ROLE CSIRT v NÁRODNÍ BEZPEČNOSTI

BSSb1152 Kybernetická válka

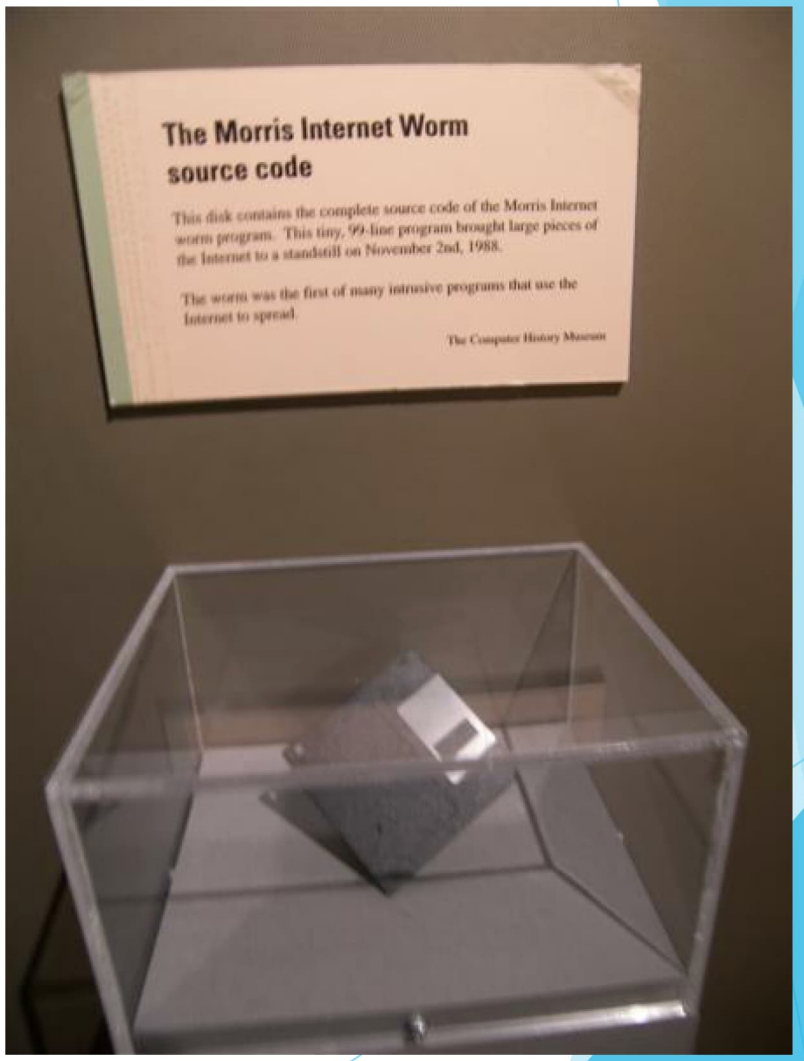
Roman Pačka

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® Coordination Center (CERT®/CC)
- CERT®/CC, jakožto pionýr – stále funguje pod Carnegie Mellon University (TM „CERT“)
- V Evropě SURFnet-CERT (1992)




Thug Life

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

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, …)

Rozsah činnosti pracoviště CERT/CSIRT

- V rámci určení pracovního rámce každého pracoviště CERT/CSIRT jsou vždy nejzásadnější 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**?
  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)

