cesnet

BEZPEČNOST

Andrea Kropáčová
CESNET

15. 5. 2024
ČZU, Praha

Hlavní mise

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

Prostředky

- 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

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

FENIX

CESNET-CERTS

- 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

CESNET-CERTS

- 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
- 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

cesnet

TF-CSIRT
Trusted Introducer

Home | Processes | Services | Directory | Events | Contact TI | Member View

Team Info
- Team Details
- Constituency
- Contact Information
- Cryptography
- Memberships
- Classification
- History

CESNET-CERTS

Accredited
since 27 Jan 2008

ACCREDITED BY TRUSTED INTRODUCER 20

Fields describing the team

Team Details

Official Name
CESNET-CERTS

Short Name
CESNET-CERTS

Country
Czech Republic

Established
15 Jan 2004

Host Organisation
CESNET, z. s. p. o. Generala Piky 430/26 160 00 Praha 6 Czech Republic

Constituency

Constituency Type
Research & Education

Country of Constituency
Czech Republic

ASNs, Domains, IP ranges
2852
48091

acad.cz
ces.net
cesnet-ca.cz

Description of Formal Constituency
CESNET-CERTS is the CSIRT team of CESNET, association of legal entities, the Czech Republic National Research and Educational Network. Its constituency covers the whole network called CESNET2, i. e, all IP addresses within the AS2852 autonomous system.

Forenzní laboratoř

- Speciální jednotka pro CESNET-CERTS **https://flab.cesnet.cz**
- 2011: start
- 2014: spuštění prvních služeb

- Poskytované služby (nadstavbové)
  - Penetrační testy
  - Zátěžové testy
  - Testy sociálního inženýrství („phishingové testy“)
  - Provoz služby Phishingator

Další jednotky v CESNET

- 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

Bezpečnostní služby CESNET

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 páteří 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	
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	

Strategie v oblasti zajištění provozu a obrany sítě

- 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)

Bezpečnostní monitoring a obrana

- **FTAS (Flow Trafic 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!

Strategie obrany proti DDoS

- 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, síťaři, FTASaři
  3. **útok je detekován** (strojově, případně jinak), **ale vzhledem k jeho charakteru nelze bezpečně aplikovat (riziko false-positives) účinou automatickou eliminaci**

     ==> uživatele informujeme v závislosti na analýze útoku - primární notifikace -> CSIRT, síťaři, FTASaři)
  4. **útok není detekován ani přímo ani nepřímo** - tzn. nevíme o něm – v tomto případě nemůžeme ani informovat

Bezpečnostní monitoring a obrana

- **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

Scanování sítě

- Cílem je
  - „legálně“ dělat to, co jiní dělají běžně ;-)
  - vytvoření DB provozovaných služeb/zařízení
  - identifikace kompromitovaných/zranitelných zařízení
- Stav scanování
  - síťové rozsahy CESNET – v plném rozsahu
  - síťové rozsahy připojených organizací – na žádost
- Pracujeme na
  - provozních podmínkách a webové prezentaci
  - obchodním modelu
  - zakomponování do reportingu
- Nástroje
  - Sner
  - Auror
  - Nessus (možno také zapůjčit licenci)

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

cesnet certs

Hledat

- 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.

Auror Home Results Statistics About

Results: 201131, Open Ports: 789, SSL/TLS results: 666, IPs scanned: 5720

Host	Favicon	Netnames	Open ports	SSL results
monitoring.eidas.cesnet.cz		CESNET-VIRTUAL	443	A
dsw5.vm.cesnet.cz		CESNET-VIRTUAL2	443	M
mdx.eduid.cz		CESNET-VIRTUAL	25, 443	A T
mcuc2.cesnet.cz		CESNET-6WEBCON-BRNO, CESNET-WEBCON-BRNO	443, 5061	F F F F
dsa2.eduid.cz		CESNET-6ANY2	443	A+
ocsp4.cesnet.cz		CESNET-VIRTUAL2	443	M
perun-api.e-infra.cz		CESNET-VIRTUAL, CESNET-6VIRTUAL	443, 636	A+ A+ B B
ejp-rd-dev1.vm.cesnet.cz		CESNET-VIRTUAL2	443	A
hedgedoc.du.cesnet.cz		CESNET-VIRTUAL, CESNET-6VIRTUAL	443	B B
perun-eosc-federation-stg.vm.cesnet.cz		CESNET-VIRTUAL	443, 636	M M
tom2.cesnet.cz		CESNET-BB1	443	A+
temaotl.vm.cesnet.cz		CESNET-DC	443	T
connect-ng-meet.cesnet.cz		CESNET-VIRTUAL2	443	B
czmuims01.ops.egi.eu		CESNET-VIRTUAL	443	M

cesnet certs

Hledat

- O NÁS
- HLÁŠENÍ INCIDENTU
- SLUŽBY
- PROJEKTY
- SPOLUPRÁCE
- ČASTÉ DOTAZY
- ODKAZY
- DOKUMENTY

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 šifrovacich 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.

Scanování sítě

- Cílem je
  - „legálně“ dělat to, co jiní dělají běžně ;-)
  - vytvoření DB provozovaných služeb/zařízení
  - identifikace kompromitovaných/zranitelných zařízení
- Stav scanování
  - síťové rozsahy CESNET – v plném rozsahu
  - síťové rozsahy připojených organizací – na žádost
- Pracujeme na
  - provozních podmínkách a webové pr
  - obchodním modelu
  - zakomponování do reportingu
- Nástroje
  - Sner
  - Auror
  - Nessus (možno také zapůjčit licenci)

Má 193.84.32.0/20 zájem ?

Sběr dat ...

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

Zdroje dat (interní i externí)

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

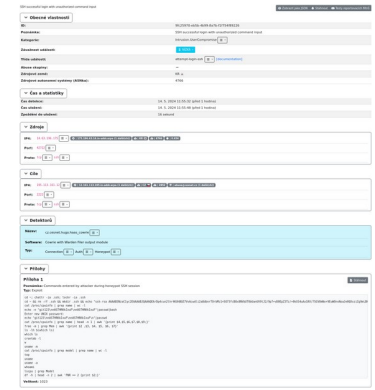

Shadowserver

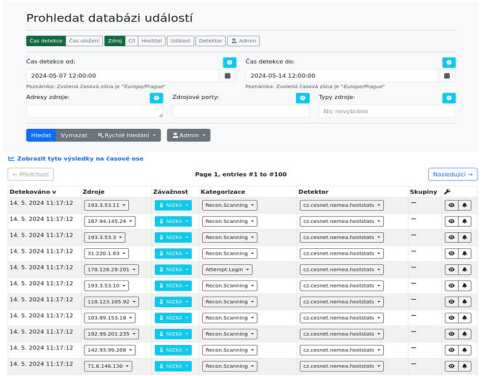
cesnet ... zpracování a distribuce dat

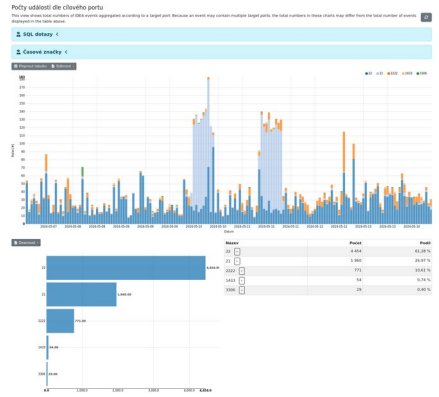
mentat

e-mail report
abuse@czu.cz

www GUI







cesnet

mentat

- 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“
- ...

