

ROLE CERT/CSIRT v NÁRODNÍ BEZPEČNOSTI



Národní úřad
pro kybernetickou
a informační bezpečnost



Historie

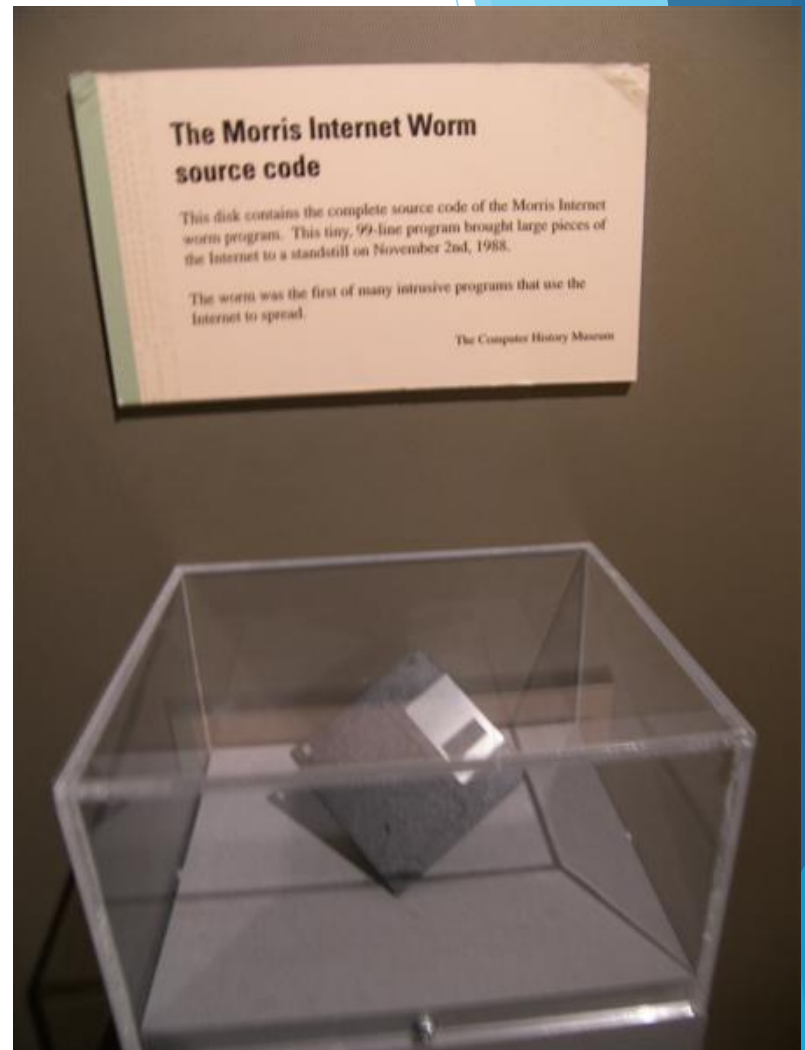
- 1988 - Morrisův červ
- Autor: Robert T. Morris
- Červ aktivován ze stanice v MIT
- Zranitelnost v Unix / ovlivněn celý internet (až 10% stanic nakaženo)
- Motiv: ?
- Usvědčen dle 1986 computer Fraud and Abuse Act
- Trest: community service, pokuta, 3 roky probace





Historie

- Vznik PS (MIT, Berkeley, Purdue, ...)
- Institucionalizace řešení kybernetických bezpečnostních incidentů → The CERT® Coordinated Center (CERT®/CC)
- CERT®/CC, jakožto pionýr - stále funguje pod Carnegie Mellon University (TM „CERT“)
- V Evropě SURFnet-CERT (1992)







CERT/CSIRT

- Dalšími názvy, s kterými se můžeme setkat jsou například:
 - IRT (Incident Response Team),
 - CIRT (Computer Incident Response Team),
 - SERT (Security Emergency Response Team),
 - CIRC (Computer Incident Response Centre)
 - a další.
- Všechny spojuje zvládání a řešení kybernetických bezpečnostních incidentů
- V každém státě na vrcholové úrovni nějaký CERT/CSIRT



Rozsah činnosti pracoviště CERT/CSIRT

- V rámci určení pracovního rámce každého pracoviště CERT/CSIRT jsou vždy nejdůležitější tyto tři otázky, které dále definují rozsah činnosti CERT/CSIRT :
 1. Jaké má CERT/CSIRT poslání? (základní principy, strategické cíle, úkoly a priority, ...)
 2. Jaká je CERT/CSIRT constituency? (pole působnosti)
 3. Jaké je organizační zakotvení CERT/CSIRT? (definice pozice v rámci interní/externí organizační struktury a systému krizového řízení)

Constituency

- Pole působnosti - Soubor subjektů, kvůli kterým byl CERT/CSIRT vytvořen/komu poskytuje a nabízí služby
- *Constituency* může být jak neomezená, kdy CERT/CSIRT poskytuje služby komukoliv, nebo omezená (ve většině případů), kdy poskytuje své služby jen vybrané, úzké komunitě
- Může být však obtížné přehledně a jednoduše definovat constituency
- **RFC 2350 standard** (základní info o možnostech kontaktování, odpovědnosti a nabízených službách)

GOVCERT.CZ

- veřejné instituce a kritická informační infrastruktura v České republice



- celá Česká republika, tzn. všichni uživatelé a všechny sítě provozované v České republice se nachází ve sféře vlivu CSIRT.CZ



- Constituency bezpečnostního týmu Masarykovy univerzity CSIRT-MU může být definována:
 - „univerzitní síť Masarykovy univerzity“
 - skrze doménu „*.muni.cz“ (tj. fss.muni.cz; ff.muni.cz; apod.)
 - a skrze rozsah IP adres (všechny IPv4 adresy z rozsahu 147.251.0.0/16, všechny IPv6 adresy z rozsahu 2001:718:801::/48)

TYPY CERT/CSIRT

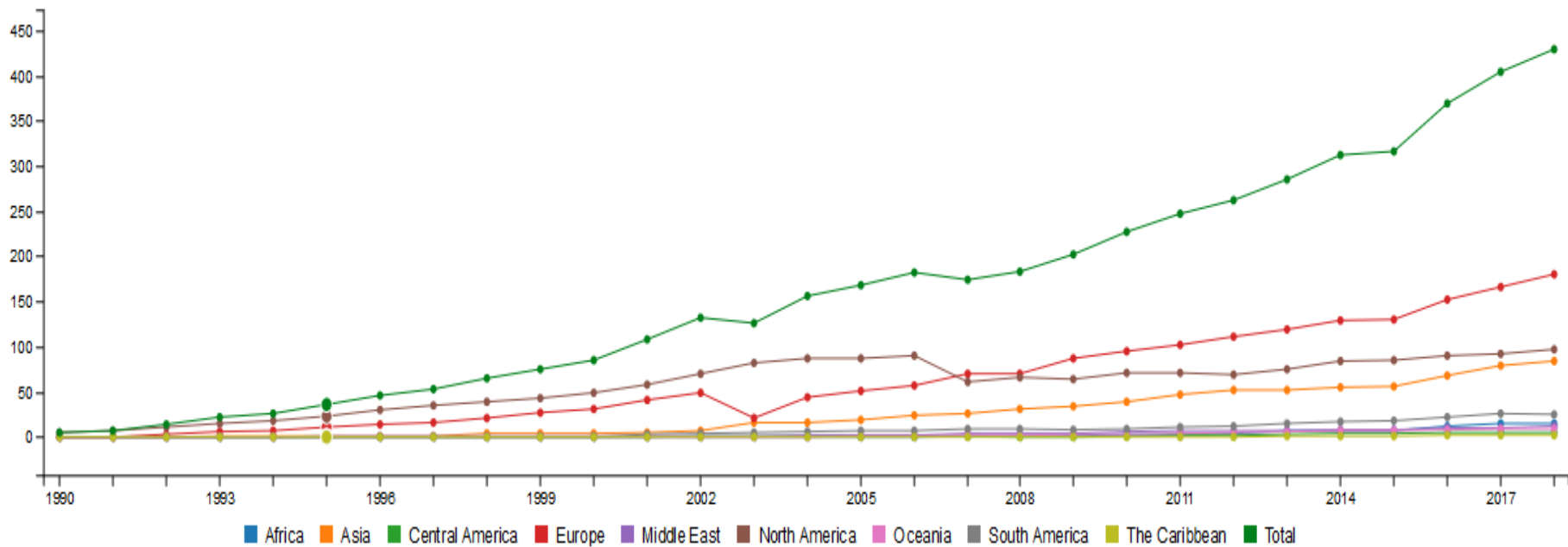
- **Národní/vládní** (GovCERT.CZ, SingCERT)
- **Regionální** (TF-CSIRT, AfricaCERT)
- **Sektorový** (ICS-CERT)
- **Akademický** (CESNET-CERTS)
- **Vojenský** (Centrum CIRC)
- **Interní** (ACTIVE24-CSIRT, CSOB-Group-CSIRT)
- **Koordinační** (GovCERT.CZ, US-CERT)
- **Produktové** (Cisco PSIRT, Adobe PSIRT)
- **Byznys / Poskytovatelé incident handling** (Team Cymru, Nixu, Mandiant)
- ...

