Efektivní sdílení informací

Zpracování dat z bezpečnostních nástrojů & reporting

CESNET, z. s. p. o.

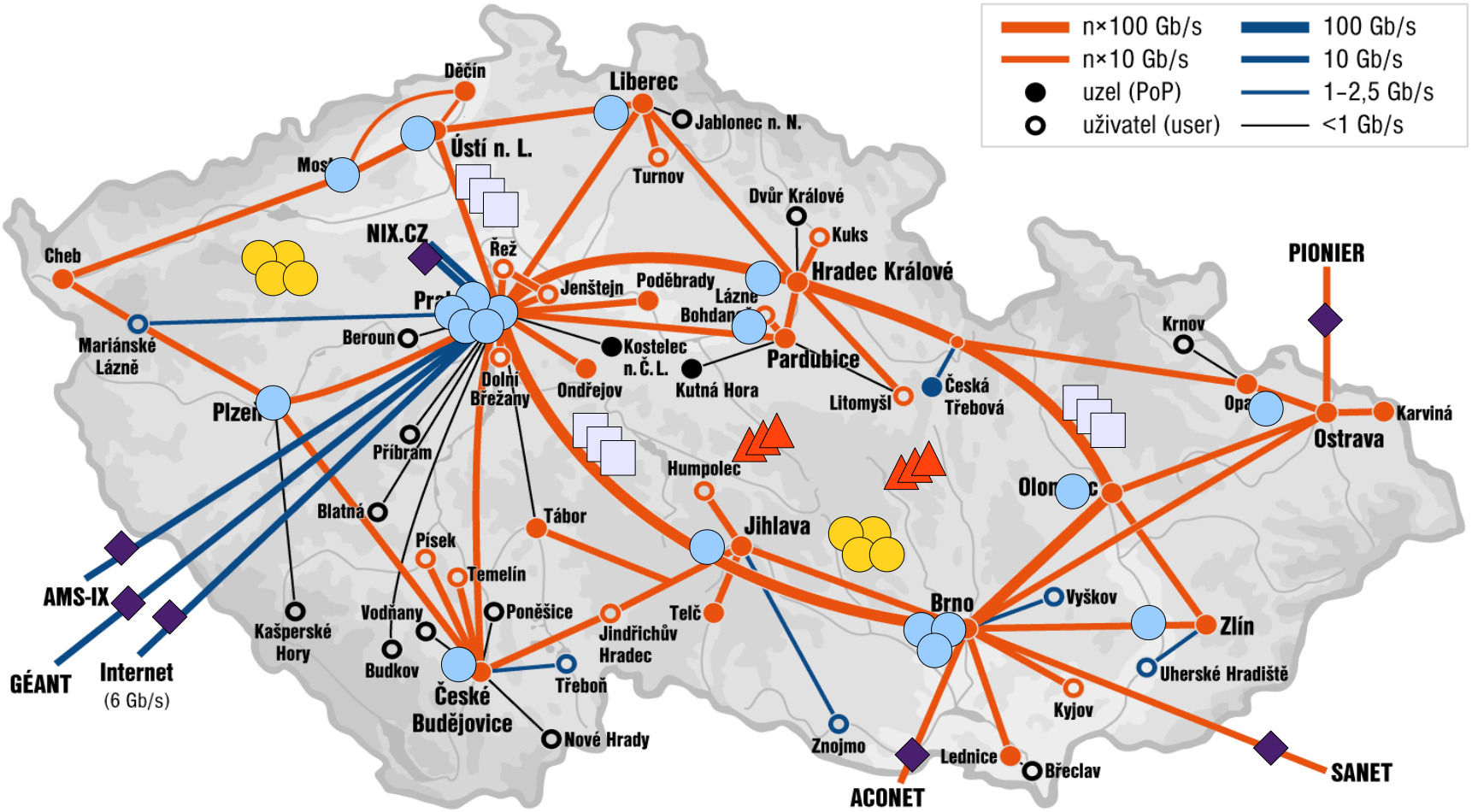
Andrea Kropáčová
andrea@cesnet.cz

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

- Provozuje síť národního výzkumu a vzdělávání CESNET2
- Založen v roce 1996
- Připojeno 27 členů (české VŠ, AV ČR) a cca 280 dalších organizací
- K e-infrastruktuře CESNET se mohou připojit instituce, které se zabývají
  - vědou, výzkumem, vývojem včetně uplatnění jejich výsledků v praxi
  - experimentálním vývojem nebo inovacemi v průmyslu i jiných oborech
  - šířením vzdělanosti, kultury a prosperity
  - vybrané sítě veřejné správy
- Hlavní cíle:
  - výzkum a vývoj informačních a komunikačních technologií
  - budování a rozvoj e-infrastruktury CESNET určené pro výzkum a vzdělávání
  - podpora a šíření vzdělanosti, kultury a poznání
- 2011 – 2015
  - ***Projekt Velká infrastruktura CESNET***

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

CESNET2



- HW accelerated probes
- large scale (backbone-wide) flow based monitoring (NetFlow data sources)