sec-op@cesnet.cz

Projekty z oblasy sběru, analýzy a sdílení dat ...

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 roztřídí podle zdrojů útoku
    - Jednotlivé organizace dostanou specifický report o svých IP

Projekty z oblasy sběru, analýzy a sdílení dat ...

NERD Network Entity Reputation Database

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?

csirt-forum @ cesnet.cz

- 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

Situational Awareness

- 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**

ČZU
–
7 respondentů

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 útočníkovi 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 útočníkovi je prostřednictvím procházení
cest umožněno omezené čtení souborů a vykonání DoS útoku [1].
CWE: 22 [3]

CVE-2024-2829 (CVSS 7.5) - neautentizovanému vzdálenému útočníkovi 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 útočníkovi 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 útočníkovi 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.

Služby Forenzní laboratoře

- Analýza událostí

https://flab.cesnet.cz

- Plošné testy e-infrastruktury na zranitelnosti
  - heartbleed, memcached, shellshock ...

- Penetrační testy
- Zátěžové testy
- Testy sociálního inženýrství („phishingové testy“)
  - na míru zákazníkovi

- Zadání --> Testy --> Zpracování --> Závěrečná zpráva & workshop
  - přehled provedených testů
  - zhodnocení výsledků (nálezů)
  - doporučení nápravných opatření
  - školení pro uživatele

FT1/FT2 školení

- 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: 11.6.-12.6. 2024*
- *FT2: 13.6.-14-6. 2024*

sluzby@cesnet.cz

The Catch

- 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 2023
  - stále možné „hrát“
  - https://www.thecatch.cz/

... Kdo si hraje, nezlobí :-)...

