CSIRT.SK
WWW.CSIRT.GOV.SK

CSIRT.SK REPORT 2015

CSIRT.SK REPORT 2015

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

OBSAH

ZHRNUTIE

Dokument, ktorý držíte v rukách, čiastočne mapuje stav informačnej bezpečnosti v Slovenskej republike a prezentuje vybrané udalosti, incidenty, štatistiky, projekty a aktivity špecializovaného útvaru na riešenie počítačových incidentov CSIRT.SK v roku 2015.

V roku 2015 útvar CSIRT.SK naďalej pokračoval v snahe zvyšovať úroveň bezpečnosti a bezpečnostného povedomia občanov na Slovensku a aj v zahraničí. Za posledný rok čelil slovenský kybernetický priestor rôznym hrozbám. Pre šírenie škodlivej aktivity na Internete bol zneužívaný nielen zahraničný kybernetický priestor, ale boli zneužívané aj slovenské domény a IP adresy.

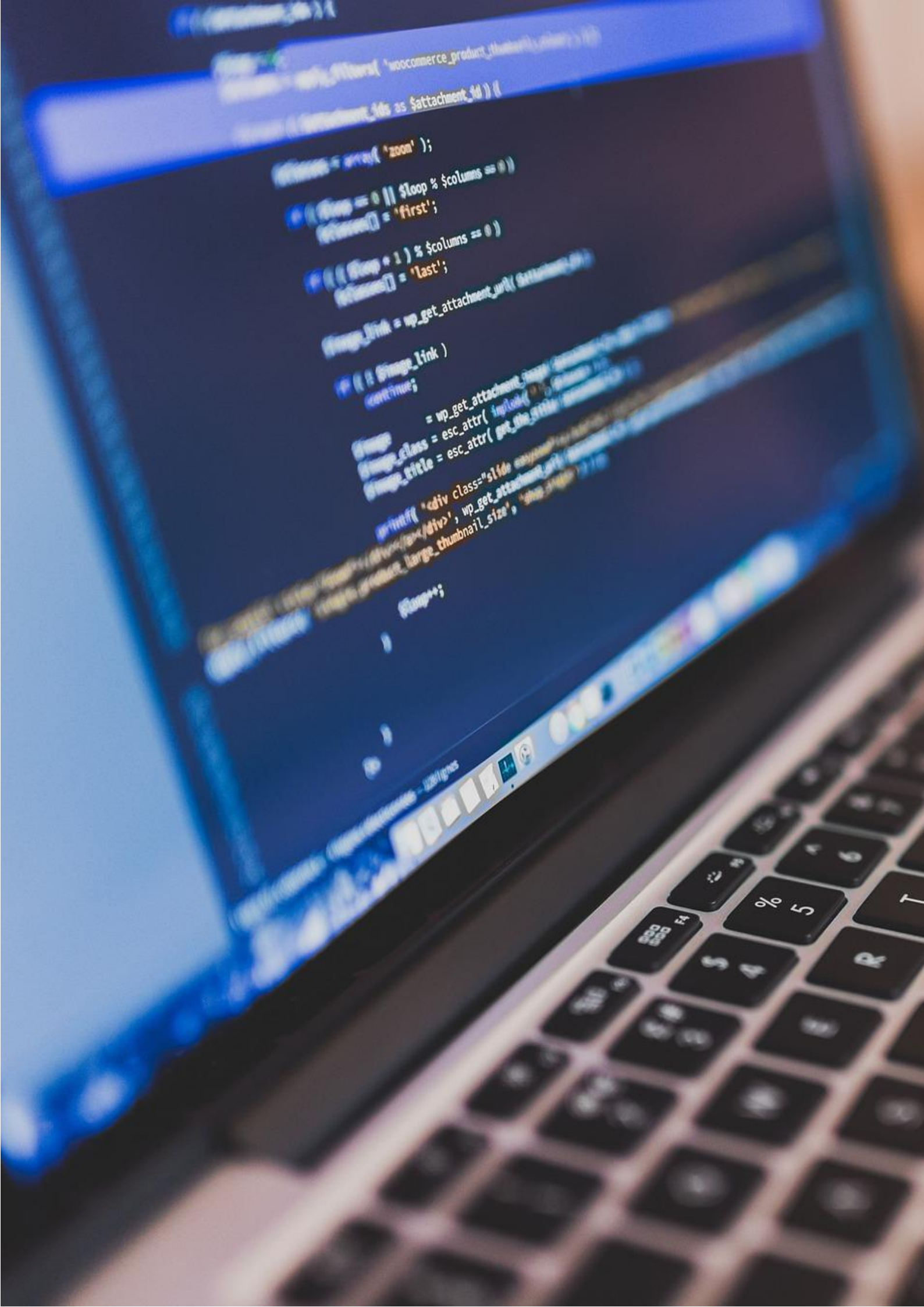
Vo všeobecnosti sa začiatok roku 2015 niesol v duchu zneužívania makier, šírenia novej verzie ransomvéru a kritickej zraniteľnosti v knižnici glibc. Ďalej sme zaznamenali opätovný nárast výskytu phishingových správ so škodlivým obsahom, zraniteľností na úrovni softvéru, ale aj hardvéru a útoku na protokol TLS. Záver roku patril exploitom zneužívajúcim zero-day zraniteľnosti v rôznych produktoch.

Vyskytli sa zraniteľnosti SSL/TLS, útoky typu watering hole, kampane CozyBear (CozyCar), zraniteľnosť Stagefright, kompromitovanie smerovačov a bankový trójsky kôň SlemBunk.

V rámci incidentov sme riešili nezabezpečené databázy MongoDB, škodlivé kódy ako Ramnit, Dyre a Dridex. Medzi zaujímavé incidenty taktiež patrili rozsiahly výskyt zraniteľnosti Rom0 a phishingové emaily zasielané ako správy Ministerstva spravodlivosti SR.

Rok 2015 nebol pre náš tím CSIRT.SK významný iba z pohľadu riešenia bezpečnostných incidentov v oblasti informačnej a kybernetickej bezpečnosti. Práve v tomto roku sme zakončili niekoľko ročnú prípravu a stali sme sa právoplatným členom združenia FIRST (Forum for Incident Response and Security Teams), rozšírili sme portfólio našich služieb a zapojili sme sa do nových medzinárodných projektov.

Ľudia sú ostražitejší a už dávno neplatí, že slepo dôverujú informačným technológiám. Hrozby nedostupnosti elektronických služieb, straty alebo zneužitia údajov sú stále prítomné. Bezpečnosť sa dotýka každého z nás, preto vám prinášame informácie o našich projektoch a aktivitách, do ktorých sa môžete zapojiť a ktorých súčasťou môže byť aj Vaša organizácia.



ÚVOD

Oblasť informačnej a kybernetickej bezpečnosti sa stáva čoraz viac skloňovanou témou aj v Slovenskej republike.

Pripravenosť na bezpečnostné incidenty a ich prevencia v sektore informačných a komunikačných technológií (IKT) je v súčasnosti veľmi dôležitá aj z dôvodu nadchádzajúceho predsedníctva Slovenskej republiky v Rade Európskej únie v druhej polovici roku 2016. Práve vďaka predsedníctvu bude SR v centre diania a bude musieť zaistiť ochranu množstva citlivých informácií, ktoré bude v súvislosti s predsedníctvom spracúvať, distribuovať a uchovávať.

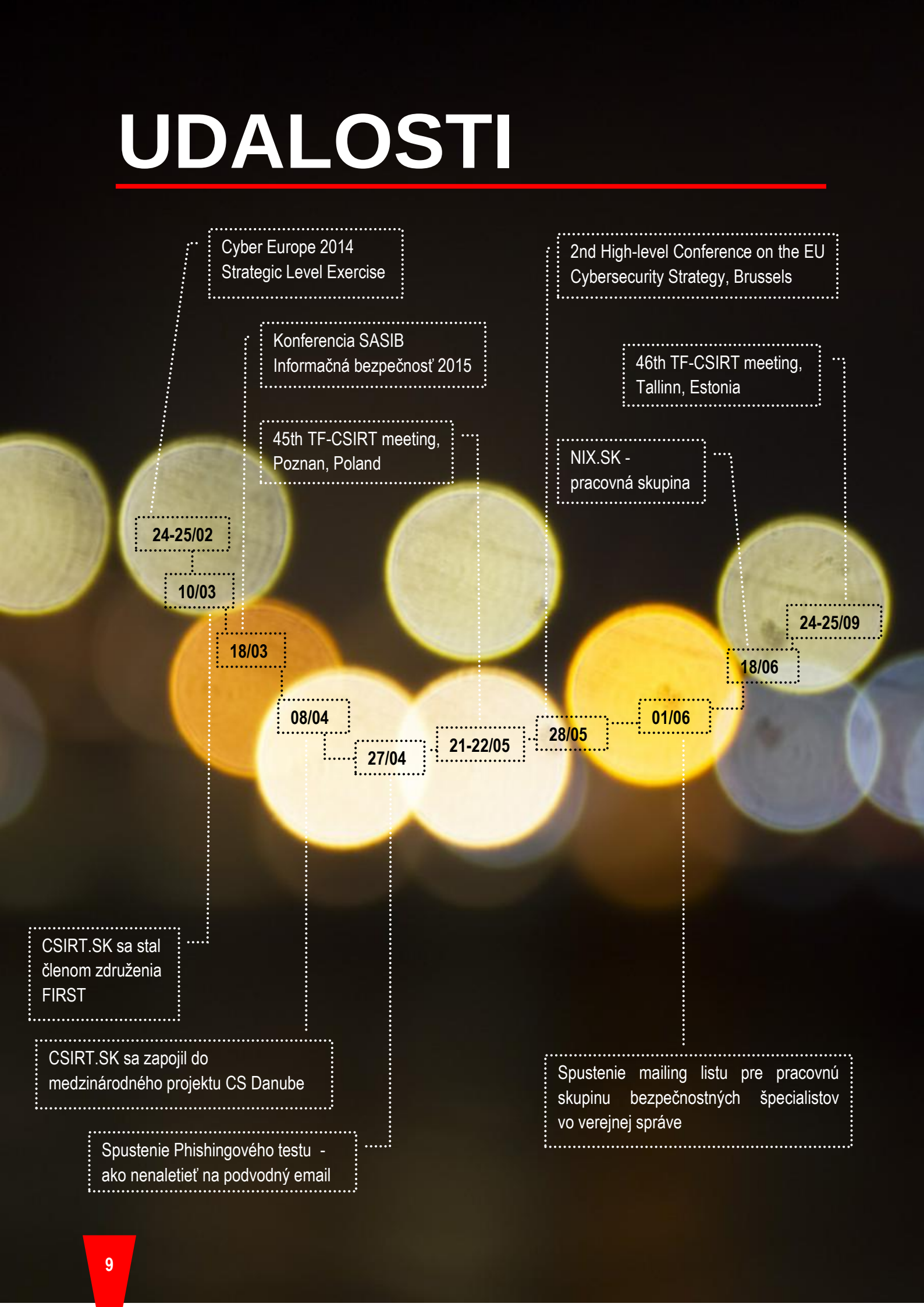
Sektor IKT je prierezovým sektorom a na jeho funkciách závisia aj ostatné sektory kritickej infraštruktúry ako napríklad energetika, priemysel, elektronické komunikácie alebo doprava. Zaistenie bezpečnosti IKT by preto malo byť spoločným záujmom verejnej správy aj súkromného sektora. Verejno-súkromné partnerstvá (PPP), jednotný postup a spolupráca všetkých inštitúcií štátnej správy pri riešení tejto problematiky sú trendom vo väčšine členských štátov EÚ a malo by tomu tak byť aj na Slovensku.

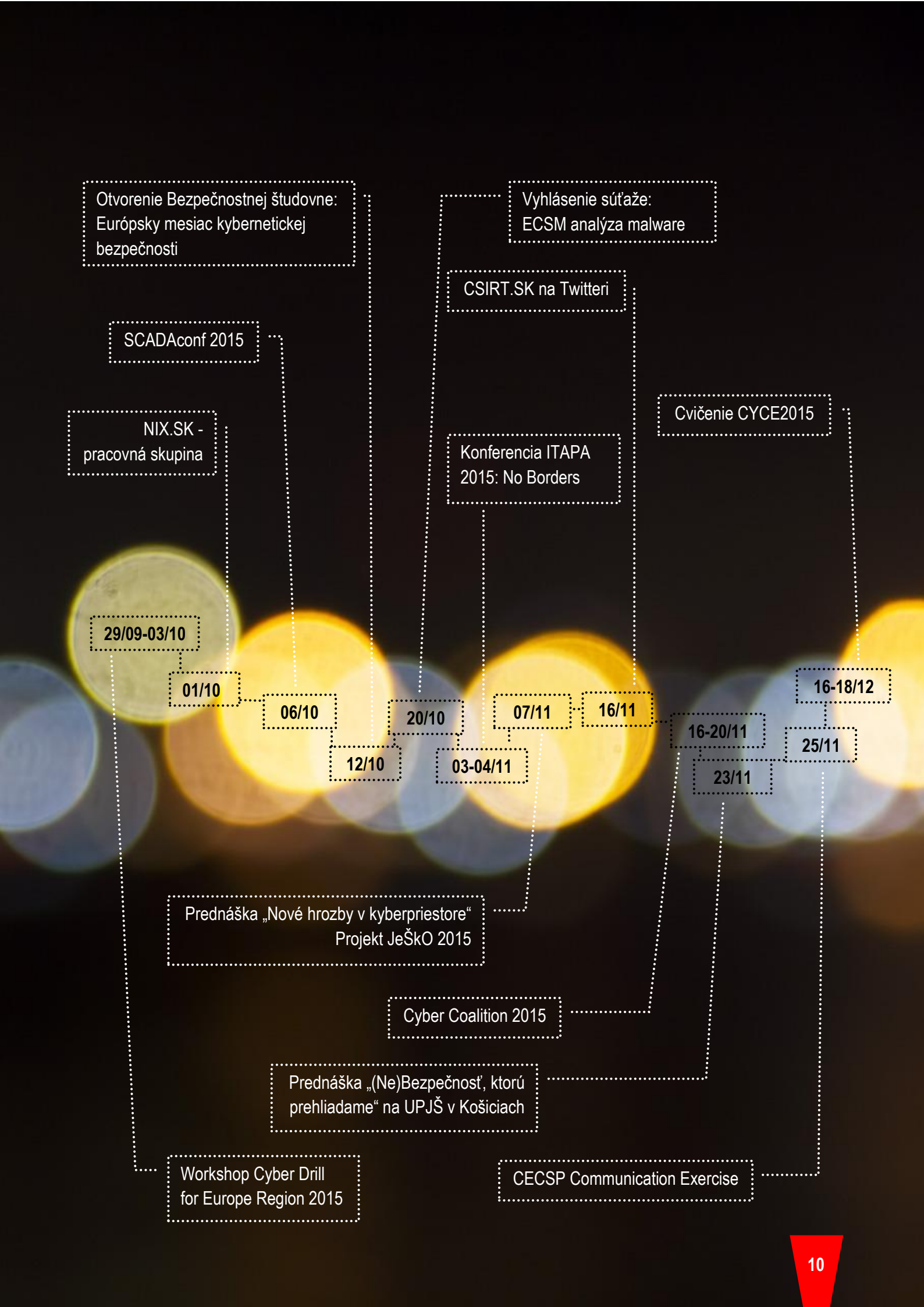
Vývoj informačných a komunikačných technológií spolu s rozšírením dostupnosti Internetu vytvorili mnohé nové ekonomické príležitosti, ale umožnili tiež vznik zraniteľností, ktorých zneužitie potenciálnymi hrozbami zvnútra aj zvonku predstavuje riziká, ktoré je potrebné periodicky prehodnocovať. Neexistuje žiaľ jednoduché opatrenie na elimináciu týchto rizík technologickým riešením.

Pre adekvátnu informačnú bezpečnosť je potrebný mnohovrstvový prístup a hĺbková ochrana na všetkých úrovniach informačných systémov, pretože v prípade len čiastkového zabezpečenia môže organizácia nadobudnúť falošný pocit istoty a bezpečia, čo je veľmi nebezpečné. Je dôležité komunikovať s odborníkmi z CSIRT/CERT tímov a im blízkeho okolia, byť informovaný a poznať hrozby, ktorým sú vaše informačné systémy každý deň vystavené.