- Honey Pots
- IDS, IPS, tar pit based systems, etc..
- SNMP based monitoring

Jak jsme začali ...

- Správci v připojených sítích provozují bezpečnostní nástroje
  - IDS, honeypoty, IPS, sondy, syslog, netflow ...
    - Sledování stavu sítě, zdraví sítě
    - Hledání kompromitovaných zařízení
    - Detekce útoků, anomálií provozu

- DILEMA – Co s daty, pro která nemám použití?
  - Zahodit?
    - To je škoda a plýtvání
  - Reportovat?
    - To je zase moc pracné, s potenciálem přejít do diskuse, dožadování se pomoci, dalších informací atd...

Jak jsme začali ...

- Správci v připojených sítích provozují bezpečnostní nástroje
  - IDS, honeypoty, IPS, sondy, syslog, netflow ...
    - Sledování stavu sítě, zdraví sítě
    - Hledání kompromitovaných zařízení
    - Detekce útoků, anomálií provozu

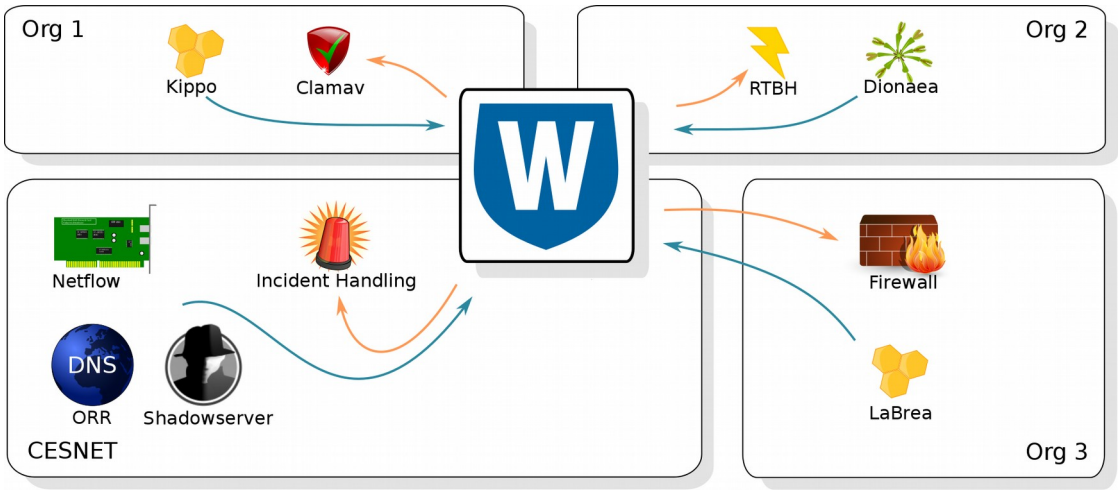
- DILEMA – Co s daty, pro která nemám použití?
  - Zahodit?
    - To je škoda a plýtvání
  - Reportovat?
    - To je zase moc pracné, s potenciálem přejít do diskuse, dožadování se pomoci, dalších informací atd...