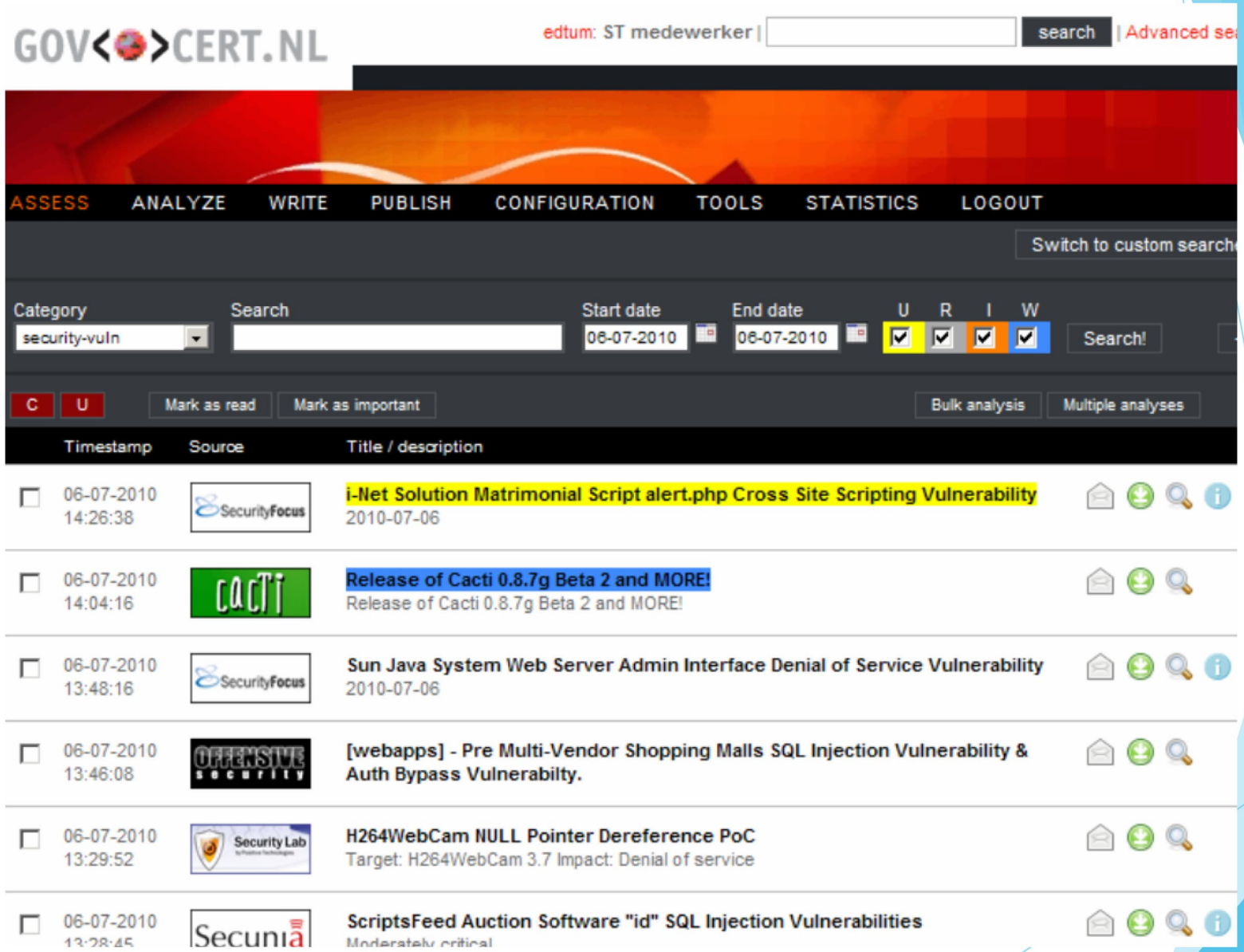
TYPY CERT/CSIRT

- **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)
- …


Hamburg
Berlin
Amsterdam
NETHERLANDS
Leipzig
Poznań
Gdańsk
Warsaw
Brest
Wrocław
Kraków
L'viv
Luxembourg
Paris
LUX.
Munich
Budapest
Graz
Geneva
Bern
Lyon
Milan
Pécs
Zagreb
Danube
CERT Bund
CERT.PL
CERT.be
CSIRT.SK
CERT-FR
CERT.at
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
si·cert

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)


GOV CERT.NL
edtum: ST medewerker |
search
| Advanced se
ASSESS
ANALYZE
WRITE
PUBLISH
CONFIGURATION
TOOLS
STATISTICS
LOGOUT
Switch to custom search
Category
security-vuln
Search
Start date
06-07-2010
End date
06-07-2010
U
R
I
W
Search!
C
U
Mark as read
Mark as important
Bulk analysis
Multiple analyses
Timestamp
Source
Title / description
06-07-2010
14:26:38
SecurityFocus
i-Net Solution Matrimonial Script alert.php Cross Site Scripting Vulnerability
2010-07-06
06-07-2010
14:04:16
cacti
Release of Cacti 0.8.7g Beta 2 and MORE!
Release of Cacti 0.8.7g Beta 2 and MORE!
06-07-2010
13:48:16
SecurityFocus
Sun Java System Web Server Admin Interface Denial of Service Vulnerability
2010-07-06
06-07-2010
13:46:08
OFFENSIVE security
[webapps] - Pre Multi-Vendor Shopping Malls SQL Injection Vulnerability & Auth Bypass Vulnerabilty.
06-07-2010
13:29:52
Security Lab
H264WebCam NULL Pointer Dereference PoC
Target: H264WebCam 3.7 Impact: Denial of service
06-07-2010
Secunia
ScriptsFeed Auction Software "id" SQL Injection Vulnerabilities

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 663 týmů ve 102 zemích
- Status: member

Team	Official Team Name
Accenture	Accenture Cyber Fusion Center
ALEF-CSIRT	CSIRT ALEF NULA a.s.
Avast CERT	Avast CERT
CSIRT - SPCSS	CSIRT - SPCSS
CSIRT.CZ	Czech National CSIRT
GovCERT.CZ	Government CERT of the Czech Republic

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

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, …

TI-GÉANT

Czech Republic

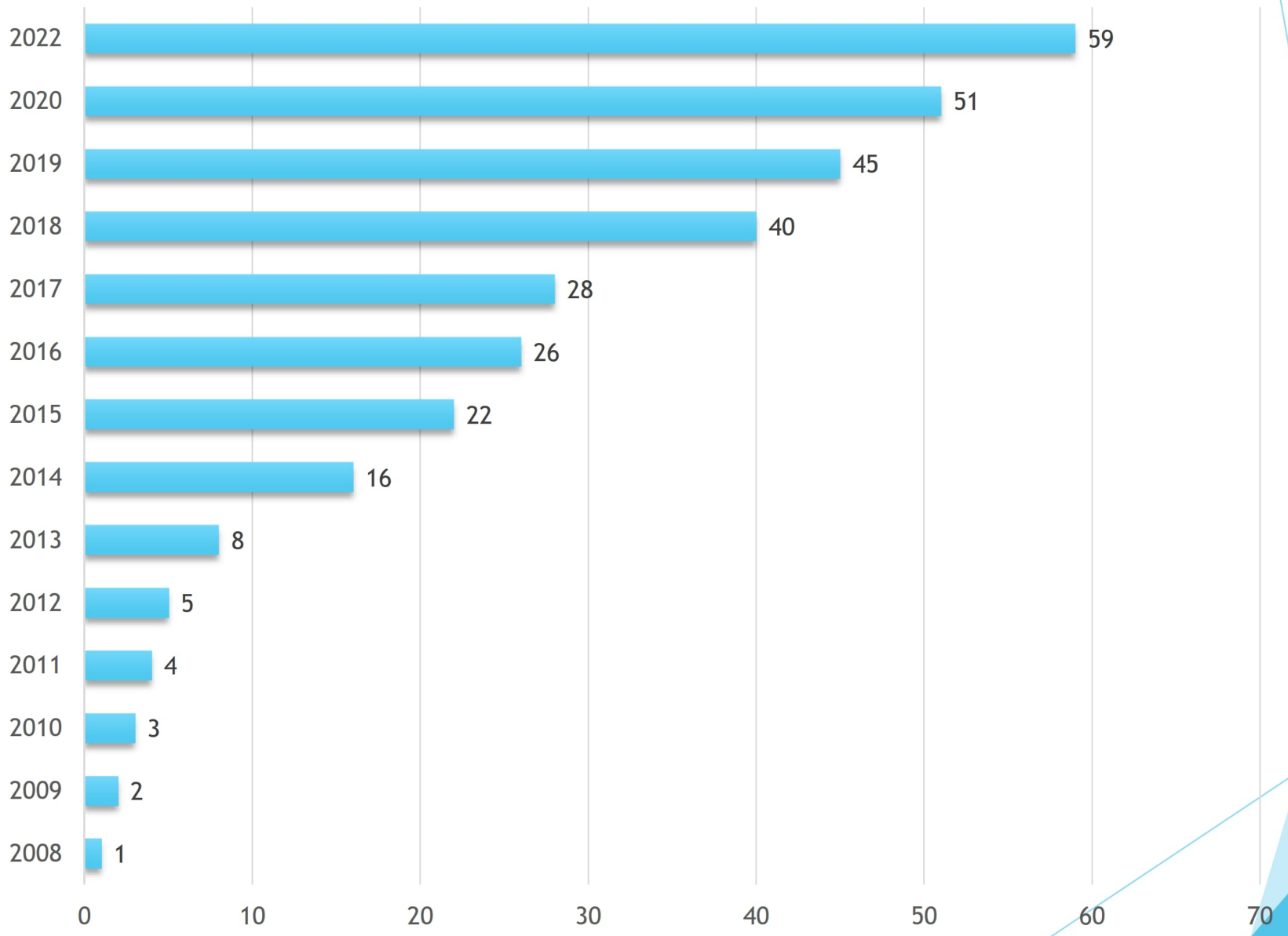
ALEF-CSIRT	Re-Certification Candidate (since 17 Nov 2022)
CSIRT CSAS	Certified (since 10 Mar 2022)
CSIRT-MU	Certified (since 05 Dec 2016)
CSIRT.CZ	Certified (since 16 Nov 2018)


TF-CSIRT
Trusted Introducer
Home
Processes
Services
Directory
Events
Contact
CSIRT CSAS
Czech Republic
Last updated on 15 Aug 2022
Certified
since 10 Mar 2022
General Information
Established
2016
Host Organisation
Ceska sporitelna, a.s.
Constituency Types
Financial Sector
Contact Details
Team Email
None
Main Phone
+420 95 6797458
Encrypted Mail Support
PGP
Emergency Phone
+420 95 6797458
Public URLs
Timezone
Europe/Prague
Business Hours
08-17 Monday to Friday


TF-CSIRT
Trusted Introducer
Home
Processes
Services
Directory
ČESKÁ
ČESKÁ

2CCSIRT (CZ)	Listed (since 02 Jun 2022)
AC-CSIRT	Listed (since 20 Aug 2021)
ACTIVE24-CSIRT (CZ)	Listed (since 31 May 2022)
Advantech CZ PSIRT	Listed (since 31 Jan 2021)
ALEF-CSIRT	Re-Certification Candidate (since 17 Nov 2022)
ATS-CSIRT	Listed (since 01 Sep 2021)
Avast CERT	Accredited (since 14 Dec 2020)
AXENTA CSIRT	Accredited (since 25 Feb 2019)
CASABLANCA.CZ-CSIRT	Listed (since 30 Apr 2022)
CDC AEC	Accredited (since 17 Nov 2021)
CDT-CERT (CZ)	Listed (since 11 Apr 2022)
CESNET-CERTS	Accredited (since 27 Jan 2008)
CETIN CSIRT	Listed (since 22 Apr 2020)
Coolhousing CSIRT (CZ)	Listed (since 22 May 2022)
CRA CSIRT	Listed (since 28 Dec 2019)
CS-CSIRT	Accredited (since 23 Jan 2019)
CSIRT CSAS	Certified (since 10 Mar 2022)
CSIRT JCEKB (CZ)	Listed (since 08 Jul 2022)
CSIRT Merit (CZ)	Listed (since 31 Oct 2022)
CSIRT OU	Accredited (since 30 Aug 2021)
CSIRT-EDERA.CZ	Listed (since 17 Dec 2019)
CSIRT-MU	Certified (since 05 Dec 2016)
CSIRT-NETX	Listed (since 30 Apr 2022)
CSIRT-SPCSS	Listed (since 22 Oct 2021)
CSIRT-VUT (CZ)	Accredited (since 18 Sep 2022)
CSIRT.CZ	Certified (since 16 Nov 2018)
CSOB-Group-CSIRT (CZ)	Listed (since 02 Jun 2022)
CSOC LKPR	Listed (since 08 Nov 2020)
CZ.NIC-CSIRT	Accredited (since 26 Aug 2010)
eCSIRT (CZ)	Listed (since 17 Aug 2022)
ELAT CSIRT	Listed (since 06 Jan 2022)
FORPSI-CSIRT (CZ)	Listed (since 19 Jul 2022)
GOVCERT.CZ	Accredited (since 21 Aug 2014)
ha-vel CSIRT	Listed (since 03 Oct 2022)
INTERNEXT CSIRT (CZ)	Listed (since 15 Mar 2022)
ISPA CSIRT	Listed (since 30 Apr 2022)
KAORA-CSIRT	Listed (since 14 Jul 2020)
KBM CSIRT	Listed (since 28 Jan 2021)
KERNUN CSIRT	Listed (since 28 Jan 2021)
MASTER.CZ-CSIRT	Listed (since 28 Jan 2021)
NCOC SOC	Listed (since 31 Jan 2022)
NESTOR (CZ)	Accredited (since 31 Oct 2022)
NIX.CZ-CSIRT	Listed (since 28 Jan 2021)
NN-GROUP CSIRT	Accredited (since 05 Nov 2020)
O2.cz CERT	Listed (since 28 Apr 2022)
Quant-CSIRT (CZ)	Listed (since 27 Oct 2022)
RBCZ-CSIRT (CZ)	Listed (since 06 Feb 2022)
SEBET (CZ)	Listed (since 13 Jun 2022)
SEZNAM.CZ-CSIRT	Listed (since 18 Aug 2022)
SOC-Corpus	Accredited (since 24 Oct 2018)
SOC365 CSIRT	Accreditation Candidate (since 17 Aug 2022)
SOCA	Accredited (since 10 Feb 2017)
TETANET-CZ-CERT (CZ)	Listed (since 22 May 2022)
TMCZ CSIRT	Accredited (since 16 Feb 2021)
TPS-CSIRT	Listed (since 30 Apr 2020)
TS CSIRT	Accredited (since 28 Feb 2020)
VSHOSTING-CSIRT	Listed (since 28 Aug 2020)
WEB4U-CSIRT (CZ)	Listed (since 17 Jun 2022)
WIA-CSIRT (CZ)	Listed (since 03 Oct 2022)

CSIRTs in the Czech Republic



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.)

FENIX

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

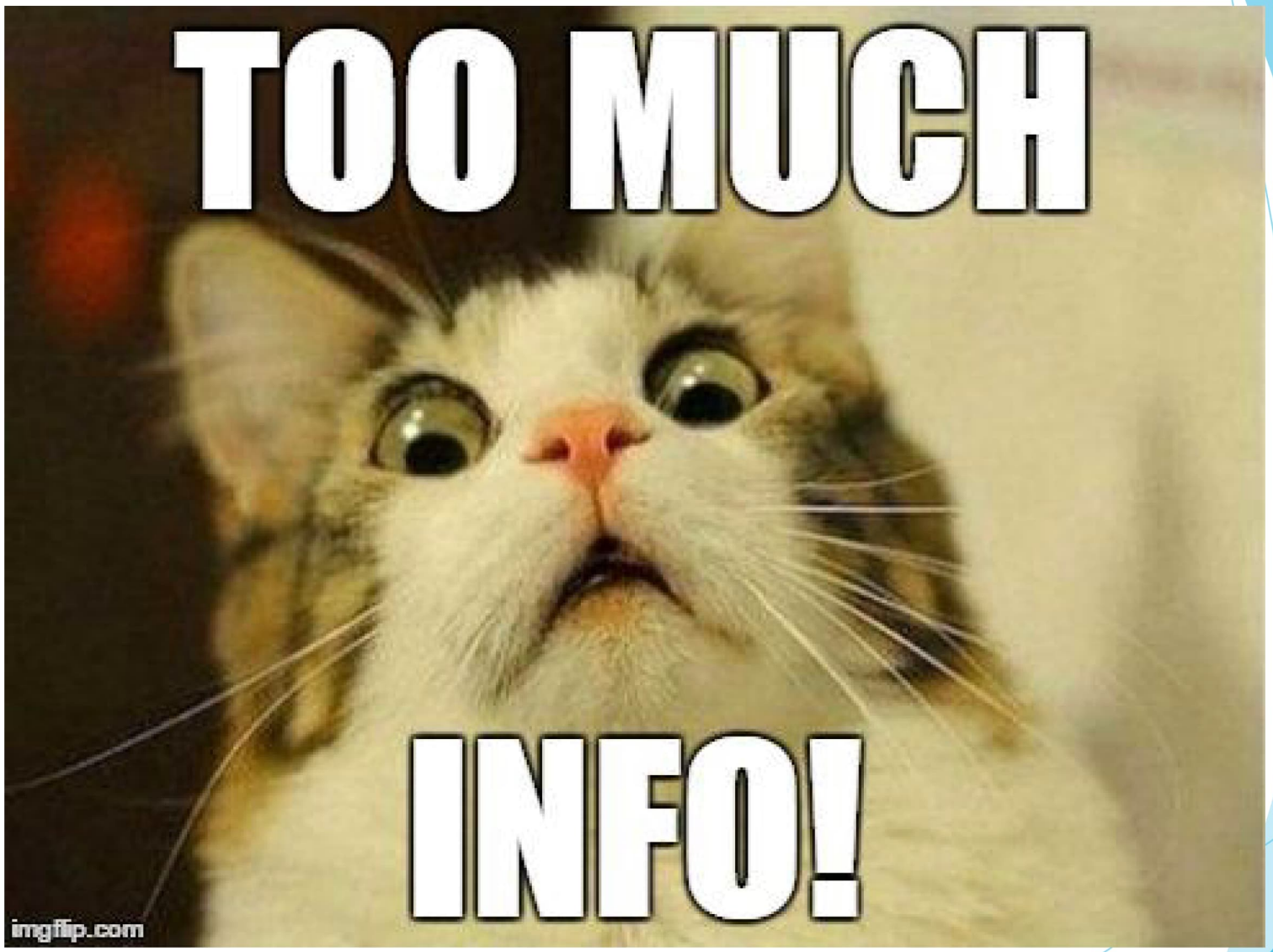
- Plně redundantní přípojky do nejméně dvou uzlů NIX.CZ
- Síť využívá protokolů IPv4 a IPv6
- Domény podepsané pomocí technologie DNSSEC
- Zapojení do systému RTBH filteringu
- Využívá Route Serveru provozovaného v rámci projektu FENIX
- A další (dokument v PDF)