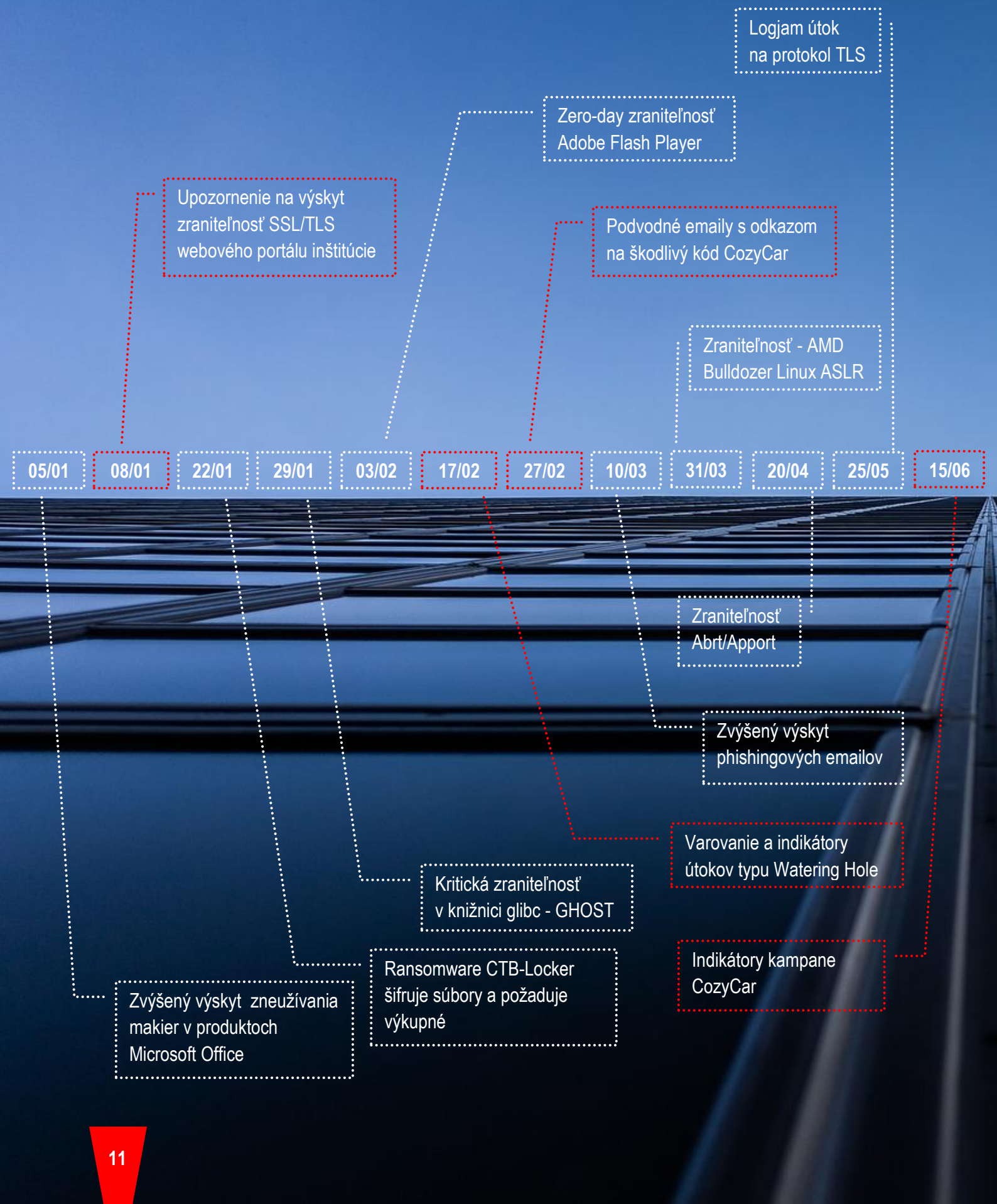
UDALOSTI
VAROVANIA
INCIDENTY

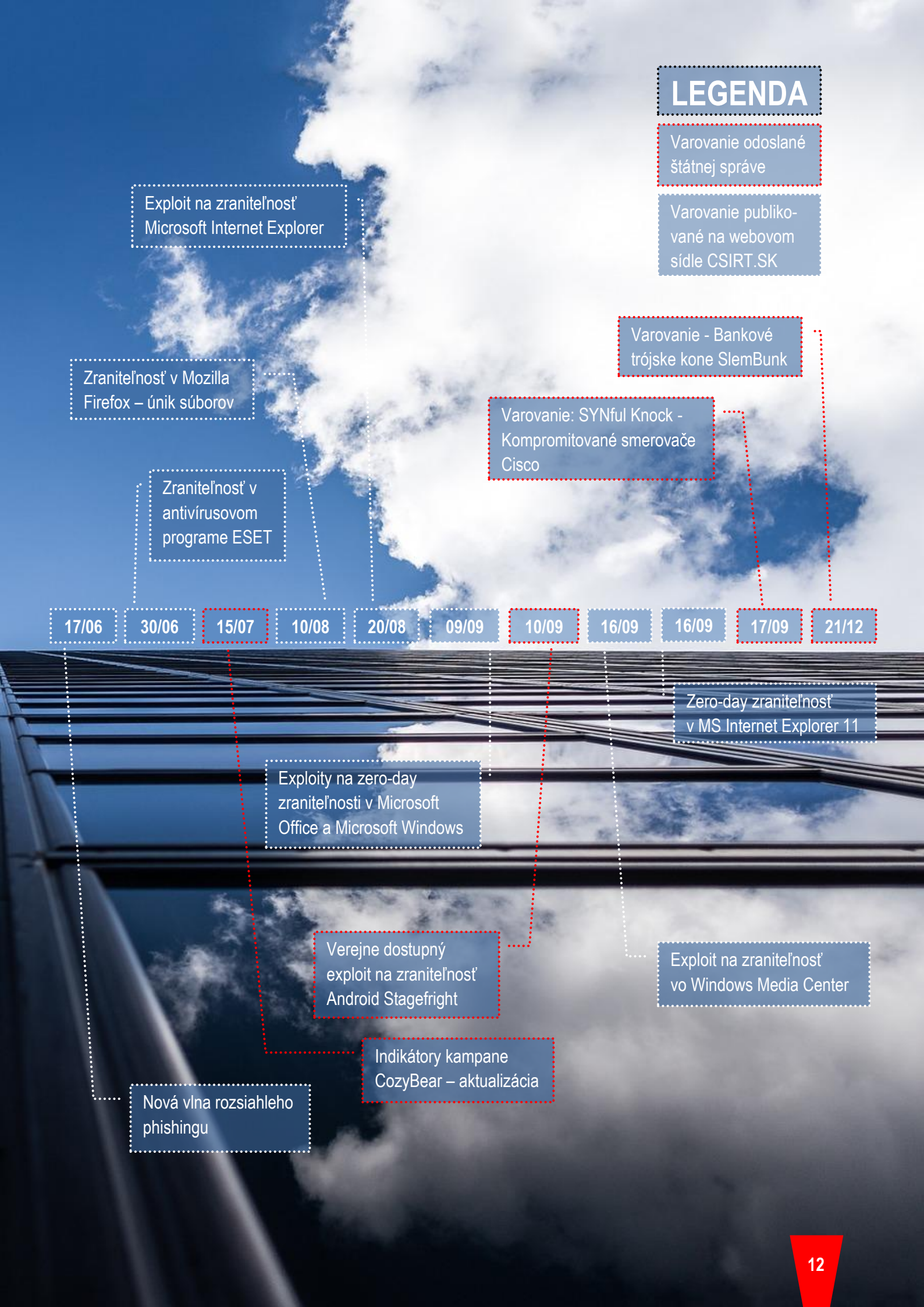
UDALOSTI


Cyber Europe 2014
Strategic Level Exercise
Konferencia SASIB
Informačná bezpečnosť 2015
45th TF-CSIRT meeting,
Poznan, Poland
2nd High-level Conference on the EU
Cybersecurity Strategy, Brussels
46th TF-CSIRT meeting,
Tallinn, Estonia
NIX.SK -
pracovná skupina
24-25/02
10/03
18/03
08/04
27/04
21-22/05
28/05
01/06
18/06
24-25/09
CSIRT.SK sa stal
členom združenia
FIRST
CSIRT.SK sa zapojil do
medzinárodného projektu CS Danube
Spustenie Phishingového testu -
ako nenaletieť na podvodný email
Spustenie mailing listu pre pracovnú
skupinu bezpečnostných špecialistov
vo verejnej správe


Otvorenie Bezpečnostnej študovne: Európsky mesiac kybernetickej bezpečnosti
Vyhlásenie súťaže: ECSM analýza malware
CSIRT.SK na Twitteri
SCADAconf 2015
NIX.SK - pracovná skupina
Cvičenie CYCE2015
Konferencia ITAPA 2015: No Borders
29/09-03/10
01/10
06/10
12/10
20/10
03-04/11
07/11
16/11
16-18/12
16-20/11
25/11
23/11
Prednáška „Nové hrozby v kyberpriestore“ Projekt JeŠkO 2015
Cyber Coalition 2015
Prednáška „(Ne)Bezpečnosť, ktorú prehliadame“ na UPJŠ v Košiciach
Workshop Cyber Drill for Europe Region 2015
CECSP Communication Exercise

VAROVANIA


Logjam útok na protokol TLS
Zero-day zraniteľnosť Adobe Flash Player
Upozornenie na výskyt zraniteľnosť SSL/TLS webového portálu inštitúcie
Podvodné emaily s odkazom na škodlivý kód CozyCar
Zraniteľnosť - AMD Bulldozer Linux ASLR
05/01
08/01
22/01
29/01
03/02
17/02
27/02
10/03
31/03
20/04
25/05
15/06
Zraniteľnosť Abrt/Apport
Zvýšený výskyt phishingových emailov
Varovanie a indikátory útokov typu Watering Hole
Kritická zraniteľnosť v knižnici glibc - GHOST
Indikátory kampane CozyCar
Ransomware CTB-Locker šifruje súbory a požaduje výkupné
Zvýšený výskyt zneužívania makier v produktoch Microsoft Office


LEGENDA
Varovanie odoslané štátnej správe
Varovanie publiko-vané na webovom sídle CSIRT.SK
Exploit na zraniteľnosť Microsoft Internet Explorer
Varovanie - Bankové trójske kone SlemBunk
Zraniteľnosť v Mozilla Firefox – únik súborov
Varovanie: SYNful Knock - Kompromitované smerovače Cisco
Zraniteľnosť v antivírusovom programe ESET
17/06
30/06
15/07
10/08
20/08
09/09
10/09
16/09
16/09
17/09
21/12
Zero-day zraniteľnosť v MS Internet Explorer 11
Exploity na zero-day zraniteľnosti v Microsoft Office a Microsoft Windows
Verejne dostupný exploit na zraniteľnosť Android Stagefright
Exploit na zraniteľnosť vo Windows Media Center
Indikátory kampane CozyBear – aktualizácia
Nová vlna rozsiahleho phishingu

VÝBER Z VAROVANÍ

UPOZORNENIE NA VÝSKYT ZRANITEĽNOSTI SSL/TLS WEBOVÉHO PORTÁLU INŠTITÚCIE

CSIRT.SK v rámci proaktívneho monitoringu zisťoval výskyt zraniteľnosti protokolu SSL/TLS na portáloch verejnej správy SR a vybraných subjektov poskytujúcich elektronické služby.

Išlo napr. o zraniteľnosť, ktorá umožňuje vykonať útok POODLE, ktorým je možné dešifrovať časti SSL/TLS komunikácie alebo podporovanie zastaraných protokolov ako napr. SSLv2.

VAROVANIE - RANSOMWARE CTB-LOCKER A INDIKÁTORY KOMPROMITÁCIE

Varovanie obsahovalo informácie o škodlivom kóde, ktorý bol šírený prostredníctvom emailov. Po aktivácii škodlivého kódu CTB-Locker, ktorý je kategorizovaný ako ransomvér, nasledovalo zašifrovanie súborov používateľa a následne bolo požadované výkupné.

Phishingová kampaň mala za cieľ rôzne spoločnosti, ale aj súkromné osoby. Dotknuté boli aj európske inštitúcie, resp. agentúry. Zaujímavá bola polymorfická povaha škodlivého kódu, keď jeho odtlačok bol rozličný u každej obeti. Identifikované boli niektoré riadiace servery (C&C), ale aj kompromitované pracovné stanice. Obsahom varovania boli analýzou zhromaždené indikátory kompromitácie, napr. záznamy v registroch, škodlivé domény a súbory, ktoré následne slúžili na odhaľovanie ostatných kompromitovaných pracovných staníc.

VAROVANIE A INDIKÁTORY ÚTOKOV TYPU WATERING HOLE

Útoky typu watering hole sú formou sociálneho inžinierstva a bývajú cielené na konkrétne organizácie, resp. na produkty, ktoré organizácia používa. Útočník kompromituje, prípadne podvrhne, webové stránky výrobcu alebo dodávateľa, ktoré sú pre používateľov z danej organizácie (napr. zamestnancov) dôveryhodné. Útočník uloží na podvrhnuté stránky exploit, ktorý využíva existujúcu zraniteľnosť. Pri návšteve danej stránky je počítač obete infikovaný škodlivým kódom.

Varovanie bolo reakciou na masívnu kampaň. Pri útokoch boli používané škodlivé odkazy na webové stránky, ktoré boli presmerovávané pomocou skracovačov URL odkazov goo.gl. Takýchto škodlivých webových stránok bolo zaznamenaných viac ako 65.

Útočníci skryli škodlivý odkaz do bloku JavaScriptového kódu, ktorý sa podobal na kód používaný Google analytics. Škodlivý odkaz sa načítal iba raz a to práve, keď používateľ pohol myšou. Takto sa snažili útočníci obísť jednoduché automatizované URL skenery.

Keďže bola použitá modifikovaná verzia Google analytics, tak bolo možné zistiť počet „kliknutí“ na škodlivé odkazy. Celkovo bolo zaznamenaných viac ako 5,2 milióna „kliknutí“.

Škodlivý kód na kompromitovaných stránkach následne zaslal útočníkom informácie o používanom prehliadači a verziách Javy a Schockwave Flash pluginu. Následne bol na prioritné ciele doručený špeciálny škodlivý kód pre konkrétnu IP adresu.

VAROVANIE - PODVODNÉ EMAILY S ODKAZOM NA ŠKODLIVÝ KÓD COZYCAR

Zaznamenali sme šírenie podvodných emailov s odkazom na škodlivý kód kampane, resp. skupiny s názvom CozyCar, známym aj ako Cozy Bear. Spear-phishingová kampaň rozosielala emailové správy, ktoré sa tvárili, že sú poslané z emailovej schránky patriacej európskej inštitúcii. Správa informovala o priloženom faxe, ktorý odkazoval na škodlivý kód. Predmet správy sa menil, rovnako ako aj odkaz na škodlivú prílohu. Po stiahnutí a samotnom spustení sa škodlivý kód inštaloval do programov spúšťaných pri štarte a vykonával ďalšiu škodlivú aktivitu podľa pokynov útočníka (napríklad sledovanie klávesnice a obrazovky, získavanie dokumentov, vykonávanie útokov na určené ciele).

Identifikované boli C&C servery, kompromitované pracovné stanice a indikátory kompromitácie (emailové adresy odosielateľov, škodlivé domény a súbory). Vo varovaní boli poskytnuté konkrétne indikátory kompromitácie.

INDIKÁTORY KAMPANE COZYBEAR

Škodlivý kód z rodiny CozyCar sa opäť šíril prostredníctvom podvodných emailových správ spravidla s predmetom „FAX REPORT", "Scanned Document", a podobne. Celkovo bolo v rámci tejto kampane zaslaných viac ako 10 000 správ. Správa obsahovala odkaz na súbor zip, ktorý obsahoval škodlivý kód. Škodlivá zip príloha bola umiestnená na kompromitovaných legitímnych serveroch s vlastnou doménou. Kompromitovaný emailový účet v tejto doméne, z ktorého boli odosielané správy, iba zvyšoval dôveryhodnosť správy. To útočníkom umožnilo zmiasť používateľov, ktorí škodlivý kód museli spúšťať manuálne. V princípe ale samotný útok nebol veľmi sofistikovaný pokiaľ išlo o doručenie a spustenie škodlivého kódu. Obsahoval však zaujímavé techniky na zabránenie jeho analýzy a samotnej detekcie, nakoľko sám detegoval rozličné virtuálne sandbox prostredia, ktoré sú používané pri analýze malvéru.

INDIKÁTORY KAMPANE COZYBEAR - AKTUALIZÁCIA

Po šírení sa predchádzajúcej phishingovej vlny CozyCar bola identifikovaná nová vlna s označením CozyBear. Škodlivý kód patril do rodiny CozyBear, nazývanej aj ako CozyCar, CozyDuke, prípadne CozyMonkey. V tejto vlne bolo identifikovaných množstvo kompromitovaných pracovných staníc, C&C serverov, škodlivých domén a súborov.

Ak bola obeť zaujímavá pre útočníka, tak bol následne „doinštalovaný" aj škodlivý kód SeaDuke. Išlo o trójskeho koňa zameriavajúceho sa na malý počet vysokohodnotných vládnych cieľov.

VAROVANIE - VEREJNE DOSTUPNÝ EXPLOIT NA ZRANITEĽNOSŤ STAGEFRIGHT (CVE-2015-1538) V OS ANDROID

CSIRT.SK zaznamenal zverejnenie exploitu zneužívajúceho zraniteľnosť Stagefright CVE-2015-1538 v OS Android. Exploit umožňoval útočníkovi vytvoriť infikovaný videosúbor vo formáte MP4. Po odoslaní tohto súboru na zraniteľné zariadenie sa otvorili zadné dvierka pre útočníka, ktorý tak mohol komunikovať a ovládať kompromitované zariadenie. Zneužitie exploitu nevyžadovalo veľkú mieru technických znalostí. Odporučili sme aplikovať najnovšie dostupné aktualizácie pre zariadenia s OS Android, avšak veľa zariadení už nie je možné aktualizovať, resp. pre ne nebola vydaná aktualizácia opravujúca túto zraniteľnosť. Preto sme odporučili zablokovať automatické sťahovanie multimediálnych správ (napr. MMS, Hangouts), respektíve ich príloh a zablokovať prijímanie MMS od neznámych čísel (ak to bolo možné).

VAROVANIE - SYNFUL KNOCK KOMPROMITOVANÉ SMEROVAČE CISCO

V Mexiku, Indii, na Filipínach a na Ukrajine boli nájdené napadnuté smerovače výrobcu Cisco. Útočníci pravdepodobne získali prístup do zariadení pomocou uhádnutých alebo ukradnutých administrátorských hesiel a následne modifikovali operačný systém IOS používaný v smerovačoch a prepínačoch firmy Cisco.

Niektoré časti pôvodného IOS boli prepísané malvérom, čo následne umožňovalo útočníkovi načítať rôzne moduly pre rozšírenie funkcionality. Útočník tak mohol spravovať načítané moduly na diaľku z prostredia Internetu po odoslaní špeciálnej sekvencie TCP paketov slúžiacich pre aktivovanie vzdialenej správy tohto malvéru (odtiaľ aj názov SYNful Knock). Tiež obsahoval zadné dvierka pre útočníka. Zadné dvierka boli prístupné prostredníctvom Telnetu alebo konzoly po zadaní backdoor hesla cez protokol HTTP. Útočník mal pri použití zadných dvierok neobmedzené systémové oprávnenia a mohol napr. odchytávať, presmerovávať alebo modifikovať komunikáciu.

Malvér bol súčasťou IOS, teda bol odolný voči vypnutiu aj reštartovaniu zariadenia. Načítal sa po každom štarte zariadenia. Útočníkom načítané moduly na rozšírenie funkcionality boli umiestnené v operačnej pamäti, teda po vypnutí/reštartovaní zariadenia neboli dostupné.

Vo varovaní CSIRT.SK odporúčal preveriť kompromitáciu smerovačov, skontrolovať kvalitu hesiel a pri potvrdení kompromitácie preinštalovať zariadenie pomocou čistého obrazu IOS priamo od spoločnosti Cisco.

VAROVANIE - BANKOVÉ TRÓJSKE KONE SLEMBUNK

CSIRT.SK v zmysle existujúcich zmlúv o spolupráci so subjektmi finančného sektora rozoslal informáciu o aktuálnej hrozbe rodiny trójskych koní SlemBunk. Ide o rodinu trójskych koní tváriacich sa ako legitímne aplikácie pre online banking niektorých známych bánk v USA, EÚ a Ázijsko-Pacifickom regióne. Škodlivý kód zachytával prihlasovacie údaje používateľov a spolu s ďalšími citlivými informáciami ich odosielal na C&C servery kontrolované útočníkmi.

Slovenské banky neboli priamym cieľom útočníkov, ale vzhľadom na prispôsobiteľnosť používateľského rozhrania trojského koňa SlemBunk je pravdepodobné, že v krátkej dobe sa môžu objaviť aj varianty SlemBunk zameriavajúce sa na klientov slovenských bánk.

Infikované aplikácie neboli zverejnené v obchode Google Play. Šírili sa najmä stiahnutím z infikovaných web stránok (prevažne s pornografickým obsahom).