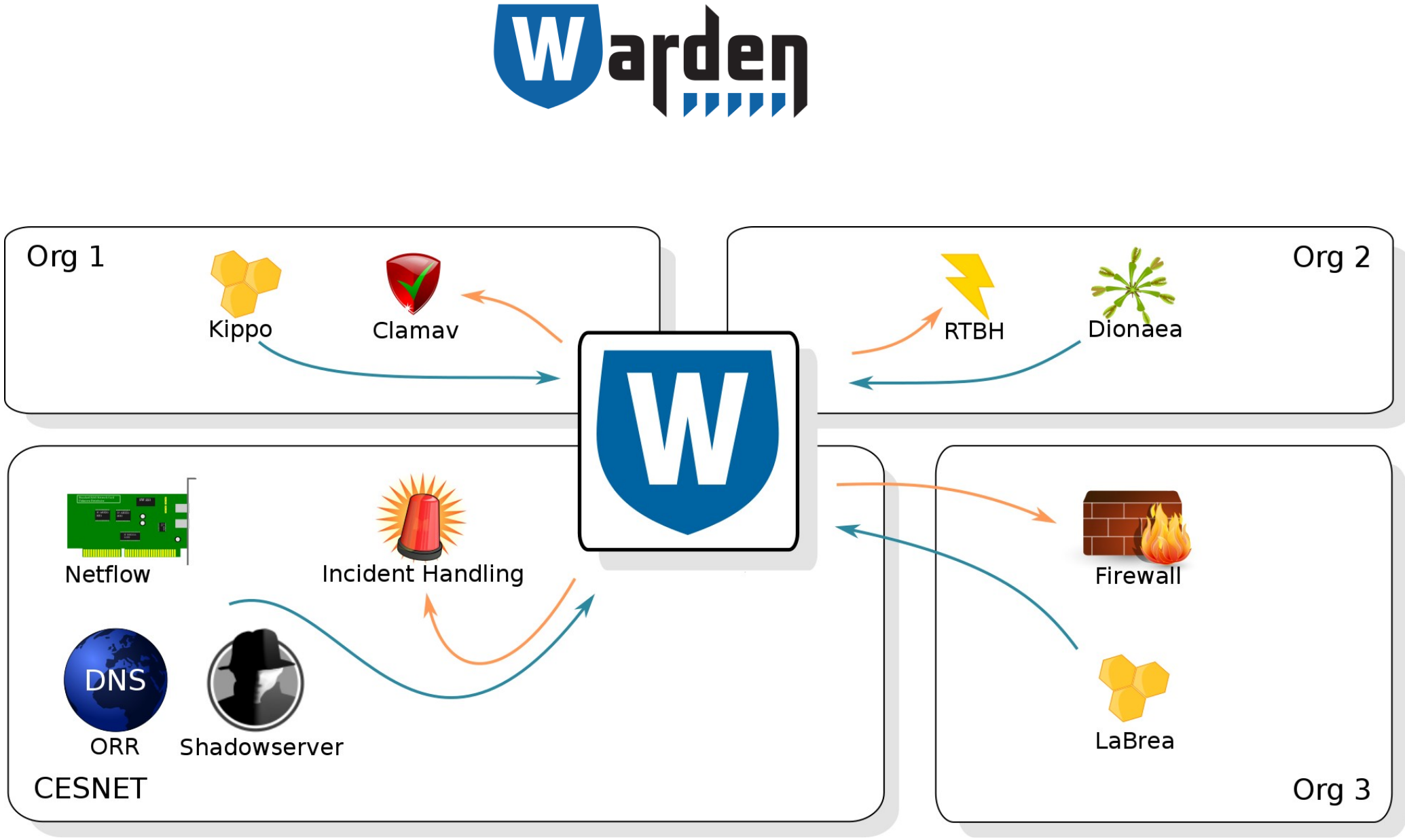
Sdílet!

- Ale – jak? A co formát? Obsah? Protokol? Klasifikace? Politika?