FIRST

- Založeno 1990
- Forum for Incident Response and Security Teams
- Sdružuje CERT komunitu na globální úrovni
- Hlavním cílem: sdílení informací a zkušeností mezi CERT pracovišti a pomoc při rozsáhlých kybernetických bezpečnostních incidentech
- Aktuálně přes 350 členů
- Status: member

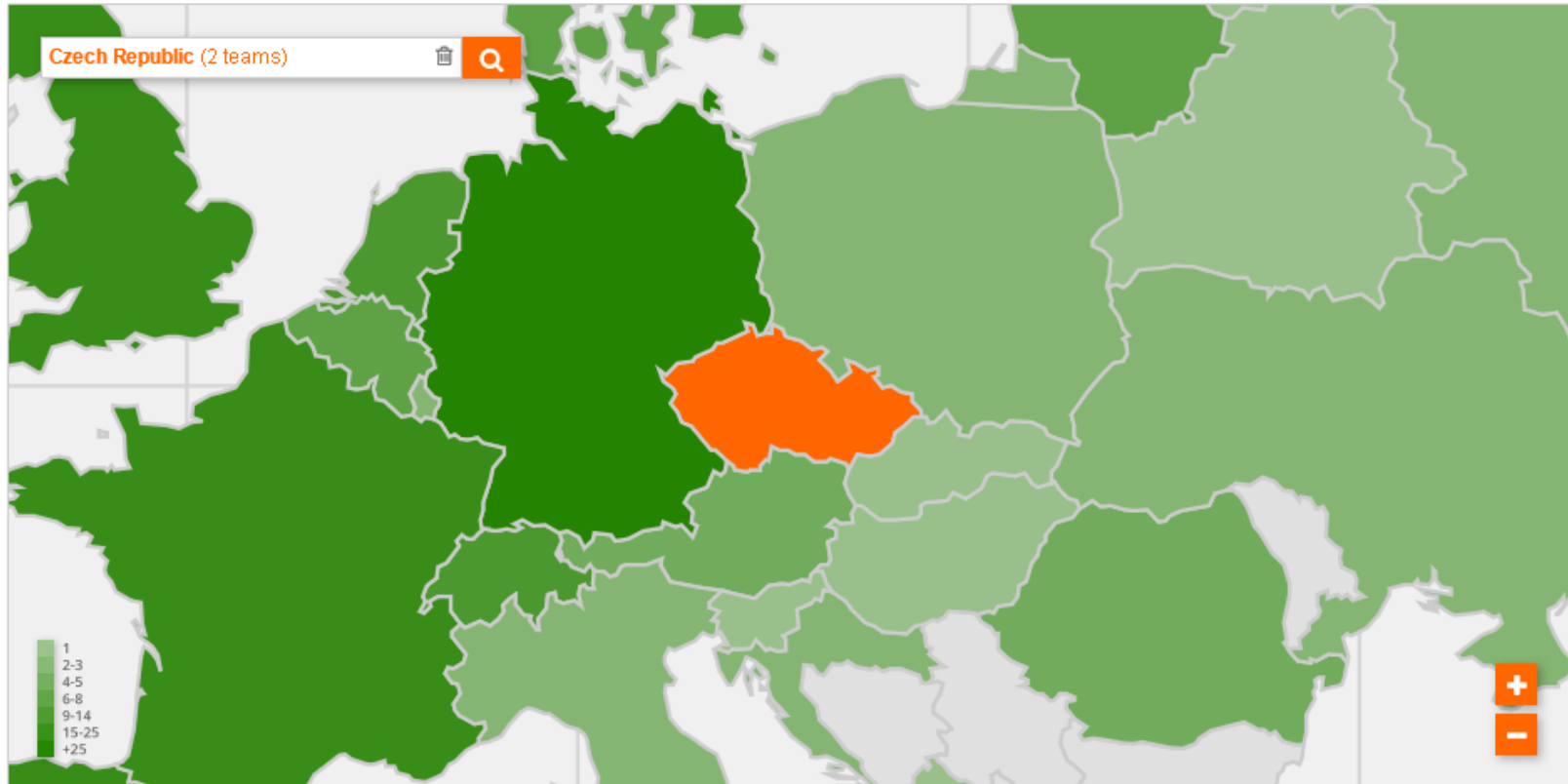


FIRST members growth by year*



(*) The statistic measurement method and regional breakdown changed in 2007.

Members around the world



Search results for: **Czech Republic** (2 teams)



Team name	Official Team name	Country
CSIRT.CZ	The Czech National CSIRT	
GovCERT.CZ	Government CERT of the Czech Republic	

FIRST follows the International Olympic Committee (IOC) country name listings.

[credits]

TI-GÉANT

- 2000 - založena evropská komunita CERT/CSIRT týmů za účelem řešení společných potřeb a budování infrastruktury, která by poskytovala důležitou podporu všem bezpečnostním týmům, zaměřeným na řešení a řízení bezpečnostních incidentů
- Pro akreditované / certifikované týmy jsou k dispozici služby, které jim umožní efektivněji spolupracovat a účinněji si vyměňovat informace



TF-CSIRT
Trusted Introducer



TI-GÉANT

- Status:
 - Listed (splnění základních požadavků)
 - Accredited (náročnější proces - standardní stupeň)
 - Certified (pouze malá část týmů / potvrzení vysoké vyspělosti týmu)
- TRANSITS / TF-CSIRT meetings
- Další regionální platformy: AfricaCERT, APNIC, ...



Czech Republic

ALEF-CSIRT	Accredited (since 14 Nov 2016)
CESNET-CERTS	Accredited (since 27 Jan 2008)
CSIRT-MU	Certified (since 05 Dec 2016)
CSIRT.CZ	Certification Candidate (since 10 Dec 2017)
CZ.NIC-CSIRT	Accredited (since 26 Aug 2010)
GOVCERT.CZ	Accredited (since 21 Aug 2014)
SOCA	Accredited (since 10 Feb 2017)

20CSIRT	Listed (since 15 Sep 2014)
ACTIVE24-CSIRT	Listed (since 09 Feb 2012)
ALEF-CSIRT	Accredited (since 14 Nov 2016)
AVEN TA CSIRT	Listing Candidate (since 04 Oct 2018)
CASABLANCA_CZ-CSIRT	Listed (since 08 Mar 2014)
CD FCERT	Listed (since 16 Jul 2014)
CEBNET-CERTS	Accredited (since 27 Jan 2008)
CETIN CSIRT	Listed (since 31 Mar 2017)
Coolhousing CSIRT	Listed (since 17 Sep 2014)
CRA CSIRT	Listed (since 09 Nov 2016)
CS-CSIRT	Listed (since 11 Mar 2016)
CSIRTSAS	Listed (since 04 Jul 2018)
CSIRT Merit	Listed (since 25 Mar 2015)
CSIRTOU	Listed (since 04 Jul 2018)
CSIRTMU	Certified (since 05 Dec 2016)
CSIRTFPOSS	Listed (since 26 Jun 2018)
CSIRFWUT	Listed (since 20 May 2014)
CSIRT.CZ	Certification Candidate (since 10 Dec 2017)
CSOB-Group-CSIRT	Listed (since 29 Oct 2014)
CZ.NIC-CSIRT	Accredited (since 26 Aug 2010)

DIAL-CSIRT	Listed (since 16 Dec 2013)
ELAT CSIRT	Listed (since 03 May 2018)
FORPSI-CSIRT	Listed (since 19 Jul 2015)
GOVCERTCZ	Accredited (since 21 Aug 2014)
ISPA CSIRT	Listed (since 13 Aug 2015)
KAORA-CSIRT	Listed (since 04 Mar 2015)
KBIM CSIRT	Listed (since 13 Dec 2017)
KERNUN CSIRT	Listed (since 09 Oct 2017)
MASTER.CZ-CSIRT	Listed (since 12 Dec 2017)
NIXCZ-CSIRT	Listed (since 13 Dec 2017)
02.cz CERT	Listed (since 01 Jan 2014)
SEBET	Listed (since 25 Oct 2014)
SEZNAM.CZ-CSIRT	Listed (since 18 Oct 2013)
SOC-Corpus	Accreditation Candidate (since 13 Aug 2018)
SOC365 CSIRT	Listed (since 15 May 2018)
SOCA	Accredited (since 10 Feb 2017)
TMOZ CSIRT	Listed (since 08 Aug 2016)
TPS-CSIRT	Listed (since 15 Mar 2017)
VSHOSTING-CSIRT	Listed (since 21 Jul 2017)
WEB4U-CSIRT	Listed (since 19 Jul 2015)