VÝBER Z INCIDENTOV

MONGODB — Február

Vo februári skupina bezpečnostných výskumníkov skenovala priestor Internetu s cieľom zistiť výskyt databáz MongoDB, ktoré sú nezabezpečené a voľne dostupné z prostredia Internetu. Informácie týkajúce sa IP priestoru SR nám boli následne zaslané. Prednastavená inštalácia databázy MongoDB nastavuje neobmedzený prístup. Po samotnej inštalácií je teda nutné manuálne pridať spôsob autentizácie, na čo však väčšina administrátorov pozabudla. Prípadný útočník teda mal citlivé údaje z týchto databáz ako na zlatom podnose. Vzhľadom na to, že tieto databázy bývajú využívané na ukladanie rôznych informácií (napr. citlivé údaje, manažment relácií, atď.), kontaktovali sme poskytovateľov Internetu (ISP), aby upozornili držiteľov jednotlivých IP adries na danú zraniteľnosť a možné hrozby.

RAMNIT — Február - December

Od februára a aj v priebehu celého roka sme pravidelne zaznamenávali hlásenia o šírení škodlivého kódu s označením Ramnit.

Ramnit je malvér infikujúci zariadenia s OS Windows. Šíril sa viacerými spôsobmi, zvyčajne pomocou spam emailov s odkazmi na kompromitované stránky a sociálne médiá, pomocou verejných FTP serverov, prípadne pri inštalácii softvérových balíkov z menej dôveryhodných zdrojov. Tento malvér umožňoval útočníkom získavať citlivé informácie z napadnutých zariadení ako napríklad bankové údaje, cookies z prehliadača pre ukradnutie identity a heslá uložené na disku. Útočníkom tiež umožňoval vzdialený prístup do počítača obete, pomocou ktorého bolo možné vzdialené ovládanie alebo tiež prístup k súborom obete. Okrem toho boli infikované zariadenia zapojené do siete botnet a mohli byť zneužívané pri vykonávaní ďalších nekalých aktivít (DDoS útoky, SPAM a pod.).

PHISHING — Marec

V marci sme zaznamenali šírenie podvodných emailov, ktoré boli falošne zasielané v mene Ministerstva spravodlivosti SR. Zachytený email bol ukážkovým príkladom techník sociálneho inžinierstva. V tomto prípade útočník pod zámienkou toho, že voči príjemcovi bolo začaté trestné konanie navádzal obeť na kliknutie na odkaz v tele emailu, na ktorom sa nachádzal škodlivý súbor s názvom *.pdf.exe.

Analytické oddelenie CSIRT.SK získalo vzorku škodlivého súboru a vykonalo jeho analýzu. Podarilo sa zistiť funkcionalitu malvéru a indikátory kompromitácie. Jednalo sa o tzv. trójskeho koňa, ktorý sa snažil získavať údaje z internetového prehliadača, odoslať ich na riadiaci C&C server a prijímať z neho príkazy. Súčasťou analýzy bolo poskytnutie odporúčaní ako odstrániť malvér z infikovaného počítača.

DYRE

Marec - September

V rozmedzí marca až septembra sme prijali niekoľko hlásení o kompromitácií zariadení v SR škodlivým kódom nazývaným Dyre. Nahlasované IP adresy najčastejšie slúžili ako proxy servery pre botnet Dyre, ktoré preposielali komunikáciu medzi riadiacimi C&C servermi a infikovanými strojmi. O tejto hrozbe sme pravidelne informovali poskytovateľov internetových služieb, aby bolo možné čo najrýchlejšie odstrániť infekcie a znefunkčniť botnetovú sieť.

Dyre je škodlivý kód (trójsky kôň), ktorý zbiera prihlasovacie údaje k online službám, primárne internetového bankovníctva. Využíval Invisible Internet Project (I2P) sieť, alternatívu siete TOR (The Onion Router). Infikované zariadenia sa stávali súčasťou botnetu, kde plnili úlohu C&C serverov. Najčastejšie sa jednalo o kompromitované domáce smerovače, prípadne servery. Tento malvér sa šíril prostredníctvom podvodných emailov obsahujúcich škodlivé prílohy ako napr. *.pdf dokument. Text emailov sa zameriaval na oznámenie o vystavení faktúry alebo zaslaní elektronického faxu.

ROM-0

Jún

Zaznamenali sme výskyt zraniteľnosti rom-0, otestovali IP adresný priestor Slovenskej republiky a následne sme naše informácie zaslali dotknutým poskytovateľom internetových služieb. Žiaľ, niektoré zariadenia už boli kompromitované. Zraniteľnosťou bolo postihnutých celosvetovo až 987 000 zariadení z toho v Slovenskej republike sa nachádzalo viac ako 3000 zariadení.

Zraniteľnosť rom-0 sa týkala celej rodiny SOHO smerovačov, ktoré vychádzali z OS ZynOS (napr. niektoré smerovače TP-LINK, AirLive a ďalšie). Išlo o chybu nedostatočnej kontroly prístupu k administračnému webovému rozhraniu, ktoré slúži pre správu zariadenia. Zraniteľný smerovač umožňoval prístup k jeho konfiguračnému súboru a jeho zmenu a to bez vyžiadania si hesla. Dôležité bolo iba poznať správny URL odkaz. V prednastavenom stave bolo administračné rozhranie dostupné cez Internet a práve preto bola táto zraniteľnosť taká nebezpečná.

V nami zaznamenaných prípadoch útočníci po získaní prístupu ihneď zmenili IP adresu primárneho DNS servera na svoju vlastnú. V jednom zo zaznamenaných prípadov použili útočníci ako primárnu IP adresu DNS servera IP adresu svojho servera, pomocou ktorého presmerovali vybranú komunikáciu. Napríklad youtube.com smerovali na svoj vlastný server, kde bola podstrčená webová stránka, ktorá požadovala aktualizovať Flash Pro a hneď aj ponúkla príslušný inštalačný súbor obsahujúci škodlivý kód.

Prvýkrát sme už koncom roka 2014 publikovali odporúčania ako odstrániť spomínanú zraniteľnosť na našej webovej stránke: http://www.csirt.gov.sk/aktualne-7d7.html?id=79.

DRIDEX

Február, Máj, November

V priebehu roka sme viackrát zaznamenali infekcie bankovým malvérom DRIDEX. Tento malvér monitoroval prístup k web stránkam prostredníctvom webových prehliadačov a v prípade prístupu na jemu známu stránku internet bankingu zmodifikoval kód stránky a ukradol tak prístupové údaje obete. Malvér sa šíril pomocou podvodných emailov s finančnou tematikou, ktoré obsahovali dokument aplikácie MS Word (*.doc). Po otvorení súboru, ak bolo povolené vykonávanie makier (alebo ich používateľ na vyzvanie povolil), VBA makro sa pokúsilo stiahnuť ďalší škodlivý kód, ktorý následne spustil DRIDEX.

Na riadenie infikovaných zariadení a získavanie citlivých informácií sa používala sieť botnet s decentralizovanou architektúrou peer-to-peer (P2P) a proxy servery. Infikované zariadenia pritom mohli byť zneužité aj na vykonávanie ďalšej škodlivej aktivity.

ZRANITEĽNOSTI

Analytický tím pravidelne publikuje Mesačný prehľad bezpečnostných udalostí vo svete aj Slovenskej republike. Uvádzame výber z nich.

JANUÁR

Zneužívanie zraniteľností CVE-2015-0310 a CVE-2015-0311 programu Adobe Flash Player na vzdialené spustenie škodlivého kódu a obídenie ochrany ASLR.

FEBRUÁR

Zneužívanie zraniteľnosti CVE-2015-0071 prehliadača Internet Explorer na obídenie ochrany ASLR.
Malware SuperFish distribuovaný na notebookoch spoločnosti Lenovo.

MAREC

Zneužívanie zraniteľnosti CVE-2015-0072 prehliadača Internet Explorer na zvýšenie oprávnení prostredníctvom XSS útoku.
Zneužívanie zraniteľností programu Adobe Flash Player na vzdialené spustenie škodlivého kódu.
FREAK útok na SSL/TLS umožňujúci vynútiť použitie kratších kľúčov pri Man-in-the-Middle útoku.

APRÍL

Zneužívanie zraniteľnosti CVE-2015-3043 programu Adobe Flash Player na vzdialené spustenie škodlivého kódu.
Zneužívanie zraniteľností platformy Java na vzdialené spustenie škodlivého kódu.

MÁJ

Koniec podpory Microsoft Office 2013 (bez Service Pack 1).
Zneužívanie zraniteľnosti CVE-2015-1701 v OS Windows na zvýšenie oprávnení a prevzatie kontroly nad systémom.
Zneužívanie zraniteľnosti CVE-2015-1671 OS Windows na spustenie škodlivého kódu a prevzatie kontroly nad systémom po otvorení infikovaného súboru Microsoft Office.
Zneužívanie zero-day zraniteľnosti CVE-2015-3090 programu Adobe Flash Player na vzdialené spustenie škodlivého kódu.
Venom – zraniteľnosť virtualizačných nástrojov umožňujúca spustiť útočníkovi z hostovanému systému škodlivý kód v hostiteľskom systéme.

JÚN

Zneužívanie zraniteľnosti CVE-2015-2360 v OS Windows na zvýšenie oprávnení a prevzatie kontroly nad systémom.
Produkty spoločnosti Cisco obsahujúce prednastavené SSH kľúče určené pre vzdialenú podporu, ktoré mohli byť zneužité útočníkom.

JÚL

Verejne známy exploit na zraniteľnosti CVE-2015-2426 v OS Windows umožňujúci zvýšenie oprávnení.
Zneužívanie zraniteľnosti CVE-2015-2424 kancelárskeho balíka Microsoft Office na spustenie škodlivého kódu po otvorení infikovaného súboru v cielených útokoch.
Zneužívanie zraniteľnosti CVE-2015-2425 prehliadača Internet Explorer na spustenie škodlivého kódu po navštívení infikovanej webovej stránky.
Štyri zero-day zraniteľnosti prehliadača Microsoft Internet Explorer pre smartfóny.
Zneužívanie zraniteľností CVE-2015-5122 a CVE-2015-5123 programu Adobe Flash Player na vzdialené spustenie škodlivého kódu.
Zraniteľnosti Android Stagefright umožňujúce vzdialenému útočníkovi spustiť škodlivý kód prostredníctvom MMS obsahujúcej infikované video.
Zraniteľnosť CVE-2015-3650 virtualizačného softvéru VMware umožňujúca lokálnemu používateľovi hostiteľského systému získať systémové oprávnenia hostiteľského systému.

AUGUST

Zneužívanie zraniteľnosti CVE-2015-1769 v OS Windows na spúšťanie škodlivých programov po vložení USB zariadenia.
Koniec podpory Windows Server 2003.
Zneužívanie zraniteľnosti CVE-2015-1642 kancelárskeho balíka Microsoft Office na spustenie škodlivého kódu po otvorení infikovaného súboru.
Android zraniteľnosti Certifi-Gate zneužívané na neoprávnené získanie privilégií, zachytávanie obrazovky zariadenia a simulovanie kliknutí a dotykov.

SEPTEMBER

Zraniteľnosti Android Stagefright 2.0 umožňujúce vzdialenému útočníkovi prevziať kontrolu nad zariadením po otvorení webovej stránky obsahujúcej infikovaný multimediálny obsah.
Zraniteľnosti TrueCrypt umožňujúce manipulovanie s diskami iných používateľov a zvýšenie oprávnení.
SYNful Knock – kompromitované smerovače Cisco.

OKTÓBER

Zneužívanie zraniteľnosti CVE-2015-7645 programu Adobe Flash Player na vzdialené spustenie škodlivého kódu v útokoch zameraných na vládne organizácie.

NOVEMBER

Zneužívanie zraniteľností programu Adobe Flash Player na vzdialené spustenie škodlivého kódu.

DECEMBER

Zneužívanie zraniteľnosti CVE-2015-6175 v OS Windows na zvýšenie oprávnení a prevzatie kontroly nad systémom.
Zneužívanie zraniteľnosti CVE-2015-6124 kancelárskeho balíka Microsoft Office na spustenie škodlivého kódu po otvorení infikovaného súboru v cielených útokoch.
Zneužívanie zraniteľnosti CVE-2015-8651 programu Adobe Flash Player na vzdialené spustenie škodlivého kódu v cielených útokoch.

AKTÍVNE SLUŽBY ŠTATISTIKY

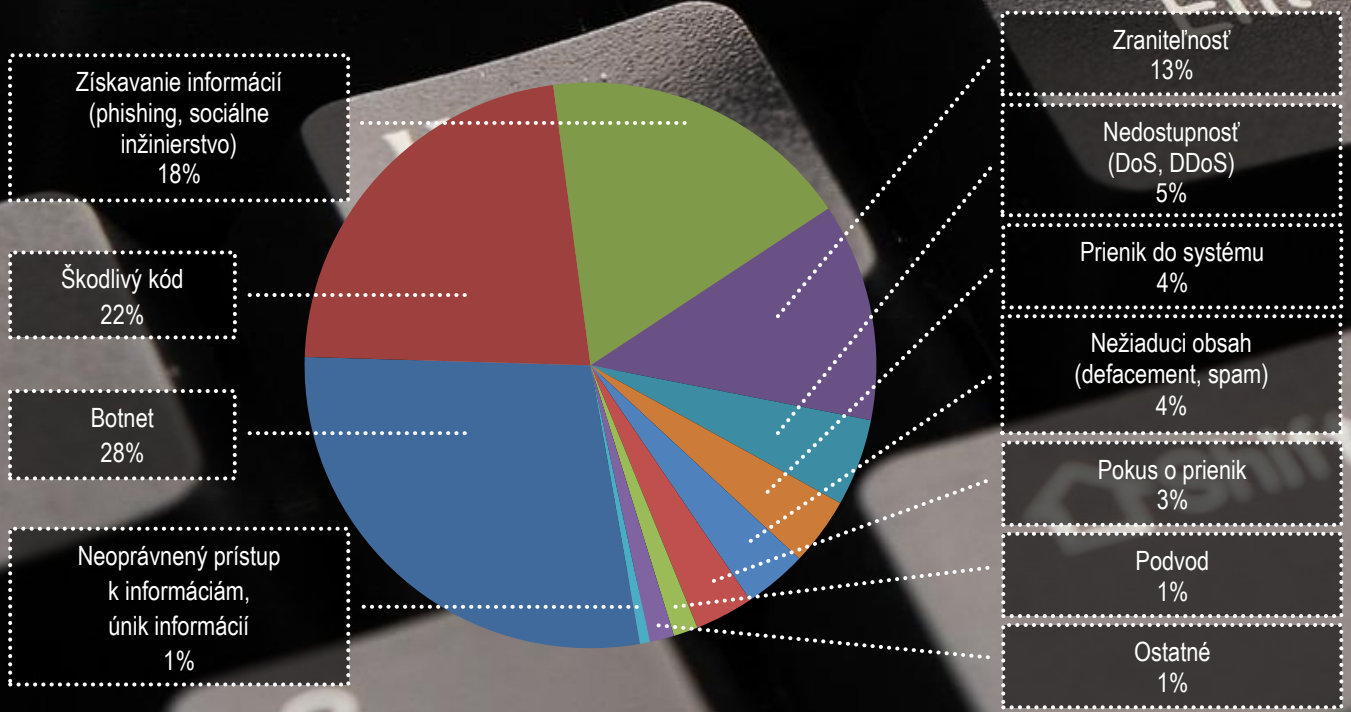
TRENDY


MC
MR
M−
OFF
7
8
M+
4
5
9
2
6
3
=
+
−
×

CISRT.SK v roku 2015 poskytoval služby potrebné na zvládnutie bezpečnostných počítačových incidentov v národnej informačnej a komunikačnej infraštruktúre, na odstránenie ich následkov a na následnú obnovu informačných systémov v spolupráci s prevádzkovateľmi, poskytovateľmi internetových služieb a inými štátnymi orgánmi. Okrem týchto základných služieb špecializovaný útvar CSIRT.SK poskytoval aj služby preventívneho a vzdelávacieho charakteru a zabezpečoval spoluprácu pri riešení bezpečnostných incidentov na medzinárodnej úrovni.

V sledovanom období v rámci aktívnych služieb špecializovaný útvar CSIRT.SK vykonával činnosti národného kontaktného bodu pre nahlasovanie škodlivej aktivity v IP adresnom priestore Slovenskej republiky. V roku 2015 bolo zaznamenaných a riešených 361 počítačových incidentov. Tieto boli nahlásené klientelou CSIRT.SK, zahraničnými partnermi, subjektmi SR alebo boli zistené priebežným monitoringom útvaru CSIRT.SK. Najčastejšie boli riešené podozrenia na prítomnosť škodlivého kódu (bota) v infraštruktúre, ktorý následne vykonával rôznu škodlivú aktivitu (skenovanie zraniteľností, pokusy o prienik, presmerovávanie alebo zasielanie podvodných emailov).

Stále pretrváva šírenie malvéru prostredníctvom podvodných emailov. Správy pod rôznou zámienkou navádzajú adresáta na spustenie škodlivého kódu v prílohe (napr. *.zip.exe) alebo na navštívenie webovej stránky pod kontrolou útočníka prostredníctvom odkazu v tele správy. Medziročne sme zaznamenali mierny pokles počtu incidentov typu phishing. Avšak zaznamenané incidenty boli pokročilejšie z pohľadu samotnej zámienky, grafického spracovania a úrovne slovenčiny. Zaznamenané prípady výskytu škodlivý kódu často súviseli s kampaňami Ramnit, Dridex a CozyCar. Na základe proaktívnej činnosti CSIRT.SK bol identifikovaný výskyt zraniteľností na zariadeniach našej klientely, ktorou je verejná správa a kritická infraštruktúra. Tieto sa najčastejšie týkali konfigurácie SSL, TLS, NTP a redakčných systémov.