Warden

- Systém pro efektivní sdílení informací o bezpečnostních incidentech
- Client/server architektura (transport, ne naskladnění dat)
- Komunitní přístup (aka „budujme bezpečnost společně“)
  - Tvoje data jsou dostupná celé Warden komunitě
  - Data celé komunity jsou dostupná Tobě
- Zasílající a odebírající klienti
- Událost (event)
- Bezpečnost
  - X509
  - encryption
  - “sanity” checks
  - peer review
- IDEA formát




Warden
Org 1
Kippo
Clamav
Org 2
RTBH
Dionaea
Netflow
Incident Handling
Firewall
DNS
ORR
Shadowserver
LaBrea
CESNET
Org 3

Lesson learned I

Připojené organizace nemají dostatek lidských zdrojů na využití otevřeného komunitního přístupu k systému Warden

=

nedokáží data odebrat a zpracovat si je.

Lesson learned I

Připojené organizace nemají dostatek lidských zdrojů na využití otevřeného komunitního přístupu k systému Warden

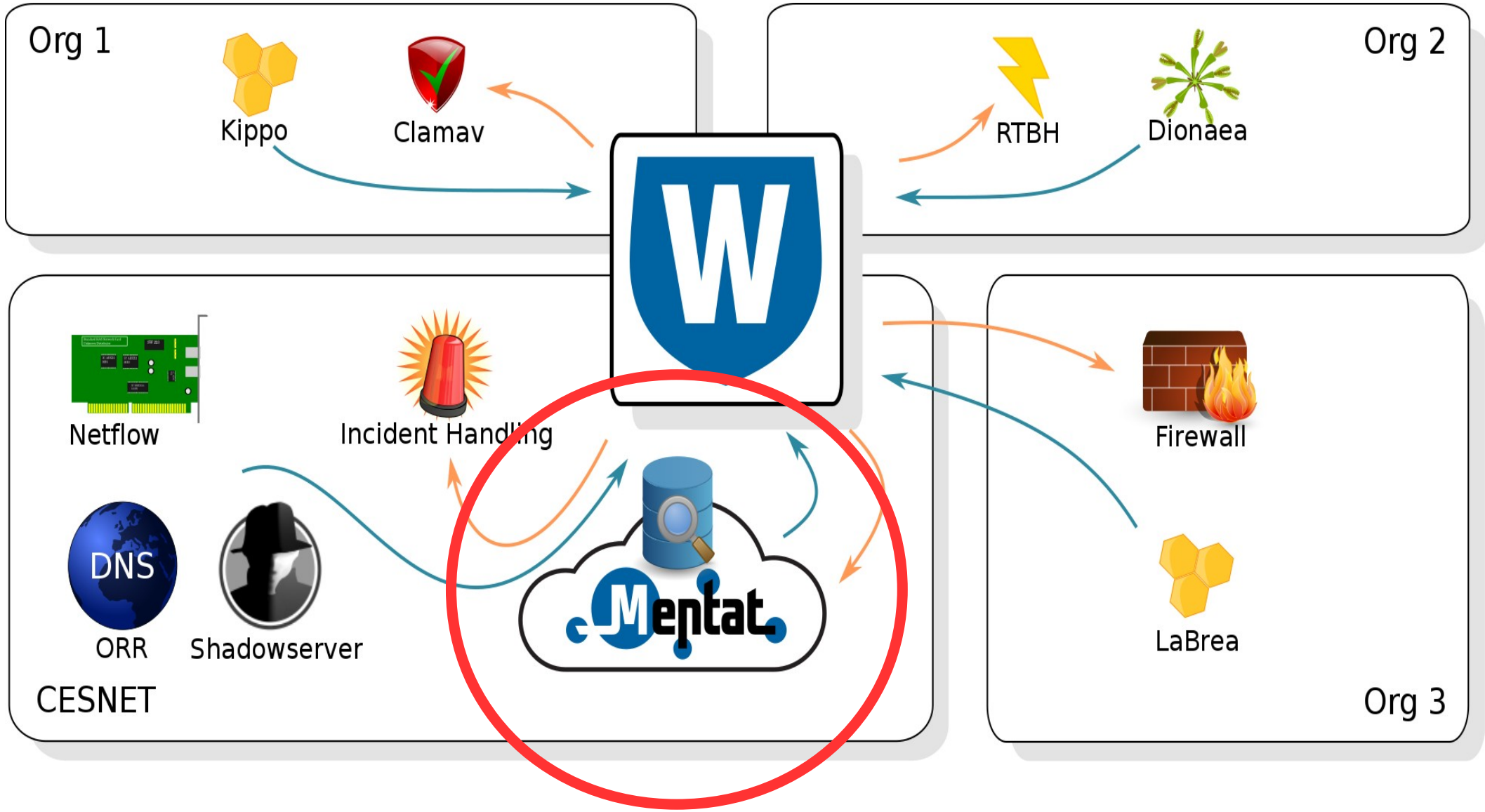
=

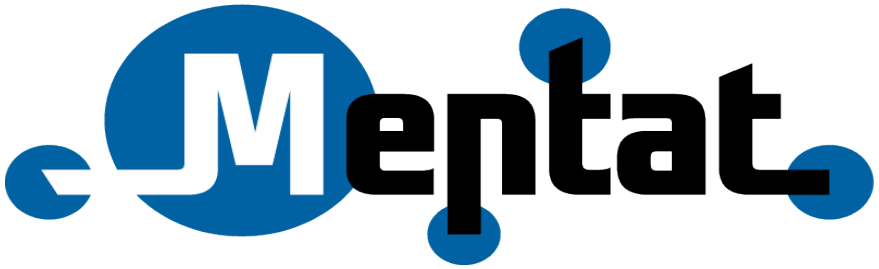
nedokáží data odebrat a zpracovat si je.

Ale chtějí tato data získávat, data jsou užitečná

=

je nutné je správcům doručit zpracovaná.


Org 1
Kippo
Clamav
Org 2
RTBH
Dionaea
Netflow
Incident Handling
Firewall
DNS
ORR
Shadowserver
Mentat
LaBrea
CESNET
Org 3



- Z hlediska architektury Warden je ***odebírající klient***
- SIEM
- Skladiště informací
- Zpracovává data (události) z Warden a od třetích stran (N6, ShadowServer, ...)
- Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
- Reporty zasílá do koncových sítí (abuse@...)

Report message

Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) související s Vaším rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

[1] Stroje na následujících IP adresách fungují jako otevřené DNS resolvery a mohou být zneužity pro masivní DDoS útoky (Open DNS Resolver):

* Analyzer: X2
* Popis: Open DNS Resolver
* Kategorie: Vulnerable.Config

IP	Čas	# událostí
[redacted]	2015-11-11 13:20:35 - 2015-11-13 03:29:49	1

* Celkem 1 událost, 1 unikátní IP adresa

Více informací o tomto typu události lze nalézt na adrese:
https://csirt.cesnet.cz/cs/services/x2

(Více provozních informací lze nalézt v příslušné části přiloženého souboru)

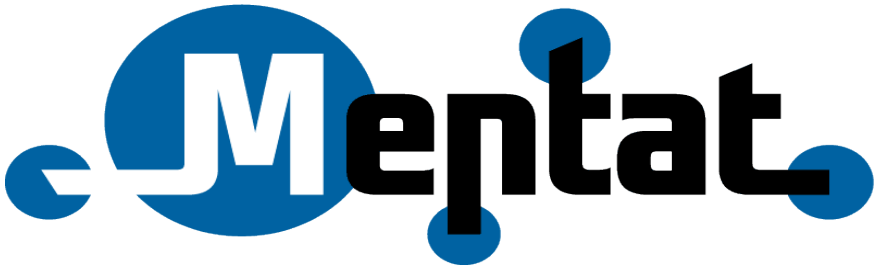
UPOZORNĚNÍ: Uvedené časy jsou okamžiky údajné detekce. Některé služby a systémy (zejména externí, jako např. ShadowServer) bohužel občas posílají informace o událostech i s několikadenním zpožděním.

Kompletní dostupné provozní informace k jednotlivým událostem lze nalézt v příslušných částech jednoho z přiložených strojově zpracovatelných souborů. V závisloti na Vašich preferencích můžete použít formát JSON, nebo CSV. Doporučujeme použít formát JSON, protože data v něm obsažená jsou úplná.

Lesson learned II

... reakce od příjemců reportů ...