CERT/CSIRT - činnosti a aktivity

- Důležitá je kooperace a důvěra se svou constituency a ostatními CERT/CSIRT
- **Esenciální součástí zvládnání a řešení kybernetických bezpečnostních incidentů + další služby (ovlivňuje finanční prostředky, technologické vybavení a lidský kapitál)**
- CERT/CC vytvořil základní klasifikaci CERT služeb, která by měla sloužit k větší konzistenci a srovnatelnosti popisu CERT služeb



CERT/CSIRT - činnosti a aktivity

- **Reaktivní služby:** základní element činnosti všech CERT. Tyto služby jsou spouštěny skrze detekovanou/nahlášenou bezpečnostní událost/incident (incident handling, vydávání varování, zvládání zranitelností, manipulace s artefakty, ...)
- **Proaktivní služby:** Tyto služby poskytují pomoc a informace za účelem připravit, chránit a zabezpečit systémy v constituency. CERT tak proaktivně přispívá ke snížení počtu incidentů v budoucnu (vývoj bezpečnostních nástrojů, IDS, proaktivní šíření informací, bezpečnostní audity, ...)
- **Management kvality bezpečnosti:** služby, které rozšiřují stávající, již zavedené služby / přidaná hodnota (poradenství, analýza rizik, certifikace, vzdělávání/školení, ...)

Kultura CERT komunity




























- CERT/CC jako pionýr a prapůvodce komunity
- Celá komunita sdílí několik klíčových principů, které pramení ze společného přesvědčení, chápání a pohledu na kybernetickou bezpečnost
- Důležitost vzájemné komunikace a především důvěry mezi členy, jako důležité prerekvizity k účinné a úspěšné spolupráci
- Důvěra („Hlava 22“):
 - Nezbytnost - iniciuje kooperaci s možným pozitivním výsledkem
 - Trusted introducer - založeno na dobrých vztazích mezi členy (využíváno např. v FIRST, TF-CSIRT)
 - Příležitost - vytváří vazby mezi členy / zapojování se do chodu komunity (např. vývoj bezp. nástrojů)

ASSESS ANALYZE WRITE PUBLISH CONFIGURATION TOOLS STATISTICS LOGOUT

Switch to custom search

Category: Search: Start date: End date: U R I W Search!

C U

Timestamp	Source	Title / description	
<input type="checkbox"/> 06-07-2010 14:26:38		i-Net Solution Matrimonial Script alert.php Cross Site Scripting Vulnerability 2010-07-06	   
<input type="checkbox"/> 06-07-2010 14:04:16		Release of Cacti 0.8.7g Beta 2 and MORE! Release of Cacti 0.8.7g Beta 2 and MORE!	  
<input type="checkbox"/> 06-07-2010 13:48:16		Sun Java System Web Server Admin Interface Denial of Service Vulnerability 2010-07-06	   
<input type="checkbox"/> 06-07-2010 13:46:08		[webapps] - Pre Multi-Vendor Shopping Malls SQL Injection Vulnerability & Auth Bypass Vulnerability.	  
<input type="checkbox"/> 06-07-2010 13:29:52		H264WebCam NULL Pointer Dereference PoC Target: H264WebCam 3.7 Impact: Denial of service	  
<input type="checkbox"/> 06-07-2010 13:28:45		ScriptsFeed Auction Software "id" SQL Injection Vulnerabilities Moderately critical	   

Sdílení informací a dat

- Nejrozumnější informace a data od dalších CSIRT, AV společností, ISP, a dalších partnerů
- Feedy/fóra:
Malc0de; Malware Domain List; Shadowserver; Zone-H; Phishtank; Abuse.ch, ...

ABUSE | ch

 PhishTank® Out of the Net, into the Tank.



shadowSERVER



HomePage

Shadowserver

Mission

Updated

Terms of Service

New

Privacy

Standards and

Guidelines

Organizations

Blog

Calendar

Future Goals

Jobs and Contributions

Press

Security Organizations

News Articles

Blogs and Forums

Misc

Presentations

Chronological

Operations Status

Knowledge Base

Technology in Use

Botnets

Botnet Detection

Honeypots

eFraud

Malware

Whitepapers

Definitions

Links

Sinkholes

Mission

Introduction

The Shadowserver Foundation is continually seeking to provide timely and relevant information to the security community at large. We also seek to increase our level of research and investigation into the activity we discover. As such, we list our goals and plans for the next six to twelve months:

Goals

- Investigate and contribute to new technologies in botnet control.
- Develop and deploy new methods for harvesting malware and studying its behavior.
- Develop and utilize additional techniques for gathering and analyzing botnet data and network flows.
- Work more closely with ISPs, Hosting and DNS providers in the identification and mitigation of botnets and malware propagation.
- Increase our collaboration with other key security organizations and researchers to share discoveries and analysis.
- Develop and release whitepapers and reports based on our research.
- Further develop our website to provide information and reports to the interested public.
- Participate in future security conferences and workgroups.
- Increase our communication with the public through irc, mailing lists, and the website.

Co se sdílí?

- Indikátory kompromitace (IoCs): virové signatury, škodlivé IP adresy, malware soubory, URL, doménové jména
- Kontextové informace např. o malware kampaních, informace o modu operandi útočníků,
- Případové studie a reporty o incidentech,
- Varování o možných či potenciálních obětech útoku,
- Dešifrovací klíče u ransomware útoků,
- Detaily zájmových účtů na sociálních sítích a další

<https://www.phishtank.com/>

<http://www.malwaredomainlist.com/mdl.php>

Jak a kolik se toho sdílí?



- List Events
- Add Event
- Import From MISP Export
- List Attributes
- Search Attributes
- View Proposals
- Events with proposals
- Export
- Automation

Published	Org	Owner Org	Id	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	CUDESO	ORGNAME	93	ttp:white	16	admin@admin.test	2016-03-23	Medium	Completed	SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE RANSOM	All	🔗 🗑️ 📄
✓	CUDESO	ORGNAME	91	ttp:white	3	admin@admin.test	2016-03-07	Low	Completed	Ad Serving Platform Used By PUA Also Delivers Magnitude Exploit Kit	All	🔗 🗑️ 📄
✓	CUDESO	ORGNAME	92	ttp:white	3	admin@admin.test	2016-03-25	Low	Completed	PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers	All	🔗 🗑️ 📄
✗	CIRCL	ORGNAME	5	ttp:white Type:OSINT	84	admin@admin.test	2016-02-13	Medium	Completed	OSINT - Turia - Harnessing SSL Certificates Using Infrastructure Chaining	All	📥 🔗 🗑️ 📄
✗	CIRCL	ORGNAME	43	ttp:white Type:OSINT	70	admin@admin.test	2016-03-21	Low	Completed	OSINT - STOP SCANNING MY MACRO	All	📥 🔗 🗑️ 📄
✓	CIRCL	ORGNAME	10	ttp:white circl:incident-classification="system-compromise"	847	admin@admin.test	2016-03-17	Low	Initial	Potential SpamBots (2016-03-17)	All	🔗 🗑️ 📄
✓	CIRCL	ORGNAME	44	ttp:white circl:incident-classification="malware"	290	admin@admin.test	2016-03-17	Low	Initial	Malspam (2016-03-17) - Dridex (122), Locky	All	🔗 🗑️ 📄
✓	CIRCL	ORGNAME	16	ttp:white	92	admin@admin.test	2016-03-16	Low	Completed	OSINT - AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device	All	🔗 🗑️ 📄
✓	CUDESO	ORGNAME	71	ttp:white	25	admin@admin.test	2016-03-11	Low	Completed	PowerSniff Malware Used in Macro-based Attacks	All	🔗 🗑️ 📄
✓	CIRCL	ORGNAME	25	malware_classification:malware-category="Ransomware"	32	admin@admin.test	2016-03-16	Low	Initial	Locky (2016-03-16)	All	🔗 🗑️ 📄