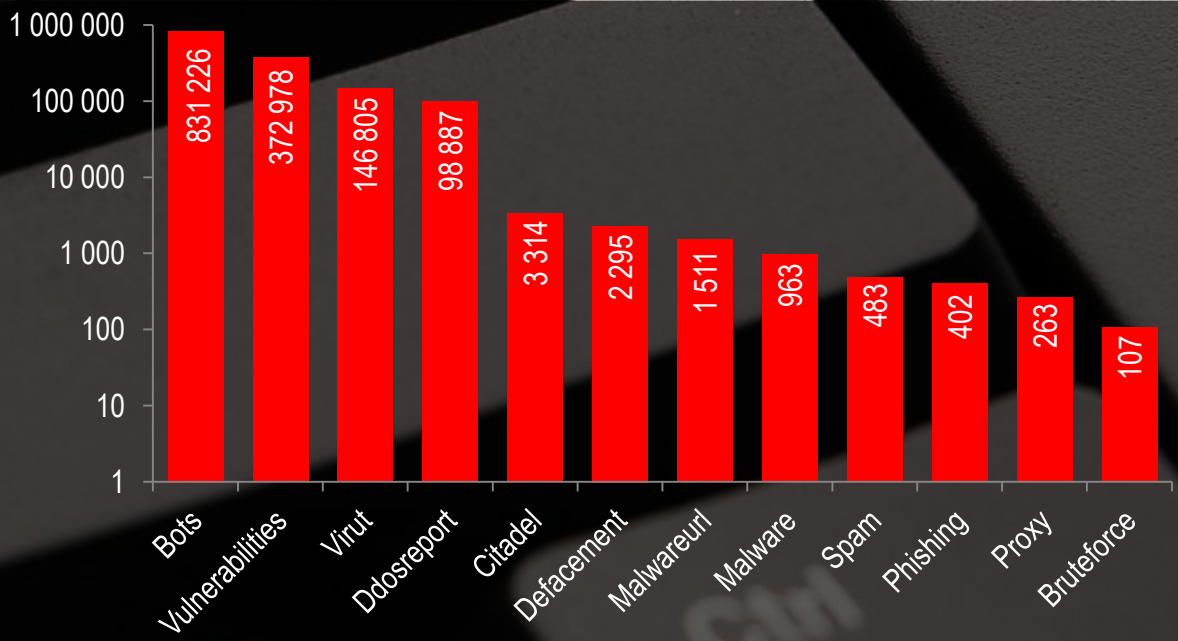


GRAF1 PODIEL JEDNOTLIVÝCH TYPOV INCIDENTOV RIEŠENÝCH CSIRT.SK V OBDOBÍ 1.1. - 31.12.2015

TYPY INCIDENTOV	2014	2015
Botnet	91	102
Získavanie informácií – (phishing, sociálne inžinierstvo)	90	64
Škodlivý kód	58	81
Nedostupnosť (DoS, DDoS)	29	18
Zraniteľnosť	20	45
Pokus o prienik	19	12
Nežiaduci obsah (defacement, spam)	16	13
Prienik do systému	9	14
Podvod	7	5
Neoprávnený prístup k informáciám/únik informácií	4	2
Ostatné	4	5
Neoprávnená modifikácia informácií	1	0
SPOLU	348	361

TABUĽKA 1 POROVNANIE POČTU A TYPOV ZÁVAŽNÝCH INCIDENTOV RIEŠENÝCH CSIRT.SK

V roku 2015 CSIRT.SK prijal viac ako 1 459 000 hlásení o možnom výskyte škodlivej aktivity z IP adries v Slovenskej republike. Hlásenia boli spracovávané denne špecializovanými automatizovanými systémami a po vyhodnotení ich závažnosti boli postupované poskytovateľom internetových služieb a inštitúciám, ktorých IP adresy boli podozrivé zo škodlivej aktivity. Zastúpenie jednotlivých typov incidentov je podobné ako v prípade verejnej správy. Najviac bol nahlasovaný výskyt botov, následne zraniteľností prostriedkov IKT a potom výskyt rôznych „rodín" malvéru. Detailné počty a typy incidentov za sledované obdobie sú uvedené v Grafe 2.



GRAF 2 TYPY INCIDENTOV HLÁSENÝCH V IP ADRESNOM PRIESTORE SR V ROKU 2015

PROAKTÍVNE SLUŽBY

TRENDY

V rámci poskytovania proaktívnych služieb CSIRT.SK publikoval varovania pred hrozbami v oblasti bezpečnosti prostriedkov IKT. Na webovom portáli www.csirt.gov.sk bolo publikovaných celkovo 16 oznámení. V mesačných prehľadoch umiestnených na web stránke CSIRT.SK (http://www.csirt.gov.sk/informacna-bezpecnost/oznamenia-a-varovania/mesacny-prehlad-858.html) boli systematicky publikované informácie o hrozbách v oblasti informačnej bezpečnosti a zraniteľnostiach zariadení. Okrem týchto aktivít bolo kontaktným osobám inštitúcií verejnej správy a partnerom útvaru CSIRT.SK zaslaných 13 varovaní pred konkrétnymi hrozbami s možným dopadom na informačné systémy a elektronické služby verejnej správy.

TRENDY

Situácia v oblasti informačnej bezpečnosti na Slovensku v roku 2015 odzrkadľovala svetové trendy. Našťastie sme nezaznamenali úniky dát v takom rozsahu ako je tomu v zahraničí. Škodlivý kód, ktorý bol detegovaný v IP adresnom priestore Slovenskej republiky, mal celosvetové pôsobenie. Z riešených hlásení incidentov môžeme spomenúť kampane, pri ktorých sa používal ransomvér, CozyBear, SlemBunk, Dyre, Dridex, atď. Rovnako odhaľovanie a zverejňovanie nových zraniteľností ako Rom0, Stagefright, zraniteľnosti SSL/TLS a kritickej zraniteľnosti v knižnici glibc viedlo nielen odborníkov, ale aj širokú verejnosť k zvýšeniu pozornosti a zamysleniu sa nad vlastnou úrovňou bezpečnosti. Celosvetový dopad malo aj používanie watering hole útoku na vybrané organizácie a firmy.

Ľudský faktor zohral dôležitú úlohu pri mnohých incidentoch. Šírenie nielen phishingu a ransomvéru, ale aj škodlivého kódu všeobecne, prostredníctvom sociálneho inžinierstva, nestráca na sile, nakoľko nie je príliš technicky a finančne náročné. V kombinácií so zanedbaním a nedodržiavaním bezpečnostných doporučení, videli sme to pri nezabezpečených databázach MongoDB, ide o neželanú kombináciu.

Odhadujeme, že v ďalšom období bude počet phishingových útokov narastať a ich úroveň sa bude zvyšovať. Jeden z prvých sme už zaznamenali v marci 2015, kedy sa šírili podvodné emaily s obsahom škodlivého kódu typu downloader, ktoré boli falošne zasielané v mene Ministerstva spravodlivosti SR. Na uskutočnenie phishingového útoku je možné použiť ľubovoľný komunikačný kanál či už email, telefón, Skype alebo iné služby.

Ďalšou špecifickou kategóriou sú APT útoky. Je však veľmi ťažké rozlíšiť štandardný útok od APT útoku. Útočníci môžu využiť štandardný škodlivý kód, ktorý podstrčia ako návnadu, a tým budú maskovať svoju činnosť v kompromitovanom prostredí. Pre tento štandardný škodlivý kód existujú rôzne nástroje na jeho odstránenie na báze indikátorov kompromitácie (IoCs), ktoré následne poskytnú obeti falošný pocit istoty a bezpečia.

Stále sa ukazuje, že ani najlepšie anti-malvér riešenie neochráni organizáciu pred cielenou kompromitáciou. Často sa zabúda na hrozbu v podobe zamestnanca, ktorý je ako vektor útoku stále podceňovaný. Riešením je v organizáciách zaviesť koncept HĺbkovejObrany, tzv. Defense in Depth alebo Castle Approach. Nemožno ale zabudnúť aj na riadenie prístupu, fyzickú bezpečnosť a ochranu samotných zariadení. Informačnú bezpečnosť je nutné chápať v kontexte všetkých jej komponentov.

Riešenie problematiky bezpečnosti riadiacich systémov a priemyselných automatizačných zariadení bude v nadchádzajúcom období kľúčové nielen z pohľadu kritickej infraštruktúry štátu, ale aj súkromného sektora. Dôležitú úlohu tu budú zohrávať nielen výrobcovia, ale aj samotní odberatelia.

Riešenie informačnej bezpečnosti sa ale netýka iba informačných systémov. Celá spoločnosť už využíva výhody Internetu 2.0 a v nadchádzajúcom období sa bude pokračovať v kreovaní Industry 4.0, ktorý začínajú využívať nielen korporácie, ale aj samotné štáty. V tejto oblasti je nosným prvkom Internet vecí, tzv. Internet of Things (IoT). Práve IoT a jeho zabezpečenie je výzvou pre bezpečnostných špecialistov, ale aj samotných výrobcov.

Integrácia chytrých mobilných telefónov do našich životov má za následok ohrozenie, ktorého sú si útočníci plne vedomí. Mobilný telefón v sebe obsahuje veľa dôležitých informácií o nás, našom súkromí a aj profesii. Veľa finančných inštitúcií napr. ponúka využívanie svojich služieb prostredníctvom mobilného telefónu a tieto služby sú finančne zaujímavým cieľom pre útočníka. Narušenie bezpečnostného mechanizmu zariadenia zásahom používateľa, napr. rootingom alebo jailbreakingom, iba útočníkovi uľahčuje kompromitáciu zariadenia. Výstrahou pre používateľov sú aj rôzne verzie ransomvéru pre mobilné zariadenia ako sú mobilné telefóny a tablety. Odhadujeme, že v najbližšom období sa útočníci čoraz častejšie budú sústrediť práve na mobilné zariadenia, na ktorých sa často nachádzajú okrem osobných informácií a súborov aj pracovné dokumenty. Nové bezpečnostné riziká prinášajú nové chytré zariadenia domácnosti ako napríklad smart TV. Ide napríklad o ohrozenie súkromia alebo možnosť prieniku do domácej siete. V roku 2015 boli zaznamenané mnohé zraniteľnosti domácich kamerových systémov, videovrátnikov a zariadení využívajúcich WiFi. Je predpoklad nárastu šírenia škodlivého kódu prostredníctvom sociálnych sietí.

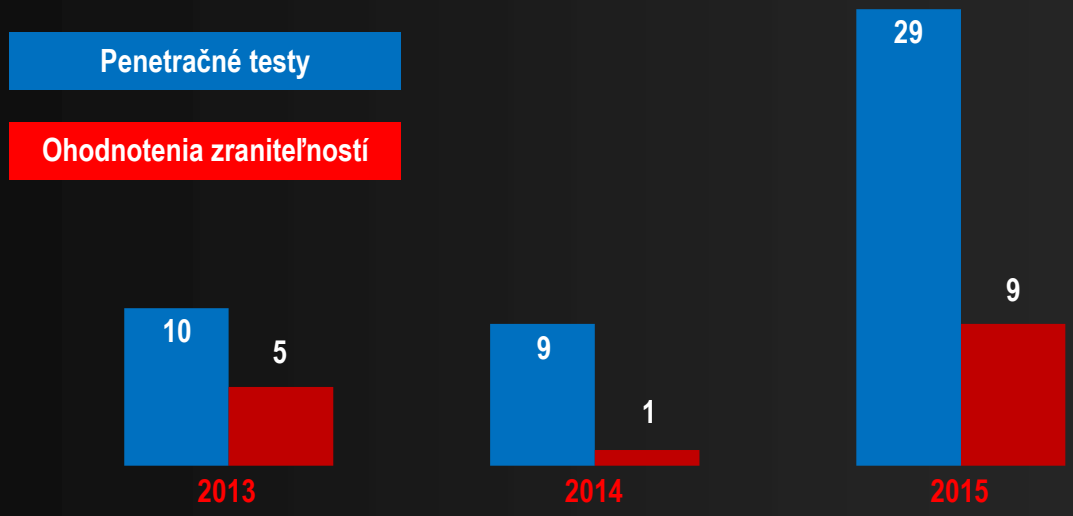
Oblasť informačnej bezpečnosti je vnímaná širokou verejnosťou a to aj zásluhou mnohých organizácií, združení a odborníkov, čo prispieva k zvýšeniu úrovne bezpečnosti nielen v samotných organizáciách, ale aj v domácnostiach. V blízkej budúcnosti by jednoduché útoky na koncového používateľa už nemali byť príliš efektívne. Dôsledkom ale bude zvyšovanie komplexnosti útokov a ich zameranie na špecifických používateľov a špecifické systémy, čo bude mať za následok aj ich ťažšie odhaľovanie.

PENETRAČNÉ TESTOVANIE

CSIRT.SK vykonáva v rámci svojej činnosti ohodnotenia zraniteľností a penetračné testy informačných systémov a sietí verejnej správy. Cieľom je overenie úrovne zabezpečenia informačných systémov pred štandardnými útokmi, identifikovanie možných zraniteľností a navrhnutie bezpečnostných opatrení. Pre inštitúcie verejnej správy vykonáva CSIRT.SK penetračné testy internou aj externou formou.

V prípade externých penetračných testov sú simulované aktivity útočníka z externého prostredia (najčastejšie siete Internet alebo Govnet). Tento typ testu sa vykonáva pre služby ako napríklad webové stránky inštitúcií alebo pre celé verejne dostupné IP rozsahy. Takýto test je vhodné vykonať pre všetky novo nasadzované verejné portály alebo služby a pre 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 resp. scenár so simulovanou kompromitáciou pracovnej stanice prostredníctvom škodlivého kódu. 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.



GRAF 3 MEDZIROČNÝ VÝVOJ POČTU PENTESTOV VYKONANÝCH CSIRT.SK

CSIRT.SK začal vykonávať penetračné testy od roku 2013. V roku 2015 sa rapídne zvýšil počet testov na 29 a ohodnotení zraniteľností informačných systémov a sietí na 9. Dôvodom bolo najmä systematické testovanie informačných systémov vytváraných v rámci OPIS (Operačný program Informatizácia Spoločnosti).

Dĺžka jedného penetračného testu aj s vypracovaním záverečnej správy sa v závislosti od zložitosti infraštruktúry pohybuje v rozmedzí od dvoch týždňov po mesiac, v prípade ohodnotenia zraniteľnosti sa jedná o maximálne týždeň.

Súčasťou penetračných testov sú aj konzultácie a súčinnosť pri odstraňovaní odhalených nedostatkov. Po ich oprave vykonávame opätovné testovanie za účelom overenia úplnosti nápravy zistených bezpečnostných zraniteľností. Takýto kontrolný test bol vykonaný pri väčšine projektov. Spolu s opakovanými testami tak CSIRT.SK vykonal bezmála 100 penetračných testov a ohodnotení zraniteľností.

CSIRT.SK pri testoch pozoroval časté opakovanie sa niektorých zraniteľností. Na základe týchto zistení a odporúčaných štandardných postupov (ako napr. OWASP) sme vypracovali kontrolný zoznam bezpečnostných opatrení pre nasadenie webového portálu do produkčného prostredia. Tento kontrolný zoznam je verejne dostupný na https://www.csirt.gov.sk/doc/Checklist.pdf, bližší popis môžete nájsť na https://www.csirt.gov.sk/bezpecnostna-studovna/aplikacna-bezpecnost/opatrenia-na-zaistenie-bezpecnosti-webovych-aplikacii-890.html.

LABORATÓRIUM NA ANALÝZU ŠKODLIVÉHO SOFTVÉRU - MALWARELAB

V prvej polovici roka 2015 útvar CSIRT.SK vytvoril tím analytikov malvéru a začal budovať MalwareLab - laboratórium určené na analýzu vzoriek škodlivého kódu. Analytický tím takto poskytuje službu analyzovania vzorky nájdenej a extrahovanej zo siete svojej klientely, čím pomáha zmierňovať následky infekcie. Výsledkom analýzy je správa, ktorá obsahuje popis funkcionality vzorky, indikátory kompromitácie a odporúčania ako postupovať pri odstraňovaní následkov infekcie, ale aj ako predchádzať prípadnej infekcii. Analytický tím priebežne analyzuje aktuálne šírené vzorky malvéru a tým si CSIRT.SK vytvára stále lepší obraz o hrozbách, ktorým čelia koncoví používatelia a administrátori inštitúcií. To nám umožňuje držať krok s aktuálnymi trendmi v oblasti malvéru.

Analytický tím počas prevádzky MalwareLabu analyzoval napr. ransomvér, bankové trójske kone, škodlivé skripty a súčasti exploit kitov.

MalwareLab poskytuje nasledovné služby:

- Proaktívne analyzovanie "mass-targeted" malvéru šíriaceho sa v rámci slovenského IP adresného priestoru. Na základe analýz podnikáme kroky k odstraňovaniu identifikovaných command&control serverov, varovaniu dotknutých inštitúcií a zdieľame tieto informácie s našimi partnermi.
- Analýza potenciálne škodlivej vzorky zachytenej našou klientelou. Cieľom tejto analýzy je poskytnúť inštitúcii informácie o funkcionalite vzorky, možnom dopade na jej infraštruktúru a činnosť inštitúcie a odporúčania ako postupovať pri odstraňovaní následkov a šírení infekcie.

AUDITY BEZPEČNOSTI

CSIRT.SK v rámci svojej činnosti vykonáva audity bezpečnosti informačných systémov pre svoju klientelu. Ide o nezávislé posúdenie aktuálnej úrovne bezpečnosti a vyhodnotenie jej súladu s požadovaným stavom, štandardom alebo internými predpismi organizácie.

Audit bezpečnosti sa vykonáva v dvoch fázach. V rámci prvej fázy audítori preskúmajú dokumentáciu, ktorú môžu tvoriť dokumenty ako bezpečnostná politika, bezpečnostné smernice, havarijné plány a plány obnovy informačných systémov, vzory zmlúv s dodávateľmi i zamestnancami, prevádzková alebo systémová dokumentácia.

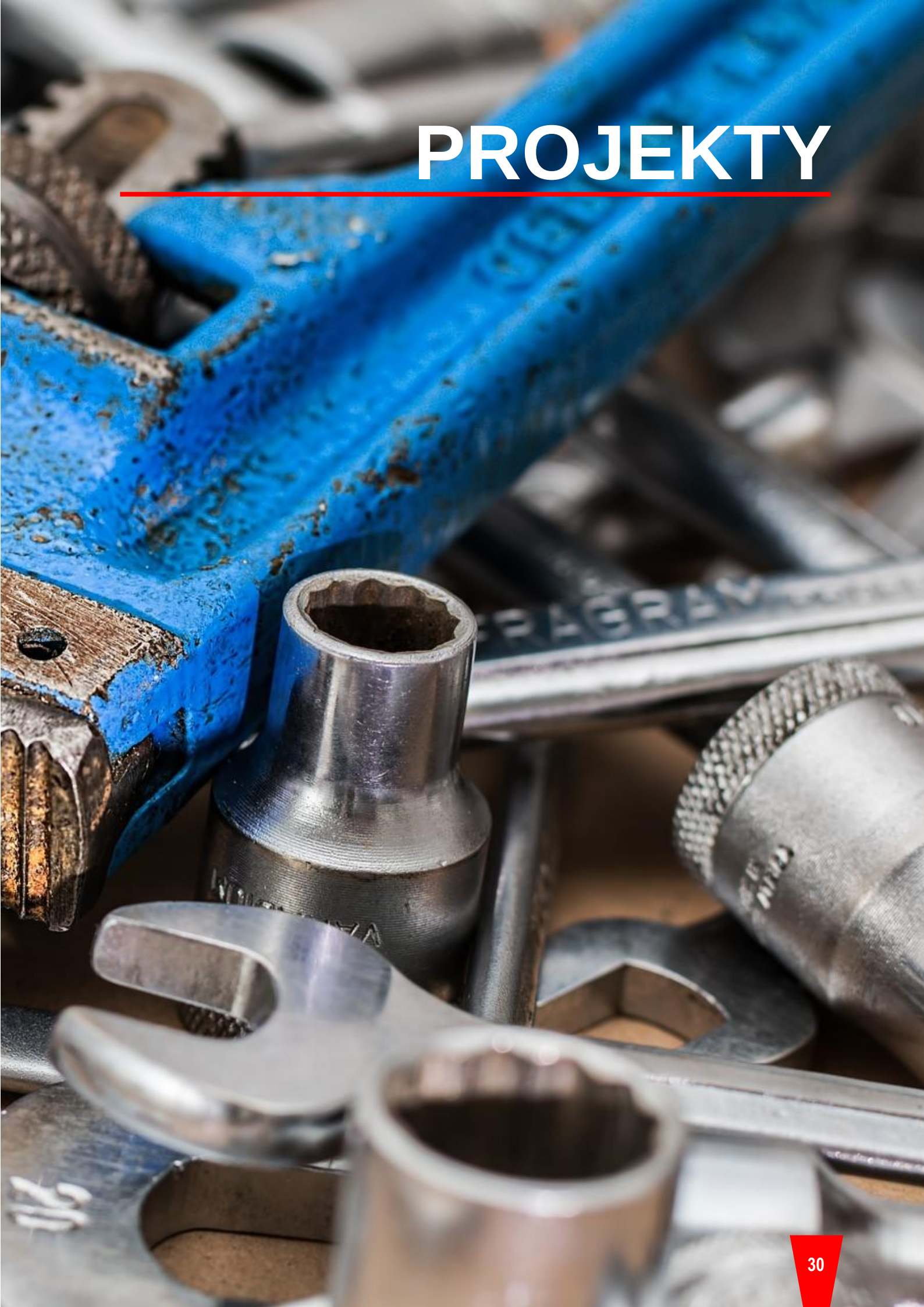
Po preskúmaní dokumentácie v prvej fáze auditu nasleduje druhá fáza - audit na mieste. Počas neho audítori vykonávajú pohovory so zamestnancami, zbierajú a skúmajú dôkazy, zaznamenávajú zistenia, pozorujú činnosti, pracovné prostredie a preskúmavajú dokumentáciu a záznamy.