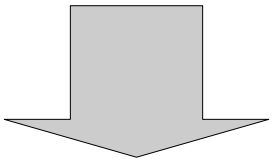
- Málo informací, nevíme co s tím máme dělat.
- Chci mít možnost report strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Tyto informace nechceme vůbec, odebíráme je přímo od zdroje.
- Data od třetích stran mají různou kvalitu
  - **Nechci!** Co si počít s informací, že IP a.b.c.d je na blacklistu X?
  - **Chci!** Informace, že IP a.b.c.d. je na blacklistu X je užitečná.
- NAT, FW, DHCP …
- Velké sítě s hierarchií správy (Uni→Fakulta→ Katedra → Pracoviště)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to reportujete znova? Včera jsem to vyřešil.



- SIEM
- Skladiště informací
- Zpracovává data (události) z Warden a od třetích stran (N6, ShadowServer, ...)
- Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
- Reporty zasílá do koncových sítí (abuse@...)
- Podpůrný nástroj CESNET-CERTS a bezpečnostní týmy připojených organizací
- **WWW rozhraní pro správce z koncových sítí**
  - **Možnost ovlivnit jak a kdy reporty dostávat a co chci dostávat**
  - **Detaily reportů**
  - **Globální dahsboardy**
  - **Statistiky**

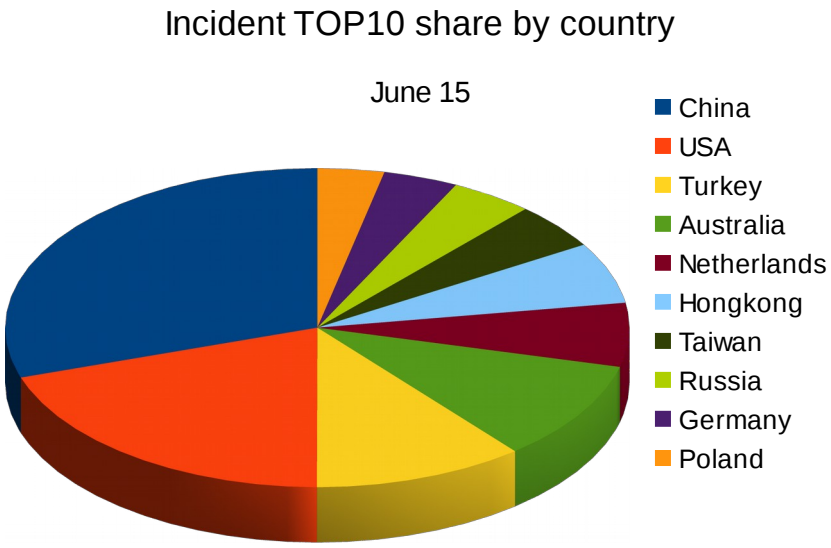
Statistiky

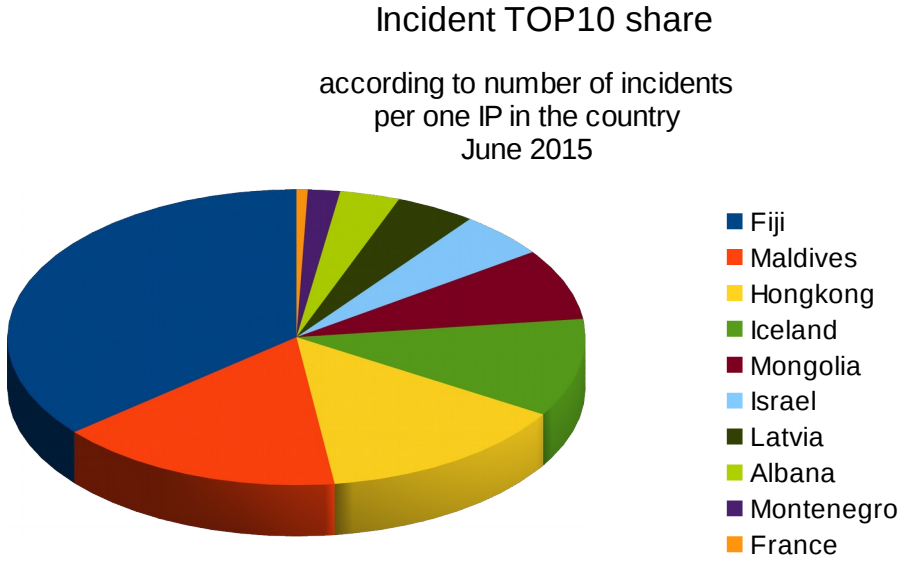
- Warden
  - 17 zasílajících klientů (zdrojů dat)
  - cca 1,1 mil událostí za den



