



BEZPEČNOST

Andrea Kropáčová

CESNET

4. 9. 2024

VUT, Brno

1. Udržet e-infrastrukturu CESNET a služby v běhu, zabezpečenou a obrany schopnou
2. Poskytnout připojeným organizacím portfolio bezpečnostních služeb
3. Sdílet informace a know-how napříč komunitou, spolupracovat
4. Uživatel a péče o něj – edukace, cvičení

- Bohaté a komplexní portfolio nástrojů a služeb pro monitoring, detekci anomálií, analýzu, mitigaci ...
- Data pro online i offline analýzu
- Soubor postupů, metod, procesů ... know-how ...
- Připravené a otestované mechanismy pro zásah
- Efektivní týmy a pracoviště – PSS, NOC, CESNET-CERTS, FLAB
- Gramotní správci

- Bohaté a komplexní portfolio nástrojů a služeb pro monitoring, detekci anomálií, analýzu, mitigaci ...
- Data pro online i offline analýzu
- Soubor postupů, metod, procesů ... know-how ...
- Připravené a otestované mechanismy pro zásah
- Efektivní týmy a pracoviště – PSS, NOC, CESNET-CERTS, FLAB
- Gramotní správci
- Národní a mezinárodní spolupráce
- Člen Fenix, fe.nix.cz



- ISMS a certifikace ISO 27001 (rok 2018)
- Povinný subjekt ZoKB
- Člen Fenix, fe.nix.cz



- Computer Security Incident Response Team
- 2004: status „listed“ od úřadu Trusted Introducer, člen TF-CSIRT
- 2008: status „accredited“ od úřadu Trusted Introducer
- Jméno: CESNET-CERTS
- Provozovatel: CESNET, z. s. p. o.
- Země působnosti: Česká republika
- Kontaktní informace:
 - <https://csirt.cesnet.cz> (veřejná i privátní část)
 - abuse@cesnet.cz, certs@cesnet.cz
 - <https://www.trusted-introducer.org/directory/teams/cesnet-certs.html>
- Typ: interní a koordinační



- Constituency type: Research & Education
- Constituency:
 - AS2852 aneb e-infrastruktura CESNET (= všechny připojené organizace)
 - AS48091 (ROWANET, Kraj Vysočina)
- Členové
 - Andrea Kropáčová, Pavel Kácha, Pavel Vachek, Daniel Studený, Jiří Ráž, Daniel Kouřil, Martin Černý, Václav Bartoš, Jaroslav Svoboda, Pavel Valach, Radko Krkoš, Pavla Hlučková, Martin Krajčí, Ondřej Pavlovič, Michaela Mačalíková
- Hlavní role/služba
 - řešení a koordinace řešení bezpečnostních incidentů
 - dostupnost: 9 – 17 v pracovních dnech
- Spolupráce
 - TF-CSIRT, TI
 - Fenix, C2S2, CSIRT.CZ
 - pracovní skupiny CESNET CSIRT

SLD
SOC BASIC

Co musí umět CSIRT, aby byl CSIRTem:

SERVICE AREAS



INFORMATION SECURITY INCIDENT MANAGEMENT

- Information Security Incident Report Acceptance
- **Information Security Incident Analysis**
- **Artifact and Forensic Evidence Analysis**
- Mitigation and recovery
- **Information Security Incident Coordination**
- Crisis management Support



VULNERABILITY MANAGEMENT

- Vulnerability Discovery/Research
- Vulnerability Report intake
- Vulnerability Analysis
- **Vulnerability Coordination**
- Vulnerability Disclosure
- Vulnerability Response



SITUATIONAL AWARENESS

- Data Acquisition
- Analysis and Synthesis
- Communication



KNOWLEDGE TRANSFER

- **Awareness Building**
- Training and Education
- Exercises
- Technical and Policy Advisory



INFORMATION SECURITY EVENT MANAGEMENT

- Monitoring and Detection
- Event Analysis

Co musí umět SOC, aby byl SOCem:

SERVICE AREAS



INFORMATION SECURITY INCIDENT MANAGEMENT

- Information Security Incident Report Acceptance
- **Information Security Incident Analysis**
- Artifact and Forensic Evidence Analysis
- Mitigation and recovery
- Information Security Incident Coordination
- Crisis management Support



VULNERABILITY MANAGEMENT

- Vulnerability Discovery/Research
- Vulnerability Report intake
- **Vulnerability Analysis**
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response



SITUATIONAL AWARENESS

- Data Acquisition
- Analysis and Synthesis
- Communication



KNOWLEDGE TRANSFER

- **Awareness Building**
- Training and Education
- Exercises
- Technical and Policy Advisory



INFORMATION SECURITY EVENT MANAGEMENT

- **Monitoring and Detection**
- **Event Analysis**

Co musí umět CSIRT-SOC, aby byl obojí:

SERVICE AREAS



INFORMATION SECURITY INCIDENT MANAGEMENT

- Information Security Incident Report Acceptance
- **Information Security Incident Analysis**
- **Artifact and Forensic Evidence Analysis**
- Mitigation and recovery
- **Information Security Incident Coordination**
- Crisis management Support



VULNERABILITY MANAGEMENT

- Vulnerability Discovery/Research
- Vulnerability Report intake
- **Vulnerability Analysis**
- **Vulnerability Coordination**
- Vulnerability Disclosure
- Vulnerability Response



SITUATIONAL AWARENESS

- Data Acquisition
- Analysis and Synthesis
- Communication



KNOWLEDGE TRANSFER

- **Awareness Building**
- Training and Education
- Exercises
- Technical and Policy Advisory



INFORMATION SECURITY EVENT MANAGEMENT

- **Monitoring and Detection**
- **Event Analysis**

- Speciální jednotka pro CESNET-CERTS
- 2011: start
- 2014: spuštění prvních služeb

- Poskytované služby (nastavbové)
 - Analýzy závažných bezpečnostních incidentů
 - Penetrační testy
 - Zátěžové testy
 - Testy sociálního inženýrství („phishingové testy“)
 - Provoz služby Phishingator

<https://flab.cesnet.cz>



- PSS, Pracoviště stálé služby, Service Desk
 - dohledové centrum, 24/7
 - dohled nad e-infrastrukturou CESNET a službami
 - budí NOC ;-)
 - www.cesnet.cz --> kontakty
- NOC
 - správci páteřní infrastruktury
 - řeší provozní a bezpečnostní problémy e-infrastruktury CESNET
 - 24/7, v nočních hodinách „on phone“
- Správci sond umístěných na perimetru
- Správci služeb

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteři a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scanování sítě	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

- Transparentní přístup
- Žádné zásahy/omezování legitimního provozu
- V případě problému se rozhodujeme na základě vyhodnocení konkrétní situace
- V případě ohrožení stability infrastruktury zasahujeme
- V případě žádosti uživatele můžeme nastavit regulaci v páteři pro koncovou síť (nepodstatná anomálie z perspektivy páteře může být likvidační pro chod koncové sítě)

- **FTAS (Flow Traffic Analysis System)**

- detekce pro základní síťové útoky a anomálie
- základní principy
 - události mající původ uvnitř připojené sítě – notifikujeme
 - události směrem dovnitř připojené sítě – regulujeme, blokujeme
- automaticky ovládá exaFS

- **Služba exaFS**

- rozhraní pro aplikaci BGPflowspec a RTBH
- regulace provozu **z** nebo **do** prefixů připojených organizací
- webový i-face, nebo API pro strojové ovládání
- součástí je proškolení uživatele

sluzby@cesnet.cz

- **Spolupráce a připravenost**

- vím, co provozuji a chci bránit (a monitorovat)
- hovořím o tom se svým upstreamem!

- Eliminace mapování prostoru pro potenciální útok (nejen DDoS)
 - limity detektorů jsou na hraně síťové části celé e-infrastruktury jsou méně citlivé, než na hraně konkrétní připojené sítě
- V případě DDoS nastává:
 - 1. útok úspěšně detekuje a eliminuje automatická obrana (FTAS, exaFS)**
==> uživatele neinformujeme
 - 2. útok detekuje a částečně eliminuje automatická obrana**
==> uživatele informujeme, pokud analýzou zjistíme potenciální dopad na službu poskytovanou uživateli (např. saturace nebo provoz v objemech blízko saturace přípojky uživatele apod.) - primární notifikace -> CSIRT, síťáři, FTASaři
 - 3. útok je detekován (strojově, případně jinak), ale vzhledem k jeho charakteru nelze bezpečně aplikovat (riziko false-positives) účinnou automatickou eliminaci**
==> uživatele informujeme v závislosti na analýze útoku - primární notifikace -> CSIRT, síťáři, FTASaři
 - 4. útok není detekován ani přímo ani nepřímo** - tzn. nevíme o něm – v tomto případě nemůžeme ani informovat

- **Služba FTAS**
- Varianta 1:
 - **zpřístupnění dat týkající se konkrétní instituce** (z hraničních boxů), uvidíte provoz, který protekl infrastrukturou, tj. provoz mezi „námi a vámi“
- Varianta 2:
 - **export vlastních dat do hlavní instance**
 - s exkluzivním přístupem pouze k vlastním datům
- Varianta 3:
 - **dedikovaná instance v síti organizace**
 - typicky velké sítě nebo sítě se specifickými potřebami

Vulnerability management

- Informace k aktuálním hrozbám
- Ověřené, důvěryhodné a ozdrojované
- Strukturovaná data o zranitelnostech, typech útoků a rizicích
- Doporučení mitigací a řešení limitujících dopady hrozeb
- 2, max 3 reporty denně do listu csirt-forum@
- Zajišťované členy bezpečnostního týmu CESNET-CERTS
- Na denní bázi
- Základ pro vulnerability management v organizaci
- **Není ale možné brát jako 100% náhradu vlastní činnosti**

Od: CESNET-CERTS <csirt-forum@cesnet.cz>
Komu odpovědět: CESNET-CERTS <certs@cesnet.cz>
Komu: sa-report@cesnet.cz
Předmět: [csirt-forum] [TLP:CLEAR] GitLab verzemi 16.11.1, 16.10.4 a 16.9.6 opravuje 5 zranitelností
Datum: Thu, 02 May 2024 12:27:05 +0200

Dobrý den,

GitLab Community Edition (CE) a Enterprise Edition (EE) verzemi 16.11.1, 16.10.4 a 16.9.6 opravují 5 zranitelností [1].

CVE-2024-4024 (CVSS 7.3) - autentizovanému vzdálenému útočnickovi s přihlašovacími údaji k účtu Bitbucket je umožněno převzít účet GitLab propojený s účtem Bitbucket jiného uživatele, pokud je Bitbucket na GitLabu používán jako poskytovatel OAuth 2.0 [1].
CWE: 287 [2]

CVE-2024-2434 (CVSS 8.5) - autentizovanému vzdálenému útočnickovi je prostřednictvím procházení cest umožněno omezené čtení souborů a vykonání DoS útoku [1].
CWE: 22 [3]

CVE-2024-2829 (CVSS 7.5) - neautentizovanému vzdálenému útočnickovi je pomocí vytvořeného filtru zástupných znaků v nástroji FileFinder umožněno vykonat DoS útok [1].
CWE: 400 [4]

CVE-2024-1347 (CVSS 4.3) - autentizovanému vzdálenému útočnickovi je pomocí škodlivě vytvořené e-mailové adresy umožněno obejít omezení instance nebo skupiny na základě domény [1].
CWE: 287 [2]

CVE-2024-4006 (CVSS 4.3) - autentizovanému vzdálenému útočnickovi je umožněno přistoupit k datům mimo omezení přístupového tokenu [1].
CWE: 863 [5]

















Zdroje:

- [1] <https://about.gitlab.com/releases/2024/04/24/patch-release-gitlab-16-11-1-released/>
- [2] <https://cwe.mitre.org/data/definitions/287.html>
- [3] <https://cwe.mitre.org/data/definitions/22.html>
- [4] <https://cwe.mitre.org/data/definitions/400.html>
- [5] <https://cwe.mitre.org/data/definitions/863.html>

S pozdravem

--

Michaela Mačalíková
Security Operations Center
CESNET, z.s.p.o.

	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Ivanti Endpoint Manager Mobile opravuje 4 z...	1.8.2024 10:02
	Cesnet Certs <csirt-forum@cesnet.cz>	[csirt-forum] Fwd: [Ticket#2024080147012081] Zranitelnosti OpenVPN...	1.8.2024 11:18
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] XWiki opravuje 5 zranitelností	5.8.2024 15:43
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Curl a libcurl opravují středně závažnou zran...	7.8.2024 10:24
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Elastic APM Server opravuje 1 zranitelnost	7.8.2024 11:37
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] SolarWinds Access Rights Manager opravuje ...	7.8.2024 12:48
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Mattermost Server opravuje 10 zranitelností	7.8.2024 17:30
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Ivanti opravuje 2 zranitelnosti ve svých prod...	8.8.2024 09:48
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Cisco Identity Services Engine opravuje 2 zra...	8.8.2024 15:08
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Jenkins weekly a LTS opravují 2 zranitelnosti	8.8.2024 17:41
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] GitLab CE a EE opravuje 11 zranitelností	9.8.2024 15:21
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] PostgreSQL opravuje 1 zranitelnost	9.8.2024 18:14
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Zabbix opravuje 7 zranitelností	12.8.2024 16:05
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] MSI opravuje 1 zranitelnost v základných do...	14.8.2024 13:41
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Elastic Kibana opravuje kritickou zranitelnost	15.8.2024 15:38
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Microsoft Windows záplatuje kritickou RCE zr...	16.8.2024 15:39
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Ivanti opravuje 8 zranitelností v různých pro...	16.8.2024 16:02
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Dovecot opravuje 2 zranitelnosti	19.8.2024 13:58
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] WordPress Zephyr Project Manager plugin o...	19.8.2024 14:51
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Kubernetes ingress-nginx opravuje 1 zranite...	19.8.2024 17:46
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] XWiki opravuje 2 zranitelnosti	20.8.2024 17:55
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] F5 opravuje 9 zranitelností v různých produk...	22.8.2024 17:53
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] GitHub Enterprise Server opravuje 3 zranitel...	23.8.2024 14:09
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] FFmpeg opravuje 3 zranitelnosti	Čt 15:46
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Cisco UCM a ISE opravuje 5 zranitelností	Pá 18:05
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] WebKitGTK a WPE WebKit opravuje 6 zranitel...	Po 17:50
	CESNET-CERTS <csirt-forum@cesnet.cz>	[csirt-forum] [TLP:CLEAR] Google Chrome opravuje 37 zranitelností	Včera 18:11

- Informace k aktuálním hrozbám
- Ověřené, důvěryhodné a ozdrojované
- Strukturovaná data o zranitelnostech, typech útoků a rizicích
- Doporučení mitigací a řešení limitujících dopady hrozeb
- 2, max 3 reporty denně do listu csirt-forum@
- Zajišťované členy bezpečnostního týmu CESNET-CERTS
- Na denní bázi
- Základ pro vulnerability management v organizaci
- **Není ale možné brát jako 100% náhradu vlastní činnosti**

VUTBR
–
3 respondenti

■ Spolupráce v CSIRT komunitě e-INFRA

- Propojuje týmy i jednotlivce,
- každý se může zapojit se svou expertízou, zkušeností, nalezenou zranitelností,
- každý může požádat o radu, konzultovat svou bezpečnostní situaci.

■ Forma mailing listu

- zápis mailem na adresu csirt-forum-subscribe@cesnet.cz
- žádosti o přihlášení jsou schváleny po validaci
- respondenty jsou zaměstnanci připojených organizací



■ Spolupráce v CSIRT komunitě e-INFRA

- Propojuje týmy i jednotlivce,
- každý se může zapojit se svou expertízou, zkušeností, nalezenou zranitelností,
- každý může požádat o radu, konzultovat svou bezpečnostní situaci.

■ Forma mailing listu

- zápis mailem na adresu csirt-forum-subscribe@cesnet.cz
- žádosti o přihlášení jsou schváleny po validaci
- respondenty jsou zaměstnanci připojených organizací

**POMOZTE vytěžit tuto službu na maximum!
Šiřte informaci o ní ve své organizaci!**

- Cílem je
 - „legálně“ dělat to, co jiní dělají běžně ;-)
 - vytvoření DB provozovaných služeb/zařízení
 - identifikace kompromitovaných/zranitelných zařízení
- Stav
 - scanujeme síťové rozsahy CESNET – v plném rozsahu
 - scanujeme síťové rozsahy statečných účastníků – na žádost pilotní provoz (VUT ano)
- Pracujeme na
 - provozních podmínkách a webové prezentaci
 - obchodním modelu
 - automatizaci (zakomponování do reportingu – aktuálně ručně)
- Použité nástroje
 - Sner, Auror, Nessus (možno také zapůjčit licenci)
- Přínosy a vlastnosti
 - včasné odhalení zranitelných zařízení
 - znáte zdroje scanování, s daty neobchodujeme, jsou využívány ve prospěch organizace
 - malý krok při plnění povinností ZoKB





SNER - Slow Network Recon Service

About project

Enrollment procedure

Use-cases

Links

Sner

Snerlytics ELK

CVE-Search

About project

<https://sner.flab.cesnet.cz/>

SNER is a proactive network monitoring service operated by CESNET for network security and research purposes within the CESNET2 network.

The service continuously maps enrolled networks, performs service discovery, and conducts fingerprinting similar to Shodan, Censys, and Shadowserver services. Participating networks can enhance their visibility within their address space and potentially receive early warnings about possible vulnerabilities.

- GitHub project: <https://github.com/bodik/sner4>
- Scanning Sources: Dynamic and identifiable via DNS as snerXX.flab.cesnet.cz.
- Scanning Techniques:
 - IP enumeration
 - DNS enumeration
 - TCP SYN scan
 - UDP service discovery
 - Service version fingerprinting
 - JA3/JARM scanning
 - TLS scanning
 - Vulnerability scanning (Nuclei)
- Data Mining Techniques:
 - Service version extraction
 - CPE-CVE correlation

Contact

flab@cesnet.cz



▶ ABOUT US

▶ INCIDENT REPORT

▶ COOPERATION

▶ FAQ

Auror scanner

If you see this page, then more than likely, you noticed a scan coming from *auror-scanner.cesnet.cz*:

- 78.128.247.178
- 2001:718:ff05:206::178

Additionally, our HTTP-based scans use a Auror-specific user agent, which can be used to filter those requests: `Mozilla/5.0 (compatible; Auror/1.1; +auror-scanner.cesnet.cz)`.

Auror is a tool for network security scanning. It scans hosts and gathers useful security-related information about available SSL/TLS, certificates, HTTP headers etc. All of the probes used in our tests are benign and do not contain exploit code. If you have any more questions please feel free to contact us at [Contact](#).

Používání zastaralého SSL/TLS

Protokoly SSL a TLS jsou používány pro zašifrování spojení mezi serverem a klientem u mnoha protokolů, např. [FTP](#), IMAP, HTTP, SMTP a mnoho dalších. Následující verze jsou zastaralé a není doporučeno je používat:

- Použití SSL 2.0 bylo zakázáno v [RFC 6176](#) v březnu 2011.
- Použití SSL 3.0 bylo zavrženo v [RFC 7568](#) v červnu 2015.
- Použití TLS 1.0 a 1.1 bylo zavrženo v [RFC 8996](#) v březnu 2021.

V současné době je bezpečné používat TLS verze 1.3. S vypnutou podporou šifrovacích algoritmů [3DES](#), [GOST](#) a [RC4](#) je možné bezpečně provozovat i starší TLS 1.2.

Vypnutí v *Apache*:

```
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

Vypnutí v *Nginx*:

```
ssl_protocols TLSv1.2 TLSv1.3;
```

Vypnutí v *Postfix*:

```
smtpd_tls_mandatory_protocols = >=TLSv1.2 smtp_tls_mandatory_protocols =  
>=TLSv1.2 smtpd_tls_protocols = >=TLSv1.2 smtp_tls_protocols = >=TLSv1.2
```

Vypnutí ve *vsftpd* je automatické od verze 3.0.4.

Hledat



▶ O NAS

▶ HLÁŠENÍ INCIDENTU

▶ SLUŽBY

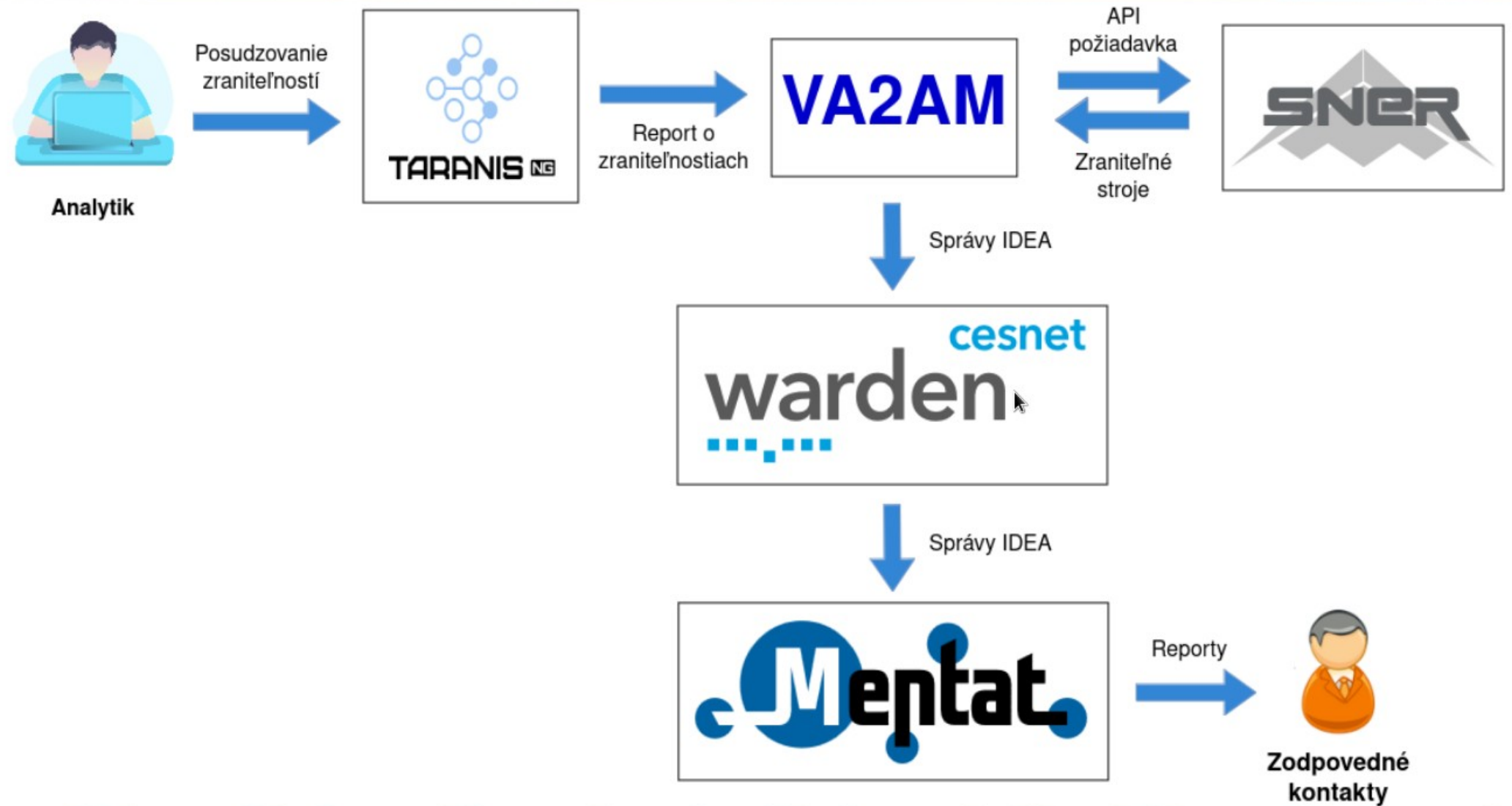
▶ PROJEKTY

▶ SPOLUPRÁCE

▶ ČASTÉ DOTAZY

▶ ODKAZY

▶ DOKUMENTY



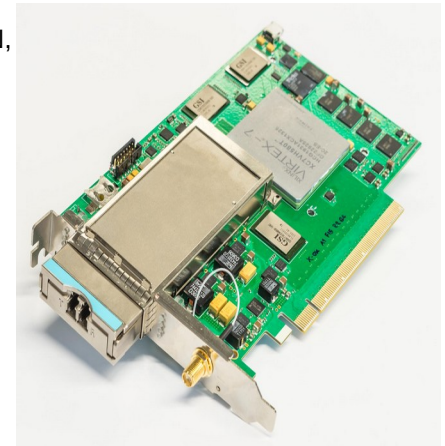
Bezpečnostní události a bezpečnostní incidenty

- Bezpečnostní události
 - ... jazykem ZKB „kybernetické bezpečnostní události“ ...
- Využíváme vlastní i externí zdroje

```
Nov 22 15:05:58 office2 postfix/smtpd[27935]: CAF18ED0073:  
client=grey.cesnet.cz[2001:718:1:6::134:228], sasl_method=LOGIN,  
sasl_username=pavelk
```



CrowdSec



ftas



USEPROTECT-NETWORK

NSHARP

NETWORK SECURITY HANDLING
AND RESPONSE PROCESS

národní
centrum
kybernetické
bezpečnosti



Shadowserver



network security incident exchange



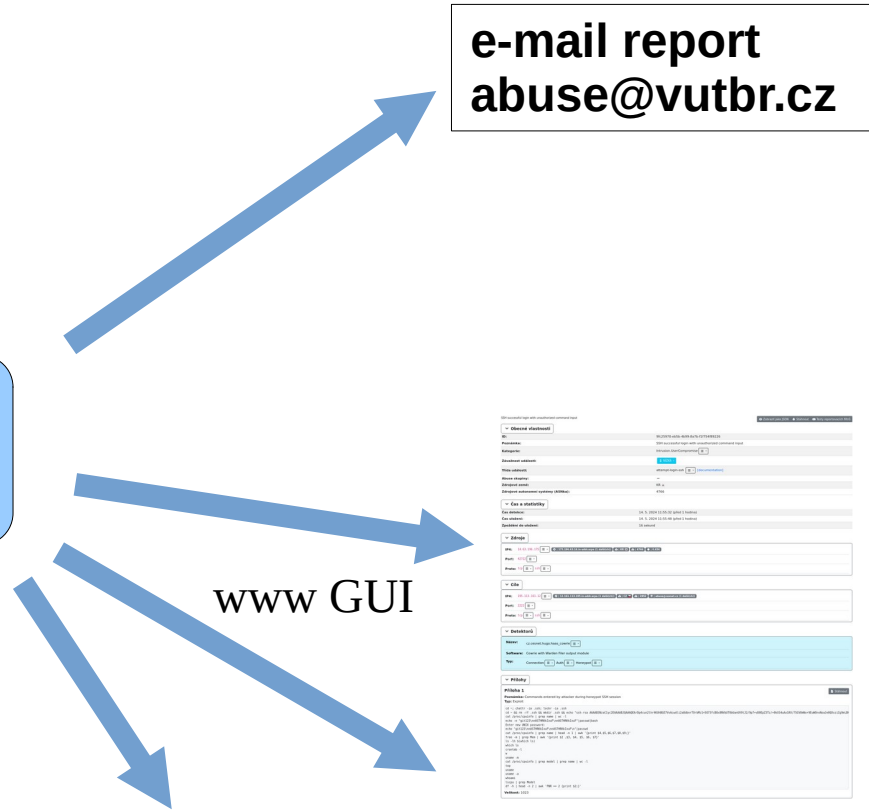
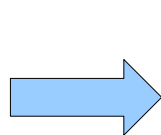
16. 5. 2024

Flowmon
Networks

TREND
MICRO
TippingPoint



mentat - Prsk CESNET-CERTS



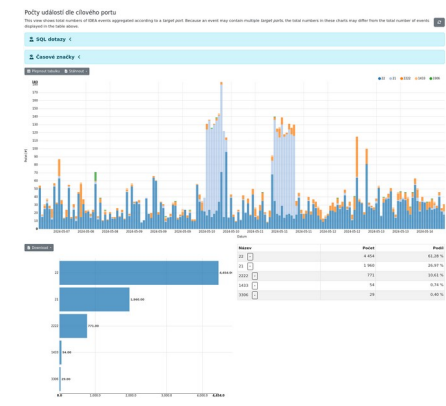
e-mail report
abuse@vutbr.cz

www GUI



Prohledat databázi událostí

Detekováno v	Zdroje	Závažnost	Kategorie	Detektor	Skupiny
14. 5. 2024 11:17:12	193.3.53.11	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	187.94.145.24	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	193.3.53.12	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	181.200.1.83	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	178.138.28.305	3. Kritická	Attempt Login	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	193.3.53.10	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	138.123.200.92	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	103.90.213.18	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	102.90.201.227	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	142.92.99.209	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-
14. 5. 2024 11:17:12	73.8.246.130	3. Kritická	Portovní Scanning	ČesneviNet.Nemesis.Hesitatis	-



- Dashboardy, grafy, statistiky ...
- Reporty (zaslané e-mailem)
 - kolik a jakých reportů přišlo za časové období
- Jaké detektory hlásí problémy
- Jaké problémy se „u mě“ vyskytují
- Které „moje“ zařízení jsou zdroji problémů
- Na jaké naše zařízení cílí útoky
- Filtrování reportů
- Přístup per organizace k datům „organizace“
- ...

Nástroje a aplikace

warden

....

- <https://warden.cesnet.cz>
- Platforma pro automatizované sdílení informací o incidentech
- Zapisující konektory zasílají události do „fronty“
- Čtoucí konektory odebírají vše, co se objevilo
- Jednotný formát (<https://idea.cesnet.cz>)
- Kdo ostatním poskytuje data, dostane se k datům ostatních

mentat

....

- <https://mentat.cesnet.cz>
- Jednotné automatizované zpracování
- Zpřístupňuje informace lidským způsobem přes GUI
- Příklad: DDoS
 - Informace dorazí přes FTAS, sondy a LaBreu do Wardenu
 - Mentat zagreguje informace z různých zdrojů
 - ... a roztrídí podle zdrojů útoku
 - Jednotlivé organizace dostanou specifický report o svých IP



<https://nerd.cesnet.cz>

- Databáze síťových entit (IP adresy, sítě, domény, ...)
- Seznam nám známých zdrojů škodlivých aktivit
... a všeho, co o nich víme
- Primární zdroj – Warden, MISP). Data jsou obohacena o další informace z externích zdrojů
- Shrnutí všech informací do reputačního skóre, predikce míry hrozby entity pro následující den (strojové učení z dostupných dat)

PassiveDNS

- <https://passivedns.cesnet.cz>
- DNS odráží okamžitý stav – Passive DNS udržuje historii
- Sleduje DNS transakce a staví databázi
- Příklady využití
 - Jaké všechny jmenné záznamy ukazují na IP a.b.c.d?
 - Jaké záznamy známe v doméně example.org?
 - Jak se měnilo doménové jméno v čase? Není to fast-flux?
 - Není příliš podobné existujícímu jménu? Nejde o phishing?

- Analýza událostí
- Plošné testy e-infrastruktury na zranitelnosti
 - heartbleed, memcached, shellshock ...
- Penetrační testy
- ~~Zátěžové testy~~
- Testy sociálního inženýrství („phishingové testy“) a služba Phishingator
 - na míru zákazníkovi
- Zadání --> Testy --> Zpracování --> Závěrečná zpráva & workshop
 - přehled provedených testů
 - zhodnocení výsledků (nálezu)
 - doporučení nápravných opatření
 - školení pro uživatele

<https://flab.cesnet.cz>



- Analýza událostí
- Plošné testy e-infrastruktury na zranitelnosti
 - heartbleed, memcached, shellshock ...
- Penetrační testy
- ~~Zátěžové testy~~
- Testy sociálního inženýrství („phishingové testy“) a služba Phishingator
 - na míru zákazníkovi
- Zadání --> Testy --> Zpracování --> Závěrečná zpráva & workshop

<https://flab.cesnet.cz>



**Plánujte!
Ozvěte se včas
a
zarezervujte
si slot!**


- přehled provedených testů
- zhodnocení výsledků (nálezu)
- doporučení nápravných opatření
- školení pro uživatele

- Hands-on školení v laboratoři pod vedením zkušených školitelů (by FLAB)
- Základy forenzní analýzy digitálních dat
- 2 dny, plus Forensic Night@CESNET

- *FT1: Zajišťování dat, vytváření časové osy ze souborového systému, následná analýza, identifikování jednotlivých stopy vedoucích k vytvoření komplexního obrazu analyzovaného incidentu. Prezentování výsledků jako součást tréninku.*

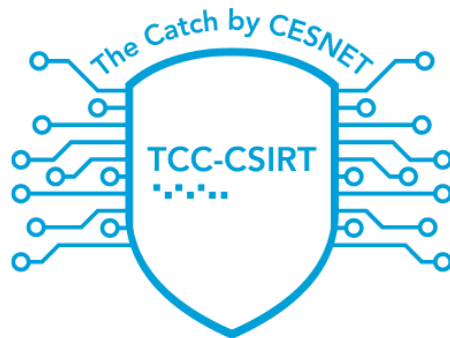
- *FT2: Analýza síťového provozu, teoretický úvod do problematiky, seznámení s postupy pro zajištění podkladů, analýzou toků v sítích (netflow) a analýzou částečného i plného záznamu provozu (packet capture). Součástí školení je také seznámení s jednotlivými nástroji používanými pro analýzu.*

- *FT1: únor/březen 2025*
- *FT2: červen 2025*



sluzby@cesnet.cz

- Hra/soutěž/školení na bázi CTF (Capture The Flag)
- CESNET příspěvek k Měsíci Kybernetické Bezpečnosti (říjen)
- Sada úloh na bázi analýzy logů, kódu, šifrování ...
- The Catch 2024, <https://www.thecatch.cz/>, **start 7 Oct 2024**



The Catch 2024

We will start in 33 days, **01:15:33!**

... Kdo si hraje, nezlobí :-)...

Phishingator



Phishingator

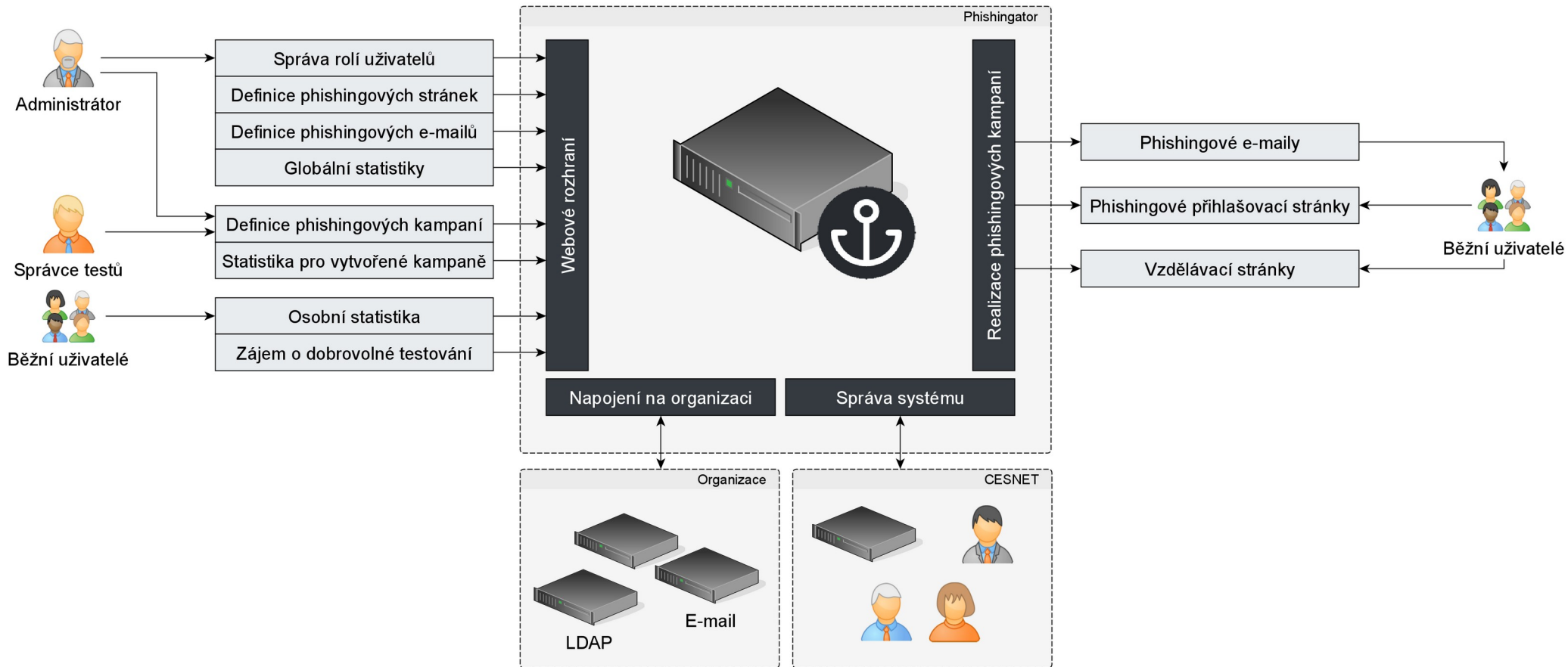
Služba Phishingator je webová aplikace, jejímž cílem je provádět praktické školení uživatelů v oblasti phishingu a sociálního inženýrství, a to odesíláním cvičných phishingových e-mailů.

Phishingator je navržen jako co nejvíce intuitivní a automatizovaný systém tak, aby jeho používání nevyžadovalo téměř žádné technické znalosti. Součástí systému je vedení jak globální, tak osobní statistiky u každého z uživatelů, a také vedení podrobné statistiky u každé phishingové kampaně.

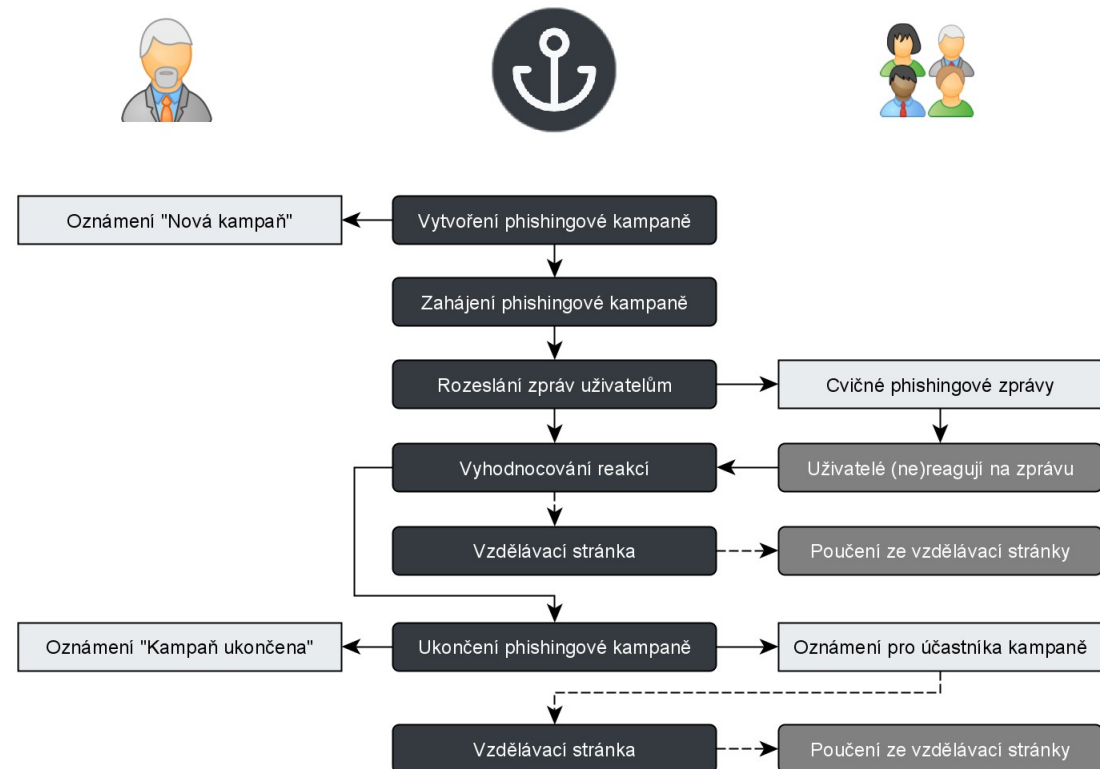
Standardní služba Phishingator obsahuje:

- provoz a správa služby na prostředcích CESNET
- podpora služby – Helpdesk
- 3x registrace domény pro cvičnou podvodnou stránku
- 3x příprava podvodné stránky
- 3x příprava vzorového podvodného e-mailu
- neomezený počet phishingových kampaní

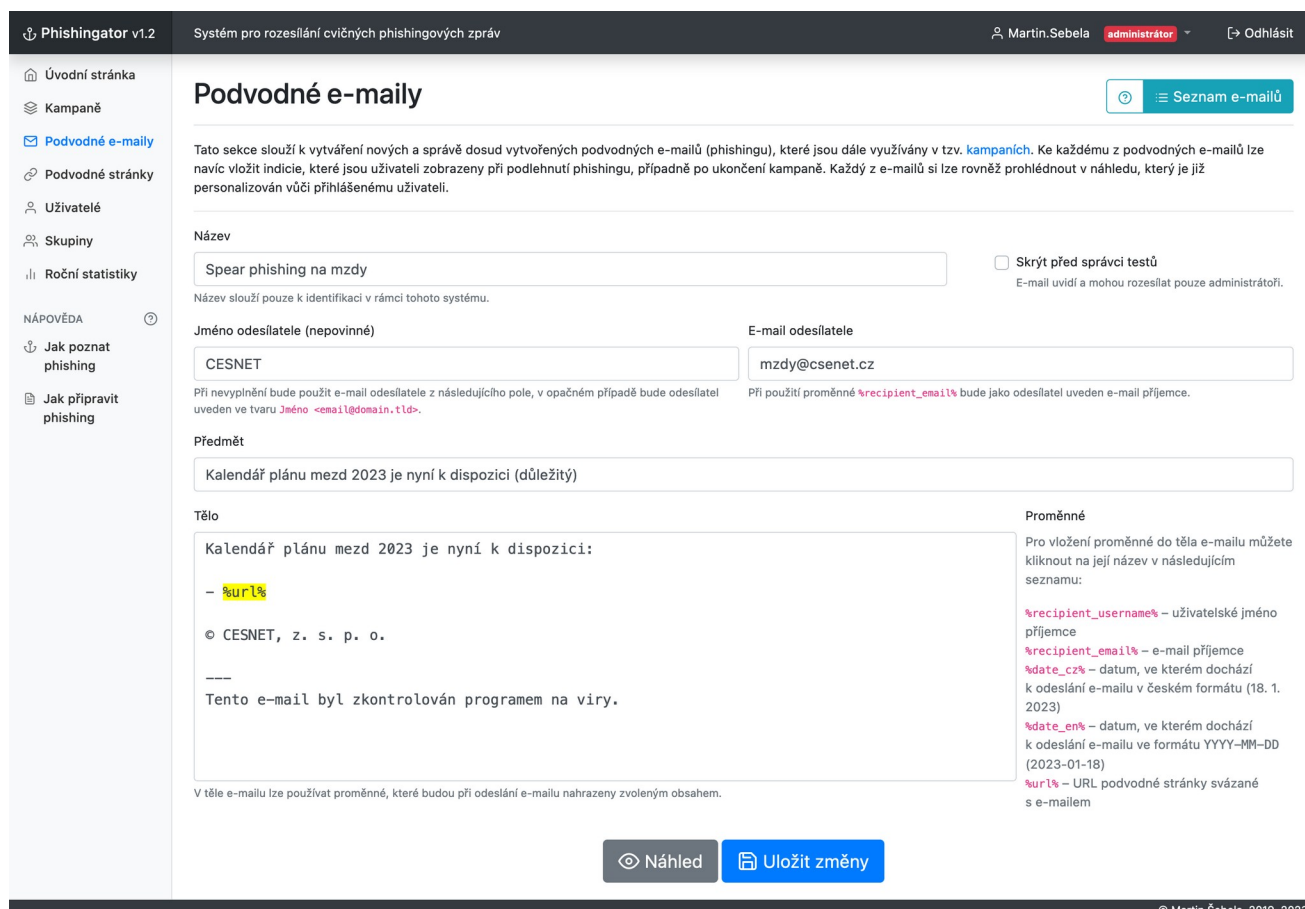
- Webová aplikace pro automatizované **rozesílání cvičných phishingových zpráv**
- Původně **bakalářská práce na ZČU (2019)**, nyní OpenSource
- **CESNET poskytuje formou Software as a Service**
 - Technicky se nemusíte o nic starat
 - Phishingator napojíme na Vaši organizaci
 - Každá organizace = **vlastní instance Phishingatoru**
- Praktický doplněk ke školení „kdykoliv a kdekoliv“
 - Přímá **konfrontace** s phishingem
 - **Cílené školení** uživatelů
 - **Zpětná vazba pro uživatele** o absolvování cvičného phishingu



- **Phishingová kampaň** = podvodný e-mail + podvodná stránka + adresáti
 - Vytvoření e-mailu a indicií
 - Nákup podvodné domény
 - Vytvoření **podvodné stránky** (šablona + URL)
 - Rozeslání e-mailů **konkrétním příjemcům**
 - Sledování **reakcí příjemců**
 - Automatická **zpětná vazba pro příjemce**



- Vytvoření **cvičného podvodného e-mailu**
 - **Jméno** odesílatele
 - **E-mail** odesílatele
 - **Předmět**
 - **Parametrizované tělo** e-mailu
 - Možnost personalizace



Phishingator v1.2 | Systém pro rozesílání cvičných phishingových zpráv | Martin.Sebela | administrátor | [Odházet]

Podvodné e-maily [Seznam e-mailů]

Tato sekce slouží k vytváření nových a správě dosud vytvořených podvodných e-mailů (phishingu), které jsou dále využívány v tzv. **kampaních**. Ke každému z podvodných e-mailů lze navíc vložit indicie, které jsou uživateli zobrazeny při podlehnutí phishingu, případně po ukončení kampaně. Každý z e-mailů si lze rovněž prohlédnout v náhledu, který je již personalizován vůči přihlášenému uživateli.

Název

Spear phishing na mzdy **Skrýt před správci testů**
E-mail uvidí a mohou rozesílat pouze administrátoři.

Název slouží pouze k identifikaci v rámci tohoto systému.

Jméno odesílatele (nepovinné) **E-mail odesílatele**

CESNET mzdy@cesnet.cz

Při nevyplnění bude použit e-mail odesílatele z následujícího pole, v opačném případě bude odesílatel uveden ve tvaru **Jméno <email@domain.tld>**. Při použití proměnné **%recipient_email%** bude jako odesílatel uveden e-mail příjemce.

Předmět

Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)

Tělo

Kalendář plánu mezd 2023 je nyní k dispozici:
– %url%
© CESNET, z. s. p. o.

Tento e-mail byl zkontrolován programem na viry.

Proměnné

Pro vložení proměnné do těla e-mailu můžete kliknout na její název v následujícím seznamu:

- %recipient_username%** – uživatelské jméno příjemce
- %recipient_email%** – e-mail příjemce
- %date_cz%** – datum, ve kterém dochází k odeslání e-mailu v českém formátu (18. 1. 2023)
- %date_en%** – datum, ve kterém dochází k odeslání e-mailu ve formátu YYYY-MM-DD (2023-01-18)
- %url%** – URL podvodné stránky svázané s e-mailem

V těle e-mailu lze používat proměnné, které budou při odeslání e-mailu nahrazeny zvoleným obsahem.

[Náhled] [Uložit změny]

© Martin Šebela, 2019–2023

Od: CESNET <mzdy@cesnet.cz>
 Předmět: **Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)**
 Kalendář plánu mezd 2023 je nyní k dispozici:

- [%url%](#) ⚠

© CESNET, z. s. p. o.

Tento e-mail byl zkontrolován programem na viry ⚠.

1. Náhled podvodného e-mailu s červeně zvýrazněnými indiciemi

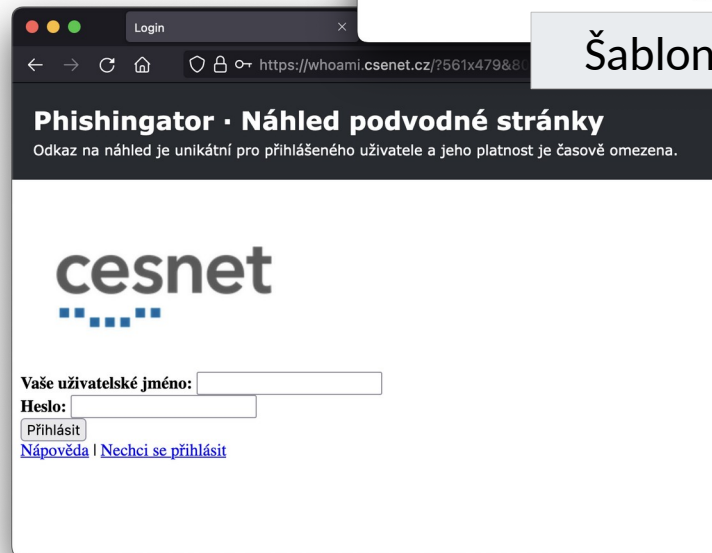
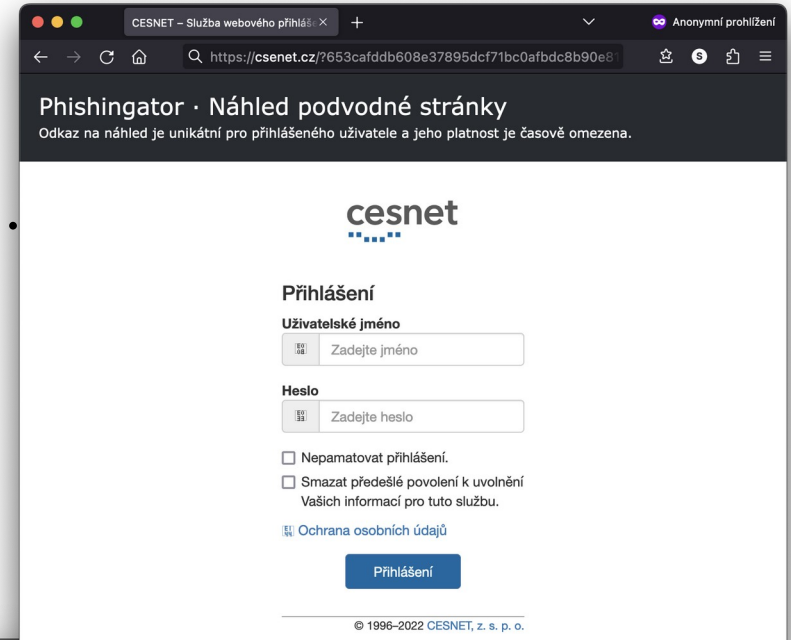
👁️ Náhled včetně indicií

Indicie (3) k rozpoznání tohoto phishingu

Indicie (podezřelý řetězec)	Nadpis	Popis (nepovinné)	
<input type="text" value="%sender_email%"/>	E-mail odesílatele	E-mail odesílatele nemá s organizací CESNET nic společného.	<input type="button" value="Smazat"/> <input type="button" value="Uložit změny"/>
<input type="text" value="%url%"/>	Podezřelá URL	Nejedná se o oficiální doménu CESNET.CZ, ale o snahu útočníka napodobit její	<input type="button" value="Smazat"/> <input type="button" value="Uložit změny"/>
<input type="text" value="zkontrolován programem na vir"/>	Tento text může připsat každý	Neříká to nic o věrohodnosti e-mailu.	<input type="button" value="Smazat"/> <input type="button" value="Uložit změny"/>

2. Přidání indicií (typických znaků phishingu), na základě kterých bylo možné phishing rozpoznat

- Nákup cvičné, phishingové **domény**, kde bude hostována podvodná stránka
 - Překlepy, snaha napodobit název organizace
 - Např. pro CESNET: **cesnet.cz** vs. **csenet.cz**, **oesnet.cz**, ..
- Nasměrování **DNS** na Phishingator
- Vytvoření **HTML šablony** pro podvodnou stránkou
- Případně vydání **HTTPS certifikátu**
- Volba **URL adresy** (různé adresáře a parametry v adrese)



Šablony podvodných stránek

- Zaznamenány reakce příjemců:
 - **Bez reakce**
 - **Návštěva podvodné stránky**
 - Vyplnění **neplatných** přihlašovacích údajů
 - Vyplnění **platných** přihlašovacích údajů

- Sledování **průběžných výsledků**

- **Data zadaná na podvodné stránce** (anonymizováno)

Systém pro rozesílání cvičných phishingových zpráv Martin.Sebela (administrátor) Změnit roli → [→] Odhlásit

Kampaně

[Seznam kampaní](#)

Tato sekce slouží k vytváření nových a správě dosud vytvořených kampaní. Každá z kampaní je svázána se zvoleným **podvodným e-mailem** a **podvodnou webovou stránkou**, na kterou se příjemce e-mailu dostane právě z obsahu tohoto e-mailu (pokud bude následovat odkazy v něm uvedené).

Základní informace

Název	Přidáno	Přidal	Podvodný e-mail	Podvodná stránka	URL podvodné stránky	Odesláno e-mailů	Spuštění rozesílání	Aktivní od	Aktivní do	RT kampaně	
Spear phishing na mzdy	10. 3. 2021	msebela	Spear phishing na mzdy	👁️	Přihlášení do SSO (věrná kopie)	https://login.████.cz	👁️ 173/173	každý den od 11:30	10. 3. 2021	11. 3. 2021	-

Konečné akce uživatelů v kampani

bez reakce	118 / 68.2 %
návštěva stránky	24 / 13.9 %
zadání neplatných údajů	9 / 5.2 %
zadání platných údajů	22 / 12.7 %

Konečné akce v kampani dle skupiny

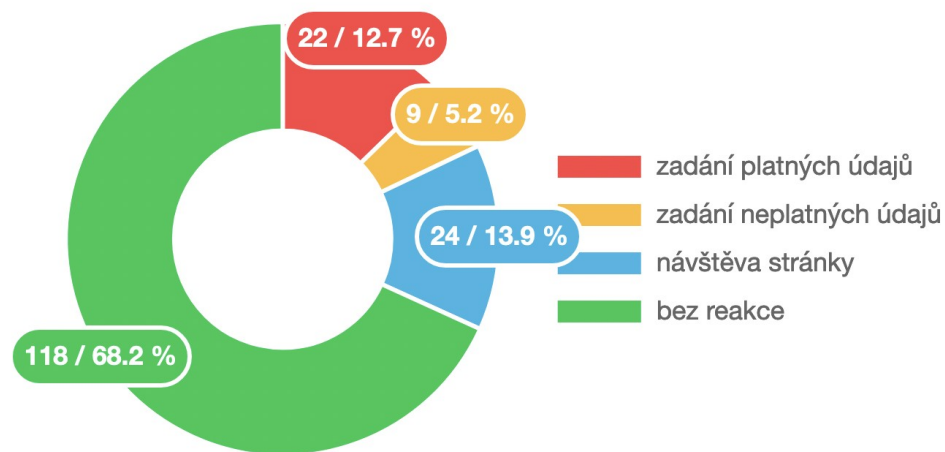
Provedené akce v kampani

bez reakce	118 / 44.2 %
návštěva stránky	90 / 33.7 %
zadání neplatných údajů	37 / 13.9 %
zadání platných údajů	22 / 8.2 %

📄 Tabulka konečných akcí
📄 Tabulka všech provedených akcí

- **Rozesláno 173** vybraným **zaměstnancům**
 - Napříč fakultami a dalšími odděleními
 - Získáno **22 platných identit** během 2 hodin
- **Všechny reakce příjemců:**
 - **Bez reakce (118)**
 - **Návštěva podvodné stránky (24)**
 - Vyplnění **neplatných** přihlašovacích údajů **(9)**
 - Vyplnění **platných** přihlašovacích údajů **(22)**

Konečné akce uživatelů v kampani



• 173 odeslaných e-mailů

1. 11:30 – odeslání cvičného phishingu
2. 11:31 – první návštěva podvodné stránky
3. 11:31 – první získaná identita
4. 11:35 – získáno 8 platných identit
5. do 12:00 – získáno 15 platných identit

20	CIV	návštěva stránky	10. 3. 2021 11:32:52	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...
19	CIV	návštěva stránky	10. 3. 2021 11:32:40	88.100.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
18	FEL	návštěva stránky	10. 3. 2021 11:32:39	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
17	CIV	návštěva stránky	10. 3. 2021 11:32:36	212.11.	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...
16	CIV	zadání platných údajů	10. 3. 2021 11:32:13	212.11.	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome... {"username":
15	KMA	zadání platných údajů	10. 3. 2021 11:32:12	88.100.	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/... {"username":
14	KIV	návštěva stránky	10. 3. 2021 11:32:09	89.102.	Mozilla/5.0 (Linux; Android 10; YAL-L41) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.86 Mobile Safari/537.36
13	FZS	návštěva stránky	10. 3. 2021 11:32:04	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
12	FPE	zadání platných údajů	10. 3. 2021 11:32:00	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/... {"username":
11	KMA	návštěva stránky	10. 3. 2021 11:31:57	88.100.	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/...
10	CIV	návštěva stránky	10. 3. 2021 11:31:56	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
9	FPE	návštěva stránky	10. 3. 2021 11:31:51	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/...
8	CIV	zadání platných údajů	10. 3. 2021 11:31:50	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP... {"username":
7	NTIS	návštěva stránky	10. 3. 2021 11:31:49	147.228.	Mozilla/5.0 (X11; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
6	CIV	návštěva stránky	10. 3. 2021 11:31:48	212.11.	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...
5	CIV	zadání platných údajů	10. 3. 2021 11:31:47	89.102.	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36 {"username":
4	CIV	návštěva stránky	10. 3. 2021 11:31:42	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...
3	CIV	návštěva stránky	10. 3. 2021 11:31:39	89.102.	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36
2	CIV	zadání neplatných údajů	10. 3. 2021 11:31:10	147.228.	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0 {"username":
1	CIV	návštěva stránky	10. 3. 2021 11:31:04	147.228.	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0

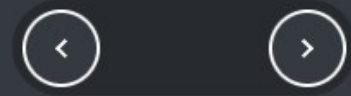
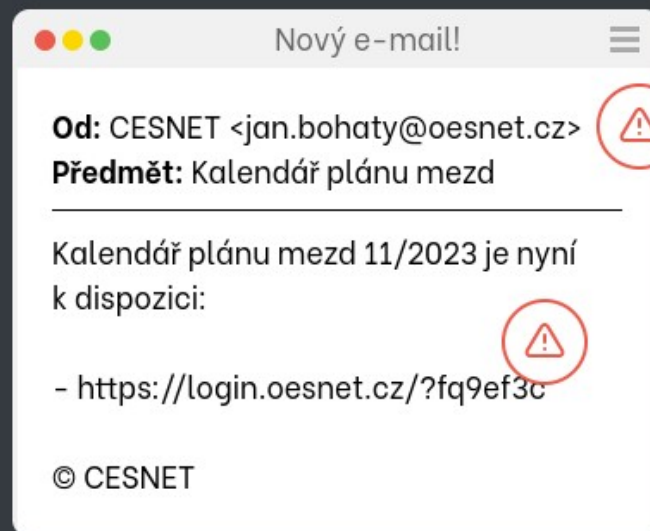


Phishingator

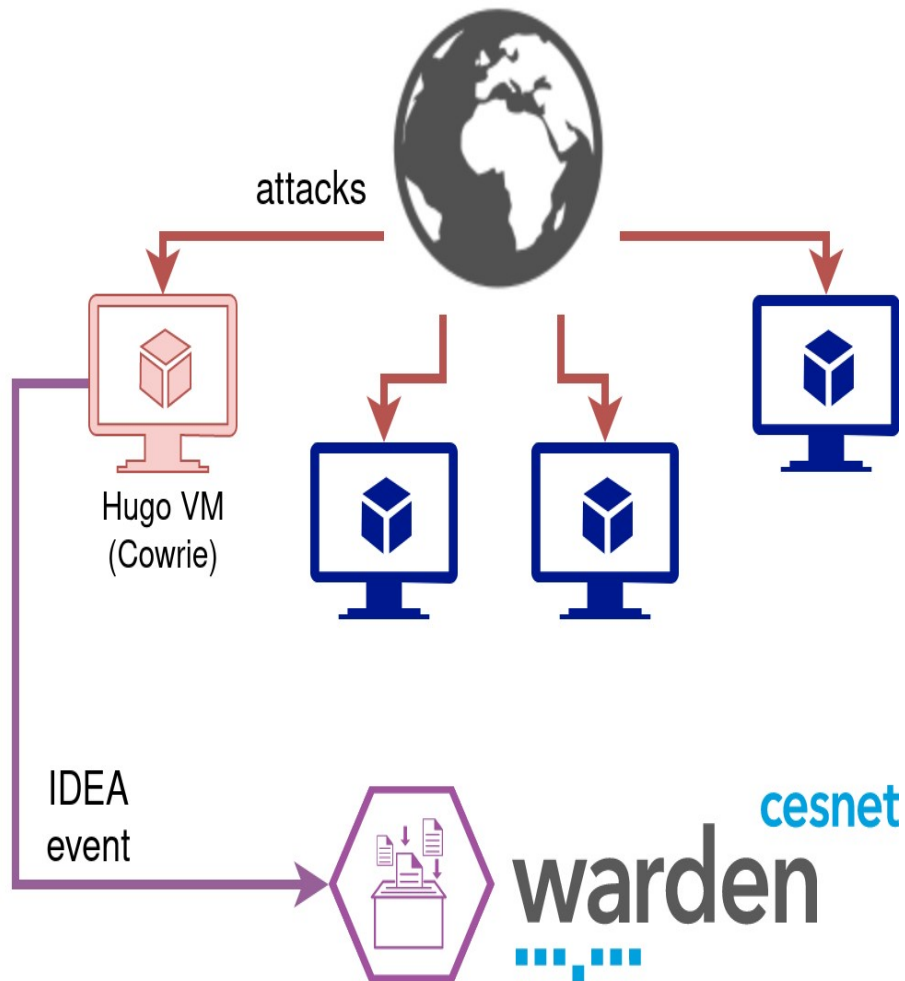
Cvičný phishing nejen na českých univerzitách

Cílem Phishingatoru je upozornit na nebezpečí phishingu a naučit uživatele odhalovat skutečný phishing.

PŘIHLÁSIT SE ▶

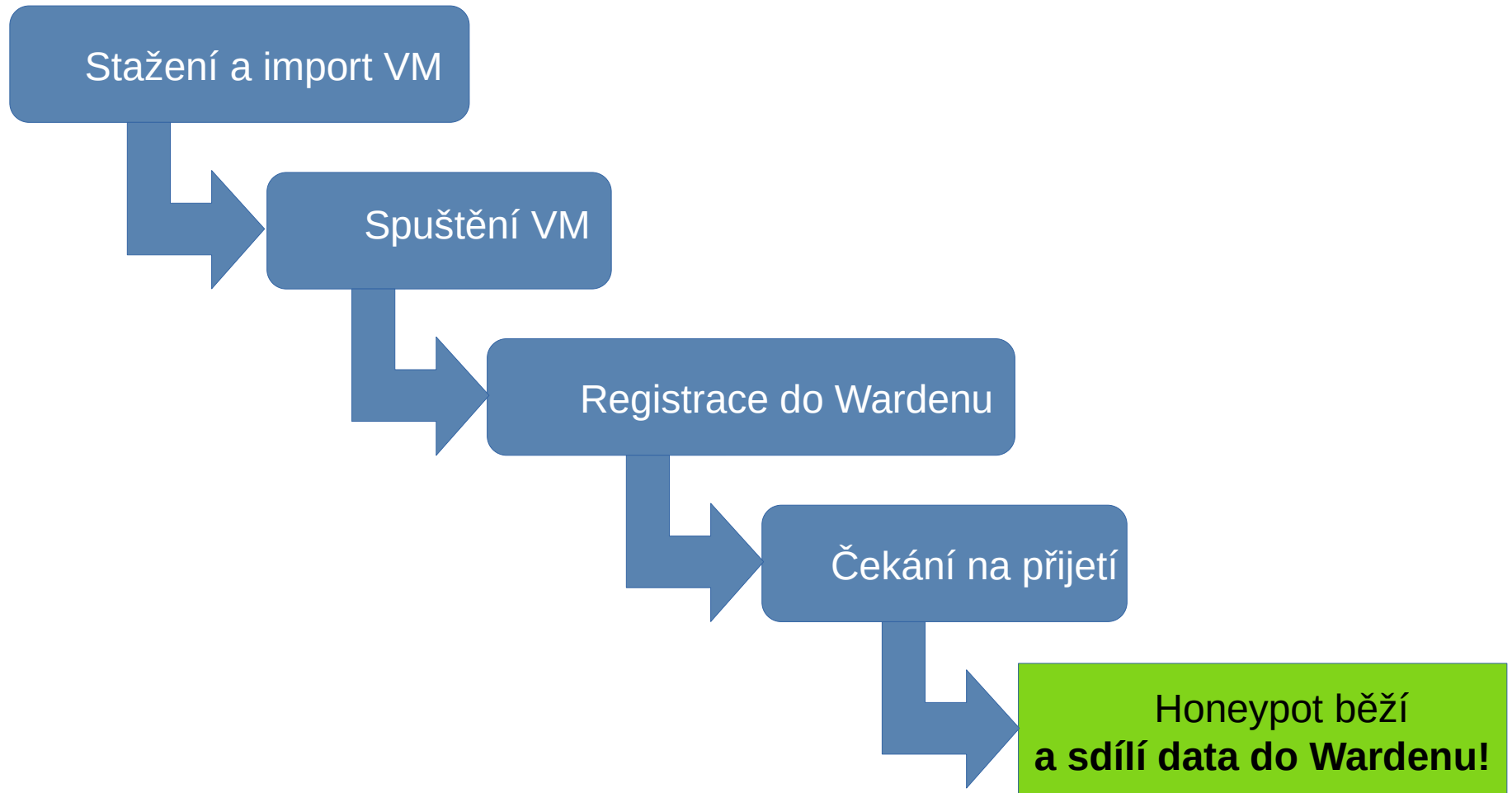


Služba Hugo **(honeypot as a service)**



- **Samočinný sběr dat o útocích ze zapojených organizací**
 - Datový zdroj pro Warden
 - Každá událost je platná
- **Cíl: co nejjednodušší start**
 - Import VM & nastavit & spustit
 - Integrovaný monitoring stavu
- **Zatím v omezeném testovacím provozu**

- Zdrojové IP adresy
 - Použité přihlašovací údaje
 - Příkazy
 - Stažený malware a jeho URL,
 - atp. atp.
-
- ochrana sítě (blocklist známých zdrojů útoku)
 - zdroj pro reputační databáze (např. **NERD**.cesnet.cz)
 - korelace dat v rámci výzkumných činností
 - detekce škodítek ve vlastní síti



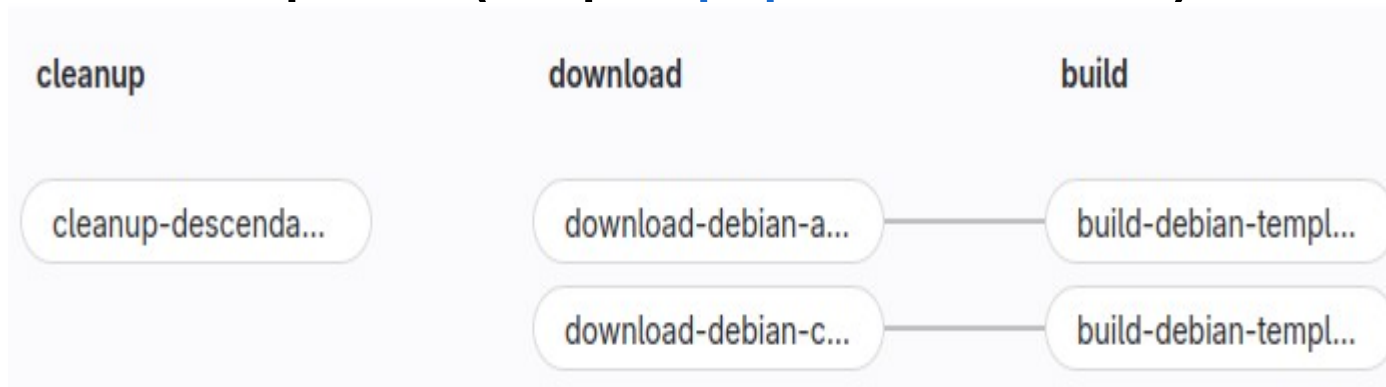
- Použité honeypoty
 - Cowrie <https://github.com/cowrie/cowrie>
 - SSH
 - Dionaea <https://github.com/DinoTools/dionaea>
 - FTP, TFTP, MySQL, MS SQL
 - Znovu zapnuta podpora pro MySQL
 - Další v budoucnu
- Drobné konfigurační změny

- Nasazené instance v sítích
 - CESNET, ČVUT (koleje), ZČU, TUL, UJEP
 - V procesu Kraj Vysočina a UPJŠ Košice
 - externí partneři

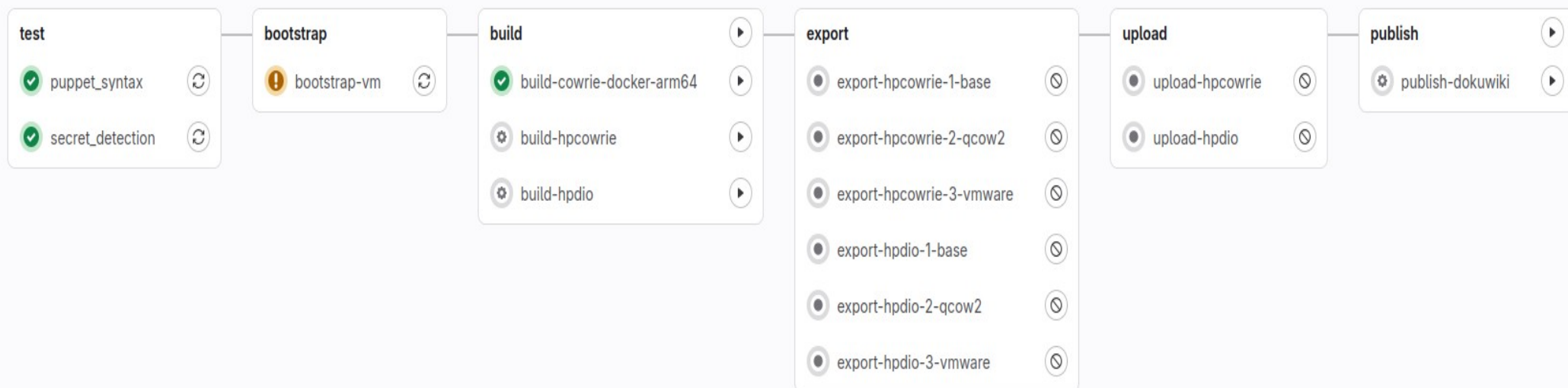
- Balíček s VM ve formátu OVA
- Ad import OVA do hypervizoru
 - QEMU/libvirt – OK (virt-v2v)
 - VirtualBox – OK
 - Proxmox – nutno OVA rozbalit, import obrazu disku (VMDK) bez obtíží
 - VMWare – úspěšný import do VMWare Workstation, ale **ne do vSphere/ESXi**
 - Důvod – nekompatibilita definice VM v OVF
 - Import obrazu disku (VMDK) bez větších obtíží (nutno po importu naklonovat)
- Řešení pro VMWare a další varianty
 - Úprava definice VM v OVF specificky pro VMWare
 - Publikace diskových obrazů ve formátech QCOW2, VMDK
 - Samostatný VMDK – volba mezi distribucí stream-optimized image a sparse image

- Zmenšen obraz disku ze 40 GB na 4 GB
- Postupný přechod na Debian 12
- Přechod z iptables na nftables
 - Lepší základ pro správu do budoucna
- Aktualizace Puppet 7
 - Technologická nutnost pro podporu některých pluginů
- Docker
 - Ve stádiu PoC
 - Funkční build Cowrie pro x86-64 a ARM64

OS template (např. [pipeline 9685](#))



Hugo (např. [pipeline 10101](#), arm64-test)



- Celý build – od tvorby šablony po publikaci imagí na web – orchestrován v Gitlab CI
- Build stroj hugo-craft pro sestavení OS a imagí
 - Není nutno zálohovat – sestavitelný z Ansible playbooků
- Testovací Docker build stroj pro ARM64

Máte zajímavý zdroj dat?

A jste ochotni data sdílet?

Ozvěte se nám!

sec-op@cesnet.cz

Máte te nudící se studenty?

Hledáte pro ně téma?

Nevíte co podat do Fondu Rozvoje?

<https://fondrozvoje.cesnet.cz>

Akce, vzdělávání

- únor 2024: BSS24
- 16. května 2024: Pracovní skupina „Bezpečnostní události“
- 6. června 2024: Ipv6 Day (seminář o Ipv6)

- říjen 2024: The Catch (start Oct 7 2024)
- únor 2025: Seminář o bezpečnosti (každý rok)
 - možná 2 denní (1. den konference, 2. den pracovní skupina)
- únor/březen 2025: FT1 a FT2
- červen 2025: FT1 a FT2
- červen: Seminář o Ipv6

- Pracovní skupiny:
 - 2022: Bezpečnostní události
 - 2022: Bezpečná architektura sítě
 - 2022: Monitoring sítě pomocí FTAS
 - 2023: ISMS
 - 2024: 16. května: Pracovní skupina „Bezpečnostní události“
- Další náměty?
 - antispamová ochrana?
 - honeypoty?
 - správa sítě?
 - orchestrační nástroje?
 - firewall?
 - zálohování?

Antispam Gateway

- Organizacím odpadá náročná správa a vývoj vlastní ochrany
- Snižuje se zátěž cílových poštovních serverů
- Doručení ohodnocených zpráv na koncový server organizace
- Robustní a modulární architektura zajišťující vysokou účinnost a dostupnost ochrany v režimu 24/7/365.
- Antispamové filtry běží na výkonných serverech, které zvládnou ochranu domén s velkým objemem provozu dat i při vysokém zatížení ve špičkách.
- Ochrana před DDoS útoky.
- Dočasný záložní poštovní server, relay funkce (zajistí pozdržení doručení zpráv až 5 dnů při výpadku primárního poštovního serveru organizace).
- Nezávislost na typu cílového poštovního serveru, možnost integrace komerčních řešení.
- Nedochází k zásahu do těla přenášené zprávy.
- Data jsou uložena v České republice.
- Podpora protokolu Ipv6.
- V souladu s nařízením NÚKIB.



- Antispam Gateway je předřazena (MX záznamy) před poštovní systémy organizace
- Trojstupňová ochrana
 1. **Kontrola blacklistů a komunikace SMTP.** Na základě výsledku je zpráva odmítnuta, greylistována, nebo předána k další analýze.
 2. **Greylisting.** Zpráva je dočasně odmítnuta, pokud obsahuje drobné nedostatky v SMTP komunikaci, nebo je alespoň na jednom blacklistu.
 3. **Spamassassin.** Filtruje zprávy před odesláním na cílový (primární) server a do hlavičky vkládá informaci o výsledku kontroly.
- Výsledek Spamassasina se vkládá do hlavičky zprávy
 - X-spam-cesnet-Status – nejdůležitější informace pro případné filtrování na straně cílového poštovního serveru, obsahuje hodnotu, zda je zpráva hodnocena jako spam (dle antispamové ochrany).
 - X-Spam-Level – informace taktéž použitelná pro filtrování, za každý bod při hodnocení přidává hvězdičku.
 - X-Spam-cesnet-Virus – výsledek testu na výskyt virů ve zprávě.
 - X-Spam-cesnet-Report – detailní výpis všech testů a hodnocení.



- Prostředí
 - možnost konfigurovat prostředí domény
 - adresy, whitelisy (provádíme kontrolu syntaxe)
 - přístup k provozním logům
 - grafické rozhraní, dostupná statistika
- Obecné podmínky
 - Nastavení cílového poštovního serveru a AG musí být v souladu. Tzn. cílový poštovní server musí přijímat všechnu poštu od AG. AG je na výskyt tohoto stavu monitorována.
 - V případě přetrvávajících a neřešených problémů s dostupností cílových poštovních serverů může být služba AG ze strany CESNETu pro danou doménu ukončena.
 - V případě problému na straně cílového poštovního serveru může být doba pozdržení zpráv na AG (relay funkce) i více než 5 dní, na žádost správce domény (zástupce organizace) může být časový limit zvýšen.
 - V případě, že dojde ke zneužití ssh přístupu na AG, bude přístup pozastaven.
 - Povinnost hlásit bezpečnostní události, podezření z narušení bezpečnosti služby, špatné fungování



- Služby
- Monitorujeme, sbíráme data, analyzujeme a:
 - bráníme
 - varujeme
 - reportujeme (a sdílíme)
- Prostředí pro spolupráci
- Zajímavé akce
- Sdílení know-how
- SOC BASIC (základní deklaraci služby)
- Kousek plnění požadavků ISMS a ZKB (a Vyhlášky)

- § 10 Řízení provozu a komunikací, písmeno
- § 18 Bezpečnost komunikačních sítí
- § 23 Detekce kybernetických bezpečnostních událostí
- § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí
- § 26 Kryptografické prostředky
- Plnění opatření vydaných NÚKIB

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz

- www.cesnet.cz
- <https://www.cesnet.cz/sluzby/>
- www.cesnet.cz/enews - e-mail Newsletter
- **sluzby@cesnet.cz**

- 1. ledna 2015
 - zákon č. 181/2014 Sb., o kybernetické bezpečnosti („ZKB“)
 - CESNET se určuje jako „provozovatel významné sítě“
- Rok 2017
 - novelizace ZKB (zohlednění NIS vyhlášky), vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti („VKB“) s účinností od 1. ledna 2018
 - CESNET se určuje jako „provozovatel digitálních služeb“
- Rok 2021: Určování CESNET za subjekt KII
 - Únor 2021: NÚKIB zahájil proces určování jako subjektu kritické infrastruktury v odvětví VI. KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY, oblasti G. Kybernetické bezpečnosti dle nařízení vlády č. 432/2010 Sb.
 - Listopad 2021: zveřejnil NÚKIB na své úřední desce návrh opatření obecné povahy („OOP“)
 - 12. 1. 2022 OOP bylo formou veřejné vyhlášky vydáno
 - 27. 1. 2022 OOP nabylo účinnosti

§ 3 Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou

- a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),
- b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
- c) správce a provozovatel informačního systému kybernetické informační struktury,
- d) správce a provozovatel komunikačního systému kybernetické informační struktury,
- e) správce a provozovatel významného informačního systému kybernetické informační struktury,
- f) správce a provozovatel informačního systému kybernetické informační struktury, pokud není správcem nebo provozovatelem podle písmene d),
- g) provozovatel základní služby, pokud není správce podle písmene f), a
- h) poskytovatel digitální služby.

Významná síť:
~ síť s přímým
propojením do
globálního internetu

Telia Sonera (dříve)
Telecom Italia Sparcle
(aktuálně)

§ 3 Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou

- a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),
- b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
- c) správce a provozovatel informačního systému kritické infrastruktury,
- d) správce a provozovatel komunikačního systému kritické infrastruktury,
- e) správce a provozovatel významného informačního systému,
- f) správce a provozovatel informačního systému základní služby, pokud není správcem nebo provozovatelem podle písmene c),
- g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
- h) poskytovatel digitální služby.

Infrastruktura
MetaCentra a
Datových úložišť

- CESNET-CERTS
 - řešení a koordinace řešení bezpečnostních incidentů (incident handling)
- Garantujeme provoz 9 – 17 v pracovních dnech
- SOC BASIC
 - https://muj.cesnet.cz/_media/cs/private/docs/cesnet_soc_basic_sld_v1_2022-05-06.pdf

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz

§ 3 Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou

- a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),
- b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
- c) správce a provozovatel informačního systému kritické informační infrastruktury,
- d) správce a provozovatel komunikačního systému kritické informační infrastruktury,
- e) správce a provozovatel významného informačního systému,
- f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),
- g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
- h) poskytovatel digitální služby.

Specifikace služby CESNET SOC BASIC

A. Název služby: CESNET SOC BASIC
Informační stránky služby: <https://www.cesnet.cz/sluzby/soc-basic/>

B. Definice služby:

Služba CESNET SOC BASIC (dále též jen „Služba“) je součástí základních služeb, které CESNET, zájmové sdružení právnických osob (dále jen „sdružení CESNET“) zajišťuje pro své členy a další připojené organizace (dále jen „Účastník“). Služba spočívá v zajištění detekce kybernetických bezpečnostních událostí a jejich vyhodnocování a ve zvládnutí kybernetických incidentů v prostředí síťové infrastruktury CESNET.

C. Popis Služby:

Bezpečnost síťové části e-infrastruktury CESNET, ochrany připojených Účastníků a jejich dat je realizována:

- architekturou zařízení, mechanismů a nastavení směrovacích protokolů,
- pokročilého monitoringu infrastruktury,
- detekcí anomálií ve všech topologických částech sítě - na vnějším perimetru síťové infrastruktury CESNET, v rámci páteřní infrastruktury a na perimetru mezi páteřní infrastrukturou a sítí Účastníka.

Nastavení a aplikovaná opatření jsou průběžně vyhodnocována a optimalizována.

Zabezpečení síťové části e-infrastruktury CESNET je realizováno následujícím postupem:

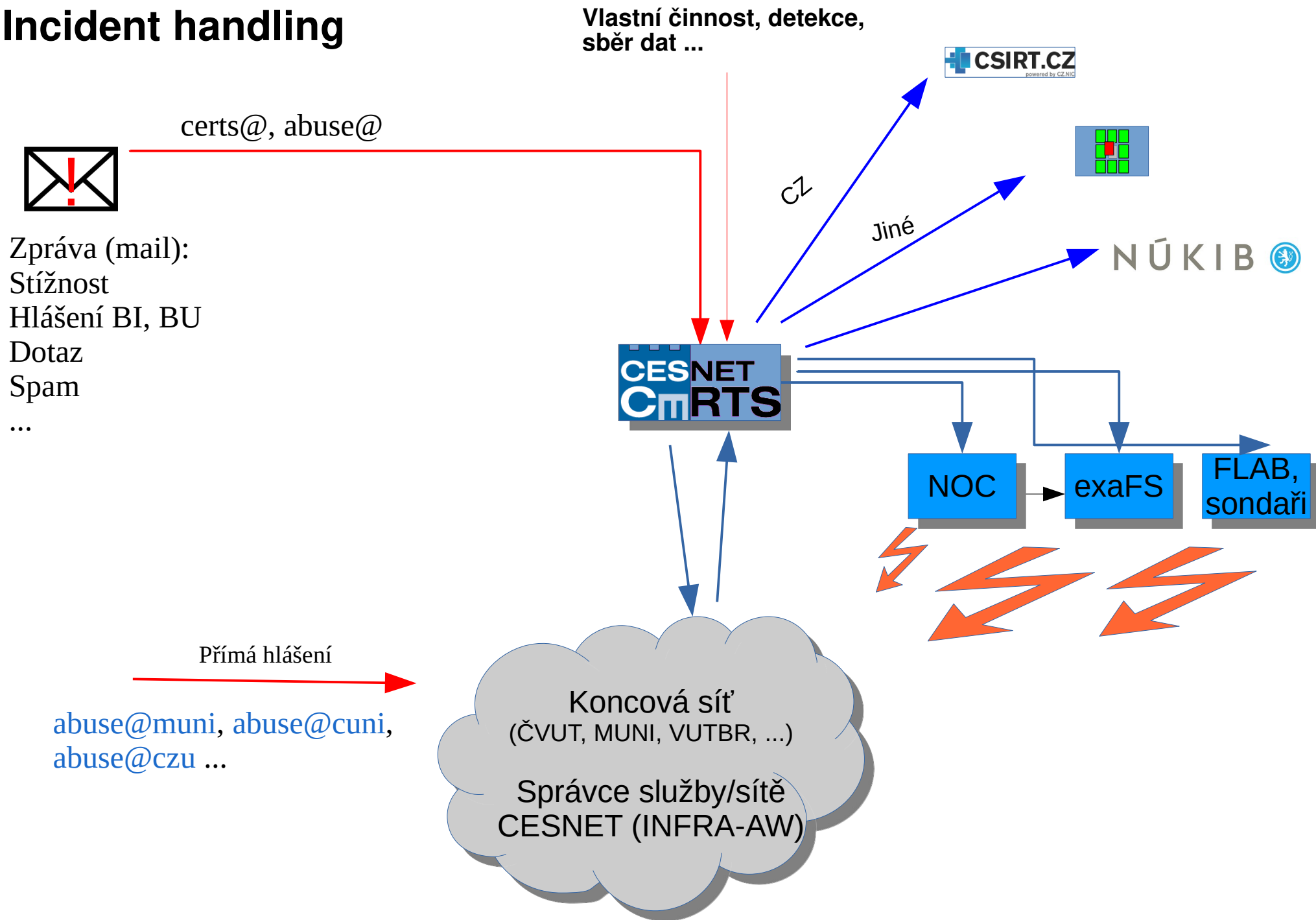
- zamezit zahlcení páteřní infrastruktury,
- zamezit zahlcení přípojek Účastníků,
- zamezit zahlcení externích propojení,
- eliminovat nelegitimní provoz,
- ošetřit anomální jevy na úrovni síťového transportu s minimalizací rizik spojených s potenciálním false-positive vyhodnocením jevů.

Koordinace řešení bezpečnostních incidentů		
Zpracování přijatých hlášení bezpečnostních incidentů a jejich předání Účastníkovi	CESNET-CERTS, Pracovní dny 9 – 17	2 hod
Kooperace a asistence s řešením bezpečnostních incidentů.	CESNET-CERTS, Pracovní dny 9 – 17	Pracovní dny 9 – 17, nebo na základě dohody sdružení CESNET a Účastníka

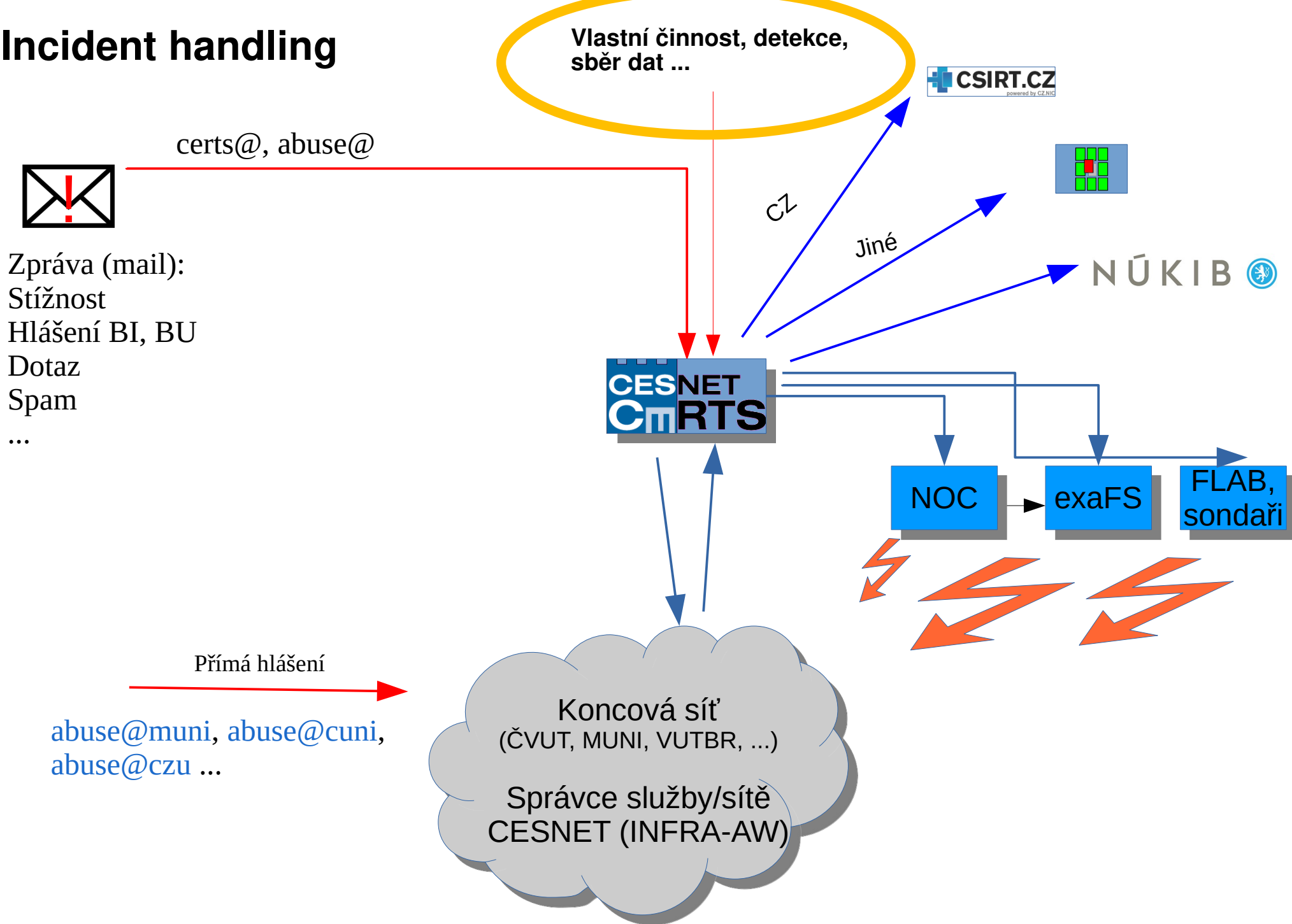
Automatizovaný sběr informací o bezpečnostních událostech a jejich distribuce Účastníkovi (reporting)	Automatizovaně 24x7	Neprodleně, v závislosti na nastavení ze strany Účastníka
Zápůjčka licence aplikace NESSUS pro vlastní otestování zranitelností	CESNET-CERTS, Pracovní dny 9 – 17	NBD ² , podle dostupných kapacit licence
Konzultace		
Základní konzultace v oblasti monitoringu, detekce anomálií a regulace provozu	Administrativní kontakt	NBD, na základě požadavku Účastníka
Vzájemná koordinace		
Vzájemné zhodnocení nastavení Služby	Administrativní kontakt	1x ročně, po dohodě sdružení CESNET a Účastníka

- Typ: interní a koordinační
- Interní:
 - pro adresové rozsahy, na kterých CESNET provozuje své služby – páteř, lokální sítě, serverové segmenty atd.
 - tedy sítě pojmenované CESNET-.*
- Koordinační
 - pro další sítě v AS2852 a Kraj Vysočina, které nepatří do předchozího výčtu
 - **... ale může přijít i leccos dalšího, co nám nepatří ...**

Incident handling



Incident handling



Prefix	Organizace
146.102.0.0/16	VŠE
147.228.0.0/16	ZČU
147.230.0.0/15	TUL + AVČR
147.251.0.0/16	MUNI
147.32.0.0/15	ČVUT + VŠCHT
158.194.0.0/16	UPOL
158.196.0.0/16	VŠB
160.216.0.0/15	UNOB + JČU
193.84.116.0/23	ICFP CAS
193.84.160.0/20	UJV ŘEŽ
193.84.192.0/19	OPF SLU
193.84.32.0/20	ČZU
193.84.53.0/24	CUNI
193.84.55.0/24	CUNI
193.84.56.0/21	CUNI
193.84.80.0/22	CESNET
195.113.0.0/16	CESNET
195.178.64.0/19	CESNET
78.128.128.0/17	CESNET
185.8.160.0/22	CESNET
2001:718::/32	CESNET



Slouží pro adresaci:

- Vlastní infrastruktury a služeb CESNET
- Připojených institucí bez vlastních IP

Summary

- Bohaté a komplexní portfolio nástrojů a služeb pro monitoring, detekci anomálií, analýzu, mitigaci ...
- Data pro online i offline analýzu
- Soubor postupů, metod, procesů ... know-how ...
- Připravené a otestované mechanismy pro zásah
- Efektivní týmy a pracoviště – PSS, NOC, CESNET-CERTS, FLAB
- Gramotní správci

cesnet Co z toho má připojená organizace

- Služby
- Monitorujeme, sbíráme data, analyzujeme a:
 - bráníme
 - varujeme
 - reportujeme (a sdílíme)
- Prostředí pro spolupráci
- Zajímavé akce
- Sdílení know-how
- SOC BASIC (základní deklaraci služby)
- Kousek plnění požadavků ISMS a ZKB (a Vyhlášky)

- § 10 Řízení provozu a komunikací, písmeno
- § 18 Bezpečnost komunikačních sítí
- § 23 Detekce kybernetických bezpečnostních událostí
- § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí
- § 26 Kryptografické prostředky

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz

Služba	Oblast využití
FTAS – sledování provozu sítě exaFS – regulace provozu sítě FTAS a exaFS – monitoring a obrana	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteři a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
csirt-forum@ - zapoj se do komunity csirt-forum@ - situational awareness Seminář o bezpečnosti (každoročně) Školení FT1 a FT2 The Catch Pracovní skupiny CESNET CSIRT Phishingator	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
Penetrační testy Zátěžové testy Analýza bezpečnostního incidentu	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Scan sítě na zranitelnosti (sner4) Individuální scan sítě nástrojem Nessus	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Mentat HaaS	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
NERD Passive DNS	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteři a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Služba	Oblast využití
FTAS – sledování provozu sítě	<p>Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.</p> <p>Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.</p>
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	<p>Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.</p>
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	<p>Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.</p>
Individuální scan sítě nástrojem Nessus	
Mentat	<p>Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.</p>
HaaS	
NERD	<p>A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení</p>
Passive DNS	

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteři a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Penetrační testy	
Zátěžové testy	
Analýza bezpečnostního incidentu	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Scan sítě na zranitelnosti (sner4)	
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Služba	Oblast využití
FTAS – sledování provozu sítě	<p>Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.</p>
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	<p>Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.</p>
Penetrační testy	
Zátěžové testy	
Analýza bezpečnostního incidentu	<p>Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.</p>
Scan sítě na zranitelnosti (sner4)	
Individuální scan sítě nástrojem Nessus	
Mentat	<p>Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.</p>
HaaS	
NERD	<p>Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.</p>
Passive DNS	
	<p>A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení</p>

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteři a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Penetrační testy	
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	
Individuální scan sítě nástrojem Nessus	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Nejnovější a připravované služby