Výstupom auditu je záverečná správa, ktorá popisuje zistené nezhody s požadovaným stavom a návrh opatrení na ich odstránenie.

KONZULTÁCIE, ŠKOLENIA A VZDELÁVANIE

Organizáciám verejnej správy CSIRT.SK poskytuje konzultačné služby vo viacerých oblastiach informačnej bezpečnosti. Táto činnosť spočíva z ohodnotenia aktuálneho stavu v inštitúcii, posúdenia miery implementácie opatrení vyžadovaných legislatívou, internými predpismi, zmluvami a medzinárodnými štandardmi vo vzťahu k bezpečnostným rizikám. Na základe identifikácie potrieb inštitúcie, identifikovaných nedostatkov a možností zlepšenia je následne možné navrhnúť postup a spôsob dosiahnutia požadovaného stavu.

CSIRT.SK poskytuje svojej klientele školenia vo viacerých oblastiach informačnej bezpečnosti. Ponúka školenia zamerané na tvorbu a prevádzku CSIRT/CERT tímov, školenia forenznej analýzy, penetračného testovania, analýzy rizík, vykonávania auditov bezpečnosti informačných systémov a školenia na zvýšenie bezpečnostného povedomia v organizácii. Naše vzdelávacie aktivity sú detailnejšie popísané v samostatnej kapitole.



PROJEKTY

ATHENA

Informačný systém Athena poskytuje službu zdieľania informácií medzi zapojenými subjektmi a špecializovaným útvarom CSIRT.SK. IS Athena umožňuje bezpečnú komunikáciu medzi zapojenými subjektmi na základe výmeny správ.

Správy v systéme Athena môžu byť zaradené do jednej z nasledovných 4 kategórií:

- **Bezpečnostné incidenty -** Informácie o bezpečnostných incidentoch, ktoré má pôvodca záujem zdieľať s vybranými inštitúciami, útvarom CSIRT.SK alebo skupinami inštitúcií. V prípade prebiehajúcich incidentov je možnosť požiadať automatizovaným spôsobom o súčinnosť útvar CSIRT.SK.
- **Varovania -** Informácie o prebiehajúcich incidentoch, aktuálnych vektoroch útokov, exploitovaných zraniteľnostiach a indikátoroch kompromitácie (IoC).
- **Odporúčané postupy -** Informácie o odporúčaných postupoch pre zabezpečenie infraštruktúr a informačných systémov. V tejto sekcii zverejňujeme metodiky pre hardening operačných systémov a aplikácií, odporúčané nastavenia a informácie na zvýšenie ochrany pred útokom.
- **Zraniteľnosti -** Informácie o aktuálnych zraniteľnostiach a postupoch ich ošetrenia, prípadne postupov na zníženie dopadov alebo pravdepodobnosti exploitácie (tzv. workaround).

Správy v systéme Athena sú z hľadiska dôvernosti klasifikované na základe Traffic Light protokolu (pozri kapitola CSIRT KOMUNITA A PRAKTICKÉ INFORMÁCIE) 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 oblastí (prednostne prevádzkovatelia prvkov kritickej infraštruktúry):

- Energetický sektor,
- Finančný sektor,
- ISP a správca domény,
- Zdravotníctvo.

Pre zapojenie organizácie do systému Athena je potrebné poslať poštou žiadosť o zapojenie sa na adresu DataCentra, rozpočtovej organizácie MF SR.

INFORMAČNÝ SYSTÉM MRM

S cieľom automatizovať činnosti operátora pri riešení nahlásených incidentov v IP adresnom priestore Slovenskej republiky vznikol v lete 2012 projekt Malicious Domain Manager (MDM). Pri špecifikácií našich požiadaviek na nový nástroj sme vychádzali z pracovných postupov pre riešenie phishingu a defacementu a predpokladu, že denne budeme musieť spracovávať cca. 800 hlásení. Pri tvorbe informačného systému sme použili existujúci český open source nástroj MDM.

MDM vzniklo zo spolupráce niekoľkých tímov v Českej republike - Laboratoře CZ.NIC a bezpečnostné tímy CZ.NIC-CSIRT a CSIRT.CZ. Česká verzia MDM bola predstavená na 35. konferencii FIRST/TF-CSIRT Technical Colloquium v Ríme v roku 2012.

Aplikácia slúži ako základný nástroj pre spracovávanie všetkých prijímaných incidentov týkajúcich sa IP adresného priestoru SR a pre spracovávanie informácií o hrozbách v doméne .sk.

Ako CSIRT.SK rástol a stal sa aktívnym členom CERT komunity, získaval nové zdroje. Počet hlásení postupne stúpol na viac ako 12 000 hlásení o možnom výskyte škodlivej aktivity v IP priestore SR denne. Do informačného systému boli integrované rôzne nástroje na overovanie škodlivosti URL odkazov a IP adries a nástroje na získavanie informácií o URL a IP adresách. Ďalej boli vylepšené korelačné a agregačné mechanizmy. Niektoré typy incidentov spracovávame hromadne pre danú IP adresu.

Takto upravený systém bol nazvaný Malicious Resource Manager (MRM). IS MRM v sebe integruje zoznam kontaktov pre klientelu CSIRT.SK a poskytovateľov internetových služieb. Ďalej umožňuje priame nahlasovanie škodlivých a phishingových URL odkazov na analýzu a obsahuje rôzne generátory dát a pohľadov, napr. generátor incidentov pre danú organizáciu, dané ISP alebo danú IP adresu. Implementovali sme nové pohľady

na získané údaje, ktoré boli potrebné pre optimalizáciu a zefektívnenie pracovných postupov. Koncom roka 2015 informačný systém MRM spracovával cca. 284 000 udalostí denne. Tieto udalosti prechádzajú rôznymi filtrami a funkciami a až potom sa výsledné udalosti dostanú ako vstup do samotného IS pre ďalšie spracovanie operátorom CSIRT.SK.

PROJEKT FENIX

Zástupcovia združenia NIX.CZ prevádzkujúceho slovenský prepojovací internetový uzol NIX.SK a zástupcovia slovenského bezpečnostného tímu CSIRT.SK podpísali memorandum o spolupráci v oblasti sieťovej bezpečnosti. Oblasť spolupráce je tiež spojená s bezpečnostným projektom FENIX, ktorého cieľom je umožniť v prípade DoS útoku dostupnosť internetových služieb subjektov zapojených v tomto projekte. Jednou z podmienok spolupráce v tomto projekte je mať vlastný bezpečnostný tím, s ktorého založením pomáha práve CSIRT.SK.

Prioritnou úlohou CSIRT.SK je neustále zvyšovanie úrovne zabezpečenia digitálneho priestoru Slovenskej republiky. Snažíme sa prinášať našej klientele aktívne a proaktívne služby, ktorých cieľom je zabezpečiť dostupnosť prevádzkovaných systémov aj počas rozsiahlych útokov, prostredníctvom koordinácie reakcie na incidenty na národnej úrovni. Projekt FENIX má potenciál významným spôsobom napomôcť klientom zabezpečiť kontinuitu poskytovaných služieb a podporuje budovanie bezpečnostnej komunity v SR.

Samotný projekt FENIX vznikol na pôde českého peeringového uzlu NIX.CZ v roku 2013 ako reakcia na intenzívny DoS útok, ktorému v marci 2013 čelili významné české médiá, banky, ale aj operátori. Projekt FENIX je určený spoločnostiam, ktoré poskytujú pripojenie významným službám a potrebujú zabezpečiť ich prevádzku v tých najkritickejších situáciách.

CS DANUBE

V rámci medzinárodného programu spolupráce sa tím CSIRT.SK zapojil do projektu Cyber Security in Danube Region pod názvom CS Danube. Projekt pod vedením asociácie CZ.NIC trvá od 1. apríla 2015 do 31. marca 2016. Jeho cieľom je posilnenie spolupráce krajín dunajského regiónu v oblasti kybernetickej bezpečnosti. S kolegami z ostatných bezpečnostných tímov máme možnosť vymieňať si informácie a know-how o riešení bezpečnostných incidentov a zdieľať medzi sebou nástroje, ktoré sú používané v rámci komunity tímov.

V projekte sú zapojené okrem Slovenskej republiky a Českej republiky aj Rakúsko, Chorvátsko, Srbsko a Moldavsko. Financovanie je zabezpečené prostredníctvom Európskeho fondu START Danube region fund pre regionálny rozvoj v dunajskom regióne.

VZDELÁVANIE CVIČENIA

PHISHINGOVÝ TEST

Na základe skúseností z našej činnosti vieme podložiť dlhodobo vzrastajúci trend zvyšovania výskytu phishingových kampaní, ktoré priamo ohrozujú obyvateľov SR. Tak ako je uvedené v časti Aktívne služby, phishing a získavanie informácií je druhým najpočetnejším typom incidentov riešených CSIRT.SK v období 1.1. - 31.12.2015.

MOTIVÁCIA

CSIRT.SK na základe zachytených podvodných elektronických správ vytvoril vlastný on-line phishingový test pre organizácie verejnej správy a širokú verejnosť s možnosťou 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.

Osobné údaje sa najčastejšie získavajú a následne aj zneužívajú prostredníctvom phishingu. 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 do mobilného telefónu, ktoré používateľa presmerujú na falošné webové stránky. Nevyžiadaná správa často obsahuje odkaz, prípadne súbor, obsahujúci skrytý vírus, ktorý sa nainštaluje bez vedomia používateľa do počítača alebo do mobilného telefónu, poškodzuje ostatné programy, mení nastavenia alebo odosiela rôzne údaje a to bez vášho vedomia.

Test pozostával zo 17 testovacích otázok. Úlohou riešiteľa testu bolo rozhodnúť či zobrazený email, ktorý prijal fiktívny používateľ Chuck Norris (chucknorris@gmail.sk), je legitímny alebo podvrhnutý útočníkom.

Po skončení testu sme poskytli používateľovi správne odpovede aj s vysvetlením toho, čo si bolo potrebné všimnúť v jednotlivých otázkach nášho testu.

ZAUJÍMAVOSTI TESTU

Test vychádzal z elektronických správ, ktoré boli zachytené operátormi špecializovaného útvaru CSIRT.SK.

Ak používateľ klikol na odkaz uvedený v podvrhnutej správe, tak bol presmerovaný na vopred pripravenú webovú stránku, na ktorej sme ho informovali, že po kliknutí na takýto odkaz by sa stal obeťou a kompromitoval by si počítač. Na stránke riešiteľ našiel odkazy na odporúčané postupy ako odhaľovať podvrhnuté emaily.

Ak používateľ klikol na odkaz v legitímnej správe, tak bol opäť presmerovaný na nami vopred pripravenú webovú stránku. V tomto prípade však riešiteľovi bolo oznámené, že tento odkaz bol v poriadku.

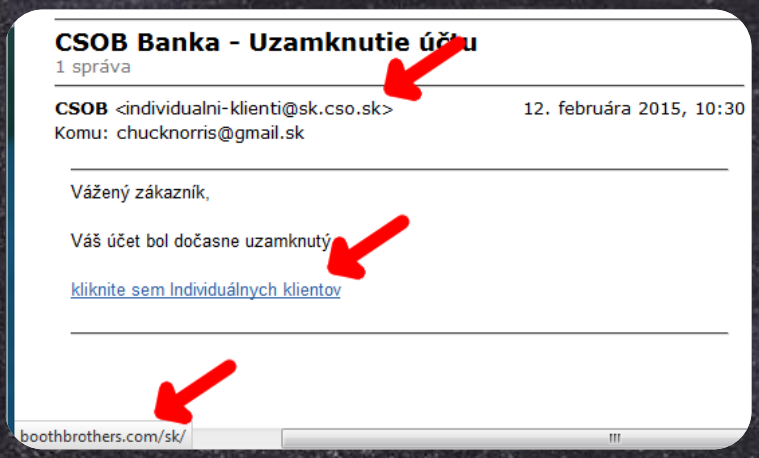
V prípade otvorenia odkazu či už z podvrhnutej alebo legitímnej správy bolo naším hlavným odporúčaním pre riešiteľa, aby sa nikdy nepokúšal otvárať odkazy na webovú stránku priamo v tele emailu.

VYHODNOTENIE TESTU

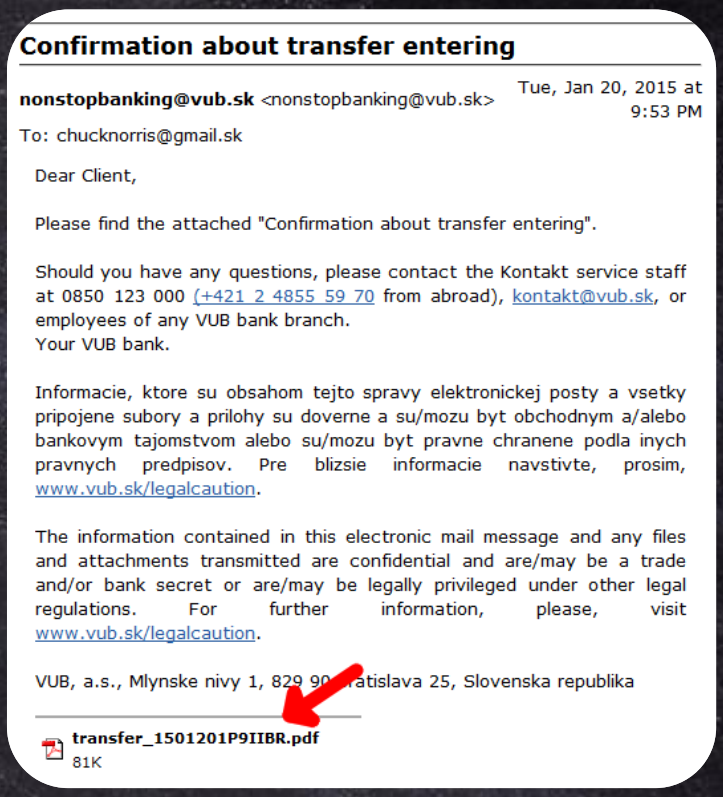
Test bol spustený dňa 28.04.2015. Od spustenia testu do 30.09.2015 bol náš test spustený presne 3224-krát. Na všetky otázky testu odpovedalo 1716 riešiteľov.

Zo všetkých zozbieraných údajov sme vyhodnotili správne a nesprávne odpovede na otázky testu. Riešitelia dosiahli najväčšiu percentuálnu úspešnosť na otázke číslo 11 – obrázok číslo 1. Najnižšiu mieru úspešnosti dosiahli riešitelia na otázke číslo 4 – obrázok číslo 2. V tomto prípade išlo o legitímnu správu, ktorá bola často označovaná za podvrhnutú. Predpokladáme, že riešiteľov zmiatla textácia správy, nakoľko sa jednalo o miešanie anglického a slovenského textu bez príslušnej diakritiky.

Celkovo sme zaznamenali až 263 kliknutí na odkazy, z čoho až 148 odkazov bolo podvrhnutých a teda škodlivých.



OBRÁZOK Č.1



OBRÁZOK Č.2

GRAF Č. 4: ÚSPEŠNOSŤ RIEŠITEĽOV, KTORÍ DOKONČILI TEST

Celý test úspešne dokončilo 1716 riešiteľov. Graf číslo 4 zobrazuje úspešnosť týchto riešiteľov testu, ktorí odpovedali na všetky otázky testu. Počtom najviac takýchto riešiteľov získalo v našom teste 8 až 11 bodov, čomu zodpovedá 6 až 9 chybných odpovedí.

Z pohľadu správnych odpovedí sme zaznamenali najmenej nesprávnych odpovedí týchto riešiteľov na otázke číslo 11. Najviac nesprávnych odpovedí sme zaznamenali na otázkach číslo 4 a 17. Obe tieto správy však boli legitímne. To značí, že riešitelia boli až nadmieru paranoidní, pokiaľ išlo o otázky v teste. Záujem o problematiku phishingu a teda aj o problematiku počítačovej bezpečnosti prevýšil naše očakávania.

Ak by sa jednalo o skutočný phishingový útok, ktorý by bol realizovaný v krátkom časovom období a v ktorom by škodlivé odkazy neboli nahlásené alebo zaznamenané službami, ktoré umožňujú ich blokovanie prehliadačmi, tak 280 kliknutí na URL odkaz by predstavovalo približne 8,7% kompromitovaných používateľov z danej testovanej vzorky.

PREDNÁŠKY A WORKSHOPY

SASIB - INFORMAČNÁ BEZPEČNOSŤ 2015

Cieľom združenia SASIB je napomáhať zvyšovaniu právneho povedomia a odborných znalostí svojich členov, ako aj odbornej a laickej verejnosti v oblasti informačnej bezpečnosti a ochrany softvéru.

Ďalším významným cieľom SASIB je zabezpečiť trvale vysokú odbornú úroveň služieb poskytovaných členmi SASIB v oblasti bezpečnosti informačných systémov a v oblasti ochrany informácií, bez ohľadu na ich charakter a typ informačného nosiča, pred možným únikom, stratou, zneužitím, neoprávnenou zmenou alebo poškodením.

SASIB si tiež kladie za cieľ podporovať aktivity orgánov štátnej správy pri vytváraní štúdií a doporučení v oblasti informačnej bezpečnosti a boji proti informačnej kriminalite.

Organizátori vyhradili pre CSIRT.SK samostatný tematický blok. V tomto bloku zazneli prednášky členov CSIRT.SK na témy „Úloha ochrany štátu pred počítačovými bezpečnostnými incidentmi“, „Riešenie počítačových bezpečnostných incidentov“ a „Penetračné testovanie inštitúcií“.

ITAPA

Medzinárodný kongres ITAPA (Informačné technológie a verejná správa) je od roku 2002 podujatím, ktoré sa zaoberá informatizáciou verejnej správy (eGovernmentom).

CSIRT.SK a NIX.CZ na ňom predniesli spoločný príspevok „Naša úloha pri zvyšovaní úrovne sieťovej bezpečnosti“ v bloku „Dáta v digitálnom svete“.

So zvyšujúcim sa počtom používateľov IKT a prevádzkovateľov kritických služieb vzrastá i počet bezpečnostných incidentov pričom najviac ohrozenými oblasťami sú financie, energetika, elektronické služby a služby poskytované štátom. Tieto javy negatívne ovplyvňujú dôveru ich používateľov a spomaľujú tak rozvoj našej digitálnej spoločnosti. Kybernetická bezpečnosť sa preto stáva jednou z priorít prevádzkovateľov sietí a elektronických služieb a taktiež vlád na celom svete, ktoré majú snahu zefektívniť obranu proti útokom na informačné systémy. Posun vo vnímaní problému kybernetickej bezpečnosti je možné vidieť taktiež v koncipovaní nových organizácií a poskytovaní nových služieb, ktoré sa aktívne venujú ochrane kybernetického priestoru a budovaniu bezpečnostnej komunity. V podmienkach Slovenskej republiky nadviazali za týmto účelom spoluprácu tím CSIRT.SK a združenie NIX.CZ, ktoré predstavilo na Slovensku projekt FENIX.

VARŠAVSKÉ BEZPEČNOSTNÉ FÓRUM

Varšavské bezpečnostné fórum je platforma pre členské štáty EÚ, NATO a Rusko, ktorá umožňuje otvorený dialóg o problematike bezpečnostnej politiky. Zástupca CSIRT.SK prezentoval názory na prijatú Európsku stratégiu kybernetickej bezpečnosti a aktuálne bezpečnostné výzvy pre Európsku úniu, diskutoval o možnostiach budovania efektívnej operatívnej siete CSIRT tímov a rozvoja odborných spôsobilostí za účelom boja proti rastúcej počítačovej kriminalite a o možnostiach posilnenia transatlantickej spolupráce v danej oblasti.

JESENNÁ ŠKOLA OBRANY 2015 - PROJEKT JEŠKO

V novembri sme prijali pozvanie Centra pre otvorenú politiku a prezentovali sme prácu a výsledky nášho útvaru CSIRT.SK vo forme populárnej prednášky v rámci projektu Jesenná Škola obrany 2015 so zameraním na informačnú bezpečnosť. Išlo o pilotný ročník projektu pre študentov stredných škôl a gymnázií zameraných na všeobecné a humanitné vzdelávanie.

Cieľom projektu bolo predstaviť a objasniť skupine študentov v maturitných ročníkoch základné témy domácej a medzinárodnej bezpečnosti, zoznámiť ich s fungovaním bezpečnostných štruktúr, rovnako ako pochopenie medzinárodného diania. Vybraní študenti sa zúčastnili víkendového pobytu v Banskej Bystrici, kde mali pripravenú sériu odborných prednášok, workshopov a diskusií. Prednášky boli zamerané na oblasti bezpečnosti, zahraničnej politiky a riešenia konfliktov.

(NE)BEZPEČNOSŤ, KTORÚ PREHLIADAME

Prednáška, ktorá bola prednesená na Univerzite P. J. Šafárika v Košiciach a na Slovenskej Technickej Univerzite v Bratislave, vyzdvihla bezpečnostné aspekty, ktorým sa často nevenuje dostatočná pozornosť, avšak väčšinou môžu byť ľahko zneužiteľné s vážnymi dôsledkami. Konkrétne bola zameraná na domáce siete a chytré zariadenia v nej (IoT), korporátne prostredia vrátane kioskov, fyzickej bezpečnosti a cielených útokov, ale uvedené sú napríklad aj nástrahy spojené s používaním prenosných zariadení. Posledná časť prednášky bola venovaná aj vývojárom aplikácií.

PREDNÁŠKY PRE FEI STU A FMFI UK

V roku 2015 boli pracovníkmi CSIRT.SK poskytnuté viaceré prednášky na témy z oblasti počítačovej bezpečnosti. V letnom semestri boli študenti predmetu Počítačová kriminalita na Fakulte elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave zoznámení s problematikou penetračného testovania. Dôraz bol kladený na postup pri testovaní webových aplikácií a stručné vysvetlenie najčastejšie sa vyskytujúcich zraniteľností webových aplikácií. Obdobná prednáška odznela v rámci predmetu Úvod do informačnej bezpečnosti na Fakulte matematiky, fyziky a informatiky Univerzity Komenského. Na pôde FEI STU sa uskutočnili ďalšie dve prednášky. Prvá opäť na predmete Počítačová kriminalita, kde bola prezentovaná problematika forenznej analýzy.

EURÓPSKY MESIAC KYBERNETICKEJ BEZPEČNOSTI

Európsky mesiac kybernetickej bezpečnosti (ECSM) je iniciatívou Európskej únie, ktorá si kladie za cieľ propagovať informačnú bezpečnosť medzi občanmi. Snaží sa o zmenu vnímania bezpečnostných hrozieb prostredníctvom propagácie informačnej bezpečnosti, vzdelávania, zdieľania odporúčaných štandardných postupov a súťaží. CSIRT.SK pri príležitosti ECSM 2015 spustil projekt Bezpečnostná študovňa a taktiež pripravil pre odbornú verejnosť súťaž v analýze malvéru.

Súťaž v analýze malvéru prebehla už aj minulý rok. Na rozdiel od minulého ročníka bola tento rok vzorka náročnejšia, čo sa mierne prejavilo na úspešnosti riešiteľov. Analyzovaná vzorka bola pripravená tak, aby sa súťažiaci pri jej analyzovaní mohli stretnúť s rôznymi základnými technikami, ktoré sa používajú aj v reálnom malvéri. Samotná súťaž mala tiež vzdelávací charakter, keďže sme účastníkom poskytli spätnú väzbu, rady a odporúčania. Po skončení súťaže sme vypracovali vzorové riešenie pre kontrolu a inšpiráciu súťažiacich a aj pre záujemcov, ktorí by si chceli dodatočne skúsiť analyzovať súťažnú vzorku.

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, bezpečnosti mobilných a webových aplikácií, ale aj aktuálnym hrozbám typu sociálne inžinierstvo a insider threat.

Obsah študovne postupne aktualizujeme a pridávame nové študijné materiály.

PUBLIKÁCIE CSIRT.SK

PRÍRUČKA PRE HARDENING OPERAČNÝCH SYSTÉMOV ZALOŽENÝCH NA LINUXOVOM JADRE

Príručka slúži ako zoznam odporúčaní, ktoré je vhodné aplikovať, aby sa znížilo riziko úspešného útoku na daný linuxový systém. Je písaná pre všeobecné použitie pre distribúcie Debian a RHEL 5. Použitie samotnej príručky je koncipované tak, že sa aplikujú potrebné úpravy zo všeobecnej sekcie a následne sa aplikujú vybrané časti zo sekcie pre konkrétnu distribúciu.

PRÍRUČKA PRE HARDENING OPERAČNÉHO SYSTÉMU WINDOWS 7

Príručka slúži ako zoznam odporúčaní, ktoré je vhodné aplikovať pre zníženie rizika úspešného útoku na daný systém. Táto príručka je zameraná na operačný systém Windows 7, konkrétne verziu Windows 7 Enterprise. Venuje sa základnej konfigurácii zabezpečenia operačného systému, siete, služieb a aplikácií.

OCHRANA PRED DDOS ÚTOKMI

Publikácia určená pre administrátorov prináša informácie o DDoS útokoch vo všeobecnosti, popisuje dôvody a ciele takýchto útokov, ku ktorým môže patriť osobný kredit, odplata, kyberterorizmus alebo odpútanie pozornosti od iného, napr. paralelného, útoku. Publikácia popisuje metódy DDoS útokov a spôsob ochrany voči nim.

PROFIL KONCOVEJ POUŽÍVATEĽSKEJ STANICE – PLATFORMA OS WINDOWS

Táto publikácia vznikla za účelom špecifikácie základných bezpečnostných opatrení pre koncovú stanicu s nainštalovaným operačným systémom na platforme Windows v domácom prostredí. Dokument definuje základnú úroveň bezpečnosti počítača a opatrenia, ktoré je potrebné aplikovať na dosiahnutie tejto úrovne. Súčasne popisuje nastavenia ochrany detí prostredníctvom rodičovskej kontroly.

ZÁKLADNÁ OCHRANA PRED ÚTOKMI NA WEB

Publikácia má za cieľ analyzovať tri základné útoky na webové stránky, ktorými útočníci najčastejšie môžu prevziať kontrolu nad zraniteľným systémom. Patrí k nim neoprávnené vykonávanie príkazov, zneužívanie zraniteľnosti v ceste k súboru a SQL injection. Publikácia poskytuje k jednotlivým útokom aj popis spôsobu ochrany voči nim.

KONTROLNÝ ZOZNAM PRE BEZPEČNOSŤ WEBOVÝCH APLIKÁCIÍ

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 stránok a je možné ho využiť pri vykonávaní interného auditu bezpečnosti webových aplikácií a webových stránok.

20 KRITICKÝCH BEZPEČNOSTNÝCH OPATRENÍ

Pretože verejná správa má na zabezpečenie ochrany a efektívnej obrany svojich informačných systémov obmedzené prostriedky, je potrebné tieto zdroje využiť efektívne a sústrediť sa predovšetkým na ochranu kritických systémov. V dokumente CSIRT.SK definoval 20 prioritných oblastí opatrení, ktoré sú aplikovateľné na rôzne typy organizácií. Slúžia na efektívne blokovanie v súčasnosti známych útokov.

METODIKA NA OCHRANU PRED PHISHINGOM A INÝMI EMAILOVÝMI HROZBAMI

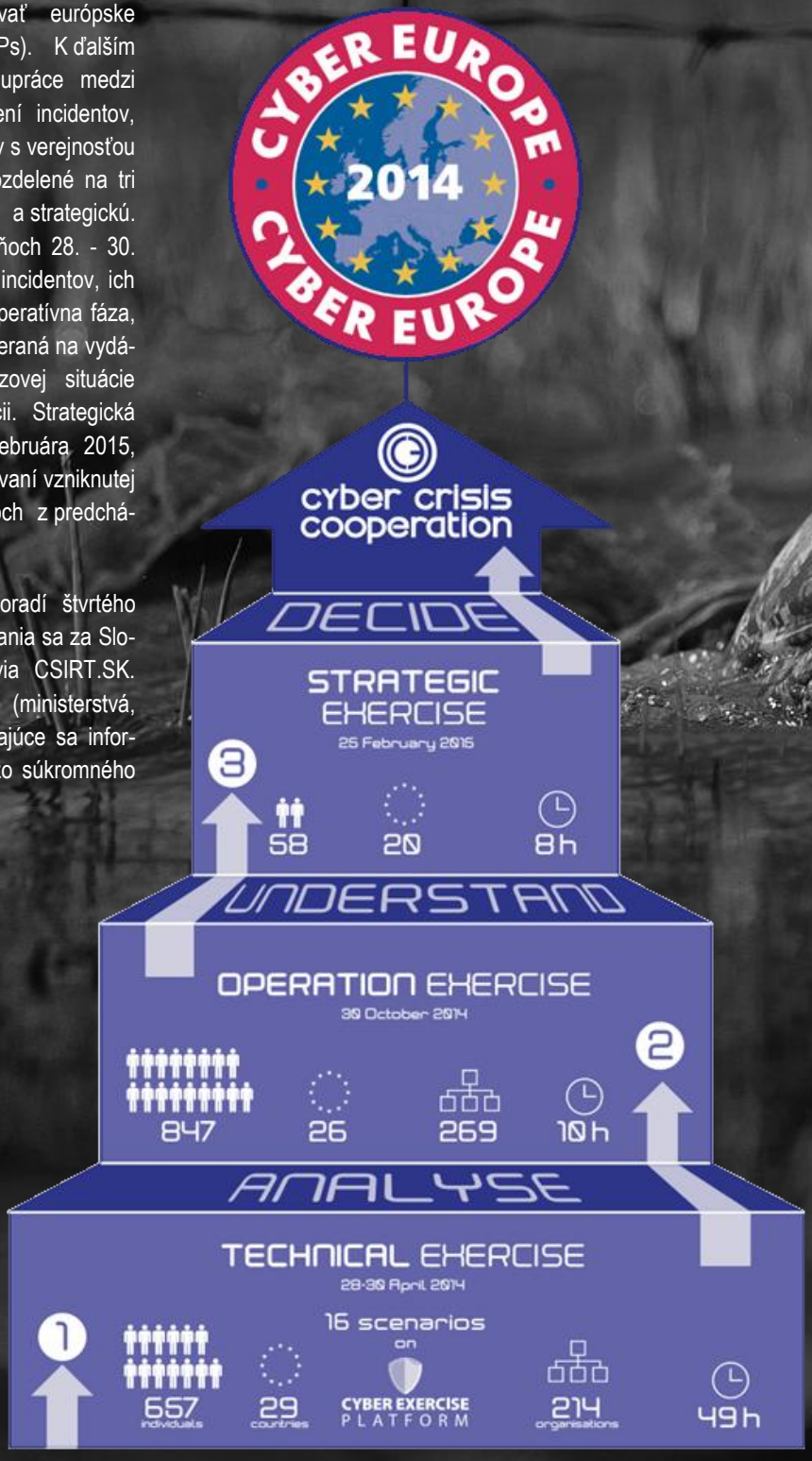
Tento dokument je koncipovaný ako stručný návod pre používateľov elektronickej pošty. Cieľom dokumentu je oboznámiť používateľov s hrozbami, ktoré prináša každodenná práca s elektronickou poštou (email), naučiť ich ako majú pristupovať k emailovým správam a v neposlednej rade tiež znížiť riziko stania sa obeťami škodlivých aktivít šíriacich sa prostredníctvom emailovej pošty.

MEDZINÁRODNÉ CVIČENIA

CYBER EUROPE

Cvičenie Cyber Europe 2014 prebehlo v troch fázach počas rokov 2014 a 2015. Zúčastnili sa na ňom tímy z 32 krajín, aby spolupracovali počas riešenia simulovaných počítačových incidentov veľkého rozsahu. Cieľom tohto cvičenia bolo poskytnúť hráčom príležitosť pre spoluprácu pri riešení významných kybernetických incidentov, otestovať národné plány, ich zvládanie a rovnako otestovať európske štandardné operatívne postupy (EU-SOPs). K ďalším cieľom cvičenia patrilo preskúmanie spolupráce medzi súkromným a verejným sektorom pri riešení incidentov, preskúmanie eskalačného procesu a vzťahov s verejnosťou počas riešenia incidentov. Cvičenie bolo rozdelené na tri eskalačné fázy - technickú, operatívnu a strategickú. Technická fáza cvičenia sa uskutočnila v dňoch 28. - 30. apríla 2014 a bola orientovaná na detekciu incidentov, ich analýzu, zmiernenie a výmenu informácií. Operatívna fáza, ktorá prebehla 30. októbra 2014 už bola zameraná na vydávanie varovaní, zmiernenie dopadov krízovej situácie a vytvorenie spoločného prehľadu o situácii. Strategická fáza cvičenia, ktorá sa uskutočnila 25. februára 2015, spočívala v diskusiách o dlhodobom zmierňovaní vzniknutej krízy a rozhodovaní založenom na vstupoch z predchádzajúcich fáz cvičenia.

V roku 2015 sa začalo s plánovaním v poradí štvrtého cvičenia Cyber Europe 2016, ktorého plánovania sa za Slovenskú republiku zúčastňujú aj zástupcovia CSIRT.SK. V prípade, že má inštitúcia štátnej správy (ministerstvá, úrady, CSIRT/CERT tímy, inštitúcie zaoberajúce sa informačnou bezpečnosťou), alebo spoločnosť zo súkromného sektora (ISP, telekomunikační operátori, poskytovatelia cloudových služieb alebo spoločnosti zaoberajúce sa informačnou bezpečnosťou) záujem zúčastniť sa na cvičení Cyber Europe 2016, kontaktuje CSIRT.SK, ktorý rád poskytne ďalšie informácie o tomto cvičení.



CYBER COALITION

V novembri 2015 sa tím CSIRT.SK aktívne zapojil do cvičenia Cyber Coalition 2015, ktoré realizovala Organizácia Severoatlantickej zmluvy. Cieľom päťdňového cvičenia bolo preveriť schopnosti spojencov a partnerov chrániť informačné a komunikačné systémy pred viacerými hrozbami ako sú napríklad mobilný malvér, spyvér alebo hacking počítačových sietí. Zároveň bola testovaná aktuálnosť interných postupov a rýchla koordinácia medzi národnými expertmi.

CSIRT.SK počas cvičenia vytvoril dva analytické tímy pre riešenie konkrétnych úloh scenára cvičenia (analýza malvéru a forenzná analýza) a ďalší zamestnanci participovali na konkrétnych úlohách v tíme rezortu Ministerstva obrany SR. Okrem technických úloh bola preverená aj komunikácia relevantných subjektov v oblasti kybernetickej bezpečnosti.

CVIČENIE PLATFORMY CECSP

Komunikačné cvičenie sa uskutočnilo 25. novembra 2015. Jeho cieľom bolo zvýšiť operatívnu spoluprácu použitím existujúcich komunikačných kanálov a mechanizmov (mailing list, wiki portál a zoznam kontaktov) s minimálnym plánovaním. Cvičenia sa zúčastnili CSIRT tímy z komunity CECSP a jeho scenár pozostával z identifikácie DoS útoku na služby operátora rozvodnej siete zemného plynu a následného precvičenia výmeny informácií a ich spracovania podľa operatívnych postupov.

CYBER DRILL

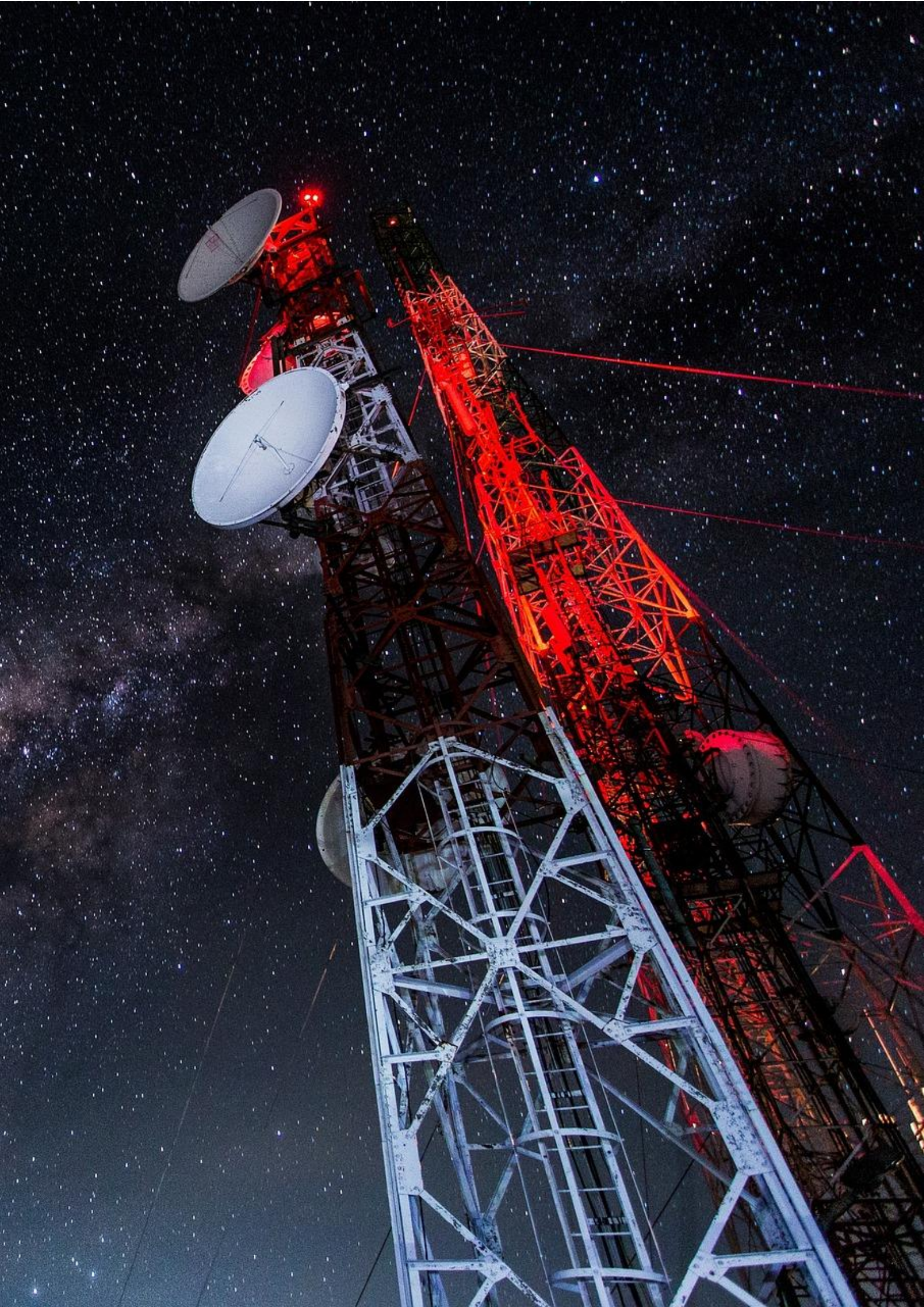
Zástupcovia CSIRT.SK sa zúčastnili workshopu CyberDrill for Europe Region 2015, ktorý bol zameraný na riešenie pokročilých typov bezpečnostných incidentov a prezentovanie štandardných postupov riešenia incidentov. Zúčastnili sa ho na základe pozvania od Medzinárodnej telekomunikačnej únie (ITU). ITU je špecializovaná agentúra Organizácie Spojených národov a medzi jej ciele patrí aj zvyšovanie dôveryhodnosti a bezpečnosti informačných a komunikačných technológií. V rámci tohto cieľa ITU organizuje workshopy CyberDrill určené pre pracovníkov národných a vládnych CSIRT tímov, telekomunikačných operátorov a vybraných organizácií jednotlivých regiónov. Predmetom workshopu boli prednášky a cvičenia zamerané na nasledovné témy:

- Aktivity ITU v oblasti kybernetickej bezpečnosti,
- Využívanie informácií o bezpečnostných hrozbách,
- Simulácie bezpečnostných incidentov špecifických pre finančný sektor,
- Komunikácia zúčastnených strán počas riešenia bezpečnostného incidentu,
- Riešenie kybernetickej krízovej situácie na národnej úrovni,
- Analýza škodlivého kódu,
- Forenzná analýza.

Účastníci workshopu si precvičili riešenie bezpečnostných incidentov simulovaných na základe skutočných incidentov a nadviazali kontakty s pracovníkmi niektorých zahraničných organizácií.

CSIRT KOMUNITA

PRAKTICKÉ INFORMÁCIE



CSIRT KOMUNITA

Skratka CSIRT je označenie jednotky pre riešenie počítačových incidentov (Computer Security Incident Response Team). Používa sa aj označenie CERT (Computer Emergency Response Team). Jednotka CSIRT predstavuje tím odborníkov, ktorých hlavnou úlohou je poskytovať služby potrebné na zvládnutie bezpečnostných počítačových incidentov, na zmiernenie alebo odstránenie ich následkov a na následnú obnovu činnosti prevádzkových informačných systémov a súvisiacich informačných a komunikačných prostriedkov. CSIRT tímy sa líšia svojimi cieľovými skupinami. Zatiaľ čo vo svete prevládajú tímy, ktoré si vytvorili komerčné spoločnosti a univer-zity, na Slovensku pôsobiaca jednotka CSIRT.SK je tímom, ktorý zriadilo Ministerstvo financií Slovenskej republiky.

Komunita tímov na riešenie počítačových incidentov je tvorená CSIRT/CERT tímami zo súkromného a verejného sektora z celého sveta. Ich vzájomná spolupráca a zdieľanie informácií nielen počas riešenia incidentu je pre nich veľmi dôležitá. Na základe svojej klientely, tzv. konštituencie, je možné CSIRT/CERT tímy rozdeliť na národné, vládne, súkromné a akademické.

V rámci CSIRT komunity existujú skupiny, ktoré organizujú výmenu informácií a pravidelné stretnutia. Patrí k nim TF-CSIRT a FIRST. TF-CSIRT podporuje spoluprácu a koordináciu tímov v rámci Európy. FIRST združuje CSIRT tímy z celého sveta a od svojich členov vyžaduje splnenie istých štandardov pre funkčnosť a bezpečnosť. Ďalšou organizáciou, ktorá významne podporuje spoluprácu CSIRT tímov je agentúra ENISA, ktorá okrem množstva iných aktivít napomáha CSIRT tímom v preverovaní ich schopností prostredníctvom cvičenia Cyber Europe.

V rámci krajín strednej Európy bola vytvorená platforma CECSP, Central European Cyber Security Platform, ktorá je zoskupením krajín Rakúsko, Česká republika, Maďarsko, Poľská republika a Slovenská republika. Cieľmi platformy CECSP je zdieľanie informácií, postupov a kapacít v oblasti informačnej bezpečnosti, vytvorenie bezpečných komunikačných kanálov na predchádzanie úniku citlivých informácií, harmonizácia stanovísk k problémom v oblasti informačnej bezpečnosti na medzinárodných fórach a vytváranie spoločných pracovných skupín.

TLP PROTOKOL

CSIRT tímy sa pri komunikácii a výmene informácií riadia tzv. TLP (Traffic Light Protocol), ktorý využíva štyri farby na indikáciu rôznych stupňov citlivosti informácií a primeraných spôsobov zdieľania týchto informácií:

TLP: RED – nezverejniteľné informácie, ku ktorým majú prístup len oprávnené osoby a nemôžu byť ďalej šírené. O týchto informáciách nie je povolené diskutovať v prítomnosti tretích osôb.

TLP: AMBER – informácie je možné sprístupniť len osobám participujúcim na výmene informácií a osobám v rámci organizácie, resp. konštituencie, a to na báze „need to know“. Toto označenie sa používa pri výmene citlivých informácií, pri ktorých je potreba ich efektívneho zdieľania medzi oprávnenými adresátmi, existuje však riziko narušenia súkromia, reputácie alebo prevádzky v prípade ich úniku.

TLP: GREEN – informácie, ktoré je možné zdieľať s ostatnými organizáciami alebo osobami v rámci širšej komunity alebo sektora, nie je ich však vhodné šíriť prostredníctvom verejne prístupných komunikačných kanálov, ako napr. webová stránka.

TLP: WHITE – informácie určené pre verejnosť, ktorých šírenie nie je obmedzené. Pri ich používaní je však potrebné rešpektovať autorské práva.

HLÁSENIE INCIDENTU

V prípade vzniku bezpečnostného incidentu je potrebné vždy kontaktovať zodpovednú osobu v rámci organizácie v závislosti od interných predpisov a štandardov, ktorými sa daná organizácia riadi (správca IS, bezpečnostný manažér a pod.). Následne je potrebné zabezpečiť prvotné úkony spojené s riešením vzniknutého incidentu, zdokumentovať všetky skutočnosti, ktoré by mohli napomôcť pri jeho riešení a vykonať potrebné kroky na odstránenie alebo zmiernenie jeho dopadov.

V prípade rozsiahlejšieho incidentu týkajúceho sa väčšej časti siete a pri možnosti identifikácie adries útočníka je potrebné kontaktovať zodpovedné osoby nadriadenej siete, poskytovateľa internetových služieb alebo správcov sietí, ktoré boli označené ako zdrojové siete (odkiaľ prichádza útok, odkiaľ bol poslaný nežiaduci obsah a pod.)

Ak boli vykonané uvedené kroky a neprichádza žiadna odpoveď od kontaktovaných strán, je potrebné kontaktovať CSIRT.SK spolu so zaslaním všetkých relevantných údajov. Bezpečnostný počítačový incident je možné nahlásiť útvaru CSIRT.SK telefonicky alebo zaslaním emailu na adresu *incident@csirt.gov.sk*. K emailu je možné priložiť prílohy a v prípade potreby využiť aj náš verejný PGP kľúč na ich zašifrovanie, ktorý je dostupný na webovom sídle CSIRT.SK v sekcii Kontakty.

Pri hlásení incidentu je nutné uvádzať korektnú emailovú adresu, ktorá je primárnym kontaktom. Ďalej je nutné uviesť jednoznačný popis incidentu a uviesť pri ňom čo najviac informácií, ktoré by mohli pomôcť pri jeho analýze a následnom spracovaní. Každá, hoci aj zdanlivo na prvý pohľad neužitočná informácia, môže byť veľmi užitočná. Podrobné kontaktné údaje a informácie o spôsobe hláseniu incidentu je možné nájsť na našom webovom sídle www.csirt.gov.sk.

POPIS INCIDENTU BY MAL OBSAHOVAŤ TIETO ÚDAJE:

Informácie o osobe v organizácii, ktorá hlási incident:

- meno, funkcia/pracovné zaradenie,
- názov organizácie, typ organizácie (štátna, súkromná),
- ďalšie dotknuté organizácie.

Informácie o incidente:

- čas začiatku incidentu (ak je známy),
- čas a spôsob zistenia,
- ide o prebiehajúci incident? (áno/nie/neviem),
- boli zneužité nejaké známe zraniteľnosti? (áno/nie/neviem),
- aké opatrenia boli vykonané,
- detailný popis - popis priebehu incidentu, aké typy útokov boli použité, odkiaľ útok smeroval, aké boli bezpečnostné opatrenia (firewall, antivírus),či boli prekonané a pod.,
- ak ide o spam pripojte úplnú hlavičku a telo emailovej správy napr. vo formáte *.eml,
- ak ide o vírus, tak dotknutý súbor zabaľte do formátu ZIP zabezpečeným heslom: „incident“,
- ak ide o phishing alebo pharming, pripojte prosím aj úplnú adresu URL,
- ak ide o sieťové skenovanie alebo útok typu odopretia služieb (DoS), pripojte prosím časové známky, časovú zónu, zdrojové a cieľové IP (prípadne MAC) adresy a porty, typ protokolu (TCP, UDP, ICMP) - ak je možné pripojte aj vzorku zachytených paketov (napr. pomocou programu WireShark).

Informácie o zasiahnutých zariadeniach a dopadoch:

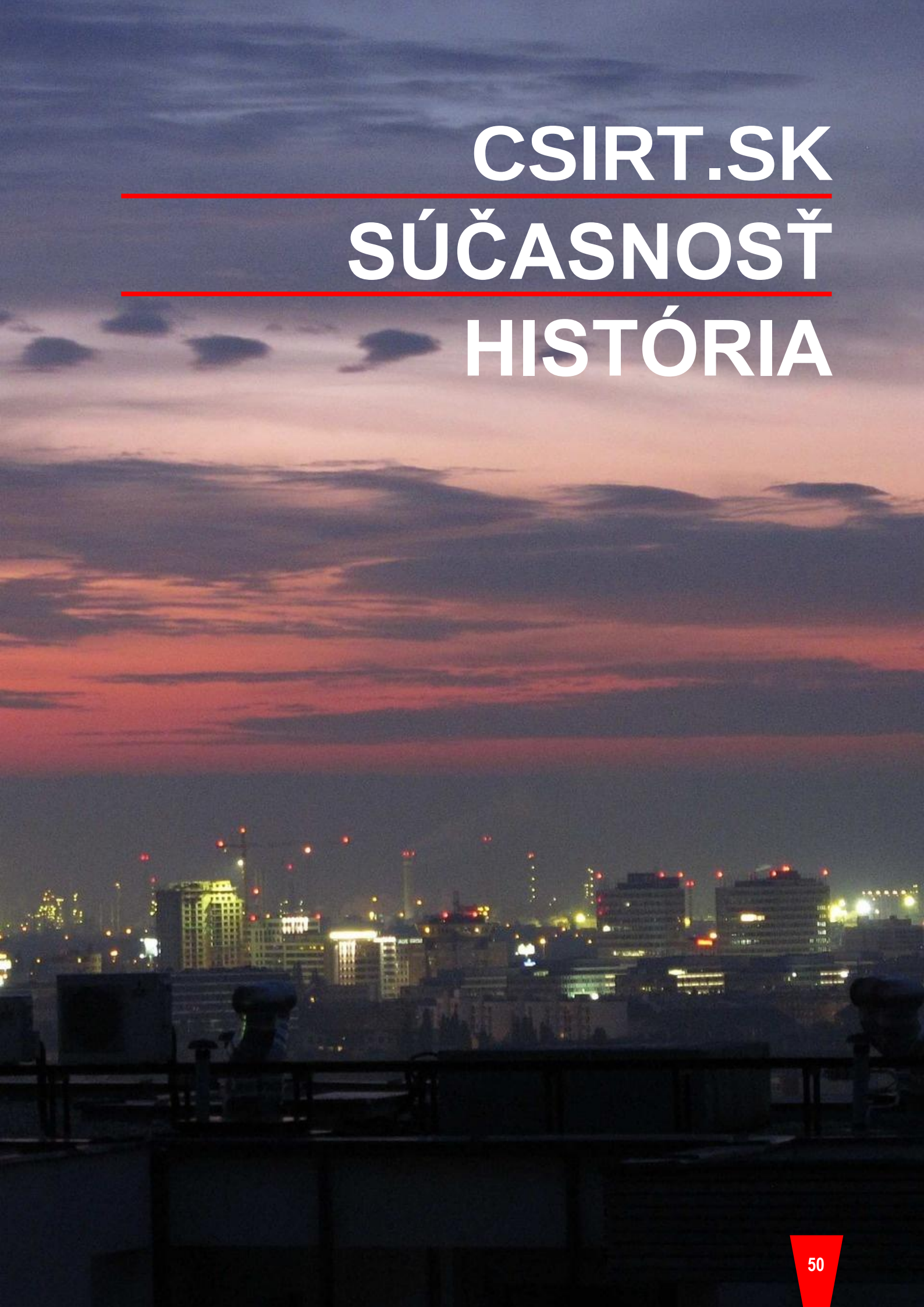
- typ a funkcia zariadenia,
- IP adresa a hostname,
- protokol a porty, na ktoré útok smeroval,
- popis hardvéru zariadenia,
- operačný systém (typ, verzia),
- zasiahnutý softvér alebo súbory,
- ide o kritické zariadenie z pohľadu pokračovania v činnosti?
- je zariadenie v prevádzke?
- kontaktná osoba pre získanie prístupu k zariadeniu,
- obsahuje zariadenie neverejné informácie?

EMAILOVÁ ADRESA PRE HLÁSENIE INCIDENTOV:

incident@csirt.gov.sk

NA PREDCHÁDZANIE INCIDENTOM CSIRT.SK PRE ORGANIZÁCIE ODPORÚČA:

- SYSTEMATICKÉ AKTUALIZÁCIE OPERAČNÝCH SYSTÉMOV SIEŤOVÝCH ZARIADENÍ, SERVEROV A PRACOVNÝCH STANÍC SO ZAMERANÍM SA NA ZARIADENIA DOSTUPNÉ Z PROSTREDIA INTERNETU
- POUŽÍVANIE SILNÝCH HESIEL ADMINISTRÁTOROV A POUŽÍVATEĽOV
- OBMEDZENIE PRÁV POUŽÍVATEĽOV NA MINIMÁLNU MOŽNÚ MIERU, TAK ABY MOHLI VYKONÁVAŤ SVOJE PRACOVNÉ ČINNOSTI
- INŠTALÁCIU ANTIVÍRUSOVÉHO SOFTVÉRU NA VŠETKÝCH PRACOVNÝCH STANICIACH A SERVEROCH A PRAVIDELNE AKTUALIZÁCIE TOHTO SOFTVÉRU
- SEGMENTÁCIU SIETE NA ODDELENÉ SEGMENTY S PODOBNÝMI BEZPEČNOSTNÝMI POŽIADAVKAMI NA ZÁKLADE ICH FUNKCIONALITY
- IMPLEMENTÁCIU ACL NA PRINCÍPE WHITELISTINGU PRE PRICHÁDZAJÚCU AJ ODCHÁDZAJÚCU KOMUNIKÁCIU
- IMPLEMENTÁCIU PORT SECURITY NA VŠETKÝCH ETHERNETOVÝCH PRÍPOJKÁCH
- ŠIFROVANIE CITLIVÝCH ÚDAJOV, ICH UKLADANIE A PRENOS IBA V ŠIFROVANEJ PODOBE
- SYSTEMATICKÚ AKTUALIZÁCIU APLIKÁCIÍ
- BLOKOVANIE JAVASCRIPTU, FLASH A JAVA FUNKCIONALÍT WEBOVÉHO PORTÁLU (S VÝNIMKAMI PRE DÔVERYHODNÉ PORTÁLY) V PREHLIADAČOCH NA PRACOVNÝCH STANICIACH
- PRAVIDELNÉ PENETRAČNÉ TESTY INFRAŠTRUKTÚRY A IMPLEMENTÁCIU OPATRENÍ NA OŠETRENIE ZISTENÝCH NEDOSTATKOV
- VYTVORENIE A IMPLEMENTÁCIU NAHLASOVANIA BEZPEČNOSTNÝCH INCIDENTOV VLÁDNEJ JEDNOTKE CSIRT.SK



CSIRT.SK
SÚČASNOSŤ
HISTÓRIA

CSIRT.SK SA STAL ČLENOM ZDRUŽENIA FIRST

Dňa 9. marca 2015 bol CSIRT.SK schválený ako riadny člen (full member) organizácie FIRST (Forum of Incident Response and Security Teams). Členstvo umožňuje tímom na riešenie počítačových incidentov efektívnejšie reagovať na počítačové incidenty poskytnutím prístupu k nástrojom, odporúčaným štandardným postupom a dôveryhodnej komunikácií s členskými tímami.

FIRST bol založený v roku 1990 ako reakcia na Internetom sa šíriace červy. Už vtedy mali incidenty dopad nielen na uzavreté skupiny používateľov alebo organizácie, ale aj na množstvo sietí prepojených prostredníctvom Internetu. Bolo zrejmé, že spolupráca a vzájomná výmena informácií o nových zraniteľnostiach a hrozbách bude pre tímy na riešenie počítačových incidentov kľúčová.

FIRST je jediným celosvetovým fórom CSIRT/CERT tímov a svojím globálnym charakterom prispieva k šíreniu existujúcich bezpečnostných iniciatív k ostatným svojim členom. FIRST organizuje pravidelné aj nepravidelné podujatia pre svojich členov a pre komunitu bezpečnostných profesionálov.

K významným udalostiam patria napr. každoročná konferencia o riešení počítačových incidentov, regionálne sympóziá a technické kolokviá a workshopy.

FIRST taktiež poskytuje množstvo zdrojov informácií pre svojich členov, ale i pre verejnosť prostredníctvom svojej bezpečnostnej knižnice. Je v nej možné nájsť veľa článkov, publikácií, prezentácií, návodov či odporúčaných štandardných postupov. FIRST umožňuje svojim členom publikovať svoje vlastné návody, odporúčania a články, ktoré umožňuje ďalej propagovať v rámci FIRST komunity.

Abecedný zoznam všetkých členov FIRST je možné nájsť na adrese: https://www.first.org/members/teams

AKO MÔŽE CSIRT.SK POMÔCŤ VAŠEJ ORGANIZÁCII

Hlavnou úlohou špecializovanej jednotky CSIRT.SK je riešenie počítačových incidentov v Slovenskej republike v spolupráci s vlastníkmi a prevádzkovateľmi postihnutých častí národnej informačnej a komunikačnej infraštruktúry, telekomunikačnými operátormi, poskytovateľmi internetových služieb a prípadne inými štátnymi orgánmi (napr. polícia, vyšetrovatelia a súdy). Ďalej budovanie a rozširovanie poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti a kooperácia so zahraničnými partnerskými organizáciami a reprezentácia SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni.

CSIRT.SK však nepredstavuje organizáciu zaoberajúcu sa vývojom bezpečnostných riešení, antivírusového a bezpečnostného softvéru. Nezaoberá sa ani vývojom opráv a aktualizácií pre zaplátanie zraniteľností v systémoch.

CSIRT.SK nezodpovedá ani za vašu informačnú bezpečnosť, ale v prípade potreby dokáže vzniknutý problém pomôcť zmierniť alebo odstrániť.

SPOLUPRÁCA V OBLASTI RIEŠENIA BEZPEČNOSTNÝCH INCIDENTOV

Špecializovaný útvar CSIRT.SK spolupracoval na národnej úrovni v oblasti riešenia bezpečnostných incidentov a zdieľania informácií o aktuálnych hrozbách a trendoch predovšetkým s bezpečnostnými útvarmi Ministerstva obrany SR, Ministerstva vnútra SR, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu a Slovenskej informačnej služby. 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.

Spolupráca bola realizovaná v oblasti reakcie na bezpečnostné incidenty, posudzovania bezpečnosti komunikačnej infraštruktúry, identifikácie aktuálnych zraniteľností a implementácie potrebných opatrení na ich odstránenie. Súčasne CSIRT.SK vykonával pre inštitúcie verejnej správy penetračné testy a ohodnocovanie zraniteľností webových aplikácií.

DataCentrum, hosťovská organizácia, pod ktorú patrí špecializovaný útvar CSIRT.SK, v roku 2015 uzavrelo v oblasti spolupráce v informačnej bezpečnosti 7 zmlúv s inštitúciami verejnej správy, akademického a bankového sektora. Ďalšie 4 zmluvy boli rozpracované a ich uzavretie sa očakáva v roku 2016.

16.2.2015 Dohoda o vzájomnej spolupráci so združením SANET

1.4.2015 Zmluva o spolupráci s VÚB, a.s.

27.4.2015 Zmluva o spolupráci s VNET, a.s.

25.5.2015 Dohoda o spolupráci s NIX.CZ, z.s.p.o.

19.7.2015 Zmluva o spolupráci a výmene informácií so Slovenskou sporiteľňou

9.10.2015 Dohoda o spolupráci so Slovenskou technickou univerzitou v Bratislave

9.10.2015 Dohoda o spolupráci s Univerzitou Komenského v Bratislave

31.12.2015 Dohoda o spolupráci s Disig, a.s.

Na medzinárodnej úrovni CSIRT.SK aktívne reprezentoval a obhajoval záujmy Slovenskej Republiky v expertných pracovných skupinách zameraných na riešenie problematiky informačnej bezpečnosti zasadajúcich na pôde Európskej agentúry pre informačnú a sieťovú bezpečnosť (ENISA) a Organizácie pre bezpečnosť a spoluprácu v Európe (OSCE). Špecializovaný útvar CSIRT.SK je členom združení TF-CSIRT a FIRST a aktívne sa zapájal do medzinárodných projektov. Taktiež je členom Stredoeurópskej platformy pre spoluprácu krajín V4 a Rakúska (CECSP) v oblasti kybernetickej bezpečnosti. Spolupráca so zahraničnými tímami CSIRT/CERT Rakúska, Nemecka, Maďarska, Českej republiky, Poľska, Španielska, USA, Holandska a ďalších krajín prebieha na dennej báze.

HISTÓRIA CSIRT.SK

1. JÚL 2009

Prvé legislatívne podmienky pre oficiálne zriadenie špecializovanej jednotky pre riešenie počítačových incidentov v SR - CSIRT.SK na základe uznesenia vlády SR č. 479/2009 v zmysle úlohy vyplývajúcej z Národnej stratégie pre informačnú bezpečnosť v SR.

1. FEBRUÁR 2010

Začiatok personálneho a technického budovania národného a vládneho tímu CSIRT.SK v SR, vytvorenie podmienok a poskytovanie prvých služieb. Nadväzovanie prvých kontaktov s klientelou a CSIRT/CERT komunitou.

13. JÚL 2010

Spustenie webového sídla CSIRT.SK za účelom prezentovania informácií o jednotke, poskytovaných službách, možnostiach komunikácie s klientelou a zverejnenie on-line formulárov pre nahlásenie bezpečnostných incidentov, prípadne objavenia zraniteľností týkajúcich sa bezpečnosti počítačových a komunikačných technológií.

14. SEPTEMBER 2010

Na základe splnenia stanovených kritérií bol udelený špecializovanej jednotke CSIRT.SK štatút „listed“, čím sa začlenila do európskej komunity TF-CSIRT (Task Force - Computer Security Incident Response Team).

4. NOVEMBER 2010

Špecializovaný útvar CSIRT.SK sa aktívne zúčastnil cvičenia CYBER EUROPE 2010, prvého celoeurópske cvičenia zameraného na ochranu kritickej informačnej infraštruktúry. Cvičenie organizovala Európska agentúra pre bezpečnosť informácií a sietí (ENISA) a Európske výskumné centrum (JRC). Zúčastnilo sa ho aktívne 22 krajín EÚ a EFTA, teda viac ako 150 odborníkov z oblasti informačnej bezpečnosti zo 70 inštitúcií z celej Európy.

13. MÁJ 2011

Špecializovaný útvar CSIRT.SK úspešne zavŕšil druhý stupeň procesu akreditácie v európskom združení CSIRT/CERT tímov TF-CSIRT (Task Force of Computer Security Incident Response Teams) a získal tak štatút „accredited“.

23. NOVEMBER 2011

CSIRT.SK v spolupráci s MF SR pripravil a realizoval prvé národné cvičenie na ochranu kritickej informačnej infraštruktúry Slovenskej republiky - Slovak Information Security Exercise 2011 - SISE 2011. Cieľom cvičenia bolo preveriť procesy a technické znalosti pri reakcii na rozsiahle IKT incidenty. Scenár simuloval kybernetický útok na inštitúcie štátnej správy, ktorý mal za následok výpadok poskytovaných elektronických služieb.

MAREC AŽ DECEMBER 2012

CSIRT.SK navrhol a vybudoval laboratórne prostredie pre poskytovanie služieb a analýzy v oblastiach testovania malvéru, forenznej analýzy, penetračného testovania a sieťového laboratória.

NOVEMBER 2012

Prvá aktívna účasť CSIRT.SK na medzinárodnom cvičení Cyber Coalition 2012 organizovanom NATO. Úlohou účastníkov cvičenia bolo analyzovať kybernetické útoky na NATO infraštruktúru a na základe získaných výsledkov pripraviť efektívne opatrenia proti nim.

6. NOVEMBER 2012

Uskutočnilo sa cvičenie Slovak Information Security Exercise 2012 - SISE 2012, ktoré bolo v poradí druhým národným cvičením zameraným na ochranu kritickej informačnej infraštruktúry (KII) v Slovenskej republike.

MAREC 2013

Prvý významný operatívny zásah CSIRT.SK pri koordinácii riešenia rozsiahleho bezpečnostného incidentu špionážneho softvéru s názvom Red October, ktorý sa zameriaval na vládne inštitúcie.

MÁJ 2013

CSIRT.SK sa stáva jedným zo zakladajúcich členov Stredoeurópskej platformy kybernetickej bezpečnosti CECSP, ktorá má za cieľ posilniť úroveň spolupráce medzi krajinami V4 a Rakúska v oblasti kybernetickej bezpečnosti.

11. AŽ 19. NOVEMBER 2013

Uskutočnilo sa Slovak Information Security Exercise 2013 - SISE 2013, ktoré bolo v poradí tretím národným cvičením zameraným na ochranu kritickej informačnej infraštruktúry (KII) v Slovenskej republike.

JÚL 2014

S cieľom overiť funkčnosť elektronických služieb informačných systémov verejnej správy MF SR rozhodlo, že špecializovaný útvar CSIRT.SK bude preverovať úroveň bezpečnosti projektov OPIS a to prostredníctvom penetračných testov.

OKTÓBER 2014

CSIRT.SK sa prvýkrát aktívne zapojil do projektu Európsky mesiac kybernetickej bezpečnosti (ECSM). ECSM je iniciatívou Európskej únie, ktorá si kladie za cieľ propagovať informačnú bezpečnosť medzi občanmi, zmeniť vnímanie bezpečnostných hrozieb a poskytnúť aktuálne informácie o informačnej bezpečnosti prostredníctvom vzdelávania a šírenia odporúčaných štandardných riešení.

9. MAREC 2015

CSIRT.SK sa stal členom organizácie FIRST (Forum of Incident Response and Security Teams). Členstvo umožňuje tímom na riešenie počítačových incidentov efektívnejšie reagovať na počítačové incidenty poskytnutím prístupu k nástrojom, najlepším praktikám a dôveryhodnej komunikácií s členskými tímami.

30. OKTÓBER 2015

Oficiálne uzatvorenie spolupráce medzi DataCentrom, Slovenskou technickou univerzitou v Bratislave a Univerzitou Komenského v Bratislave. Spolupráca bude realizovaná v oblasti informačnej bezpečnosti pri vytváraní kapacít schopných riešiť celospoločenské problémy, spoločnej tvorbe informačných zdrojov a budovaní spoločných laboratórií.

ROK 2015

CSIRT.SK pomáha pri budovaní CSIRT/CERT komunity na Slovensku.

ODBORNÉ TERMÍNY A SKRATKY

ACL	(access control list) zoznam pre riadenie prístupu určuje kto alebo čo má povolenie pristupovať k objektu a aké operácie s ním môže vykonávať
APT	advanced persistent threat
ASLR	(Address space layout randomization) technika ochrany pred útokmi zneužívajúcimi pretečenie zásobníka, tzv. buffer overflow
ATHENA	systém zdieľania informácií vyvinutý útvarom CSIRT.SK
AUTENTIZÁCIA	overenie identity subjektu
BACKDOOR	(zadné dvierka) metóda umožňujúca obísť bežnú autentifikáciu. Autentizácia bráni neoprávnenému používateľovi vniknúť do počítačového systému
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)
C&C	(command and control) server používaný na riadenie botnetu na diaľku
CECSP	Central European Cyber Security Platform
CSIRT.SK	špecializovaný útvar pre riešenie počítačových bezpečnostných incidentov v Slovenskej republike; bol definovaný uznesením vlády SR č. 479 z 1. júla 2009
CVE	(common vulnerabilities and exposures) zoznam verejne známych zraniteľností v oblasti informačnej bezpečnosti
CYBER COALITION	séria cvičení informačnej bezpečnosti, ktoré organizuje agentúra ENISA
CYBER EUROPE	séria cvičení informačnej bezpečnosti, ktoré organizuje NATO
DATACENTRUM	rozpočtová organizácia Ministerstva financií 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
DNS	(domain name system) systém doménových mien prekladá názvy domén na IP adresy
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.

ECSM	Európsky mesiac kybernetickej bezpečnosti
ENISA	Európska agentúra pre sieťovú a informačnú bezpečnosť
EU-SOPs	štandardné operatívne postupy pre riešenie kybernetických incidentov v Európskej únii
Exploit	program, dáta alebo sekvencia príkazov, ktoré využívajú programátorskú chybu, ktorá spôsobí pôvodne nezamýšľanú činnosť softvéru.
FEI STU	Fakulta elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave
FIRST	fórum tímov pre riešenie počítačových incidentov
FMFI UK	Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
FTP	Protokol prenosu súborov
Hardening	proces, pri ktorom sa zvyšuje bezpečnosť informačného systému
IKT	informačné a komunikačné technológie
Incident handling	proces riešenia incidentov
I2P	(Invisible Internet Project) anonymná peer-to-peer distribuovaná komunikačná vrstva postavená na open source nástrojoch
IoC	(indikátor kompromitácie) artefakt pozorovaný v sieti alebo v operačnom systéme, ktorý s vysokou mierou istoty označuje vniknutie do systému
IoT	(internet of things) sieť fyzických objektov, zariadení, vozidiel, strojov a iných objektov, ktoré sú vybavené elektronikou, softvérom, senzormi a pripojením k sieti, čo týmto objektom umožňuje zber a výmenu údajov
IP adresa	logický číselný identifikátor daného uzla v sieti, ktorý komunikuje s inými uzlami prostredníctvom protokolu IP
ISP	poskytovateľ internetového pripojenia
ITU	Medzinárodná telekomunikačná únia
Jailbreaking	proces odstránenia softvérových obmedzení v operačnom systéme iOS od spoločnosti Apple, ktorý umožňuje prístup ku koreňovým adresárom
MAC adresa	identifikačné číslo sieťového adaptéra slúžiace na jednoznačnú identifikáciu sieťového rozhrania v lokálnych počítačových sieťach
Malvér	(malware, škodlivý softvér) všeobecný názov pre škodlivé programy

MAN-IN-THE-MIDDLE útok prostredníctvom odpočúvania komunikácie medzi účastníkmi tak, že sa útočník stane aktívnym prostredníkom

MRM Malicious resource manager

NIX.CZ spoločnosť združujúca českých i zahraničných poskytovateľov internetových služieb za účelom vzájomného prepojenia ich sietí

OS operačný systém

PAKET blok prenášaných dát v počítačovej sieti

PENETRAČNÝ TEST test, ktorý odhalí formou pokusu o neoprávnený prienik do systémov slabiny a mieru zraniteľnosti organizácie

PGP počítačový program, ktorý umožňuje šifrovanie a podpisovanie

PHARMING podvodná technika používaná na získavanie citlivých údajov od obetí útoku

PHISHING činnosť, pri ktorej sa podvodník snaží vylákať od používateľov ich digitálnu identitu napríklad prihlasovacie mená, heslá, údaje k bankovému účtu a podobne

POČÍTAČOVÝ BEZPEČNOSTNÝ INCIDENT porušenie alebo bezprostredná hrozba porušenia bezpečnostných politík, bezpečnostných zásad alebo štandardných bezpečnostných pravidiel prevádzky informačných a komunikačných technológií

PORT SECURITY technika zvyšovania bezpečnosti pomocou konfigurácie individuálnych switch portov tak, aby povolili iba špecifikované množstvo zdrojových MAC adries

PROXY SERVER server, ktorý umožňuje klientom nepriame pripojenie k inému serveru

RANSOMVÉR (ransomware) druh malvéru, ktorý zabraňuje prístupu k infikovanému počítaču, a spravidla vyžaduje zaplatenie výkupného (anglicky ransom) za sprístupnenie počítača

ROOTING proces umožňujúci získať privilegovaný prístup (root access) v operačnom systéme Android

SASIB Slovenská asociácia pre informačnú bezpečnosť

SISE (Slovak information security exercise) cvičenie na ochranu kritickej informačnej infraštruktúry v SR

SOCIÁLNE INŽINIERSTVO spôsob manipulácie ľudí za účelom vykonania určitej akcie alebo získania určitej informácie

SPAM nevyžiadaná pošta

SQL INJECTION	bezpečnostná chyba založená na možnosti manipulovať s dátami v databáze bez nutnosti vlastníctva legitímnych prístupových údajov
SSH	secure shell
SSL/TLS	protokoly, ktoré slúžia na šifrovanie dát
SW	softvér
TCP	Transmission Control Protocol
UDP	User datagram protocol
ICMP	Internet Control Message Protocol
TF-CSIRT	(Task Force of Computer Security and Incident Response Teams) zoskupenie vládnych, národných, akademických a privátnych CERT/CSIRT tímov v Európe. Hlavnou úlohou je podporovať spoluprácu takýchto tímov na medzinárodnej úrovni, výmenu informácií a skúseností z oblasti informačnej bezpečnosti.
TICKETOVACÍ SYSTÉM	SW na spracovanie riešenia incidentov
TLP	(Traffic Light protokol) systém klasifikácie informácií pri ich zdieľaní
TROJAN	(trójsky kôň) program, ktorý vykonáva deštruktívnu činnosť, pričom sa skrýva za užitočnú činnosť
URL	(Uniform Resource Locator) je formát mien používaný na označenie zdroja na internete
WATERING HOLE	stratégia útoku, pri ktorom útočník vytipuje stránky, ktoré obeť alebo skupina obetí často navštevuje a následne tieto stránky infikuje škodlivým kódom
WHITELISTING	zoznam alebo register entít, ktorým sa poskytujú osobitné oprávnenia, služby alebo prístupy
WORKAROUND	obídenie problému v systéme
XSS ÚTOK	(cross-site scripting útok) je metóda narušenia webových stránok využitím bezpečnostných chýb v skriptoch
ZERO-DAY ZRANITEĽNOSŤ	novoobjavená programátorská chyba systému alebo aplikácie, ktorá nie je jej autorom známa alebo doteraz opravená
ZRANITEĽNOSŤ	bezpečnostná chyba, slabina alebo nedostatok v systéme

CSIRT.SK
WWW.CSIRT.GOV.SK