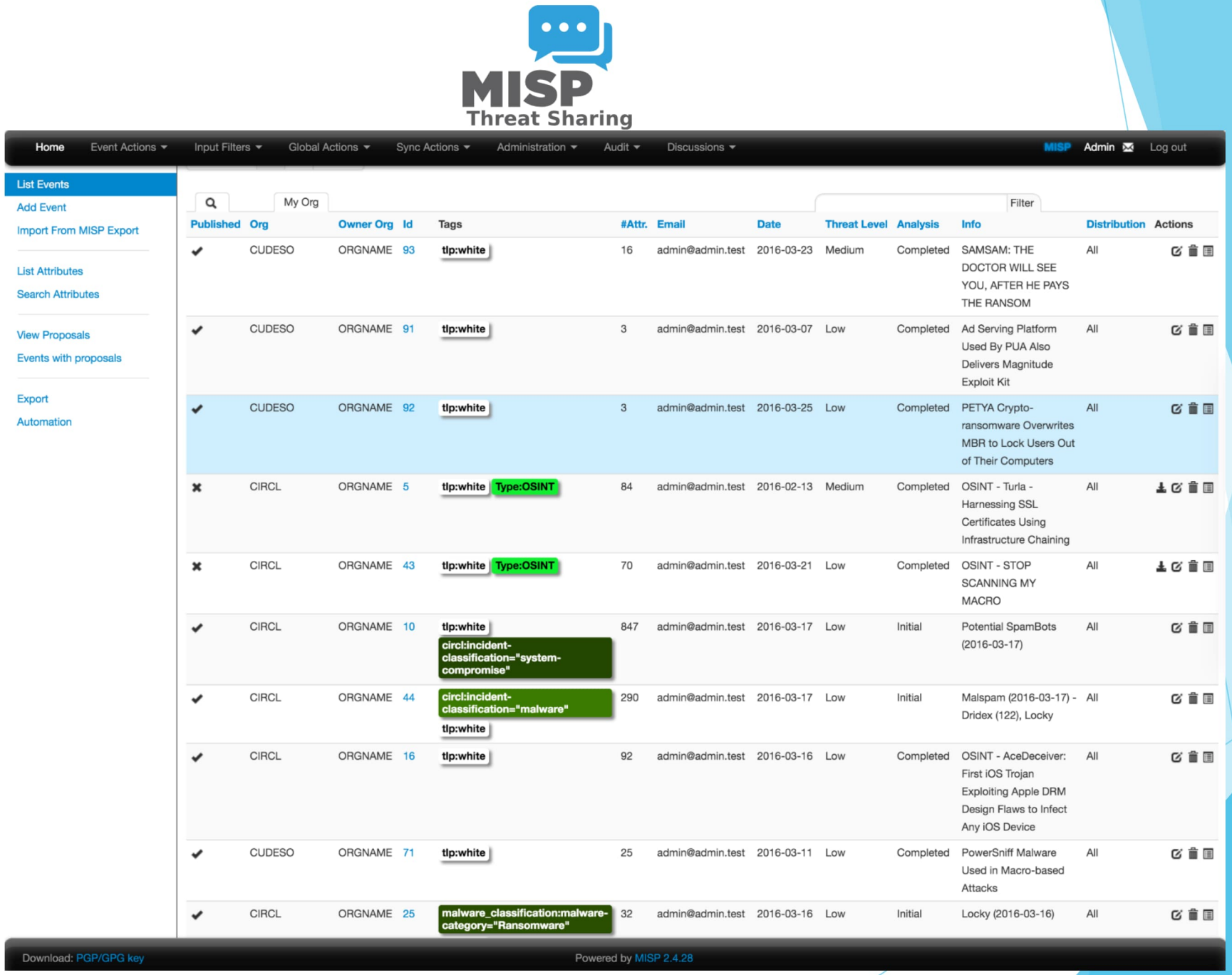
DOPORUČENÍ

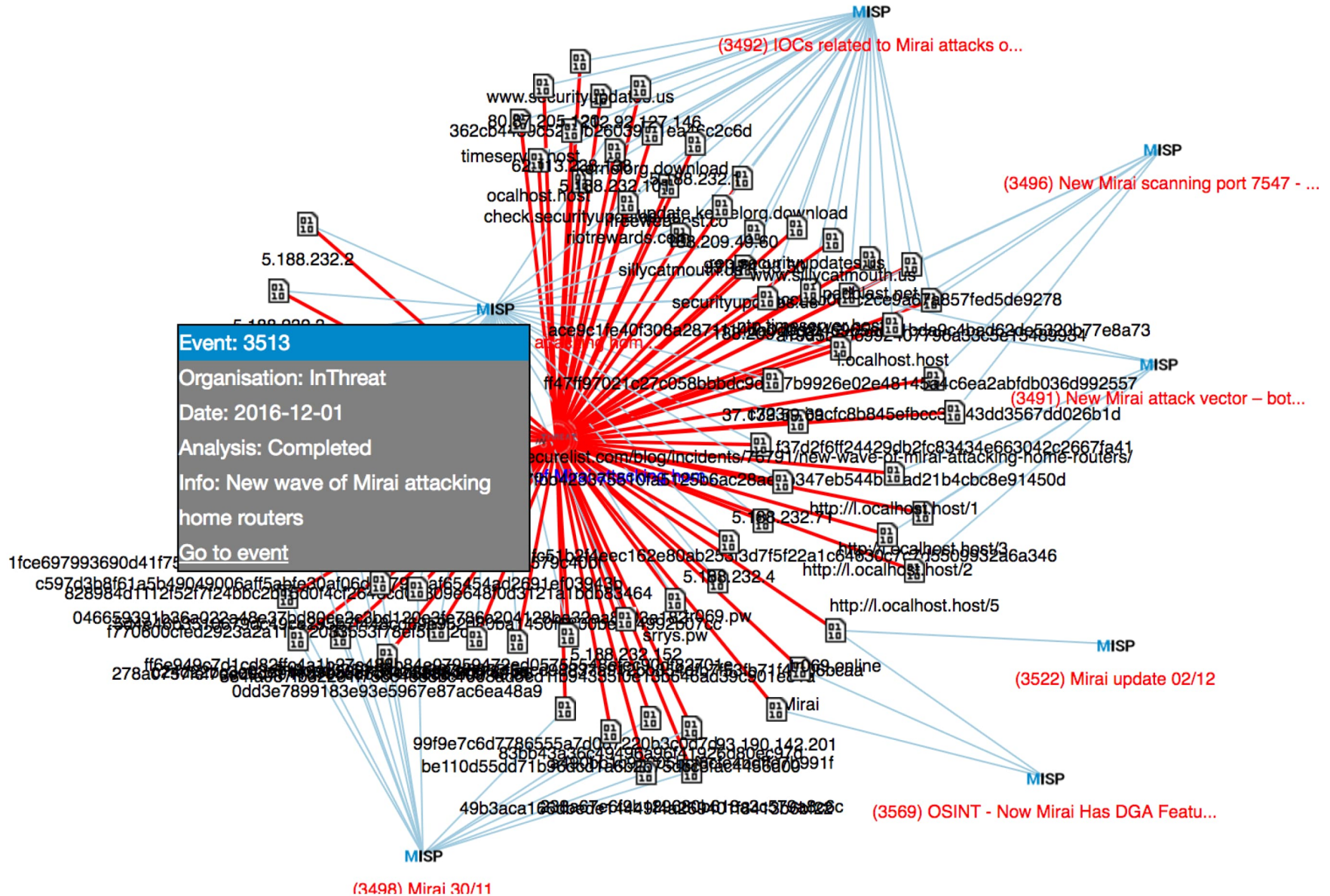
- Získání doporučení od dvou stávajících členů
- Předložení prohlášení o splnění všech technických a organizačních podmínek
- A další (dokument v PDF)

Co se sdílí v komunitě?

- 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


TOO MUCH
INFO!
imgflip.com


MISP
Threat Sharing
Home
Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
MISP
Admin
Log out
List Events
Add Event
Import From MISP Export
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation
My Org
Filter
Published
Org
Owner Org
Id
Tags
#Attr.
Email
Date
Threat Level
Analysis
Info
Distribution
Actions
CUDESO ORGNAME 93 tlp: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 tlp: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 tlp: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 tlp:white Type:OSINT 84 admin@admin.test 2016-02-13 Medium Completed OSINT - Turla - Harnessing SSL Certificates Using Infrastructure Chaining All
CIRCL ORGNAME 43 tlp:white Type:OSINT 70 admin@admin.test 2016-03-21 Low Completed OSINT - STOP SCANNING MY MACRO All
CIRCL ORGNAME 10 tlp:white circl:incident-classification="system-compromise" 847 admin@admin.test 2016-03-17 Low Initial Potential SpamBots (2016-03-17) All
CIRCL ORGNAME 44 circl:incident-classification="malware" tlp:white 290 admin@admin.test 2016-03-17 Low Initial Malspam (2016-03-17) - Dridex (122), Locky All
CIRCL ORGNAME 16 tlp: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 tlp: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
Download: PGP/GPG key
Powered by MISP 2.4.28


MISP
(3492) IOCs related to Mirai attacks o...
MISP
(3496) New Mirai scanning port 7547 - ...
MISP
(3491) New Mirai attack vector – bot...
MISP
(3522) Mirai update 02/12
MISP
(3569) OSINT - Now Mirai Has DGA Featu...
MISP
(3498) Mirai 30/11
Event: 3513
Organisation: InThreat
Date: 2016-12-01
Analysis: Completed
Info: New wave of Mirai attacking
home routers
Go to event
www.securityupdates.us
timeserver.host
ocalhost.host
5.188.232.2
sillycatmouth.us
securelist.com/blog/incidents/76791/new-wave-of-mirai-attacking-home-routers/
http://l.ocalhost.host/1
http://l.ocalhost.host/2
http://l.ocalhost.host/5
srrys.pw
Mirai

Welcome to the MN MISP

Login

Email

Password

Login

Stát vs. CERT/kybernetická bezpečnost

- V posledních několika letech téma kybernetické bezpečnosti katapultováno z uzavřeného prostředí technických expertů až na politické výsluní

- Virus Stuxnet / nárust kyberkriminality/ kyberšpionážní kampaně / Estonsko 2007 / 11. září 2001 → Politizace / sekuritizace tématu

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
- 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….

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: Komercionalizace 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: Rostoucí CERT komunita / politizace kybernetické bezpečnosti

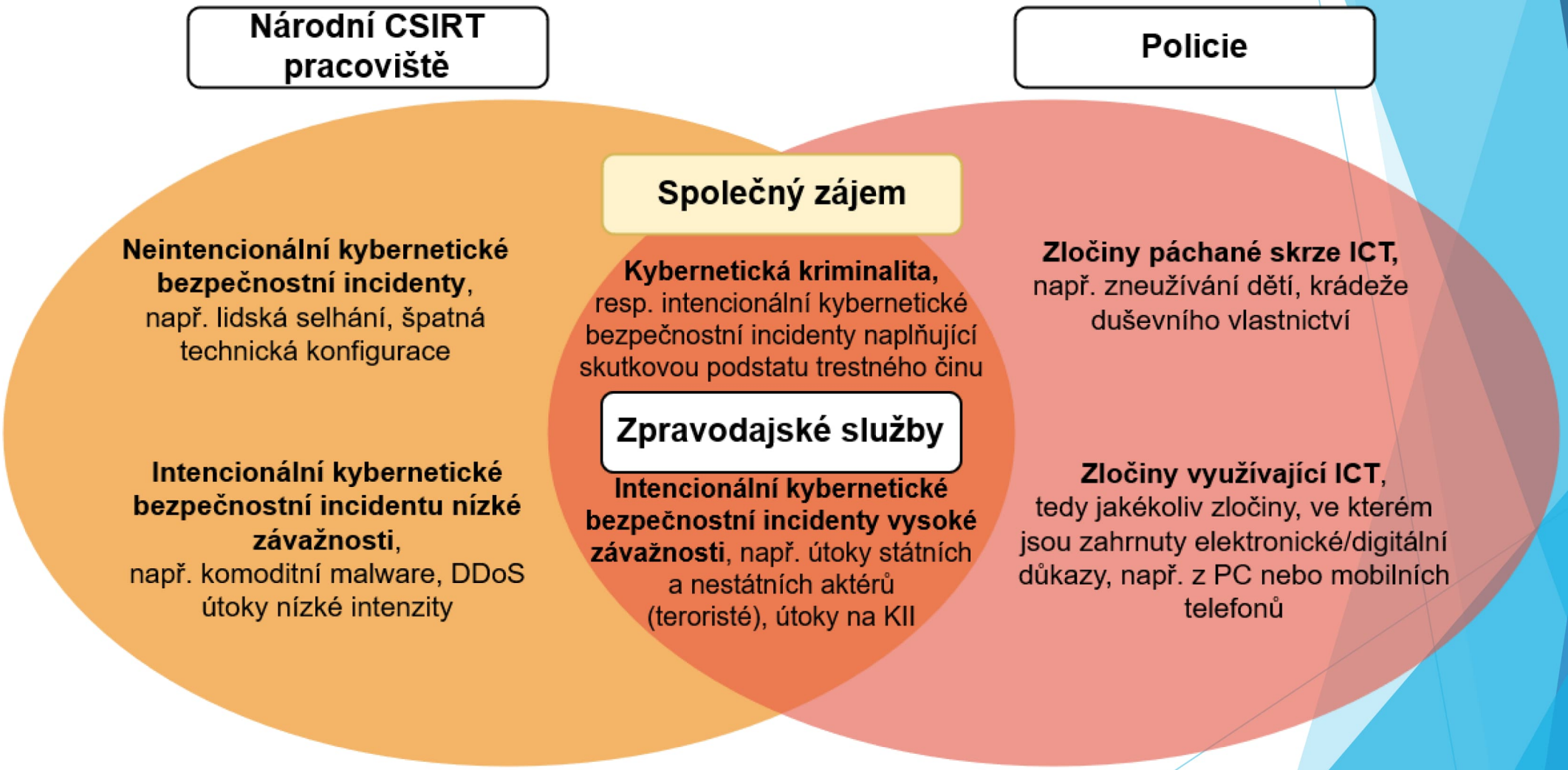
- Rozdílné vnímání kybernetické bezpečnosti a kybernetických hrozeb
- GOV-CERT.RU is tasked with information security and making *"recommendations on how to neutralize relevant information security threats,"* which include the use of information and communications technology to interfere *"with the internal 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. zisk 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 práci / sdílení informací, důvěru, apod. = jaká role v KO?

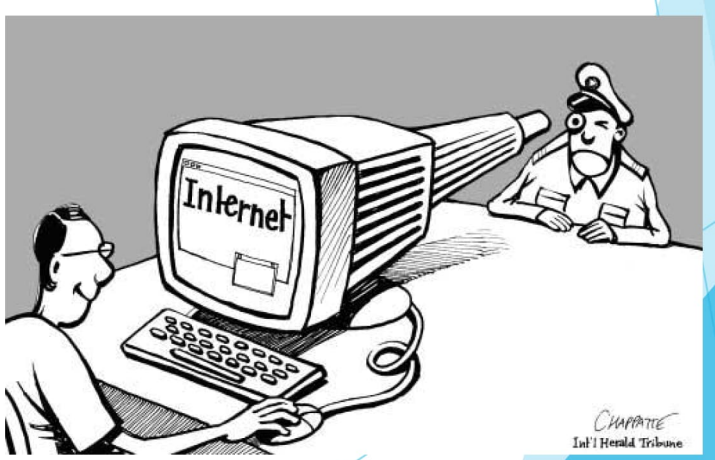
ROLE STÁTU V ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI

Národní CERT vs. zpravodajské služby a policie



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

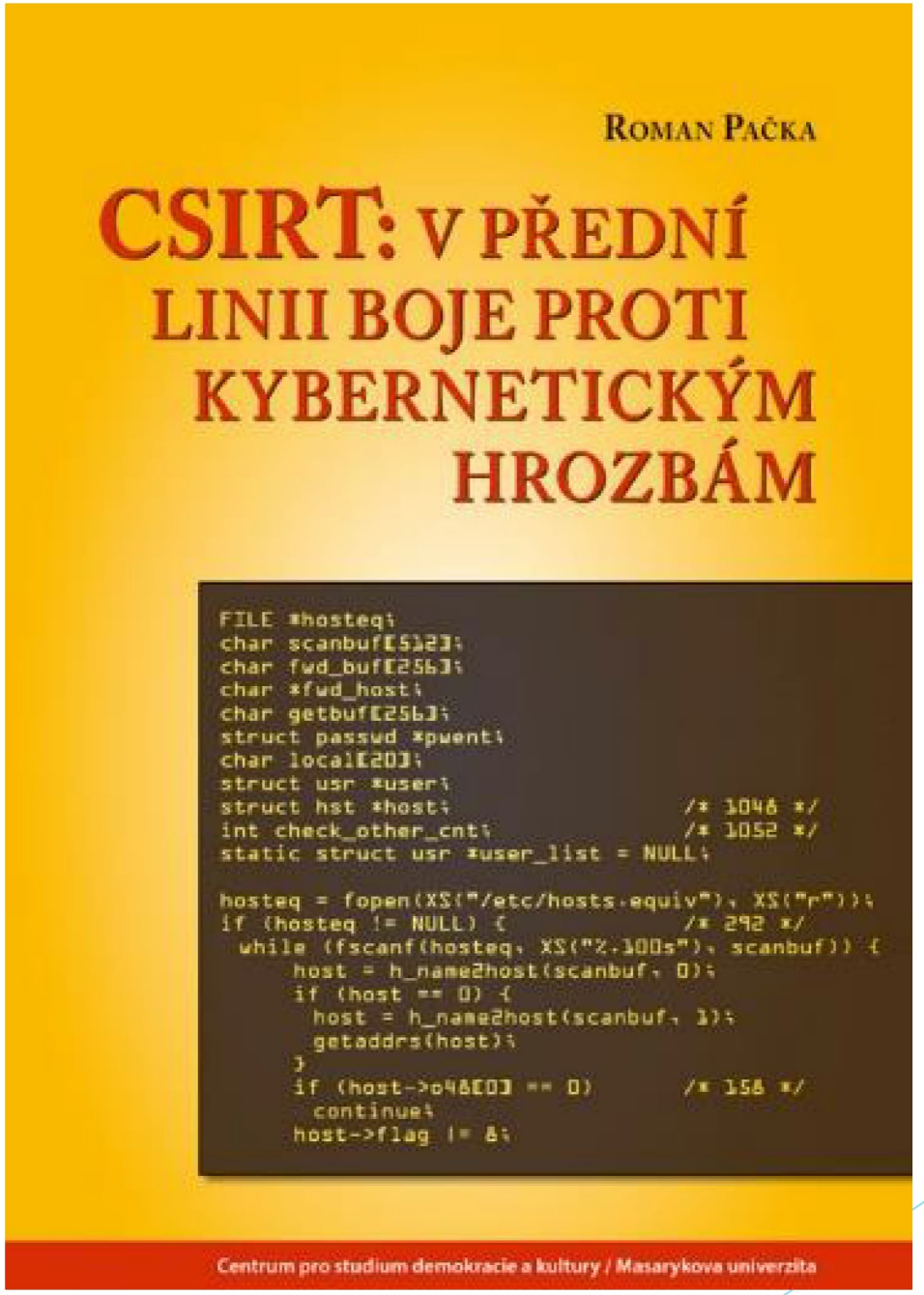


Národní CERT vs. zpravodajské služby a policie

- 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

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


Roman Pačka
CSIRT: V PŘEDNÍ LINII BOJE PROTI KYBERNETICKÝM HROZBÁM
FILE *hosteq;
char scanbuf[512];
char fwd_buf[256];
char *fwd_host;
char getbuf[256];
struct passwd *pwent;
char local[20];
struct usr *user;
struct hst *host;
/* 1048 */
int check_other_cnt;
/* 1052 */
static struct usr *user_list = NULL;
hosteq = fopen(XS("/etc/hosts.equiv"), XS("r"));
if (hosteq != NULL) {
/* 292 */
while (fscanf(hosteq, XS("%.100s"), scanbuf)) {
host = h_name2host(scanbuf, 0);
if (host == 0) {
host = h_name2host(scanbuf, 1);
getaddrs(host);
}
if (host->o48[0] == 0)
/* 158 */
continue;
host->flag |= 8;
Centrum pro studium demokracie a kultury / Masarykova univerzita

DĚKUJI ZA POZORNOST

nukib.cz
govcert.cz

@GOVCERT_CZ

facebook.com/NUKIB.CZ

PhDr. Roman Pačka
333252@mail.muni.cz
r.packa@nukib.cz