cesnet

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

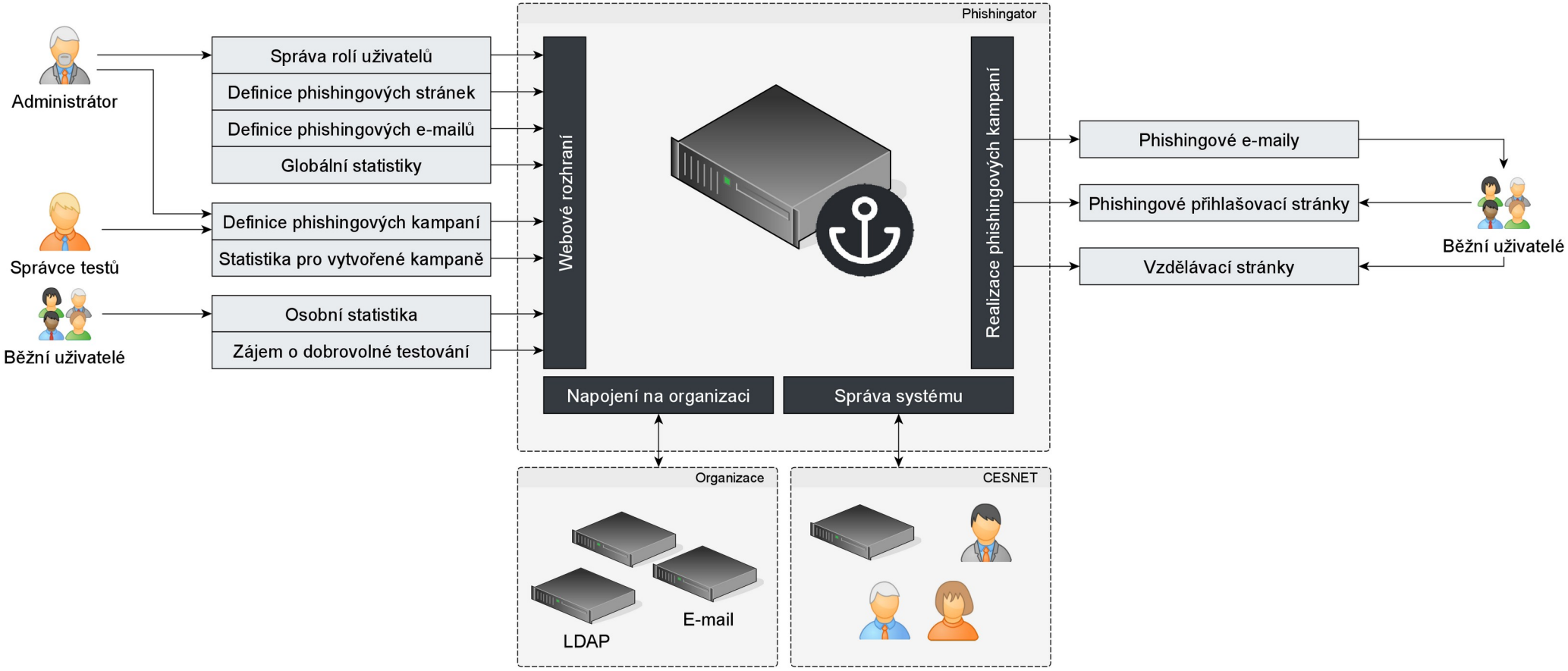
Služba Phishingator

- 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

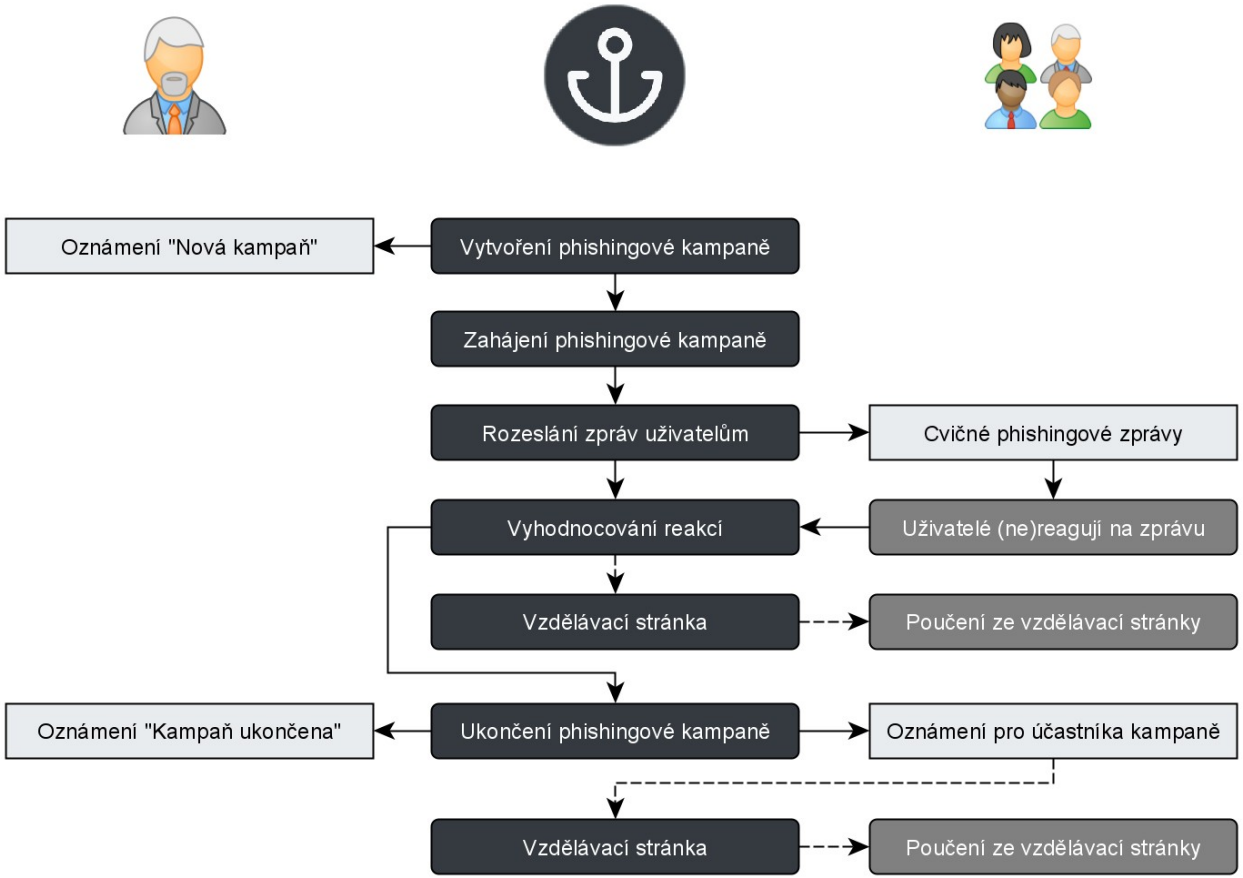
Služba Phishingator



Průběh phishingové kampaně

- **Phishingová kampaň** = podvodný e-mail + podvodná stránka + adresáti

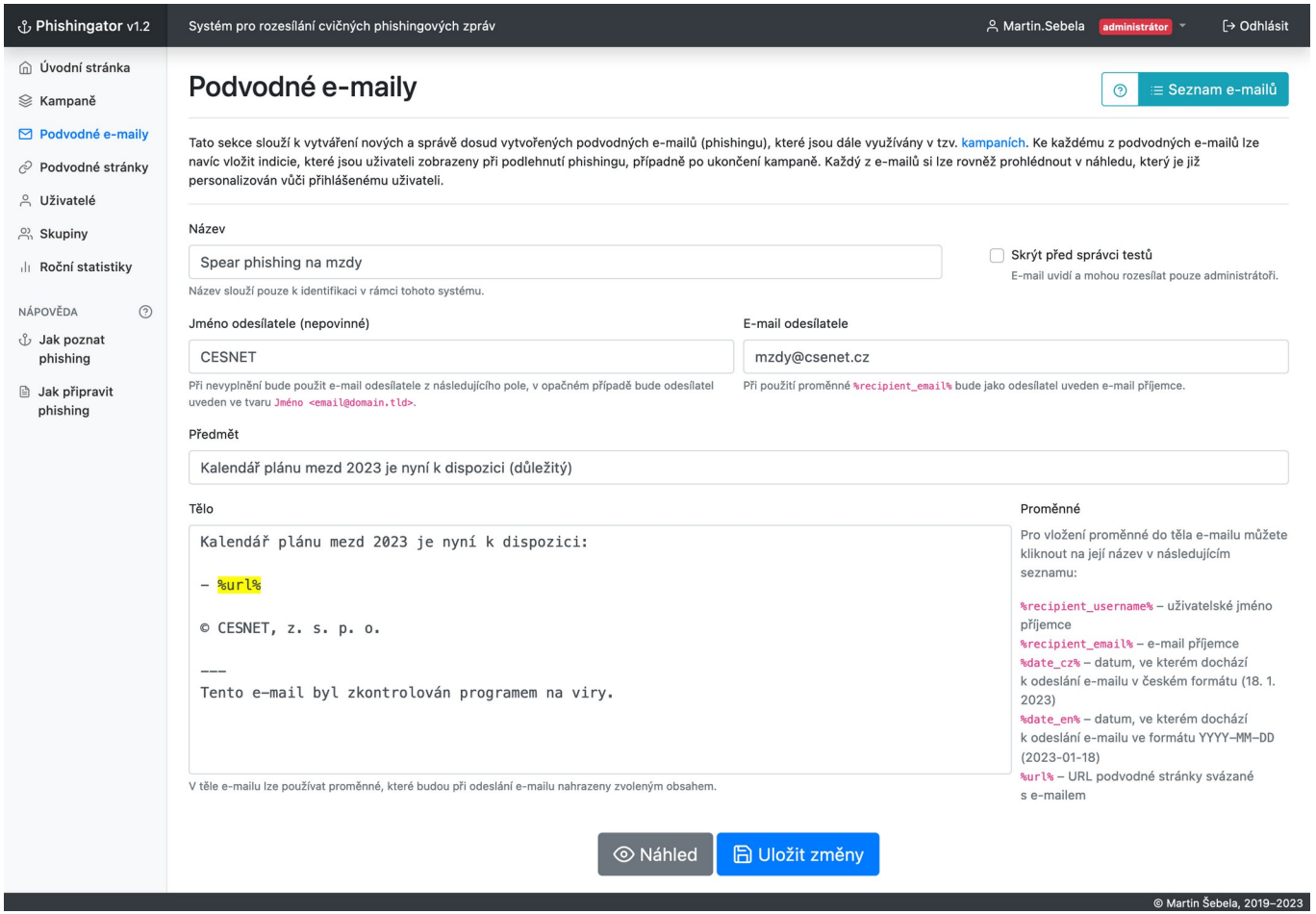
1. Vytvoření **e-mailu** a **indicií**
2. Nákup podvodné **domény**
3. Vytvoření **podvodné stránky** (šablona + URL)
4. Rozeslání e-mailů **konkrétním příjemcům**
5. Sledování **reakcí příjemců**
6. Automatická **zpětná vazba pro příjemce**