- Mentat
  - cca 60 reportů denně, cca 300 týdně (na cca 320 připojených organizací)

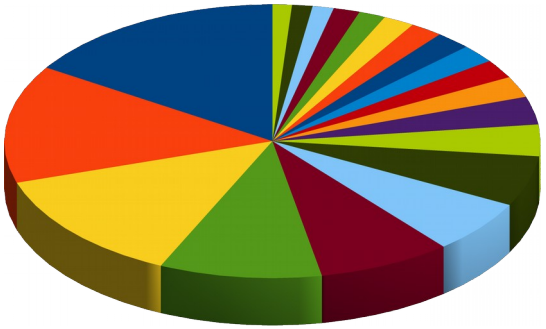
Statistiky


Incident TOP10 share by country
June 15
China
USA
Turkey
Australia
Netherlands
Hongkong
Taiwan
Russia
Germany
Poland


Incident TOP10 share
according to number of incidents
per one IP in the country
June 2015
Fiji
Maldives
Hongkong
Iceland
Mongolia
Israel
Latvia
Albana
Montenegro
France

TOP 20 incident share by AS

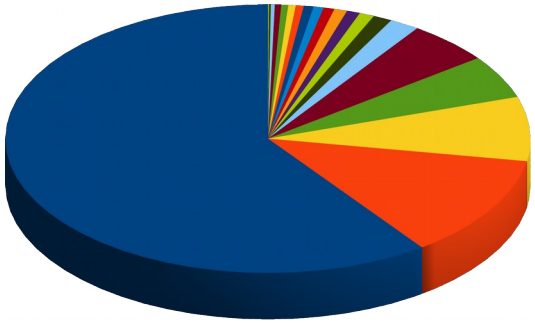
June 2015



- Chinanet CN
- Turk Telekomunikasyon Anonim Sirketi TR
- SoftLayer Technologies Inc. AU
- CNCGROUP China169 Backbone CN
- CHINANET jiangsu province backbone CN
- Ecatel LTD NL
- Data Communication Business Group TW
- CariNet, Inc. US
- SoftLayer Technologies Inc. HK
- Hurricane Electric, Inc. US
- HOT NET LIMITED HK
- PlusServer AG DE
- University of Michigan US
- Jazz Telecom S.A. ES
- Biznes-Host.pl sp. z o.o. PL
- MCI Communications Services, Inc. d/b/a Verizon Business US
- 013 NetVision Ltd. IL
- Contabo GmbH DE
- CNCGROUP IP network China169 Beijing Province Network CN
- Abovenet Communications, Inc US

TOP 20 incident share by AS

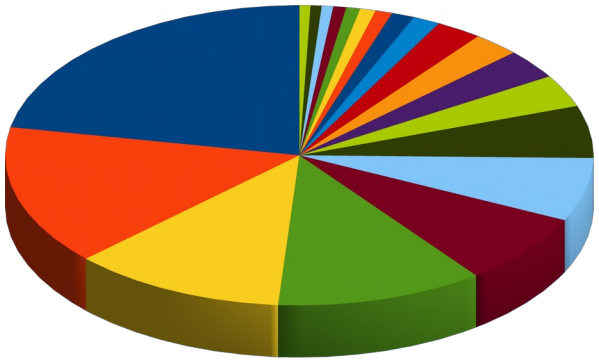
according to number of incidents
per one IP from AS
June 2015



- HOT NET LIMITED
- Przedsiebiorstwo Uslug Specjalistycznych ELAN mgr inz.
- Nikultsev Aleksandr Nikolaevich
- Ecatel LTD
- DELORIAN Internet Services Artur Grabowski
- Nagravision SA
- DataClub S.A.
- PE Voronov Evgen Sergiyovich
- Livenet Sp, z o.o.
- WEDOS Internet, a.s.
- Storm Systems LLC
- MediaServicePlus Ltd.
- Black Fox Limited
- CariNet, Inc.
- Iradeum Trading Ltd.
- DataWagon LLC
- DDNET SOLUTIONS SRL
- HOSTKEY B.V.
- Hosting Solution Ltd.

Incident TOP20 share by Czech ISP

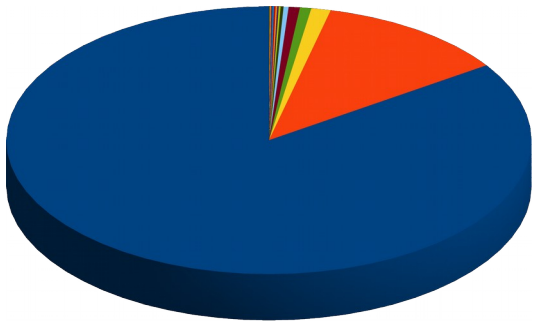
June 2015



- WEDOS Internet, a.s.
- FDCservers.net
- O2 Czech Republic, a.s.
- OVH SAS
- Liberty Global Operations B.V. (UPC ČR)
- CESNET z.s.p.o.
- METRONET s.r.o.
- Media a.s.
- itself s.r.o.
- Vodafone Czech Republic a.s.
- PODA a.s.
- T-Mobile Czech Republic a.s.
- CD-Telematika a.s.
- Starnet s.r.o.
- T-Mobile Czech Republic a.s.
- CoProSys a.s.
- ISP Alliance a.s.
- WIA spol. s.r.o.

Incident TOP20 share by Czech ISP

according to number of incidents
per one IP address from AS
June 2015



- WEDOS Internet, a.s.
- FDCservers.net
- Pe3ny Net s.r.o.
- Ladislav Rudolf
- MAXTEL s.r.o.
- Vodafone Czech Republic a.s.
- Druzstvo EUROSIGNAL
- FreeTel, s.r.o.
- Brno University of Technology
- Futurenet ISP s.r.o.
- CoProSys a.s.
- Tlapnet s.r.o.
- Humlnet s.r.o.
- Marek Smutny
- WMS s.r.o.
- CESNET z.s.p.o.
- Dial Telecom, a.s.
- TTNET Czech Republic
- INTERNET CZ, a.s.
- VSHosting s.r.o.

Lesson learned III

... současnost & budoucnost ...

- Umíme data dostat na jedno místo, zpracovat a doručit.
- **ALE!**
  - Sdílet syrová *primární* data nestačí!
  - Data získaná z bezpečnostních nástrojů jedné sítě nestačí!
  - Sdílet na úrovni jedné sítě (ISP/organizace) nestačí!

Lesson learned III

... současnost & budoucnost ...

- Umíme data dostat na jedno místo, zpracovat a doručit.
- **ALE!**
  - Sdílet syrová *primární* data nestačí!
  - Data získaná z bezpečnostních nástrojů jedné sítě nestačí!
  - Sdílet na úrovni jedné sítě (ISP/organizace) nestačí!
- **Proč?**
  - Primárních dat je moc.
  - Některé problémy nemusíme zaznamenat.
  - Chybí souvislosti, nevidíme celkový obraz.

Co dál ...

- Nové a další zdroje primárních dat v síti CESNET2
- Obohacení dat
- Inteligentní analýzy, korelace
- Sdílení dat a informací na národní a mezinárodní úrovni
- *Nové a další zdroje primárních dat mimo síť CESNET2*
- *Nové zdroje od tzv. třetích stran*

Zapojení partnerů

- Odebírání dat
  - Přímo (konektor, vlastní zpracování, naskladnění a využití)
  - Formou e-mail reportu

- E-mail reporty
  - Ze systému Mentat
  - Data příslušející Vaší organizaci (constituency)
  - Bezpečnostní události, kde zdrojem je IP adresa Vaší constituency

Zapojení partnerů

- Zasílání dat
  - Provozujete bezpečnostní nástroj a jste ochotní data sdílet?
    - Jaká data?
    - Za jakých podmínek? Částečná anonymizace? Jen data relevantní pro CESNET2?
  - Máte vhodné místo v síti pro umístění nějakého bezp. nástroje?

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz