzájomne si vymieňali informácie a komunikovali na európskej úrovni prostredníctvom tele-konferencií. Cvičenie bolo pripravené tímom C3 z agentúry ENISA a zahrnuli do neho aj profesionálnych novinárov, ktorí na hráčov vyvíjali tlak telefonickými i emailovými žiadosťami o informácie a prispievali tak k realistickosti cvičenia. Rovnako k nej prispeli aj profesionálne vyzerajúce falošné spravodajské televízne vstupy, ktoré postupne informovali o rastúcej kybernetickej kríze v Európe a odhalili aj totožnosť whistleblowera, ktorý zo spoločnosti rozširujúcej škodlivý softvér exfiltroval údaje a snažil sa ich poskytnúť novinárom. V živom vysielaní z webovej kamery v jeho byte bolo následne vidieť ako jeho byt prepadli maskovaní útočníci a odvliekli ho nevedno kam.

Hráčom sa nakoniec vďaka vynikajúcej vzájomnej spolupráci podarilo poskladať všetky kúsky skladačky a zmierniť túto krízu vytvorením vakcíny proti škodlivému kódu, ktorý napadol mnoho európskych informačných systémov.

Súčasťou programu cvičení v roku 2016 od agentúry ENISA bolo aj cvičenie EuroSOPEx 2016, ktoré bolo zamerané na kontaktné body v členských štátoch, a ktorého cieľom bolo precvičiť znalosti EU-CSOPs a umožniť ich praktické použitie s využitím ich podpornej infraštruktúry. Cvičenie hráčom tiež umožnilo preveriť kontaktné body jednotlivých členských štátoch a oboznámiť sa s pilotnou Platformou spolupráce jednotiek CSIRT.

5.6 Cyber Coalition

V priebehu roka 2016 sa tím CSIRT.SK aktívne zapojil do prípravy a priebehu cvičenia Cyber Coalition 2016. Najväčšie cvičenie organizované Organizáciou Severoatlantickej zmluvy zamerané na oblasť kybernetickej obrany sa uskutočnilo na prelome mesiacov november a december. Zúčastnilo sa na ňom spolu viac ako 700 odborníkov informačnej bezpečnosti a právnych expertov. Cvičenie, ktoré je organizované každoročne, bolo riadené z riadiaceho strediska v CCDCOE v Estónsku. Počas neho na vyriešení simulovaných kybernetických incidentov spolupracovalo 27 krajín NATO, partnerských krajín a Cyber Defense Staff EU.

Úlohou účastníkov cvičenia bolo identifikovať hrozby a zmierniť možné dopady, ako aj zabrániť šíreniu škodlivej aktivity. Dôležitou súčasťou bolo preverenie spolupráce tímov a zúčastnených krajín, efektívne zdieľanie informácií o kybernetických incidentoch a koordinácia aktivít kybernetickej obrany.

CSIRT.SK v spolupráci so spoločnosťou ESET v rámci cvičenia riešil technické aspekty troch simulovaných bezpečnostných udalostí, a to so zameraním na vyšetrenie, elimináciu bezpečnostných incidentov a návrh opatrení v oblasti kybernetickej bezpečnosti. Dôležitou súčasťou bolo preverenie spolupráce všetkých zapojených inštitúcií a subjektov na národnej úrovni.

Počas cvičenia sa na simuláciu a automatizáciu cvičebného prostredia využíval NATO Cyber Range, ktorý je komplexným informačným systémom umožňujúcim imitáciu skutočných počítačových sietí a dátovej prevádzky.

5.7 Crossed Swords

V dňoch 9.-11.2.2016 sa v estónskom Talline uskutočnil 2. ročník (3. vrátane pilotného) medzinárodného cvičenia kybernetickej bezpečnosti Crossed Swords. Ide o cvičenie zamerané na činnosť Red Teamov, ktorých primárnym cieľom je vykonanie protiútoku voči kybernetickým cieľom. Ofenzívne ladenie scenárov odlišuje Crossed Swords od iných cvičení, ktoré sú majoritne zamerané na defenzívnu činnosť.

Cvičenia sa zúčastnilo približne 30 členov Red Teamu, ktorým bolo primárne cvičenie určené. Úlohou bola Rapid Response, teda promptná odpoveď na simulovanú bezpečnostnú krízu v regióne. Samotný Red Team bol rozčlenený na 3 podtímy, podľa znalostí a preferencii účastníkov:

- NET – tím zameraný na sieťové útoky, prieskum siete, mapovanie infraštruktúry,
- Client Side – zameranie na útoky na klientov, získavanie prístupu v nájdených sieťových segmentoch,
- WEB – tím zameraný na webové služby, útoky na webové servery, prehľadávanie obsahu serverov a podobne. V tomto tíme pôsobila aj pracovníčka CSIRT.SK.

Na zvládnutie úloh bola kľúčová spolupráca a výmena informácii v rámci tímov ako aj medzi jednotlivými subtímami. Možnosť otestovať svoje riadiace schopnosti mali vedúci subtímov, ktorí sa každý deň cvičenia menili. Organizátori zabezpečili aj Blue team, ktorý simuloval „obete“ útokov Red Teamu. Monitorovanie aktivít na sieti, výstavbu virtuálnej infraštruktúry a organizáciu celého cvičenia vykonávali ďalšie tímy. Spätná väzba z monitoringu činnosti účastníkov bola výrazným benefitom pretože podľa nej mohli účastníci prispôsobiť svoje ďalšie kroky.

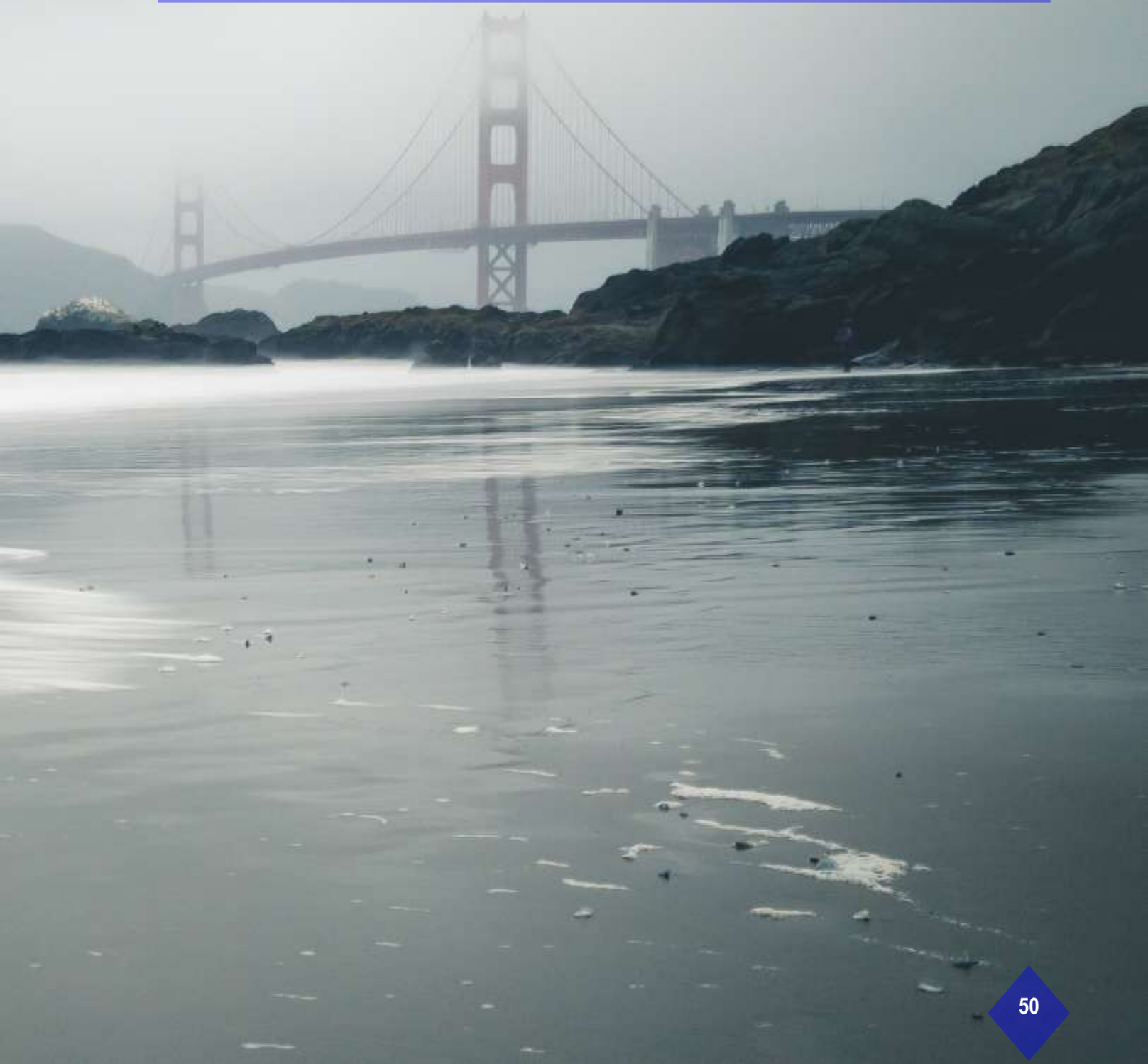
Cvičenie poskytlo iný pohľad na postupy v prípade kybernetickej hrozby. Väčšina cvičení sa zameriava na obrannú a preventívnu stránku. Vzhľadom na povahu dnešných útokov je však potrebné rozvíjať aj ofenzívnu stránku kybernetickej obrany.

5.8 Locked Shields

V dňoch 18. - 21.4. 2016 sa uskutočnilo pravidelné medzinárodné cvičenie kybernetickej bezpečnosti Locked Shields 2016. Ide o najväčšie podujatie tohto typu, ktoré organizuje NATO. Zamestnanci CSIRT.SK sa cvičenia aktívne zúčastnili. Základ tímu tvorili odborní pracovníci CSIRT.MIL. Na cvičení participovali aj profesionáli v oblasti kybernetickej bezpečnosti z civilného sektora. Táto aktivita sa uskutočnila na pracovisku MO SR v Trenčíne.

Cieľom cvičenia bol praktický tréning obrany pred kybernetickými útokmi rôzneho druhu v simulovaných podmienkach. Je pritom potrebné zohľadňovať ako technické stránky cvičenia (detekcia útokov, ochrana kritických systémov pred napadnutím, zabezpečenie dostupnosti a použiteľnosti chránených systémov, aktívna obrana, forenzná analýza a získavanie stôp/dôkazov o útokoch a podobne), tak aj netechnické aspekty (právne dôsledky, komunikácia s médiami a iné).

Tím Slovenskej republiky dosiahol výrazný úspech, keď v konkurencii 20 tímov z krajín NATO, ktoré sa zúčastnili cvičenia, obsadil v konečnom hodnotení prvé miesto. Členovia víťazného tímu, vrátane zástupcov CSIRT.SK, boli ocenení aj prezidentom Slovenskej republiky Andrejom Kiskom.



ÚSPECHY

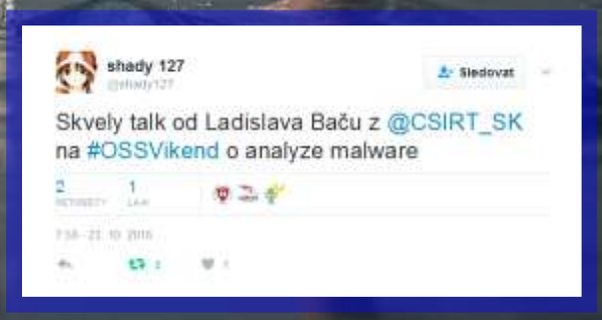
REFERENCIE A MÉDIÁ

Identifikácia 0-day zraniteľností

Tím CSIRT.SK objavil dve zraniteľnosti v produktoch spoločnosti Adobe, konkrétne v Adobe Flash Player, Adobe Reader, Adobe Acrobat , Adobe Acrobat Reader DC a Adobe Acrobat DC. Tieto zraniteľnosti boli nahlásené PSIRT tímu spoločnosti Adobe a v spolupráci s touto spoločnosťou boli odstránené. Analytické oddelenie CSIRT.SK zároveň zaznamenalo zneužitie zraniteľnosti CVE-2016-4116 v jednej vzorke malvéru, ktorá bola v čase nahlásenia zraniteľnosti stará minimálne 2 roky, išlo teda o aktívne zneužívanú 0-day zraniteľnosť. V oboch prípadoch bola zraniteľnosť spôsobená nesprávnou kontrolou pri načítavaní dynamicky linkovaných knižníc. Útočník mohol tieto zraniteľnosti zneužiť na načítanie vlastnej knižnice, ktorá obsahuje škodlivý kód (DLL hijacking). Takýto kód môže byť následne za istých okolností spustený s oprávneniami správcu systému a útočník tak môže prevziať kontrolu nad napadnutým zariadením.

Twitter

CSIRT.SK
Zamestnanci CSIRT SK budú mať až 5 prednášok na konferenci Informačná bezpečnosť 2017.
INFORMAČNÁ BEZPEČNOSŤ 2017


shady 127
Sledovať
Skvely talk od Ladislava Baču z @CSIRT_SK na #OSSVikend o analyze malware

CSIRT.SK
@CSIRT_SK
Slovenský tím vyhral cvičenie #LockedShields 2016! ccdcoe.org/slovakia-wins- ...
NATO CCD COE
Slovakia Wins #LockedShields 2016 Ahead of NATO and Finland

Referencie

„Na Slovensku pôsobí veľmi efektívny tím CSIRT.SK, špecializovaný útvar pre riešenie počítačových incidentov a slovenskí experti na kybernetickú bezpečnosť, vrátane tých vojenských, pravidelne participujú na medzinárodných tréningoch a súťažiach, kde obsadzujú popredné pozície..“
- Rastislav Kačmár, Slovak Security Policy Institute, október 2016.

Expertný dream team: „Nemôžem zabudnúť na konštruktívnu komunikáciu s ľuďmi z CSIRT-u „
- Daniel Rabina, SND, jún 2016

„I would hereby like to express my gratitude to you for participating in the fourth installment of the Antall József Summer school, thereby contributing to its successful realization. Based on the feedback we gained from the participants, your lecture was informative and gave a detailed overview of the topic. I hope that we will be able to welcome you as lecturer of our future events.
- Péter Antall, Antall József Knowledge Centre, júl 2016

Médiá

Recenzie | Novinky | TichéPC | Fórum | Články

Zoznam.sk

Domov › Novinky

Rozhovor o mesiaci kybernetickej bezpečnosti CyberSecMonth

Pondelok 24 oktober 2016, Autor: Pavel Bobik

Verzia pre tlač | Komentáre (0) | Send by email | Vybrali SME

EÚ každoročne organizuje mesiac kybernetickej bezpečnosti. V dnešnom rohovore si priblížime čo je cieľom tejto akcie.

O mesiaci kybernetickej bezpečnosti hovoríme s ing. Henrichom Slezákom z CSIRT.SK

Môžete nám priblížiť čo je CyberSecMonth?

European Cyber Security Month (ECSM) je kampaň Európskej únie, ktorá má za cieľ propagáciu kybernetickej bezpečnosti medzi občanmi EÚ. Snaží sa o zmenu vnímania bezpečnostných hrozieb prostredníctvom propagácie informačnej bezpečnosti, vzdelávania, zdieľania dobrých praktík a súťaží. Aj CSIRT.SK sa do tejto aktivity zapojil prostredníctvom prednášok a súťaže v analýze škodlivého kódu. Viac informácií je možné nájsť v našej tlačovej správe na http://www.csirt.gov.sk/aktualne-7d7.html?id=116 alebo priamo na stránke ECSM https://cybersecuritymonth.eu/

Najčítanejšie recenzie | Najčítanejšie novinky

TEST AMD RYZEN R7 1800X - zmŕtvychvstanie pre AMD (32)

Otestovali sme AMD Ryzen – najvýkonnejší procesor od AMD súčasnosti. Do redakcie sa nám dostal jeden z TOP kusov Ryzenu 7 1800X na svete. Nami testovaný kus ide pretaktovať vysoko...

Xiaomi Mi5s - ultrasonický skener v akcii (4)

Samsung Gear S3 - all in one hodinky na vašom zápästí (0)

SONY PlayStation 4 Pro + VR - nová dimenzia hrania + Súťaž o hru Gravity Rush 2 (0)

Testujeme teplovodivé pasty (11)

facebook

MINISTERSTVO ZDRAVOTNÍCTVA SLOVENSKEJ REPUBLIKY

Titulná stránka | FAQ | Mapa stránky | Kontakty | Textová verzia | Čierno-biela verzia | Kontrastná verzia | English

O ministerstve | Zdravotná starostlivosť | Materiály a dokumenty | Médiá | SK PRES

Domov

- Ministerstvo zdravotníctva
- Materiály a dokumenty
- Zdravotná starostlivosť
- Kategorizácia a cenotvorba
- Vzdelávanie a uznávanie kvalifikácií
- Projekty a výzvy
- Mediálne informácie
- Legislatíva a financovanie
- Zahraničné vzťahy a Európska únia
- Generická preskripcia
- Inštitút zdravotnej politiky
- Spoločnosť pre zavedenie unitárneho systému verejného zdravotného poistenia a.s.
- Farmácia
- Informačná bezpečnosť a ochrana údajov

Domov › Informačná bezpečnosť a ochrana údajov | Späť | Tlačiť

Informačná bezpečnosť a ochrana údajov

Vážení poskytovatelia zdravotnej starostlivosti

Bezpečnosť je pre nás prvoradá, preto by sme Vás radi upozornili, že pred dvoma rokmi ukončila spoločnosť Microsoft podporu a aktualizáciu systému Windows XP. Počítače s Windows XP sú tak vo zvýšenej miere ohrozené vírusmi a škodlivým softvérom. Zároveň s ukončením podpory Windows XP prestávajú aktualizácie svojich aplikácií pre tento systém vydávať i nezávislí dodávatelia. Z tohto dôvodu je ďalšie používanie operačného systému Windows XP bezpečnostným rizikom, ktoré by ste mali zvážiť, pokiaľ ho budete používať na prihlasovanie sa do Národného zdravotníckeho informačného systému (NZIS). **Aj špecializovaný útvar CSIRT.SK používanie operačného systému Windows XP neodporúča.** Jeho používanie znamená pre poskytovateľov zdravotnej starostlivosti podľa CSIRT.SK bezpečnostné i legislatívne riziká. Od 8. apríla 2014, kedy spoločnosť Microsoft pre tento operačný systém ukončila podporu, nie sú preň už naďalej vydávané aktualizácie, bezpečnostné záplaty a hotfixy. Používanie tohto systému predstavuje riziko nákazy pracovnej stanice viacerými druhmi škodlivého softvéru s veľmi negatívnymi potenciálnymi dôsledkami. Patrí k nim predovšetkým únik citlivých informácií, ich modifikácia alebo zničenie. Pre poskytovateľov zdravotnej starostlivosti to znamená priame ohrozenie osobitných kategórií osobných údajov a podľa názoru CSIRT.SK je spracúvanie týchto údajov na takto zraniteľnom systéme porušením povinnosti *„chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením"* ustanovenej zákonom č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení. Prevádzkovateľ, ktorým je každý poskytovateľ zdravotnej starostlivosti je povinný prijať bezpečnostné opatrenia zodpovedajúce spôsobu spracúvania osobných údajov, pričom musí vziať do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov a rozsah možných rizík spôsobilých narušiť bezpečnosť a funkčnosť informačného systému. **Medzi opatrenia**, ktoré ustanovuje vyhláška Úradu na ochranu osobných údajov SR č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení v platnom znení, okrem iného, **patrí aj „aktualizácia operačného systému a programového aplikačného vybavenia".**

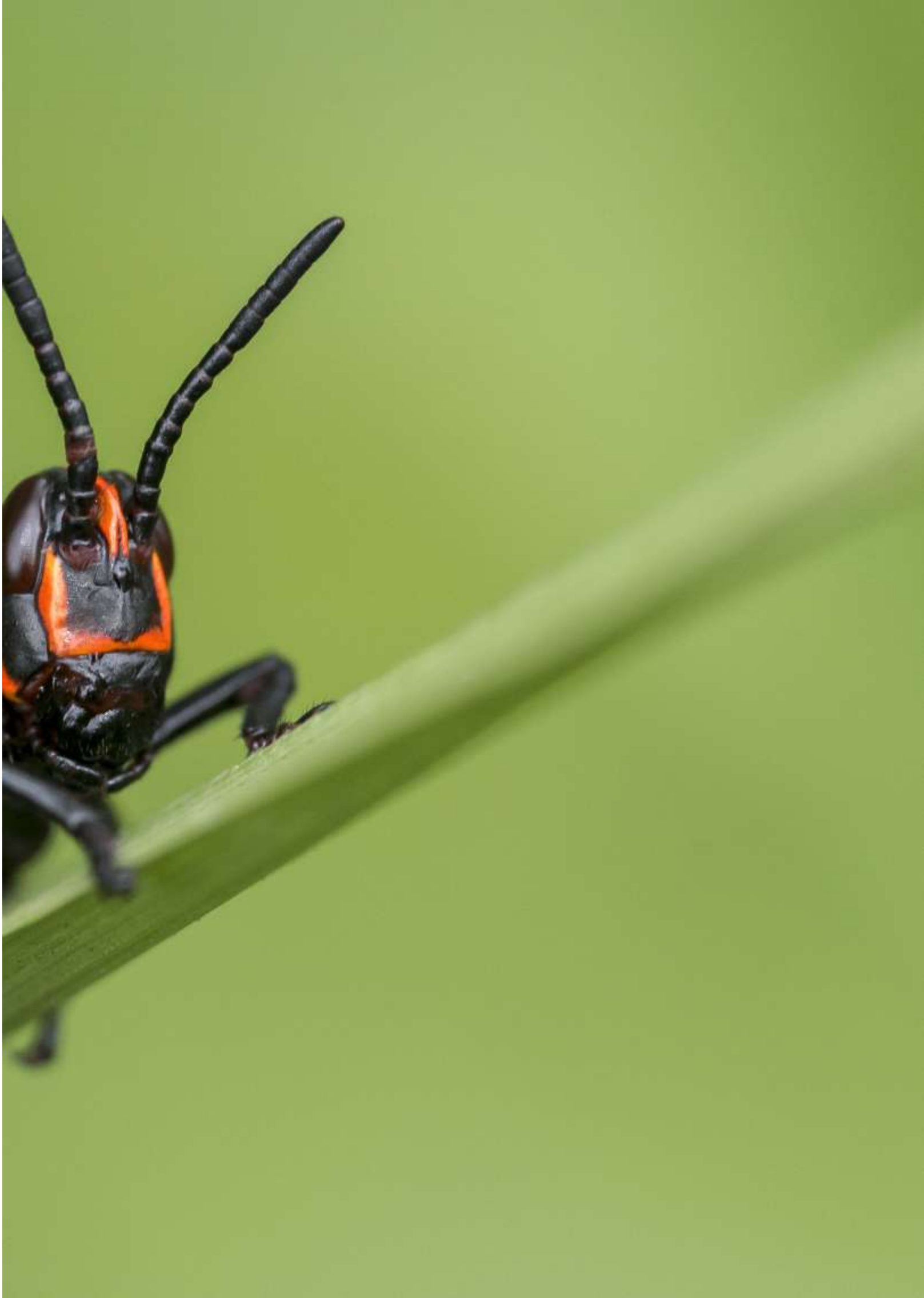
TERMÍN Y A

SKRÁTKY

0-day zraniteľnosť	zraniteľnosť, ktorá nie je všeobecne známa, resp. pre ňu neexistuje záplata
Anonymous	anonymné a decentralizované nehierarchické hacktivistické hnutie
APT	(advanced persistent threat) pokročilá trvalá hrozba
autentifikácia	overenie identity subjektu
backdoor	(zadné dvierka) metóda umožňujúca obísť bežnú autentifikáciu
blue team	odborný tím, ktorého úlohou je obrana IS pred reálnymi útočníkmi a pred red teamom v rámci cvičení v oblasti kybernetickej bezpečnosti
botnet	sieť kompromitovaných zariadení ovládaných útočníkom bez vedomia ich vlastníkov s cieľom využitia ich výpočtovej kapacity na realizáciu neželanej aktivity (napr. zasielanie spamu a phishingových správ, alebo realizáciu útokov typu DDoS) a pod.
C&C	(Command and Control) server používaný na riadenie botnetu na diaľku
C3	(Cyber Crisis Cooperation) tím pripravujúci cvičenia Cyber Europe v rámci agentúry ENSIA
cache	vyrovnávacia pamäť, ktorá slúži na prechodné ukladanie dát alebo sekvencií programu
CBMs	Confidence Building Measures
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CECSP	Central European Cyber Security Platform
CERT®	Computer Emergency Response Team, ochranná známka Carnegie Mellon University
cookies	malý súbor, ktorý WWW server pošle prehliadaču, ktorý ho uloží na počítači používateľa a slúži na uchovanie informácii špecifických pre klienta alebo webovú stránku
CRON	nástroj, ktorý sa používa pre automatizovanie opakovaných úloh prostredníctvom pravidelného spúšťania skriptov v OS Unix
CSIRT	Computer Security Incident Response Team
CVE	(Common Vulnerabilities and Exposures) zoznam identifikátorov verejne známych zraniteľností informačnej bezpečnosti
CVV	(Card Verification Value) 3 – 4 miestne číslo na kreditnej karte, používajúce sa pri platbách, pri ktorých nedochádza k fyzickému kontaktu karty s platobným terminálom
DataCentrum	materská organizácia CSIRT.SK a rozpočtová organizácia MF SR
defacement	útok na webovú stránku, ktorý má za cieľ zmeniť jej vzhľad, často umiestnením vlastnej stránky propagujúcej politické, náboženské alebo iné názory
defense in depth	(castle approach) bezpečnostný koncept, pri ktorom je naprieč informačným systémom umiestnených mnoho vrstiev bezpečnostných opatrení s úmyslom poskytnúť redundanciu v prípade zlyhania jednej alebo viacerých bezpečnostných vrstiev
DLL hijacking	
DNS	(domain name system) systém doménových mien prekladá názvy domén na IP adresy
DNS amplification	
DoS/DDoS útok	(denial of service / distributed denial of service attack) odmietnutie služby, resp. distribuované odmietnutie služby, je technika útoku na internetové služby alebo stránky. Dochádza pri nej k zahlteniu služby požiadavkami, ktoré môže spôsobiť pád alebo nefunkčnosť a teda nedostupnosť pre ostatných používateľov. V prípade DDoS útoku sa použije viac ako jeden stroj, prípadne botnet.
drive-by-download	technika, pri ktorej sa škodlivý kód sťahuje zo siete Internet bez vedomia používateľa
dry run	skúšobné prevedenie činnosti za účelom odhalenia nedostatkov
EC3	European Cybercrime Centre
ECSM	European Cyber Security Month
ENISA	Európska agentúra pre sieťovú a informačnú bezpečnosť
EU-CSOPs	EU Cyber Standard Operating Procedures

exploit	program, dáta alebo sekvencia príkazov, ktoré využívajú programátorskú chybu, ktorá spôsobí pôvodne nezamýšľanú činnosť softvéru.
exploit kit	softvérový balík na prevádzku webových serverov za účelom identifikácie zraniteľností a ich zneužitia infekciou malvérom
FEI STU	Fakulta elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave
file/data carving	obnova súborov z povrchu disku na základe jeho štruktúry
FIRST	fórum tímov pre riešenie počítačových incidentov
flood útok	útok zahltením, ide o jeden z typov DDoS útokov
FMFI UK	Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
forenzná analýa	aplikácia metodickej sady techník a postupov na získanie digitálnych dôkazov o kybernetickej kriminalite a na jej ďalšie vyšetrovanie
freemail	bezplatná služba emailu
FTP	file transfer protocol
Govnet	nadrezortná informačná sieť SR, ktorá slúži na efektívnu a bezpečnú výmenu informácií. Vznikla na základe ustanovenia vlády SR č. 310/1993
hardening	proces konfigurácie, pri ktorej sa zvyšuje bezpečnosť informačného systému
HTTP GET	typ požiadavky protokolu HTTP na dáta od špecifikovaného zdroja
IB	informačná bezpečnosť
ICS/SCADA	Industrial Control Systems / Supervisory Control and Data Acquisition
IoC	Indicator of compromise
IoT	Internet of Things
IP	Internet Protocol
IRS	Internal Revenue Service
IS	informačný systém
ISP	Internet service provider
IT	informačné technológie
KP SR	Kancelária prezidenta Slovenskej republiky
kritická infraštruktúra	súbor prvkov podľa zákona č. 45/2011 Z.Z.
log záznam	záznam o činnosti a behu IS
MRM	(Malicious Resource Manager) nástroj CSIRT.SK na správu informačných zdrojov o škodlivej aktivite
malvér	škodlivý softvér
IPMI	Intelligent Platform Management Interface
MO SR	Ministerstvo obrany SR
mutex	(mutual exclusion) synchronizačný mechanizmus v OS
MZVaEZ SR	Ministerstvo zahraničných vecí a európskych záležitostí SR
NASES	Národná agentúra pre sieťové a elektronické služby
NATO	Organizácia Severoatlantickej zmluvy, ktorej je SR súčasťou od roku 2004
NBS	Národná banka Slovenska
NBÚ	Národný bezpečnostný úrad
NCKB	Národné centrum kybernetické bezpečnosti
NTP(d)	Network Time Protocol (daemon)
OBSE	Organizácia pre bezpečnosť a spoluprácu v Európe, SR je účastníckym štátom od roku 1993
online skimming	technika na neoprávnené získanie údajov o kreditnej karte
open-resolver	DNS server odpovedajúci na požiadavky mimo svojej domény. Open resolvery bývajú použité napríklad pri útokoch typu DNS Amplification.
OPII	Operačný program Integrovaná infraštruktúra
OS	operačný systém
OSINT	(open-source intelligence) typ informácií využívaných pri spravodajskej činnosti, ktoré sú získané z tzv. otvorených zdrojov, teda voľne dostupných informačných kanálov
penetračný test	test, ktorý formou pokusu o neoprávnený prienik do systémov odhalí slabiny a mieru zraniteľnosti organizácie
PF UPJŠ	Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach

phishing	činnosť, pri ktorej sa podvodník snaží vylákať od používateľov ich digitálnu identitu, napríklad prihlasovacie mená, heslá, údaje k bankovému účtu a podobne
počítačový incident	porušenie alebo bezprostredná hrozba porušenia bezpečnostných politík, bezpečnostných zásad alebo štandardných bezpečnostných pravidiel prevádzky informačných a komunikačných technológií
PZ SR	Policajný zbor SR
ransomvér	(ransomware) druh malvéru, ktorý zabraňuje prístupu k infikovanému počítaču, a spravidla vyžaduje zaplatenie výkupného (anglicky ransom) za sprístupnenie počítača
red team	odborný tím, ktorého úlohou je preveriť bezpečnosť IS simulovaním aktivít útočníkov
rootkit	balík počítačových programov, pomocou ktorých je možné maskovať prítomnosť malvéru v počítači
sinkhole server	DNS server, ktorý poskytuje falošné informácie na zabránenie použitia legitímneho DNS záznamu server, slúžiaci na monitorovanie a zabraňovanie komunikácie v rámci siete botnet
SIS	Slovenská informačná služba
SW	softvér
NIS	network and information systems
sociálne inžinierstvo	spôsob manipulácie ľudí za účelom vykonania určitej akcie alebo získania určitej informácie
spam	nevyžiadaná pošta
spyware	špehovací malvér
SSH	secure shell
SSL/TLS	(Secure Sockets Layer / Transport Layer Security) protokoly, ktoré slúžia na šifrovanie dát
TF-CSIRT	Task Force of Computer Security and Incident Response Teams
tiketovací systém	SW na spracovanie riešenia incidentov
TLP	(Traffic Light Protocol) systém klasifikácie informácií pri ich zdieľaní
trojan	(trójsky kôň) program, ktorý vykonáva deštruktívnu činnosť, pričom sa skrýva za užitočnú činnosť
TTL	time to live
UAV	unmanned aerial vehicle
UPnP	Universal Plug and Play
URL	Uniform Resource Locator



CSIRT.SK
WWW.CSIRT.GOV.SK