Z pohledu administrátora – vytvoření phishingu

- Vytvoření **cvičného podvodného e-mailu**

1. **Jméno** odesílatele
2. **E-mail** odesílatele
3. **Předmět**
4. **Parametrizované tělo** e-mailu
5. Možnost personalizace



Z pohledu administrátora – vytvoření phishingu

Od: CESNET <mzdy@csenet.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

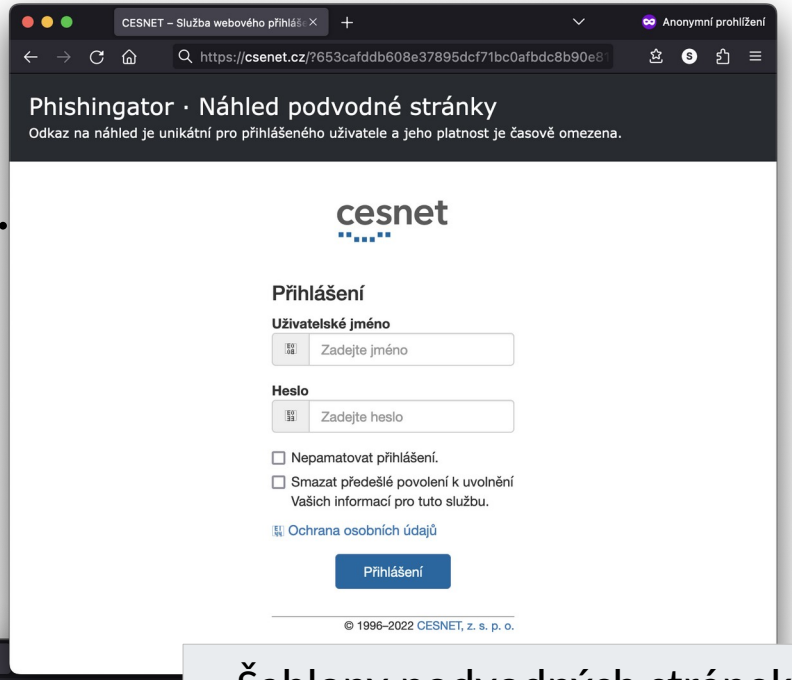
Indicie (3) k rozpoznání tohoto phishingu

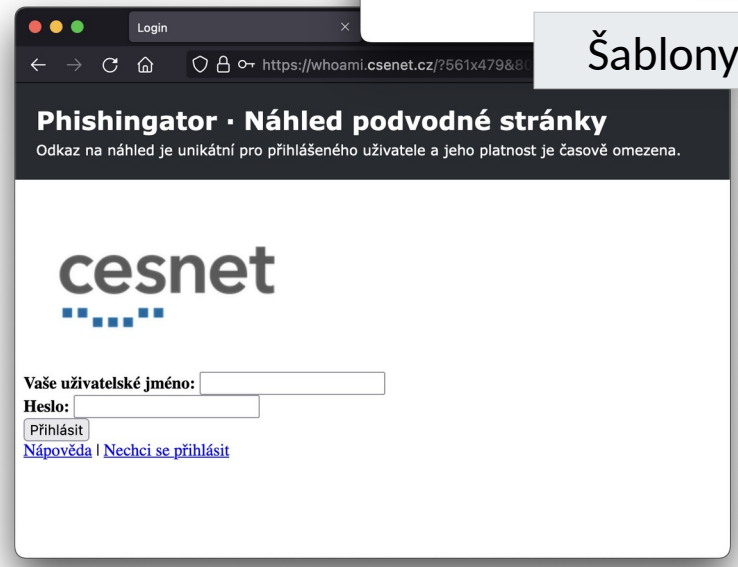
Indicie (podezřelý řetězec)	Nadpis	Popis (nepovinné)	
%sender_email%	E-mail odesílatele	E-mail odesílatele nemá s organizací CESNET nic společného.	Smazat / Uložit změny
%url%	Podezřelá URL	Nejedná se o oficiální doménu CESNET.CZ, ale o snahu útočníka napodobit její	Smazat / Uložit změny
zkontrolován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

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

Z pohledu administrátora – vytvoření podvodné stránky

- 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)