Event: 3513

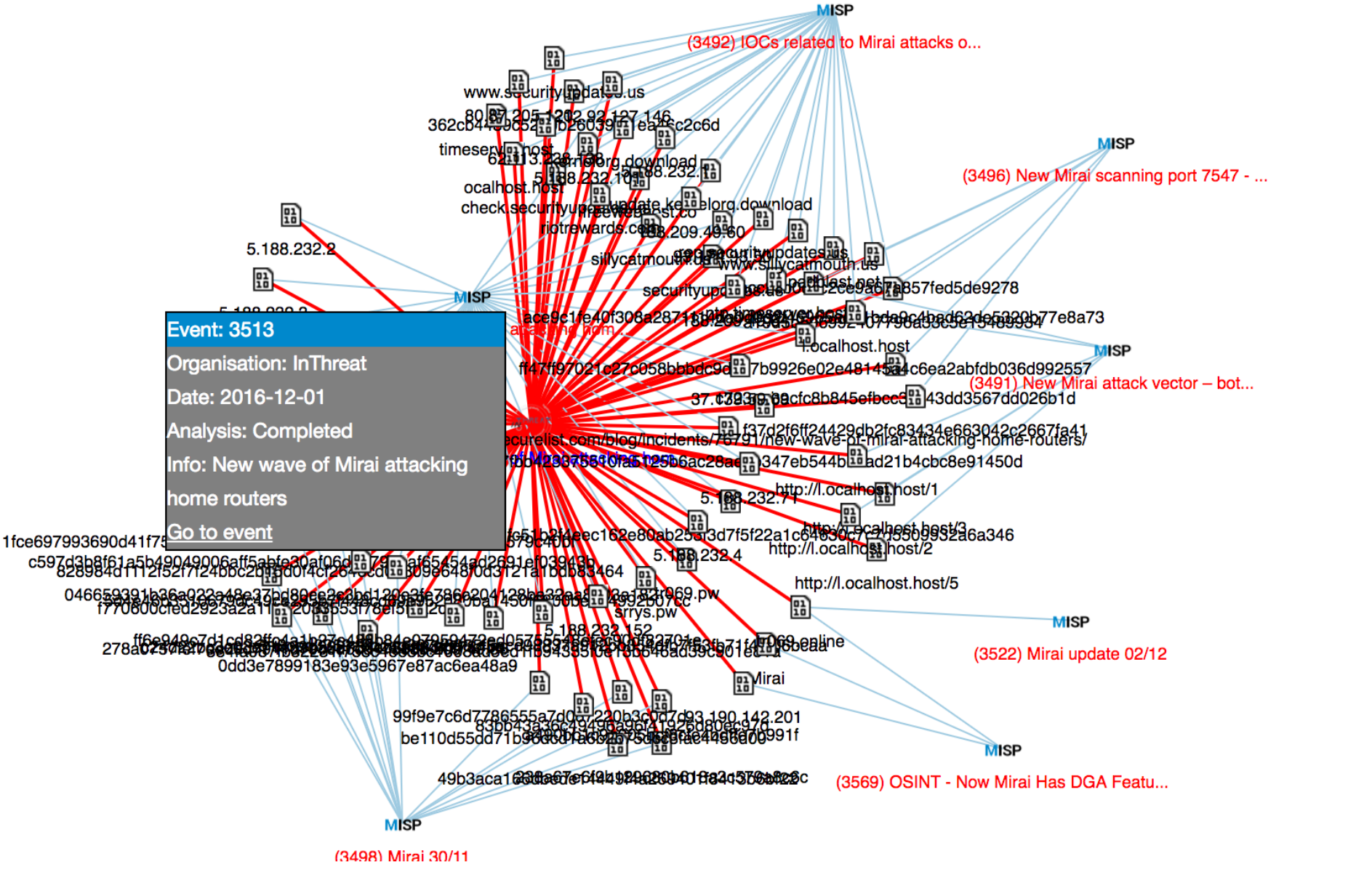
Organisation: InThreat

Date: 2016-12-01

Analysis: Completed

Info: New wave of Mirai attacking home routers

[Go to event](#)



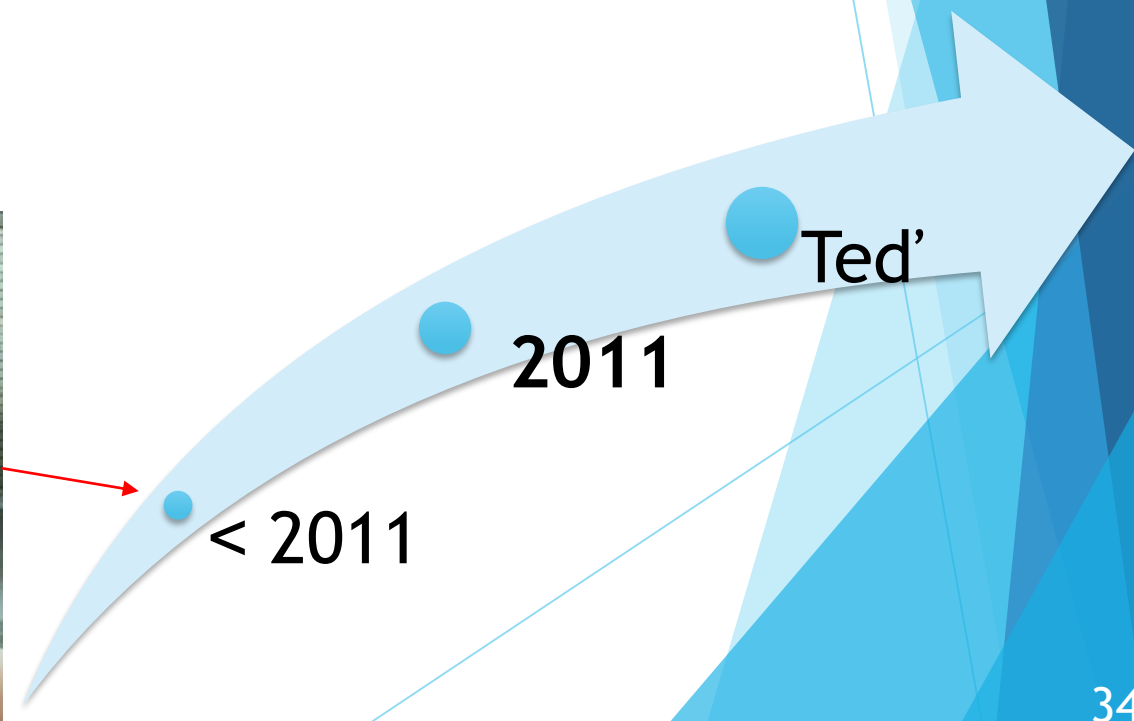
(3498) Mirai 30/11

Stát vs. CERT/kybernetická bezpečnost

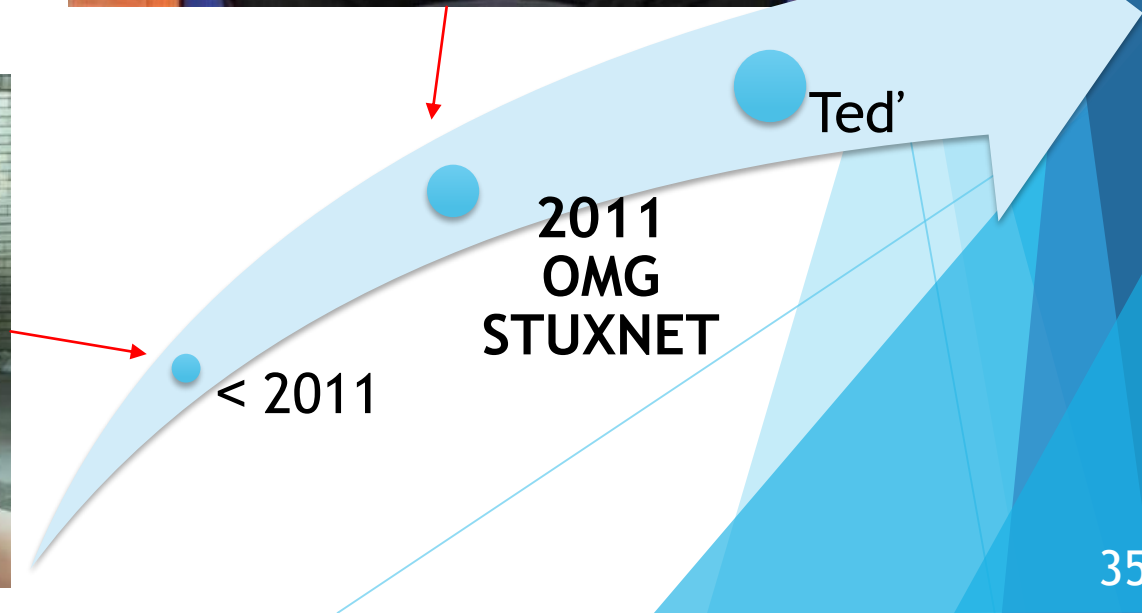
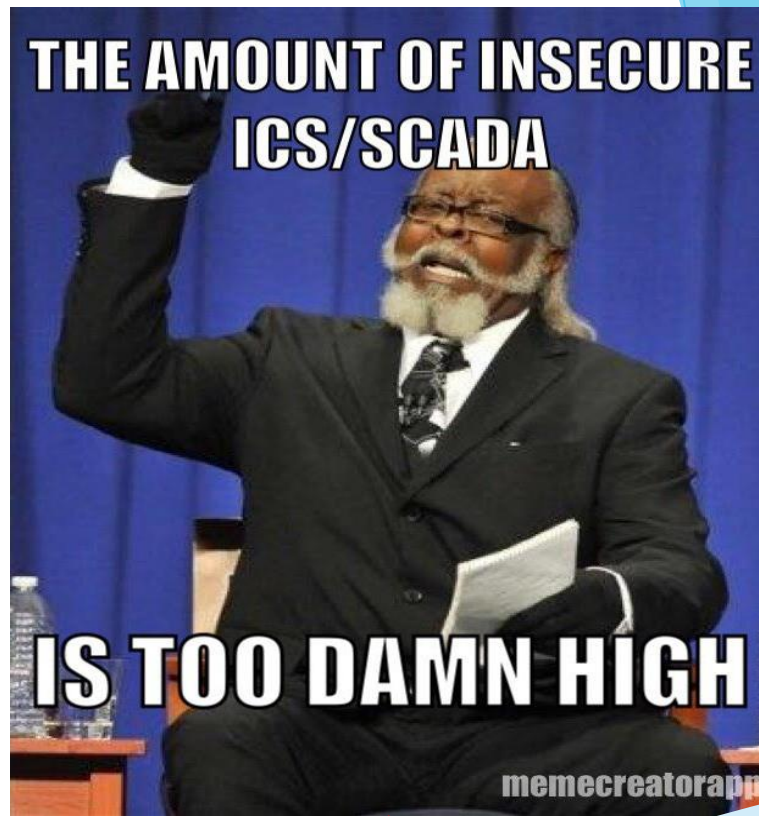
- V posledních několika letech téma kybernetické bezpečnosti katapultováno z uzavřeného prostředí technických expertů až na politické výsluní
- Virus Stuxnet / nárůst kyberkriminality / kyberšpionážní kampaně / Estonsko 2007 / 11. září 2001 → Politizace / sekuritizace tématu



ICS/SCADA cyber security



ICS/SCADA cyber security



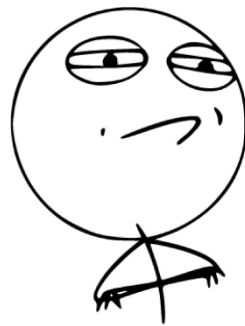
Stát vs. CERT/kybernetická bezpečnost

- Rozšíření ve dvou směrech:
Vertikálním: od expertní úrovně k úrovni politické
Horizontálním: z USA a dalších pár vyspělých evropských zemí do téměř všech ostatních států světa
- Nejnovější trend: řešit kybernetickou bezpečnosti skrze strategicko-vojenskou optiku (aktivní protiopatření, kybernetická obrana, kybernetické zastrašování, ...)



Vybrané výzvy: CERT jako policy aktér

- Povaha CERT komunity akademická vs. fungování státního aparátu
- Národní/vládní CERT musí nacházet ideální rovnováhu mezi fungováním v rámci CERT komunity a plněním politických cílů a povinností
- Národní/vládní CERT mají specifickou „netechnickou“ agendu
- Nové výzvy....



CHALLENGE ACCEPTED

Vybrané výzvy: Sdílení informací a vzájemná důvěra

- Otázka odpovědnosti / poškození reputace / důvěry constituency
- Vnitrostátní právní předpisy (např. zákony o datové lokalizaci)
- Čína, Vietnam, Írán, Rusko X Austrálie, Kanada
- Různé důvody/politické cíle:
 - od zajištění ochrany osobních údajů svých občanů
 - až k ochraně státní suverenity
 - či podpoře růstu domácí digitální ekonomiky

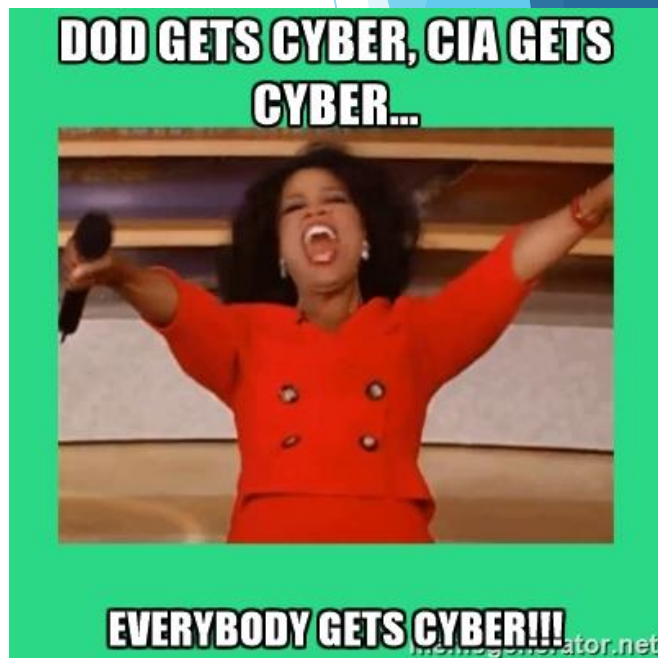
Vybrané výzvy: Komeracionalizace kybernetické bezpečnosti

- Komodifikace a kumulace zranitelností (zero-days vulnerabilities)
- Zdroj financí např. pro soukromé firmy (nákup/vyhledávání)
- Podporuje konkurenční prostředí (paradoxně nenavyšuje kyberbezp.)
- Případ NSA / státem kupované zranitelnosti?
- Negativně působí na spolupráci v CERT komunitě

ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

Vybrané výzvy: Rostoucí CERT komunita / politizace kybernetické bezpečnosti

- Status národní/vládní CERT sebou nese mnoho zodpovědnosti, ale také benefitů (zejména lepší přístup k finančním prostředkům, citlivým informacím, ...)
- Resorty/instituce mohou usilovat o převzetí agendy / vstup aktérů, kteří nejsou a nemají být součástí CERT komunity
- Volby mohou mít zásadní vliv na směřování a rozvoj CERT
→ hrozba rozkladu celého konceptu kybernetické bezpečnosti v zemi během pár dní
- CERT obětí politického boje - negativně působí na bezpečnostní situaci nejen na národní, ale i na mezinárodní úrovni



Vybrané výzvy: Pozice CERT v systému zajišťování národní bezpečnosti



- Rozdílné vnímání kybernetické bezpečnosti a kybernetických hrozeb
- GOV-CERT.RU is tasked with information security and making *“recommendations on how to neutralize relevant information security threats,”* which include the use of information and communications technology to interfere *“with the internal affairs of the sovereign state, [and] violation of public order,”*
- Může vést k porušování lidských práv, svobody slova, apod.
→ ostatní CERT se mohou vyhýbat sdílení informací, spolupráci

Vybrané výzvy: Kyberprostor jako nová operační (vojenská) doména

- Aktivnější role státu v kyberprostoru / používání aktivních prostředků a nástrojů:
 - Zajišťování kybernetické obrany v reálném čase (schopnost reagovat efektivně a dostatečně rychle)
 - Schopnost aktivní identifikace a rekognoskace nepřítele v kyberprostoru (spočívá v lokálním i vzdáleném shromažďování informací, tj. získání logů či dat ze síťového provozu; OSINT; monitoring zranitelností, aj.)
 - Schopnost provádět odvetné (tzv. hacking back) i preemptivní kybernetické útoky (např. nasazení malware, modifikace síťového provozu, provádění DoS/DDoS útoků proti útočníkovi, apod.)
- Nedotýká se přímo CERT, ale má vliv na efektivitu jeho práce / sdílení informací, důvěru, apod. = jaká role v KO?

ROLE STÁTU V ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI



*Kybernetická
obrana*



Ochrana KII



Kybernetická
kriminalita



Působení
zpravodajských
služeb

KYBERNETICKÁ BEZPEČNOST STÁTU

Národní CERT vs. zpravodajské služby a policie

Národní CSIRT pracoviště

Neintencionální kybernetické bezpečnostní incidenty,
např. lidská selhání, špatná technická konfigurace

Intencionální kybernetické bezpečnostní incidentu nízké závažnosti,
např. komoditní malware, DDoS útoky nízké intenzity

Společný zájem

Kybernetická kriminalita,
resp. intencionální kybernetické bezpečnostní incidenty naplňující skutkovou podstatu trestného činu

Zpravodajské služby

Intencionální kybernetické bezpečnostní incidenty vysoké závažnosti, např. útoky státních a nestátních aktérů (teroristé), útoky na KII

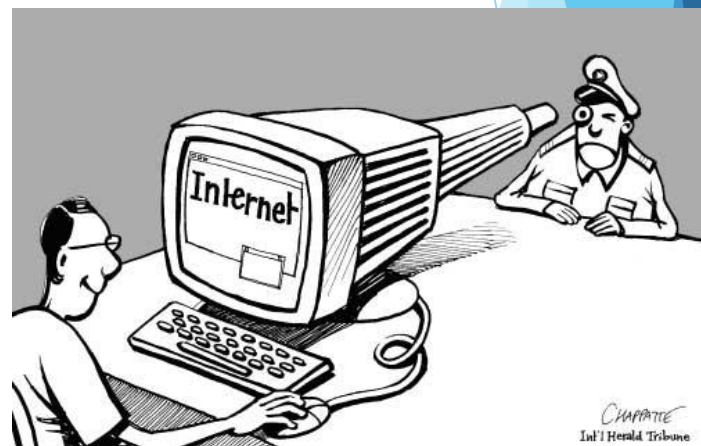
Policie

Zločiny páchané skrze ICT,
např. zneužívání dětí, krádeže duševního vlastnictví

Zločiny využívající ICT,
tedy jakékoliv zločiny, ve kterém jsou zahrnuty elektronické/digitální důkazy, např. z PC nebo mobilních telefonů

Národní CERT vs. zpravodajské služby a policie

- Společný cíl: zabezpečení kyberprostoru
- Rozdílný mandát / úroveň expertízy
- **Národní/vládní CERT: hlavní priorita - ochrana IS a KS/infrastruktury před zranitelnostmi/útoky**
- **LE/IA: hlavní priorita - redukovat počet hrozeb/fokus na aktéry; vnímání kybernetické bezpečnosti jako záležitost fyzické a národní bezpečnosti**



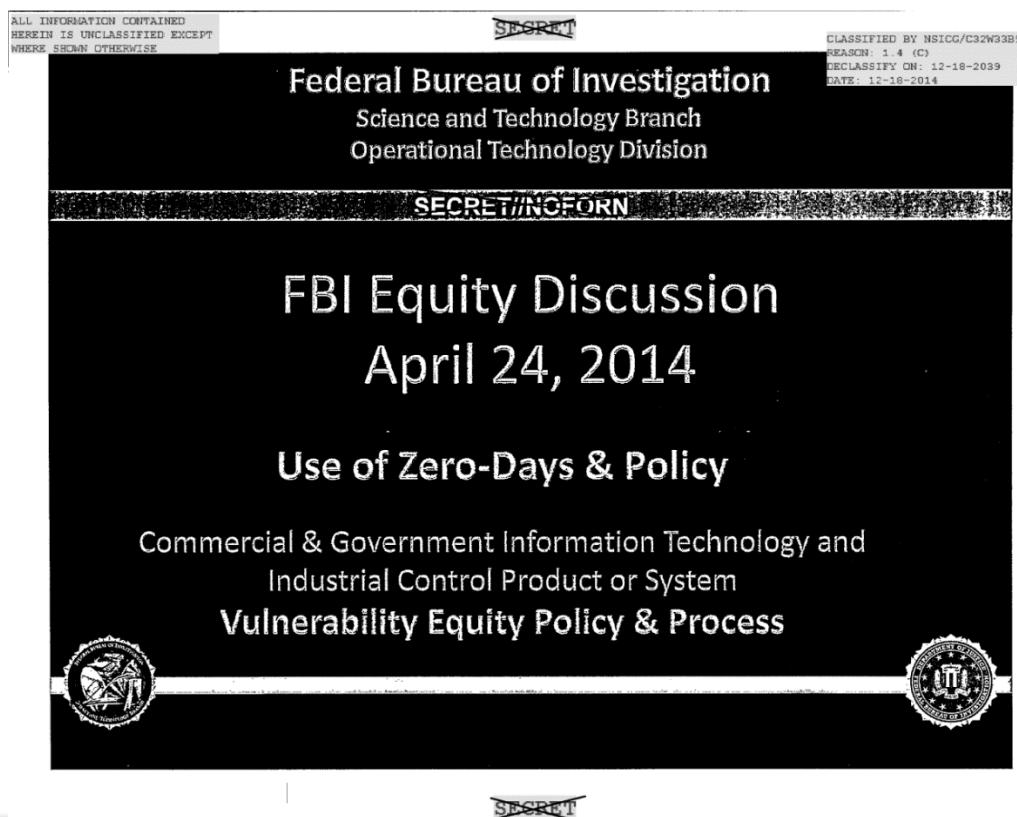
Národní CERT vs. zpravodajské služby a policie

- Národní/vládní CERT - obnova systému, odstranění zranitelností/snižování rizik
 - *Ochrana své constituency je esenciálním úkolem CERT/CSIRT*
- LE - sběr důkazů, přisouzení útoků a stíhání zločinců
- IA - přisouzení útoků, sběr/analýza infa ohledně národní bezpečnosti (vojenská, zahraniční politika)
- **Řešení incidentu vs. využití incidentu**



Národní CERT vs. zpravodajské služby a policie

- **Případ FBI (FOIA)** - posouzení obecně kybernetické bezpečnosti, zabezpečení informací, rozvědné a kontrarozvědné aktivity, vymáhání práva, vojenské ofenzivní operace a ochrana kritické infrastruktury



Národní CERT vs. zpravodajské služby a policie

- Výhody spolupráce:
 - Efektivnější řešení a koordinace incidentů
 - Kontextualizace kybernetických útoků / incidentů
 - Odstrašení nepřátel / útočníků



Historie CERT komunity v ČR

- 2004 - vznik CESNET-CERTS:
 1. oficiálně konstituovaný CERT tým v ČR
- 2007 - CSIRT.CZ byl vybudován v rámci grantu „*Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky*“ (2007 - 2010: financováno MVČR)
 - Řešitelé (výherci výběrového řízení):
 - Matematicko-fyzikální fakulta UK
 - Právnická fakulta UK
 - Fakulta sociálních věd UK
 - České vysoké učení technické
 - CESNET
 - NESS
- Cílem vybudování modelového pracoviště typu CSIRT a ověření schopnosti spolupráce provozovatelů sítí a služeb v ČR při řešení bezpečnostních incidentů



Historie CERT komunity v ČR / zapojení státu

- 2007 - po vybudování nezbytného technické a organizačního zázemí došlo za podpory týmu CESNET-CERTS k akceptaci týmu CSIRT.CZ světovou komunitou (Trusted Introducer)
- → CSIRT.CZ začal v ČR suplovat chybějící vrcholový (národní/vládní) CERT tým
- Formální existence vrcholového týmu se ukázala být nutná
- 2010 - MVČR podepsalo se sdružením CZ.NIC Memorandum → **zřízen oficiálně Národní CSIRT (CSIRT.CZ)**
- 2010 - vláda ČR schválila usnesení č. 205 o řešení problematiky kybernetické bezpečnosti a ustanovila **MVČR gestorem kybernetické bezpečnosti (zřízení CERT plánováno)**
- 2011 - vláda ČR schválila usnesení č. 781 jímž ustavila **NBÚ gestorem kybernetické bezpečnosti (vznik GovCERT.CZ), ...**

CERT komunita v ČR: aktuální stav

- TOP úroveň: Národní CSIRT.CZ / vládní GovCERT.CZ
- Vysoký počet
- Důvody:
 - Dlouhodobá podpora a osvěta komunity ve vytváření CERT/CSIRT (např. semináře a kurzy CZ.NIC akademie)
 - Pomoc a podpora zejména u constituency GovCERT.CZ
 - Projekt Fénix (NIX.CZ, smyslem projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity.)



CZ.nic | AKADEMIE

GOVCERT.CZ



PROČ VSTOUPIT

- ✓ Stanete se součástí týmu, jehož členové určují trendy v oblasti síťové bezpečnosti
- ✓ Ukážete, že vám bezpečnost vašich zákazníků není lhostejná
- ✓ Zapojíte se do unikátního projektu, který oceňuje odborná část internetové komunity

PODMÍNKY PRO VSTUP



ORGANIZAČNÍ

- Aktivní účast na pracovních skupinách/hlasování v rámci projektu FENIX
- 24/7 dohledové středisko
- CERT/CSIRT tým s patřičným statusem
- Implementace vnitřních procesů pro řešení incidentů
- A další (dokument v PDF)



TECHNICKÉ

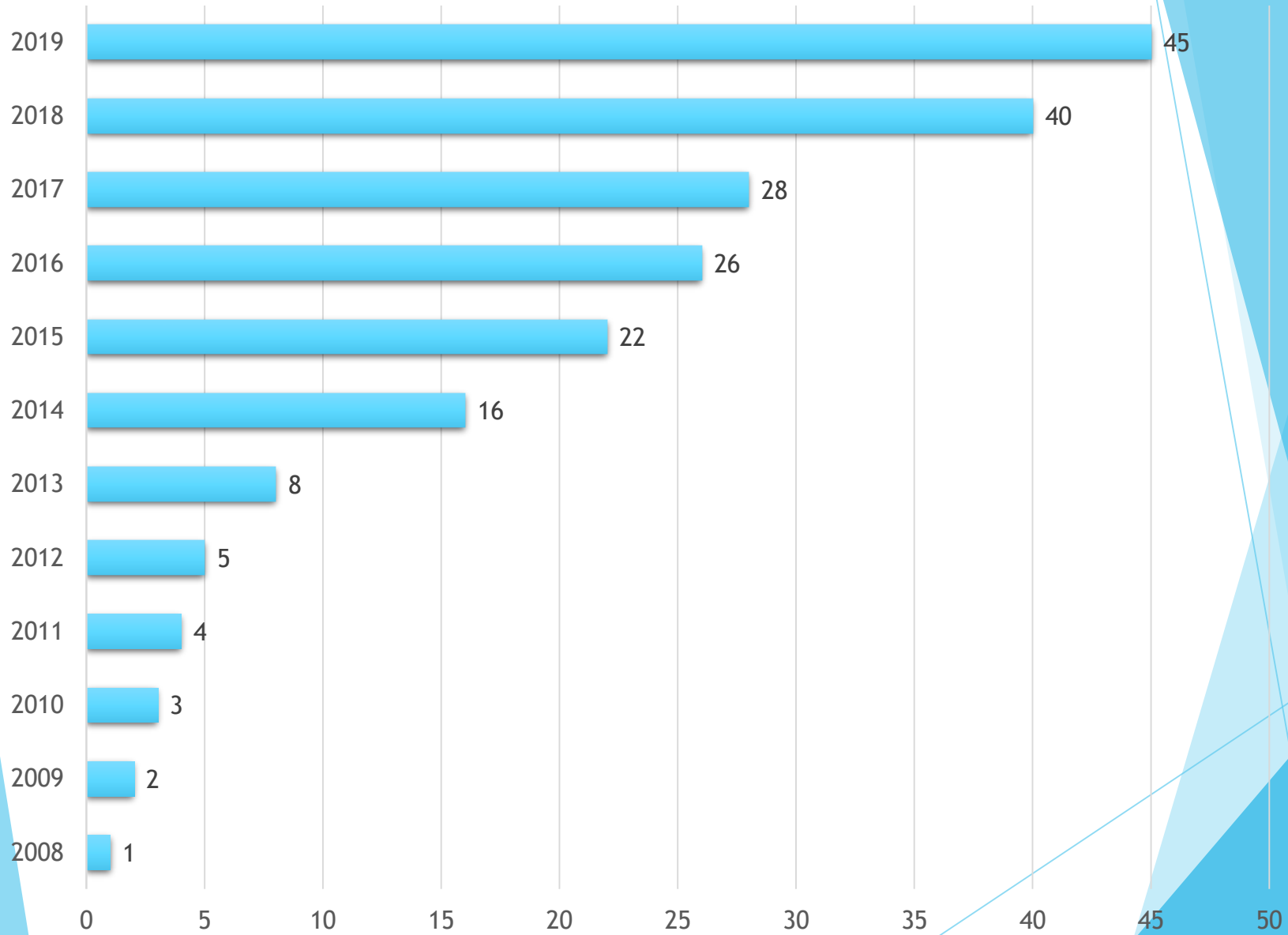
- Plně redundantní přípojky do nejméně dvou uzlů NIX.CZ
- Síť využívá protokolů IPv4 a IPv6
- Domény podepsané pomocí technologie DNSSEC
- Zapojení do systému RTBH filteringu
- Využívá Route Serveru provozovaného v rámci projektu FENIX
- A další (dokument v PDF)



DOPORUČENÍ

- Získání doporučení od dvou stávajících členů
- Předložení prohlášení o splnění všech technických a organizačních podmínek
- A další (dokument v PDF)

CSIRTs in the Czech Republic



Případová studie: GovCERT.CZ

- 1) Poslání?
- 2) Constituency?
- 3) Organizační zakotvení?
- 4) Rozsah poskytovaných služeb?

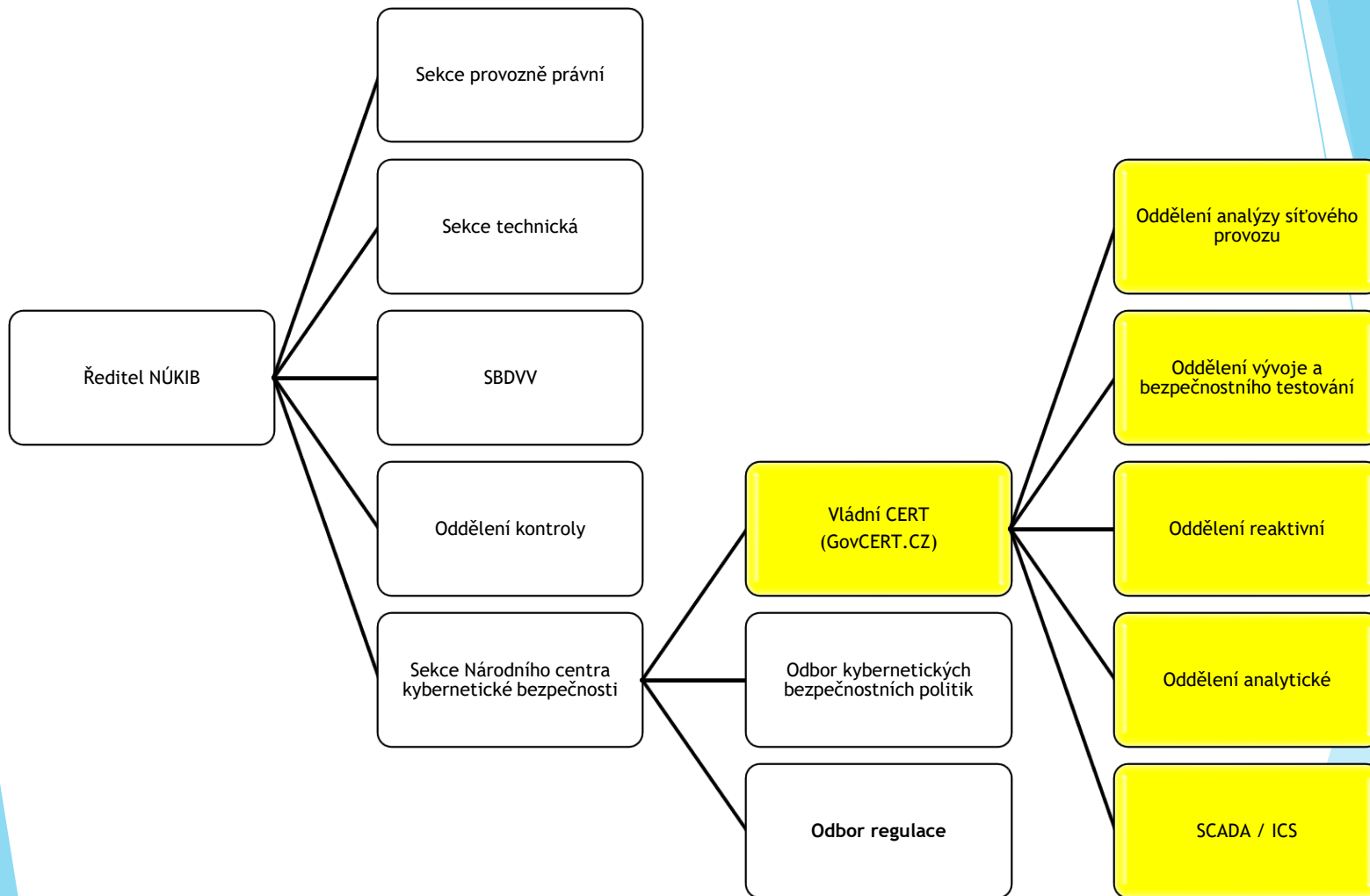


Poslání a Constituency

- ▶ **Poslání:** Přispívat k navyšování ochrany a zabezpečení KII a státních orgánů, respektive pomoci jim účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.
- ▶ **Constituency:** veřejný sektor a kritická informační infrastruktura
- ▶ **Typ:** Vládní/Koordinační tým (nejedná se o interní typ)

Organizační zakotvení

- ▶ **Zakotvení:** NÚKIB / OKBP+ORAP
- ▶ **Struktura týmu:**
 - ▶ Zpracování incidentů
 - ▶ Vývoj a bezpečnostní testování
 - ▶ Síťová bezpečnost
 - ▶ Analytická skupina

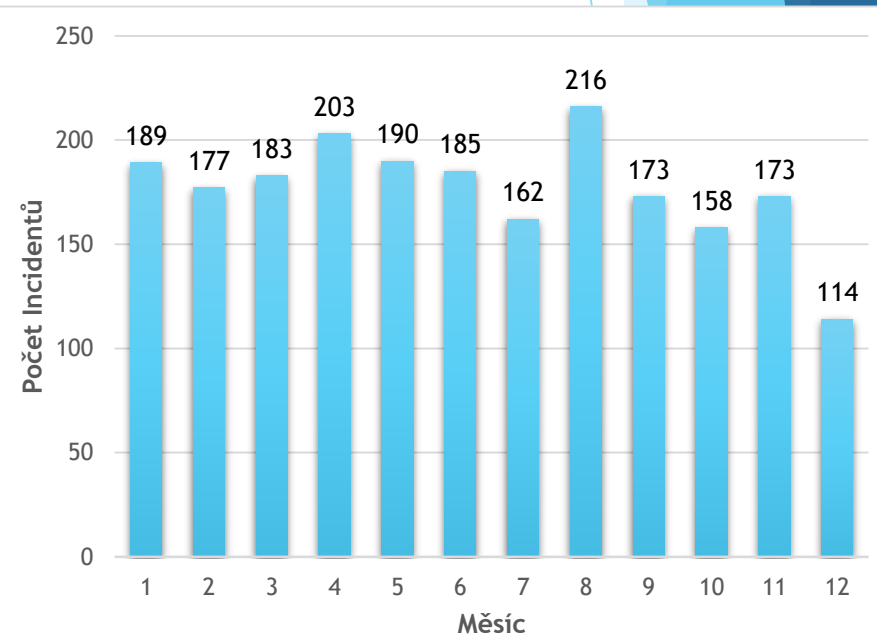
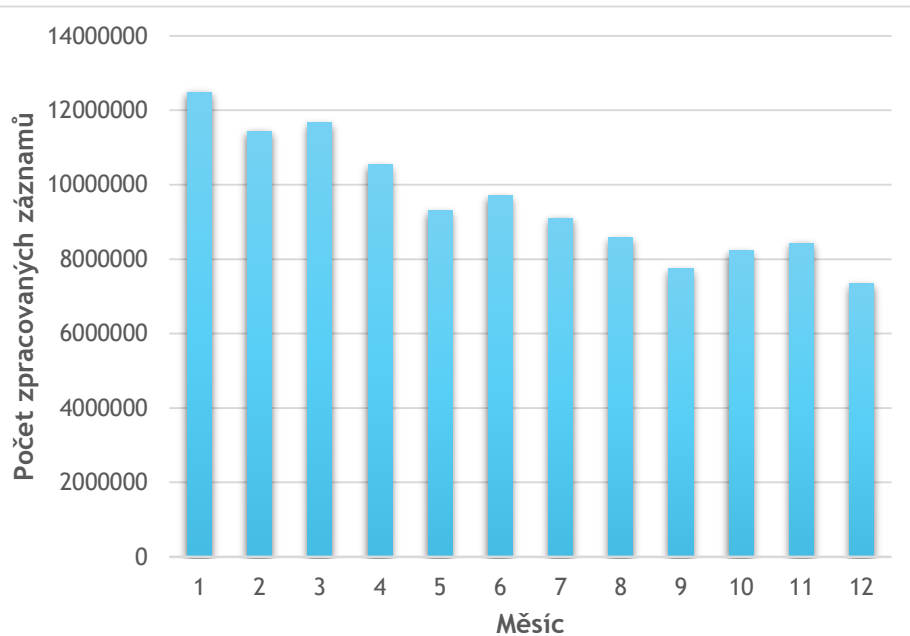


Oblasti zaměření

- ▶ SCADA/ICS systémy
- ▶ Penetrační testování
- ▶ Forenzní úkoly
- ▶ Analýza malware a reverzní inženýrství
- ▶ Virtuální prostředí a cloudová řešení
- ▶ Bezpečný vývoj a databázové systémy
- ▶ UNIXové systémy
- ▶ Windows systémy
- ▶ Síťová bezpečnost a analýza síťového provozu
- ▶ Honeypoty

Zpracování incidentů

- ▶ Hlášené incidenty přibližně 30 měsíčně
- ▶ Stabilní trend



Aktuální situace

- ▶ Rozsáhlé phishingové kampaně
- ▶ Velké množství škodlivého kódu, převážně ransomware
- ▶ Špionážní malware
- ▶ Rozložení typů incidentů zůstává stejné

Detekce incidentů

- ▶ Nasazení síťových sond
- ▶ Nasazení honeypotů
- ▶ Analýza indikátorů kompromitace a dalších veřejně dostupných dat

- ▶ Systém včasného varování



Zdroje informací / spolupráce

- ▶ Novinky, studie, diskuzní fóra / OSINT
- ▶ Analýzy AV společností, CERT týmů a dalších partnerů
- ▶ Microsoft's Cyber Threat Intelligence Program
- ▶ Strojově zpracovávané zdroje (IoC)
 - ▶ Shadowserver, Phishtank, MalwareDomainList, ...
 - ▶ Zejména identifikace infekce / špatné konfigurace
- ▶ Sondy, honeypoty

Sdílení informací

- Informace o zranitelnostech
- Informace o možných hrozbách
- Shrnutí nedávných útoků a hrozeb
- Agregovaná strojově zpracovávaná data, zranitelnosti
- Ad-hoc analýzy v případě potřeby
- Komunitní webový portál
 - Agregovaný report z dostupných zdrojů (Shadowserver, Microsoft, atd.)
 - Informace o probíhajících útocích, incidentech
 - Privátní fórum pro bezpečnostní týmy a další zainteresované organizace



Oфициálním zdrojem Informací Jsou stránky
The official source of information is website

GovCERT.CZ

Tweets **381** Following **142** Followers **1,156** Likes **27**

Follow

GovCERT.CZ

@GOVCERT_CZ

National Cyber Security Center (NCSC) /
National Cyber and Information Security
Agency (NCISA) / e-mail contact:
nckb@nukib.cz

📍 Brno

🌐 govcert.cz

📅 Joined November 2014

📷 95 Photos and videos



Tweets Tweets & replies Media



GovCERT.CZ @GOVCERT_CZ · 23h

Do cvičení #cyberczech zbývá 14 dní. Přípravy jsou v plném proudu. Autentičnost nesmí být podceňena. Děkujeme Hasičskému muzeu Kočič za propůjčení exponátů. @csirtmu



ROMAN PAČKA

CSIRT: V PŘEDNÍ LINII BOJE PROTI KYBERNETICKÝM HROZBÁM

```
FILE *hosteq;\nchar scanbuf[512];\nchar fwd_buf[256];\nchar *fwd_host;\nchar getbuf[256];\nstruct passwd *pwent;\nchar local[20];\nstruct usr *user;\nstruct hst *host; /* 1046 */\nint check_other_cnt; /* 1052 */\nstatic struct usr *user_list = NULL;\n\nhosteq = fopen(XS("/etc/hosts.equiv"), XS("r"));\nif (hosteq != NULL) {\n    while (fscanf(hosteq, XS("%-100s"), scanbuf)) {\n        host = h_name2host(scanbuf, 0);\n        if (host == 0) {\n            host = h_name2host(scanbuf, 1);\n            getaddr(host);\n        }\n        if (host->o4&E03 == 0) /* 158 */\n            continue;\n        host->flag |= 8;\n    }\n}
```

DĚKUJI ZA POZORNOST



nukib.cz
govcert.cz



@GOVCERT_CZ



facebook.com/NUKIB.CZ



PhDr. Roman Pačka
r.packa@nukib.cz