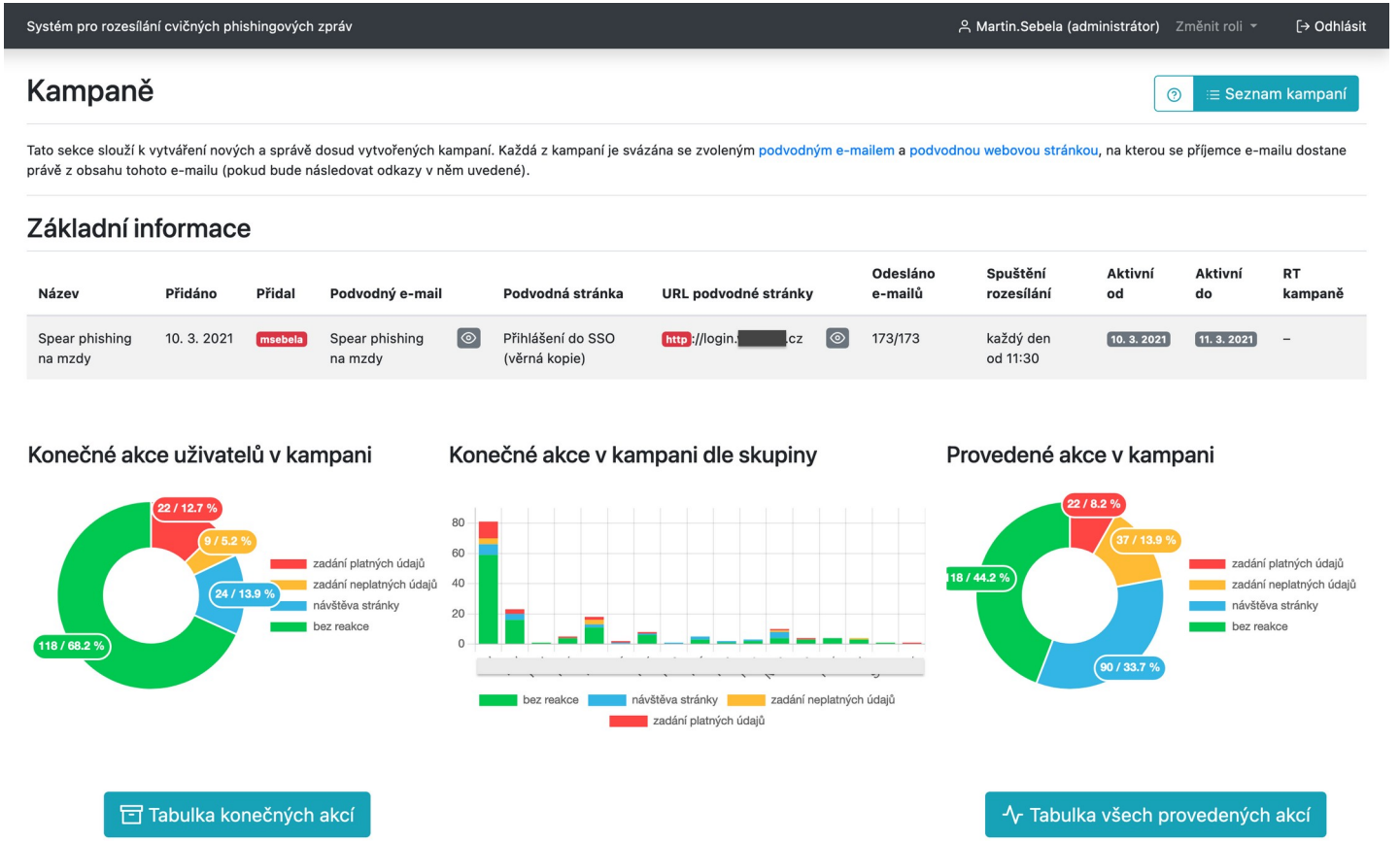




Šablony podvodných stránek

Z pohledu administrátora – výsledky kampaně

- 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)



Z pohledu administrátora – výsledky cvičného phishingu (příklad)

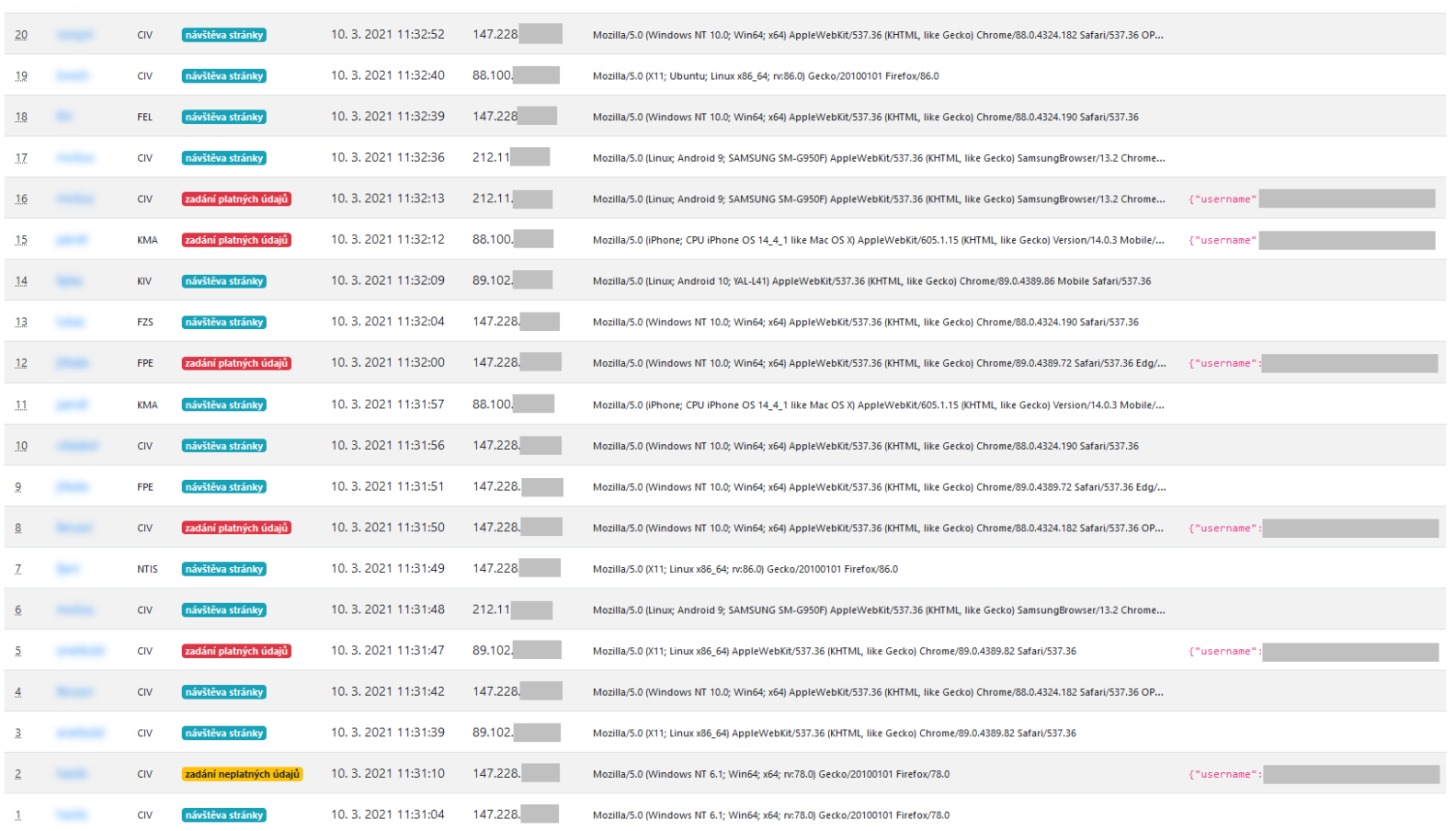
- **Rozesláno 173** vybraným **zaměstnancům**
  - Napříč fakultami a dalšími odděleními
  - Získáno 22 platných identit během 2 hodin

- **Všechny reakce** příjemců:
  - **Bez reakce (118)**
  - **Návštěva podvodné stránky (24)**
  - Vyplnění **neplatných** přihlašovacích údajů **(9)**
  - Vyplnění **platných** přihlašovacích údajů **(22)**

Z pohledu administrátora – vytvoření phishingu

- **173** odeslaných **e-mailů**

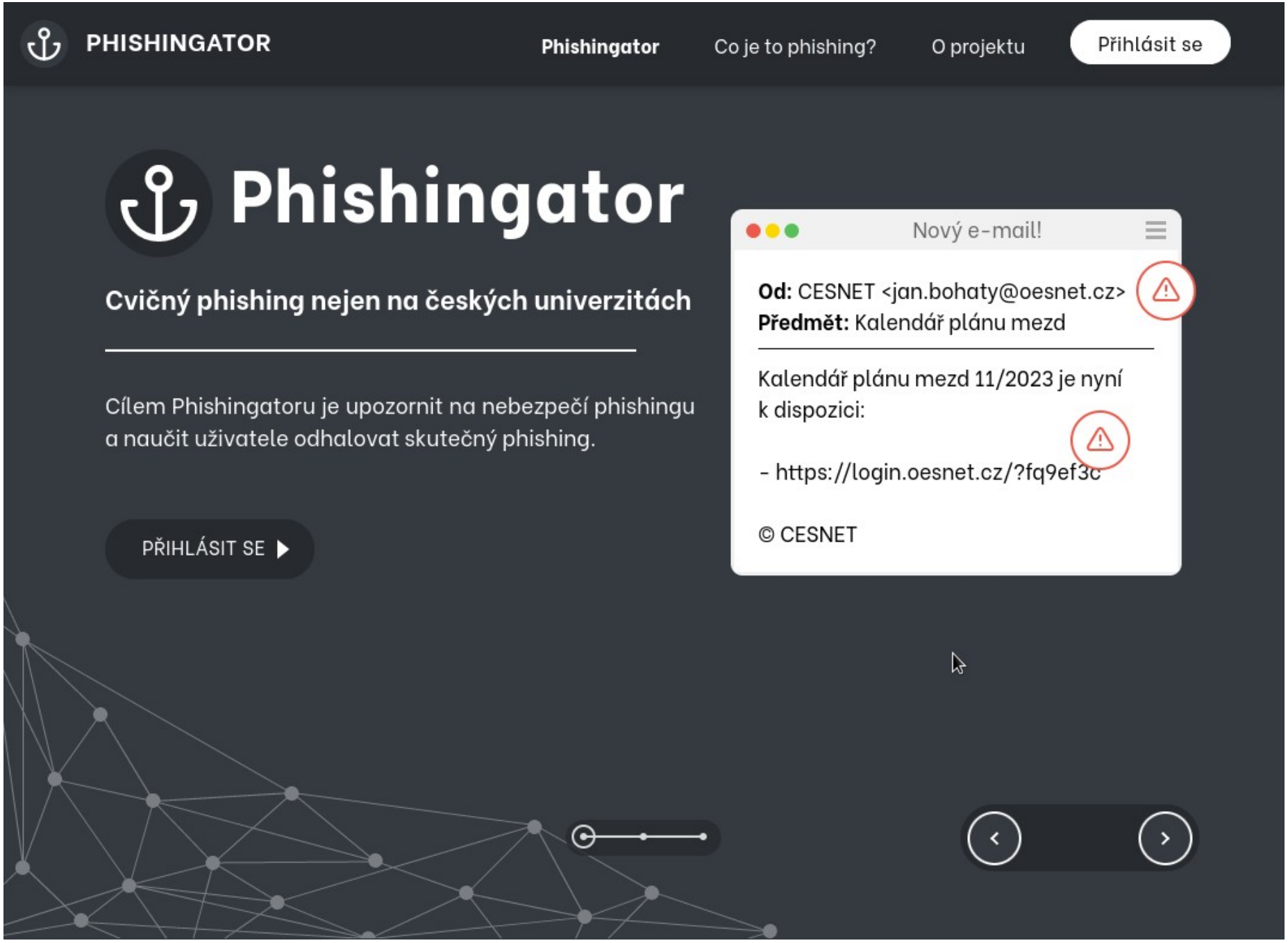
1. **11:30** – odeslání cvičného phishingu
2. **11:31** – první návštěva podvodné stránky
3. **11:31** – první získaná identita
4. **11:35** – získáno 8 platných identit
5. **do 12:00** – získáno 15 platných identit



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	

cesnet

https://phishingator.cesnet.cz



Projekt Hugo

(aneb sdílejme data)

Honeypoty

- Zachytáváme nezvané hosty.
- Umístíme návnadu (např. otevřené SSH či SQL) na strategickou pozici v síti.
  - A pak čekáme ...

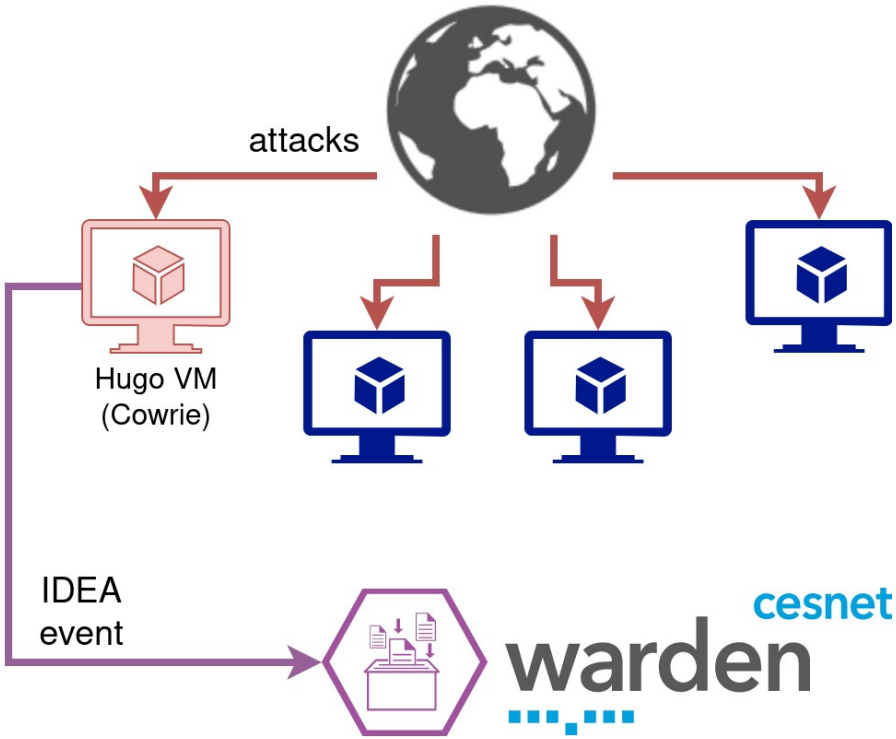
Dionaea Muscipula – Mucrow (CC-BY-SA 3.0)

- Každé připojení je platná událost.
  - Kdo se pokouší připojit?
  - Omyl, nebo záměr?
  - Pokusy o prolomení hesla? Jaké údaje použili?
  - O co se pokusí, jakmile dostanou přístup?

Užitečné info z honeypotů

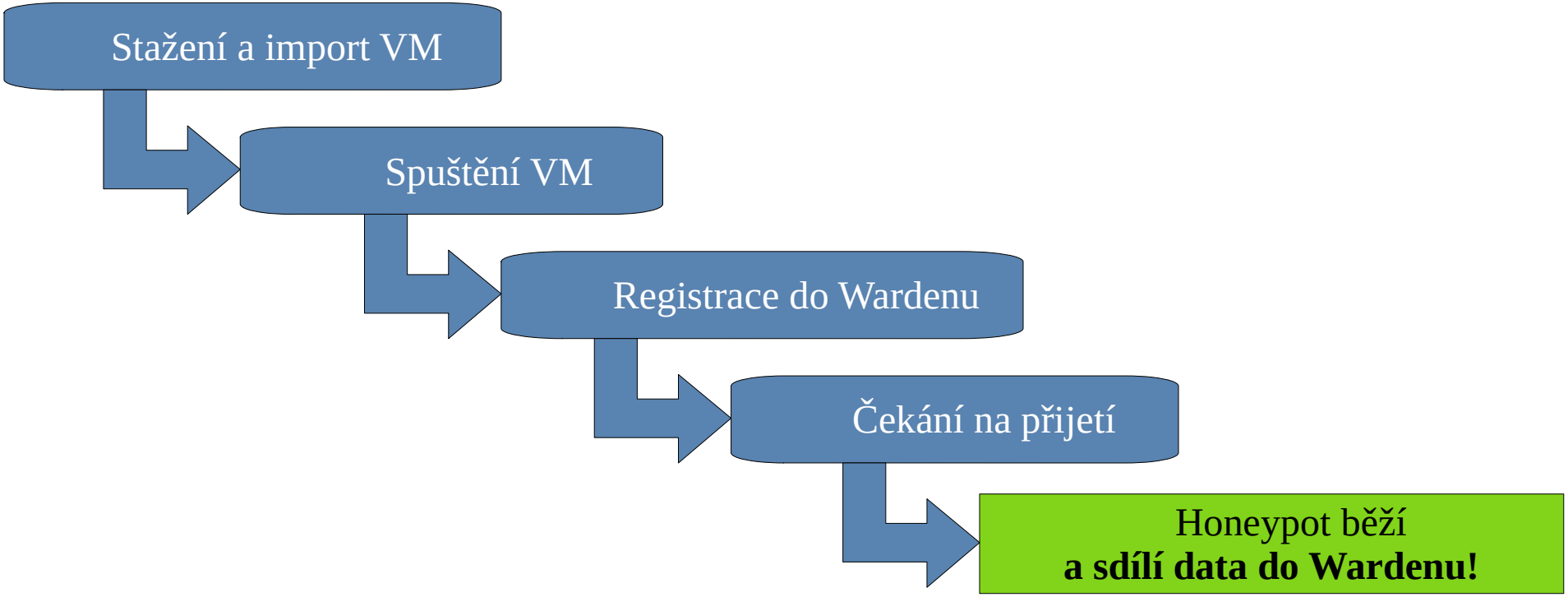
- Zdrojové IP adresy
- Použité přihlašovací údaje
- Příkazy
- Stažený malware a jeho URL,
- atp. atp.
  - → ochrana sítě (blocklist známých zdrojů útoku)
  - → zdroj pro reputační databáze (např. .cesnet.cz)
  - → korelace dat v rámci výzkumných činností
  - → detekce škodítek ve vlastní síti

Cíle HUGO



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

Ideální případ registrace



Cowrie, dionaea

- Cowrie
  - SSH, Telnet
  - Fiktivní “Debian” – některé unixové příkazy fungují (ping, wget), jiné částečně (ifconfig, dmesg), další předstírají (apt-get)
  - –

Cypraea caputserpentis – NOAA (Public domain)

- Dionaea
  - SMB, MSSQL, (T)FTP, MySQL, HTTP(S), SIP
  - Emulace shellcode (libemu)
  - Emulace cmd.exe (bind/connectback)
  - P0f, Pcap – **pasivní fingerprinting útočníkova systému**
  - –

Dionaea Muscipula – Mucrow (CC-BY-SA 3.0)

Zapojte se!

Máte zajímavý zdroj dat?

A jste ochotni data sdílet?

Ozvěte se nám!

sec-op@cesnet.cz

Akce, vzdělávání

- 6. 2. 2024: Seminář o bezpečnosti (každý rok)
- 27.2. - 28.2. FT1
- 29.2. - 1.3. FT2
- 16. května 2024 – pracovní skupina CESNET CSIRT
- 6. června: Seminář o Ipv6
- xx. červen – pracovní skupina pro oblast ISMS
- 11.6. - 12.6. FT1
- 13.6. - 14-6. FT2
- říjen 2024: The Catch

Pracovní skupina CESNET CSIRT

čtvrtek 16. 5. 2024 10:00 → 15:00 Europe/Prague

Telehouse

Popis: Registrace na pracovní skupinu CESNET CSIRT určenou pro výměnu zkušeností v oblasti bezpečnosti a diskusi aktuálních bezpečnostních témat. Pracovní skupina se bude konat 16. května 2024 od 10:00 (s předpokládaným koncem okolo 15:00), účast je možná osobně v sídle CESNETu (budova Telehouse), a nebo videokonferenčně.

Registrace: *Registroval/a jste se do této události.* 81 Zobrazit podrobnosti

Účastníci: A [redacted]

10:00 → 12:00 **Dopolední program**

- Systém Mentat (Pavel Kácha, Radko Krkoš)
  - https://mentat-hub.cesnet.cz, nástroj pro automatizovaný reporting kybernetických bezpečnostních událostí
  - Co v něm nebylo a teď je
  - Co jste od něj vždycky chtěli a on to umí - správa zranitelností
- Zkušnosti se zpracováním dat a zpojením do systému Warden z VŠE (L. Pavlíček)
- Vulnerability Assesment/Management (Radko Krkoš)
  - reporty do csirt-forum@
  - reporty do Wardenu
  - skenování síťových infrastruktur (SNER, Auror)
- Diskuse

12:00 → 13:00 **Oběd**

13:00 → 15:00 **Odpolední program**

- ZoKB: Cesta od (kybernetické bezpečnostní) události ke (kybernetickému bezpečnostnímu) incidentu (v CESNET)
- HUGO - honeypot v krabici
- URL evaluator - co s načatým URL
- Diskuse

Bezpečnostní služby CESNET

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 páteří 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	
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	

Služba Antispam Gateway

- Anti-spam/vir ochrana příchozího mailového provozu
  - nepřijetí (odmítnutí) nevyžádané pošty
  - doručení ohodnocených zpráv na koncový poštovní server
  - rovněž *záložní poštovní server* (*relay)*
- Výhody
  - odpadají náklady na údržbu vlastní antispam ochrany
  - vysoká spolehlivost (robustní řešení)
  - více domén -> více zkušeností -> **větší účinnost**
  - váš e-mail provoz je „v bezpečí“
  - nedochází k zásahu do těla přenášené zprávy
  - ***vyhovuje nařízením NÚKIB***
- Prostředí
  - ... možnost konfigurovat prostředí domény
  - přístup k provozním logům
  - grafické rozhraní, dostupná statistika

Kontakty

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

CESNET a ZoKB

- 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

ZKB - § 3 – CESNET (stav od ledna 2015)

§ 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 systém[illegible] podle písmene d),

c) správce a provozovatel informačního syst[illegible]itické infor[illegible]truktury,

d) správce a provozovatel komunikačního systém[illegible]ury,

e) správce a provozovatel významného informačn[illegible]

f) správce a provozovatel informačního systému [illegible] správcem nebo provozovatelem podle písmen[illegible]

g) provozovatel základní služby, pokud není spr[illegible] písmene f), a

h) poskytovatel digitální služby.

Významná síť:
~ síť s přímým propojením do globálního internetu

Telia Sonera (dříve)
Telecom Italia Sparcle (aktuálně)

ZKB - § 3 – CESNET (stav od září 2017)

§ 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 inf ury,

d) správce a provozovatel komunikačního systému kritick y,

e) správce a provozovatel významného informačního sy

f) správce a provozovatel informačního systému základ správcem nebo provozovatelem podle písmene c)

g) provozovatel základní služby, pokud není s vcem nebo provoz telem podle písmene f), a

h) poskytovatel digitální služby.

Infrastruktura MetaCentra a Datových úložišť

KBU a KBI

- 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

ZKB - § 3 – CESNET (stav od 27. 1. 2022)

§ 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 zvládání 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.

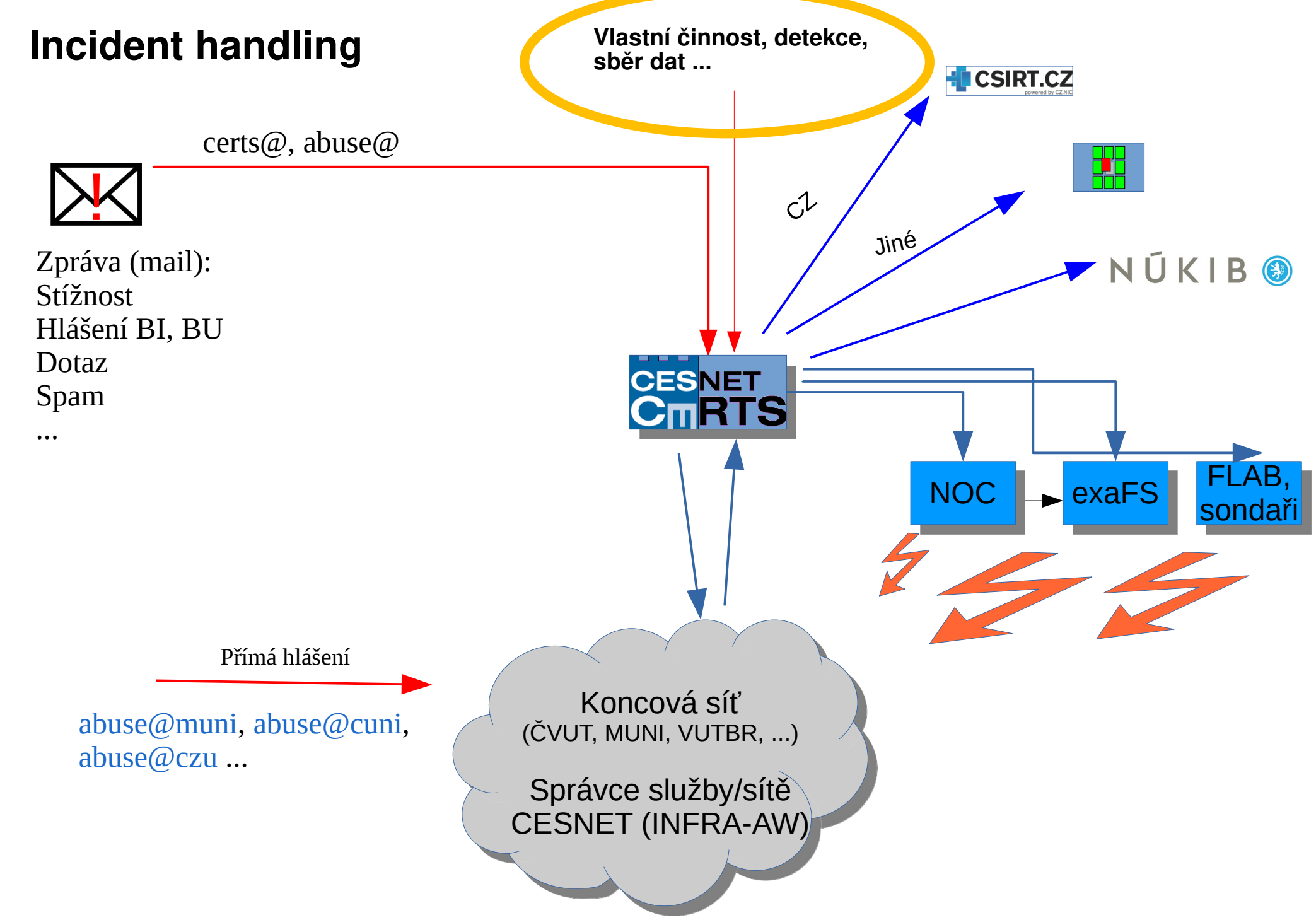
Koordinace řešení bezpečnostních incidentů		
Zpracování přijatých hlášení bezpečnostních incidentů a jejich předání Účastníkovi	CESNET-CERTS, Pracovní dny 9 – 17	2 hod
Kooperace a asistence s řešením bezpečnostních incidentů.	CESNET-CERTS, Pracovní dny 9 – 17	Pracovní dny 9 – 17, nebo na základě dohody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

CESNET-CERTS

- 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



cesnet

AS2852

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

Prostředky

- 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

Co z toho má připojená organizace

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

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz