Efektivní sdílení informací o bezpečnostních událostech

Pavel Kácha <ph@cesnet.cz>

LinuxDays 2015

CESNET

- Založen v roce 1996
- Členové

  25 českých univerzit
  Akademie věd ČR
  Policejní akademie ČR

- Hlavní cíle

  Provoz a rozvoj sítě národního výzkumu a vzdělávání CESNET2
  Podpora vědy a výzkumu v oblasti pokročilých síťových technologií a aplikací
  Podpora a šíření vzdělanosti, kultury a poznání

www.cesnet.cz

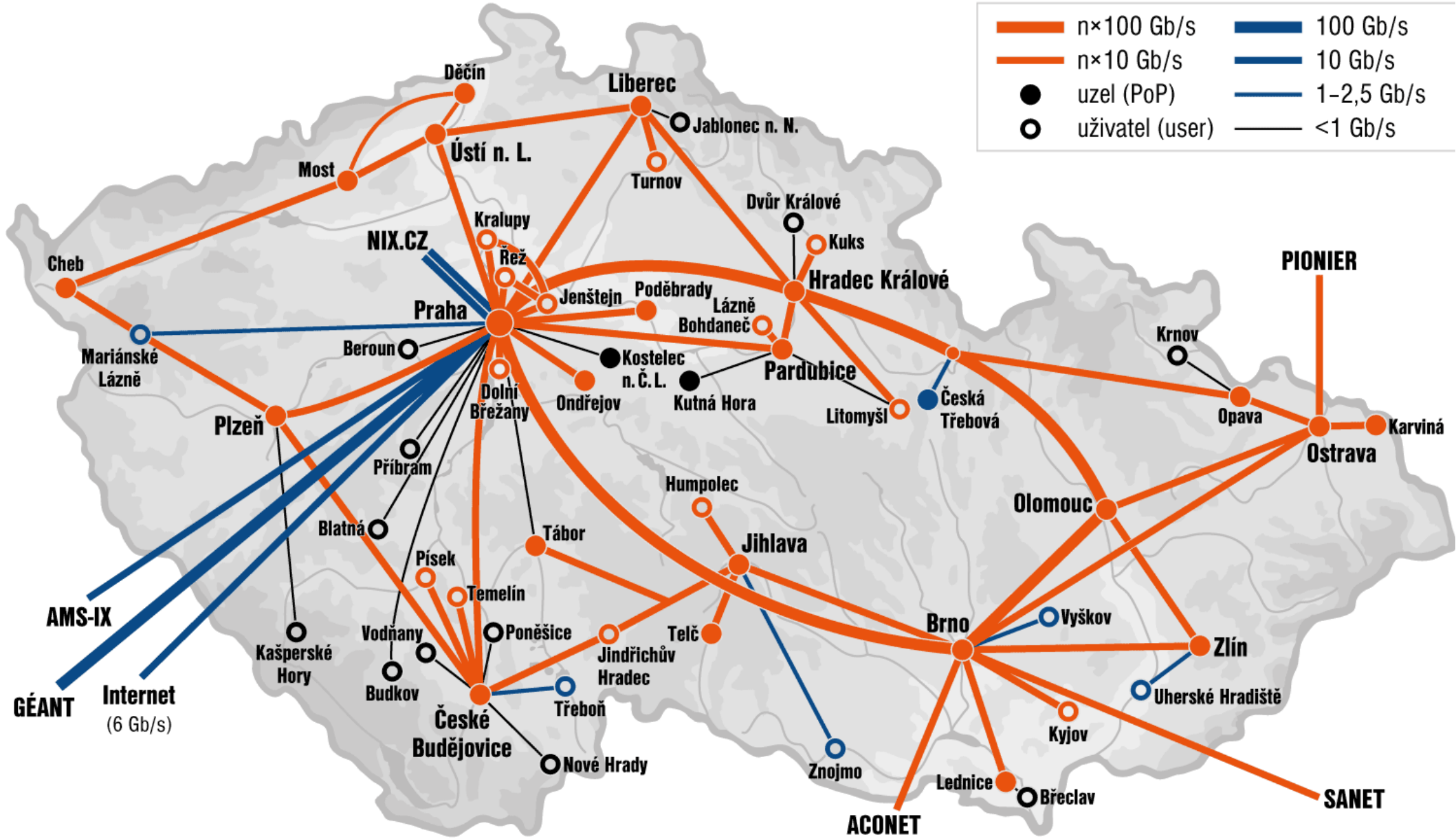
Bezpečnost

CESNET-CERTS (csirt.cesnet.cz, certs@cesnet.cz)

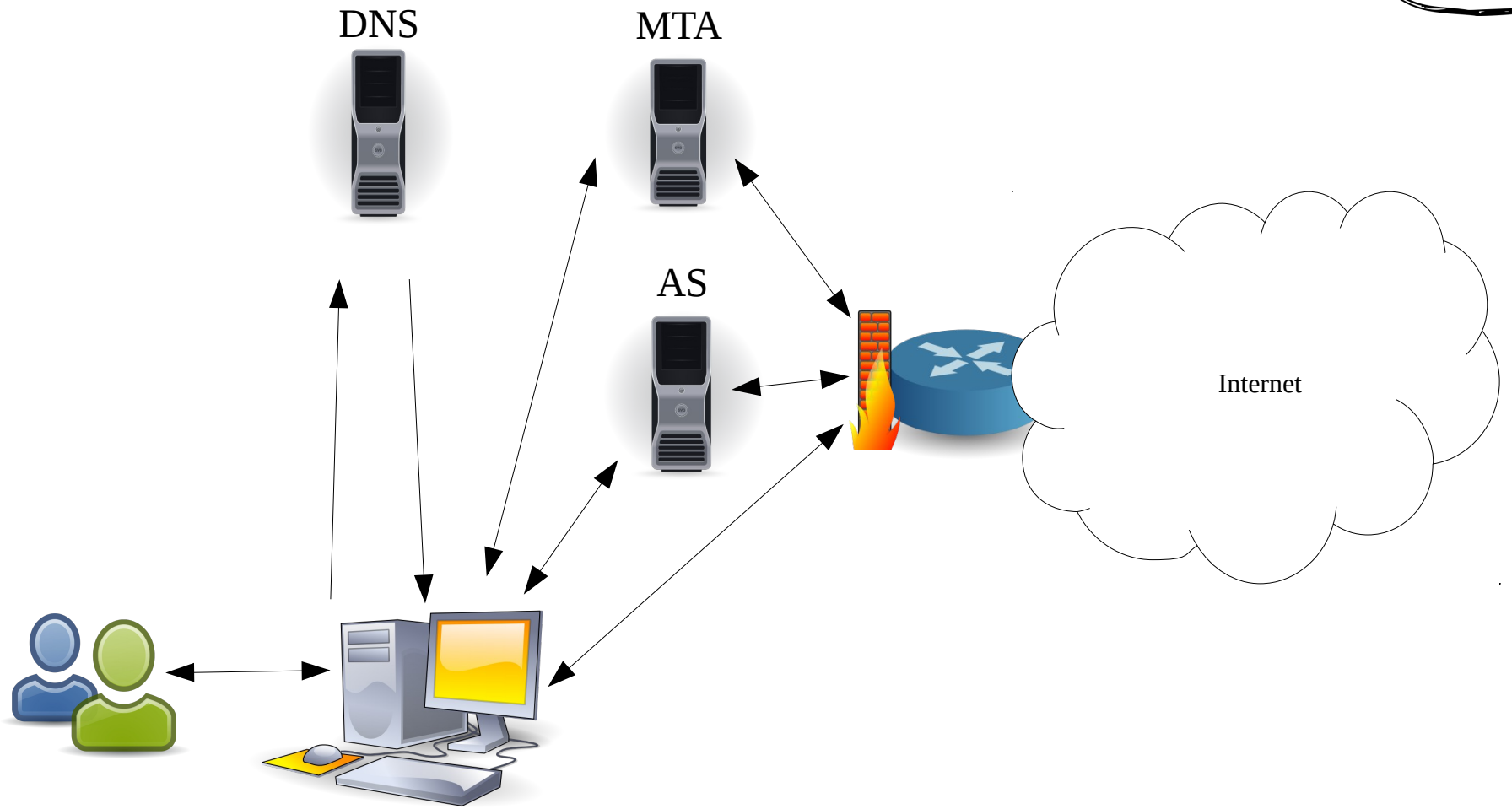
- Snaha o centrální a důvěryhodný kontaktní bod
- Řešení a koordinace BI v síti CESNET2
- Projekty pro podporu bezpečnosti

  Forenzní laboratoř
  Sledování provozu sítě
  IDS, Audit, Honeypoty
  Mentat, Warden
  Osvěta
- Spolupráce s dalšími projekty a týmy

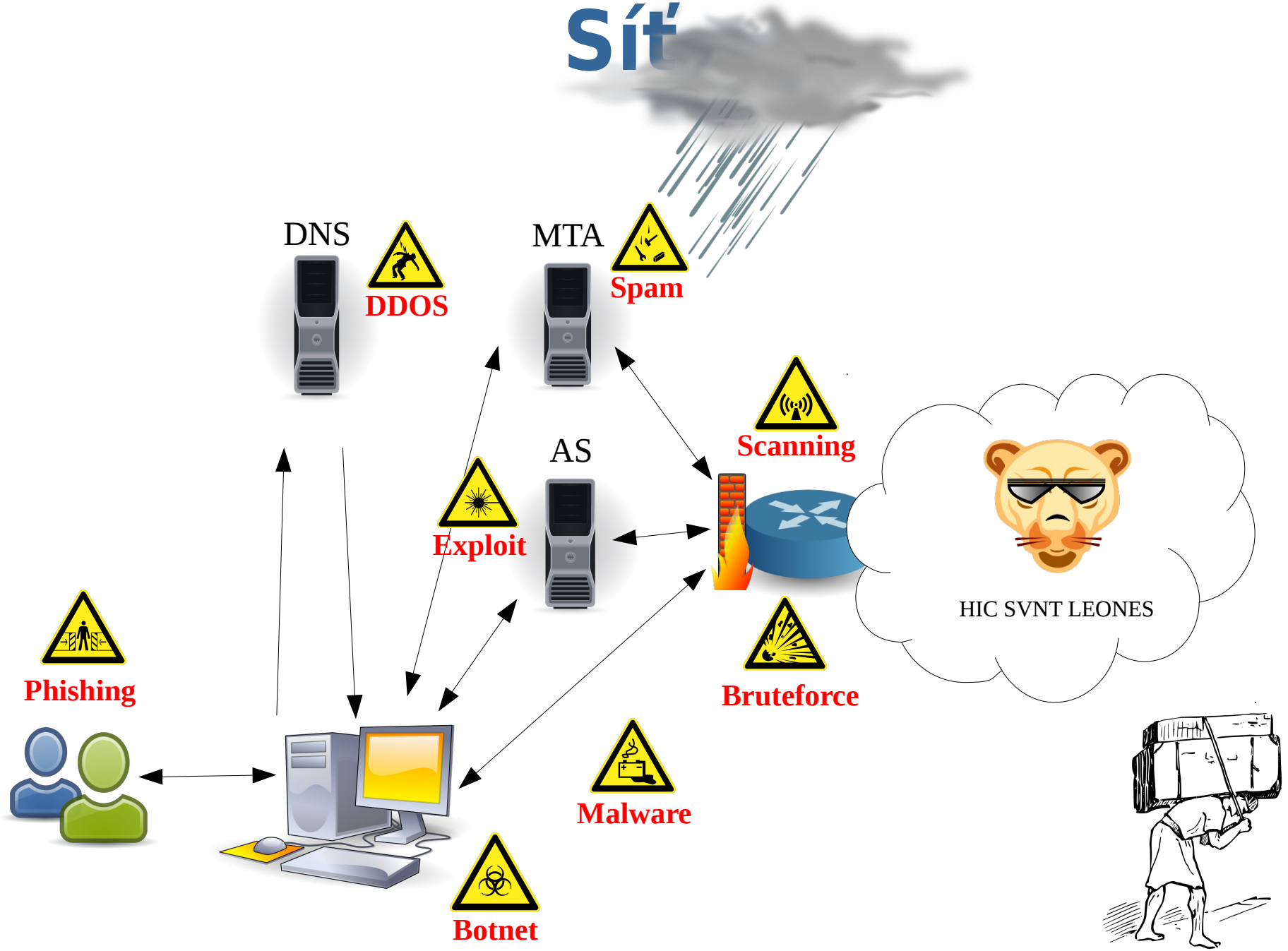
  (CSIRT.CZ, WIRT ZČU, CSIRT-MU)


n×100 Gb/s
n×10 Gb/s
uzel (PoP)
uživatel (user)
100 Gb/s
10 Gb/s
1–2,5 Gb/s
<1 Gb/s
Děčín
Liberec
Jablonec n. N.
Ústí n. L.
Most
Turnov
Dvůr Králové
Kuks
Kralupy
NIX.CZ
Řež
Cheb
Hradec Králové
PIONIER
Jenštejn
Poděbrady
Praha
Lázně Bohdaneč
Mariánské Lázně
Beroun
Krnov
Kostelec n. Č. L.
Pardubice
Dolní Břežany
Ondřejov
Kutná Hora
Česká Třebová
Litomyšl
Opava
Karviná
Plzeň
Ostrava
Příbram
Humpolec
Olomouc
Blatná
Tábor
Jihlava
Písek
Temelín
AMS-IX
Vyškov
Brno
Zlín
Vodňany
Poněšice
Telč
Kašperské Hory
Jindřichův Hradec
Budkov
Uherské Hradiště
GÉANT
Internet
(6 Gb/s)
Třeboň
Kyjov
České Budějovice
Znojmo
Lednice
Nové Hrady
Břeclav
SANET
ACONET

Síť



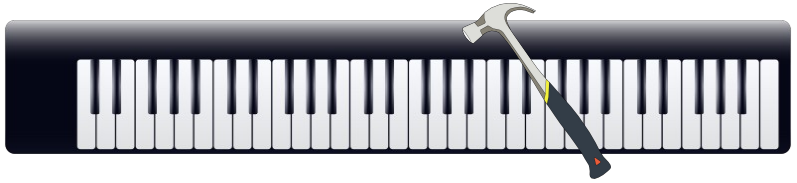
Síť


DNS
DDOS
MTA
Spam
AS
Exploit
Scanning
HIC SVNT LEONES
Bruteforce
Phishing
Malware
Botnet

Sbíráme data

Řešení problémů

Jaká práva má uživatel?
Byl požadavek předán dál?
S jakou skončil chybou?
Proč?

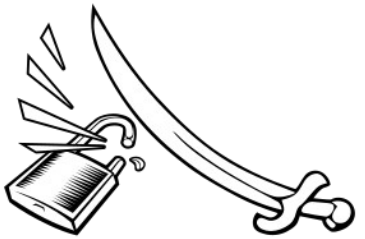


Ladění služby/sítě

Kolik požadavků v jakých okamžicích služba vyřizuje?
Na jaké cíle?
Kde je vhodné optimalizovat?
Kde jsou úzká místa?

Bezpečnost

Nejsou požadavky na službu neobvyklé?
Na konkrétní stránku? Adresu?
V neobvyklém množství? Formátu?
Nepřistupuje klient na místo, kam přístup mít nemá?



Ochrana provozovatele

„Za dětskou pornografii na serveru neneseme zodpovědnost,
neboť ji tam nahrál uživatel X v čase Y z adresy Z“


WHO WATCHES THE WATCHMEN?
BY: BATSYX

Logování

- Logová hlášení aktivních démonů
  Postfix, Bind, Apache, SSHd...
- Autentizační a autorizační záznamy
  Přihlášení ke službám, síťové autorizace (DHCP, WPA)
  Důležité akce
- Zprávy o hardware
- Události na síti
  ARP, DHCP
  Přístupy na uzavřené porty
  Anomální provoz

```
[06/Dec/2014:12:34:37 +0100]
        195.113.134.228 grey.cesnet.cz
        "GET /search?Gravity+free+download HTTP/1.1" 200 1986 "-"
        "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.14pre)
        Gecko/20101204 Ubuntu/9.10 (karmic) Namoroka/3.6.14pre"
```

```
 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
 Nov 22 15:05:58 office2 postfix/cleanup[30693]: CAF18ED0073:
        message-id=<20131122140558.GC1700@cesnet.cz>
 Nov 22 15:05:59 office2 postfix/qmgr[2599]: CAF18ED0073:
        from=<ph@cesnet.cz>, size=7206, nrcpt=1 (queue active)
 Nov 22 15:06:00 office2 postfix/smtp[31597]: CAF18ED0073:
        to=<oleg@cesnet.cz>, relay=postino.cesnet.cz[195.113.144.242]:25,
        delay=2.1, delays=1/0/1/0.11, dsn=2.0.0,
        status=sent (250 2.0.0 rAME5x59029798 Message accepted for delivery)
```

NIDS

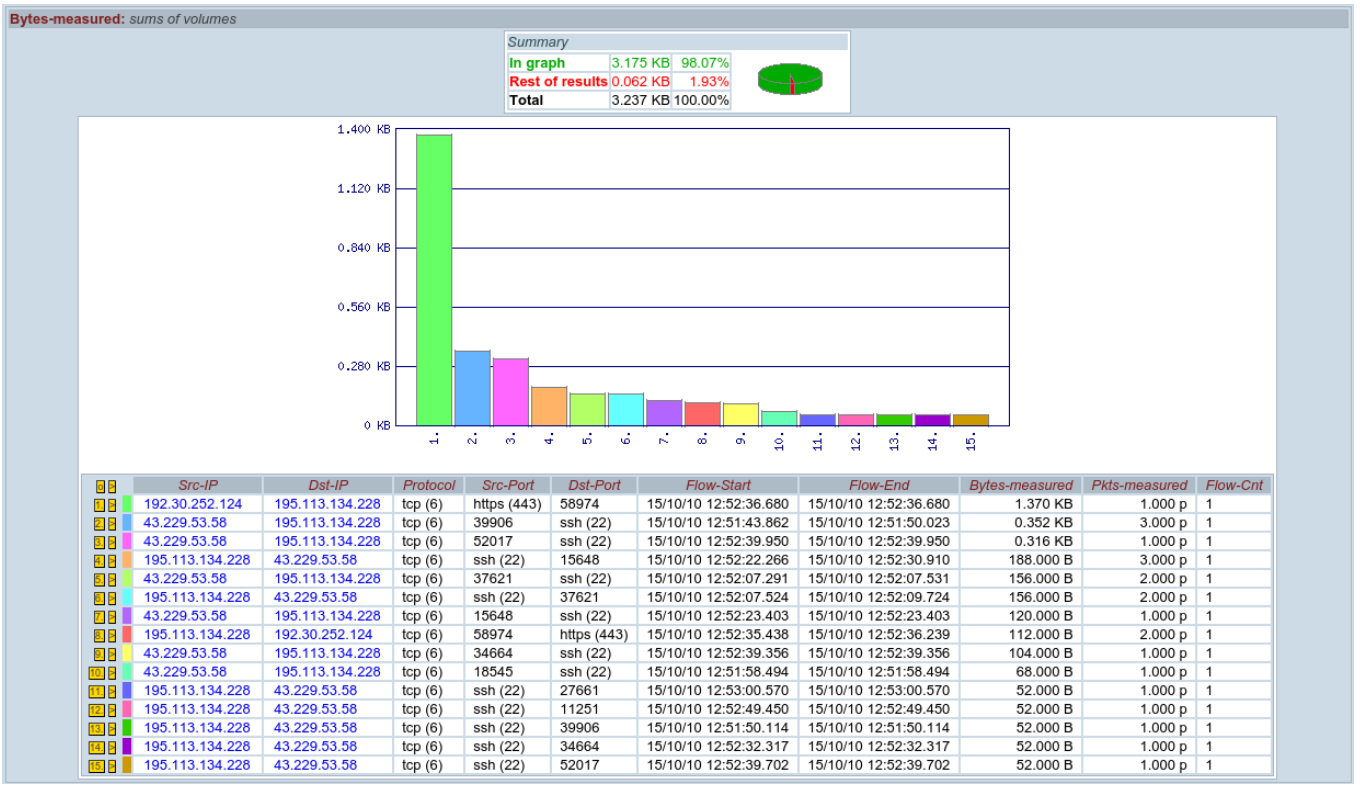
- Sledování síťového provozu, detekce (síťová vrstva)
  - Scan/sweep, (D)DOS, pokusy o přetečení zásobníku, injekci shellkódu, anomálie/statistiky
- *Snort*, *Bro, Suricata*
  - Hledání anomálií na základě databáze vzorků
- *LaBrea*
  - Sledování příchozího provozu na blocích nepřidělených adres
  - (A jeho brzdění – tarpitting)

Honeypot

- Kippo/Cowrie
  - Bruteforce na SSH
  - Fiktivní „Debian“ – řada příkazů skutečně funguje (ping, wget), řada jen částečně (ifconfig, dmesg), nebo funkci finguje (apt-get)
  - Po odhlášení neodhlásí :-)
- Dionaea
  - SMB, MSSQL, (T)FTP, MySQL, HTTP(S), SIP
  - Emulace shellkódů (libemu)
  - Emulace cmd.exe (bind/connectback)
  - P0f, Pcap – pasivní informace systému útočníka
- Záznam kompletního útoku, stažené soubory

FTAS – NetFlow

- Hlášení o spojeních ze síťových prvků
- Interface, adresy, protokoly, porty, TOS
- IPFIX: možnost dalších informací



Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Flow-Start	Flow-End	Bytes-measured	Pkts-measured	Flow-Cnt
192.30.252.124	195.113.134.228	tcp (6)	https (443)	58974	15/10/10 12:52:36.680	15/10/10 12:52:36.680	1.370 KB	1.000 p	1
43.229.53.58	195.113.134.228	tcp (6)	39906	ssh (22)	15/10/10 12:51:43.862	15/10/10 12:51:50.023	0.352 KB	3.000 p	1
43.229.53.58	195.113.134.228	tcp (6)	52017	ssh (22)	15/10/10 12:52:39.950	15/10/10 12:52:39.950	0.316 KB	1.000 p	1
195.113.134.228	43.229.53.58	tcp (6)	ssh (22)	15648	15/10/10 12:52:22.266	15/10/10 12:52:30.910	188.000 B	3.000 p	1
43.229.53.58	195.113.134.228	tcp (6)	37621	ssh (22)	15/10/10 12:52:07.291	15/10/10 12:52:07.531	156.000 B	2.000 p	1
195.113.134.228	43.229.53.58	tcp (6)	ssh (22)	37621	15/10/10 12:52:07.524	15/10/10 12:52:09.724	156.000 B	2.000 p	1
43.229.53.58	195.113.134.228	tcp (6)	15648	ssh (22)	15/10/10 12:52:23.403	15/10/10 12:52:23.403	120.000 B	1.000 p	1
195.113.134.228	192.30.252.124	tcp (6)	58974	https (443)	15/10/10 12:52:35.438	15/10/10 12:52:36.239	112.000 B	2.000 p	1
43.229.53.58	195.113.134.228	tcp (6)	34664	ssh (22)	15/10/10 12:52:39.356	15/10/10 12:52:39.356	104.000 B	1.000 p	1
43.229.53.58	195.113.134.228	tcp (6)	18545	ssh (22)	15/10/10 12:51:58.494	15/10/10 12:51:58.494	68.000 B	1.000 p	1
195.113.134.228	43.229.53.58	tcp (6)	ssh (22)	27661	15/10/10 12:53:00.570	15/10/10 12:53:00.570	52.000 B	1.000 p	1
195.113.134.228	43.229.53.58	tcp (6)	ssh (22)	11251	15/10/10 12:52:49.450	15/10/10 12:52:49.450	52.000 B	1.000 p	1
195.113.134.228	43.229.53.58	tcp (6)	ssh (22)	39906	15/10/10 12:51:50.114	15/10/10 12:51:50.114	52.000 B	1.000 p	1
195.113.134.228	43.229.53.58	tcp (6)	ssh (22)	34664	15/10/10 12:52:32.317	15/10/10 12:52:32.317	52.000 B	1.000 p	1
195.113.134.228	43.229.53.58	tcp (6)	ssh (22)	52017	15/10/10 12:52:39.702	15/10/10 12:52:39.702	52.000 B	1.000 p	1

HW sondy + Nemea

- FPGA, 100 Gb/s flow
- Zpracovávají i informace z aplikačních protokolů
  - např. rozpoznání HeartBleed
- Rychlá statistická analýza
  - DNS/NTP/SNMP amplification

Třetí strany

Botnety, scany, Poodle, Freak

Otevřené rekurzivní DNS

Spam, problematické MTA

Botnety, malware

Botnety

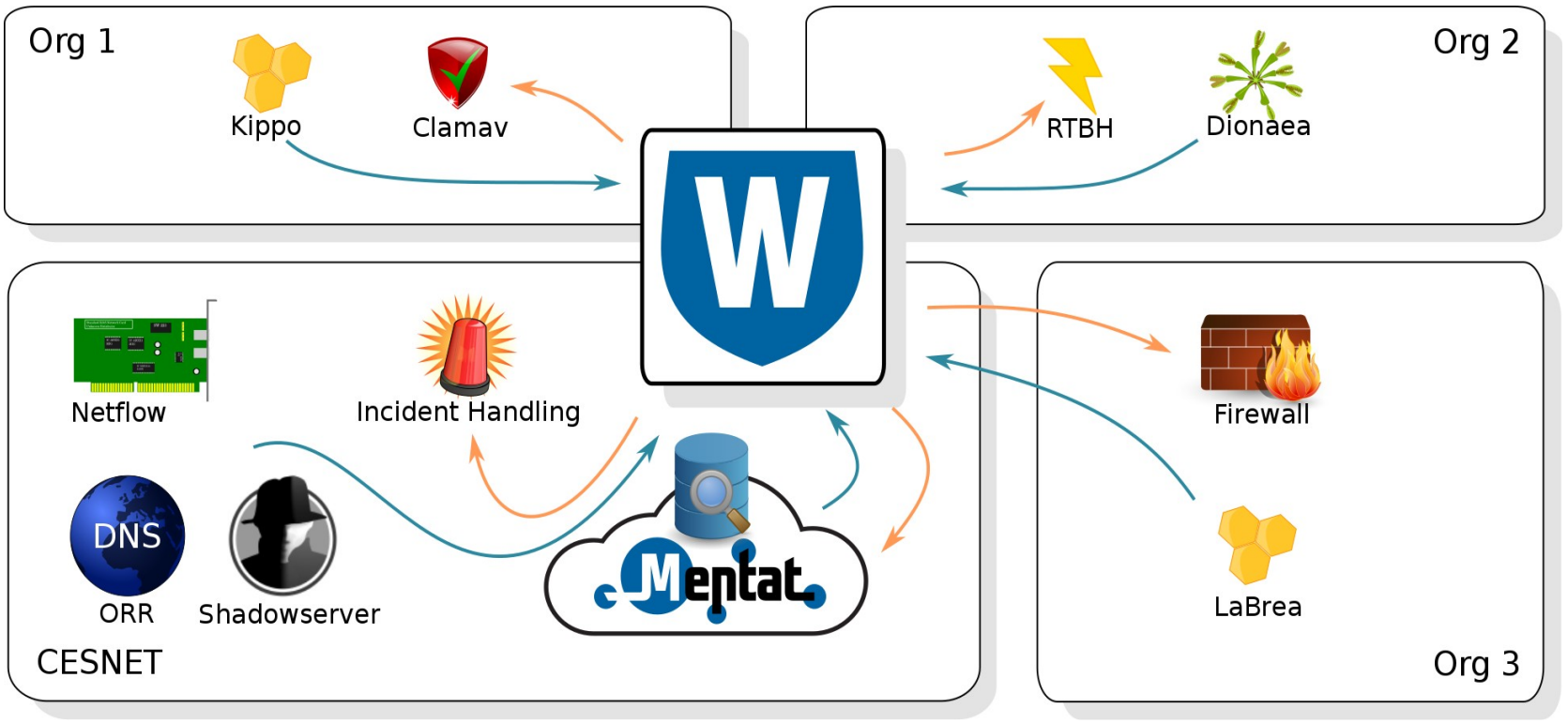
Data, data, data...

- Administrátoři často také provozují svoje
  - IDS, sondy, honeypoty, syslog
- Vyberou si data, užitečná pro ně
  - *... a zahodí zbytek*

Co třeba... sdílet?

Warden 3

- *Klient/server* (glorifikovaná fronta – transportní kanál, ne databáze)
- *Komunita*
  - Reciprocita – všechna vaše data jsou dostupná pro wardení komunitu
  - ... a všechna data od komunity jsou dostupná vám
- *Výkon, hromadné operace*
- *Filtrování*
- *Bezpečnost*
  X509
  šifrování
  kontroly dat
  peer review
- *Open/Libre*



IDEA – Intrusion Detection Extensible Alert

Botnet C&C


```
{
  "Format": "IDEA0",
  "ID": "cca3325c-a989-4f8c-998f-5b0e971f6ef0",
  "DetectTime": "2014-03-05T15:52:22Z",
  "Category": ["Intrusion.Botnet"],
  "Description": "Botnet Command and Control",
  "Source": [
    {
      "Type": ["Botnet", "CC"],
      "IP4": ["93.184.216.119"],
      "Proto": ["tcp", "ircu"],
      "Port": [6667]
    }
  ]
}
```


Honeypot


```
{
  "Format": "IDEA0",
  "ID": "2E4A3926-B1B9-41E3-89AE-B6B474EB0A54",
  "DetectTime": "2014-03-22T10:12:31Z",
  "Category": ["Recon.Scanning"],
  "ConnCount": 633,
  "Description": "EPMAPPER exploitation attempt",
  "Ref": ["cve:CVE-2003-0605"],
  "Source": [
    {
      "IP4": ["93.184.216.119"],
      "Proto": ["tcp", "epmap"],
      "Port": [24508]
    }
  ],
  "Target": [
    {
     "Port": [135]
    }
  ]
}
```


- JSON *(NoSQL friendly)*, ale mělká a silně typovaná struktura *(SQL friendly)*
- Rozšiřitelnost *(producenti mohou přidat svoje klíče a data)*
- Schopnost označit anonymizovaná, nepřesná, neúplná či podvržená data
- Schopnost rozlišit události, kde jsme hlavní zdroj, třetí strany, agregované/korelované události
- Slovníky *(mkII, tagy pro popis Source/Target/Detector)*

Příklad – blacklist

- SSH bruteforce blacklist

```
Target.Proto contains “ssh”
and not (
   Source.Anonymised or
   Source.Imprecise or
   Source.Spoofed
)
and DetectTime in [now, now-30d]
and (
   (Category == “Attempt.Login” and ConnCount > 100)
   or Category == “Intrusion.*”
)
```

Warden – HTTP API

- Server – Python, WSGI (Apache), MySQL
- Protocol – HTTPS + JSON

```
$ curl 'https://warden.example.com/getEvents?count=1&id=12'
{"lastid": 13,
 "events": [
  {"Format": "IDEA0",
   "ID": "48fb18c4-435d-4cd8-ad8a-fb4c2998f3d0",
   "Category": ["Test"],
   "DetectTime": "2014-10-19T15:22:20.409128Z"}]}

$ curl --request POST --data '{#$%^' 'https://.../sendEvents'
{"error": 400,
 "method": "getEvents",
 "message": "Deserialization error, cause was ValueError: Expecting
property name: line 1 column 1 (char 1)",
 "detail": {
  "args": "{#$%^"
 }
}
```

Technický vývoj směřuje vždy od primitivního přes komplikované k jednoduchému. – Antoine de Saint-Exupéry

Warden – Python API

```
wclient = Client(
    **read_cfg("warden_client.cfg"))

# -- or --

wclient = Client(
    url = 'https://.../warden3',
    keyfile = 'etc/key.pem',
    certfile = 'etc/cert.pem',
    cafile = 'etc/tcs-ca-bundle.pem',
    timeout = 10,
    errlog = {"level": "debug"},
    filelog = {"level": "debug"},
    idstore = "MyClient.id",
    name = "cz.cesnet.honeypot.kippo"
)
```

```
# receiving
ret = wclient.getEvents(count=10)
for e in ret:
    print e
if isinstance(ret, Error):
    print("Error: %s" % ret)

# sending
event = {
   "Format": "IDEA0",
   "ID": str(uuid4()),
   "DetectTime": isostamp(datetime),
   "Category": ["Test"]
}
ret = wclient.sendEvents([event])
if not ret:
    print("Error: %s" % ret)
```

Warden-Filer

- Daemon (rc skript) nebo cronjob
- Odesílání
  - Stačí vytvořit IDEA soubory v adresáři
  - Filer je uchopí odešle
- Přijímání
  - Filer stahuje událostí ze serveru a ukládá je jako soubory
  - Vy si je vezmete a zpracujete
- **Platformě nezávislé** – můžete s JSON událostmi pracovat v jakémkoliv jazyce a jakkoliv uznáte za vhodné

Mentat SIEM

Search alerts

Alert database search

Source: 127.0.0.1 **Target:** 127.0.0.1 AND OR

From: 2012-12-12 12:12:12 **To:** 2012-12-12 12:12:12

Detector:
--- Unspecified ---
cesnet.au1/LaBrea
cesnet.au1/SSERV
cesnet.au1/X4

Category:
Anomaly.Traffic
Attempt.Exploit
Attempt.Login
Availability.DDoS
Availability.DoS

Search
Go Advance

If you use certain queries often, you might consider saving them:

--- Personal query --- Unique name for the query Save

Displaying items **1** to **30** (**30** items) | Page **1** Next

#	Detected	Source	Target	Categorization	
1	2015-09-22 13:18:05	-- undisclosed --	211.240.36.71	Availability.DoS	
2	2015-09-22 13:13:23	-- undisclosed --	193.87.171.19	Availability.DoS	

Report M20150922M-F4amT

Unprotected access: https://mentat-hub.cesnet.cz/mentat/unauth/report/32WvuPYwWXpyaxZAhxMo

Severity	Abuse	Created
medium	abuse@vstecb.cz	2015-09-22 08:06:37

Report timing

Time period	2015-09-22 06:00:00 - 2015-09-22 08:00:00 (2h)
Delay	6m 37s
Report sent	2015-09-22 08:06:37 | Report mailed to abuse contact 'abuse@vstecb.cz'

Report magnitude

Event count	400 (400 entered filtering, 0 blocked)
IP count	1 unique IP address
Diversisty	1 analyzer, 2 categories

Report message

```
Vážení kolegové,

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

 [1]     Systémy na následujících IP adresách jsou infikovány známým malware
    součástí botnetu (Botnet Drone):

    * Analyzer:  X4
    * Popis:     Botnet Drone
    * Kategorie: Intrusion.Botnet/Malware
    ================================================================================
     IP             | Čas                                          | # událostí
    ================================================================================
    195.113.220.250 | 2015-09-21 15:44:53 - 2015-09-22 07:14:44 | 400
    --------------------------------------------------------------------------------
-
```

Poučení

Nejsou lidi.

- Nejen u nás, ale i v sítích, které se účastní

→ Snažíme se poskytnout data i jinak

- Přehledy, dashboardy
- Starosvětské mailové reportování

  (A je potřeba ho dobře vyladit, aby pomáhalo, ale nezahlcovalo.)

→ Hledáme cesty pro rozšíření dosahu *našich* detektorů

- Virtualization, docker
- Tunelování
- Lehkotonážní sondy

- *Chceš pracovat jako vývojář? Ozvi se.*
- *Máš nápad na diplomku či bakalářku související s bezpečností? Ozvi se.*

Tvým účelem není předvídat budoucnost, ale umožnit ji. – Antoine de Saint-Exupéry, Citadela

A ještě...

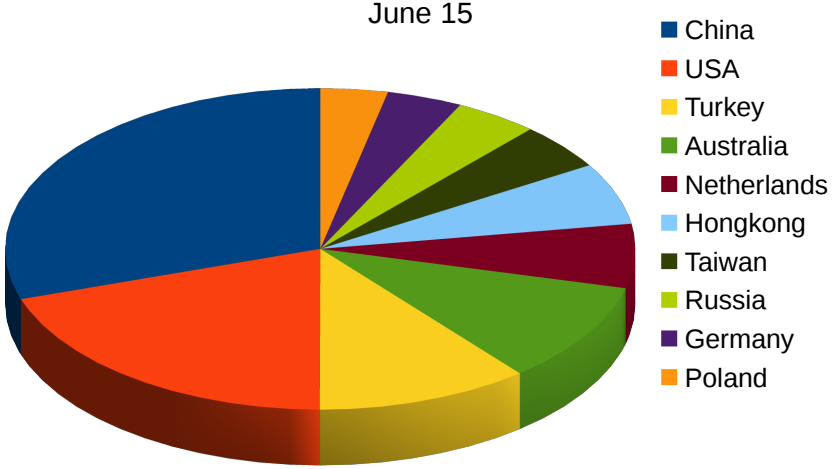
- Konektory
  - Kippo
  - Dionaea
  - BitTorrent snooper
  - RT submitter

A dál?

- fail2ban konektor
- Generátory blacklistů
- Vizualizace
- Analýza, korelace
  - Reputation shield
- Knihovny – IDEA
- Procesy

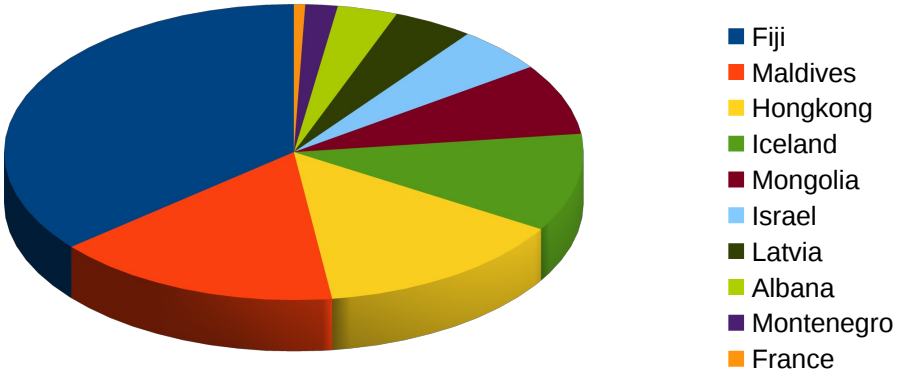
Incident TOP10 share by country

June 15



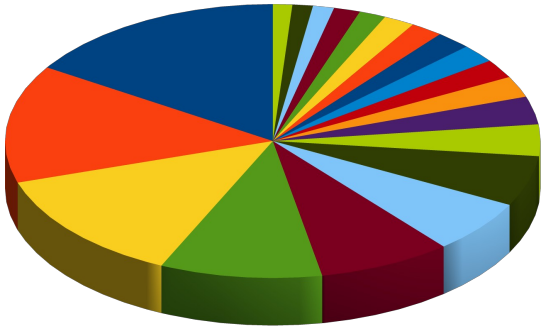
Incident TOP10 share

according to number of incidents
per one IP in the country
June 2015



TOP 20 incident share by AS

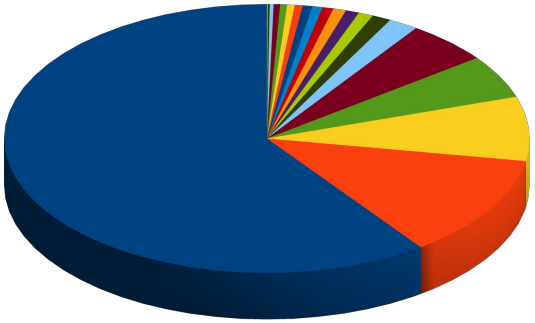
June 2015



- 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

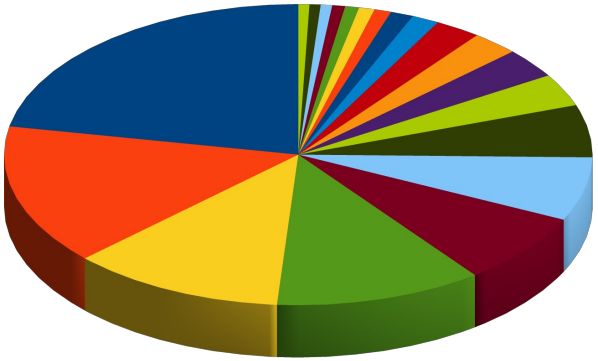
according to number of incidents
per one IP from AS
June 2015



- HOT NET LIMITED
- Przedsiebiorstwo Uslug Specjal-istycznych 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

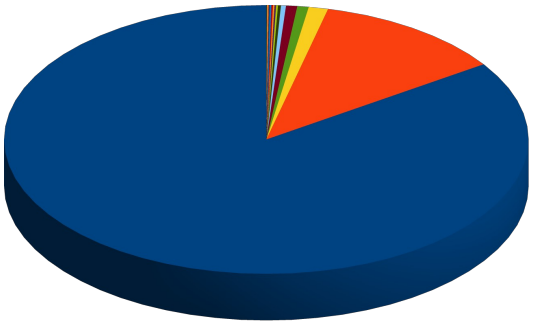
June 2015



- 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.
- GEMNET s.r.o.
- SMART Comp. a.s.

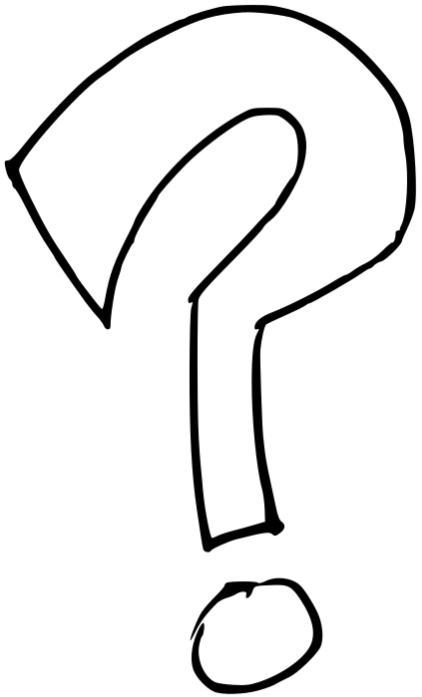
Incident TOP20 share by Czech ISP

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.

Děkuji za pozornost.



Přeprava pošty, přenos lidského hlasu, přenos pohyblivých obrázků – v našem století, stejně jako v těch ostatních, zůstává smyslem našich největších úspěchů sbližovat lidi. – Antoine de Saint-Exupéry

Děkuji za pozornost.

- !SecurityFest!: https://www.cesnet.cz/sdruzeni/akce/security-fest/

- Pavel Kácha: ph@cesnet.cz
- CESNET-CERTS: https://csirt.cesnet.cz/
- Warden: http://warden.cesnet.cz/
- IDEA: https://csirt.cesnet.cz/IDEA

  Reputation shield: http://repsh.cesnet.cz/
- Nemea: https://www.liberouter.org/technologies/nemea/
- FTAS: https://www.cesnet.cz/wp-content/uploads/2015/01/Sledovani_provozu_site.T.Kosnar.pdf

- Cowrie: https://github.com/micheloosterhof/cowrie
- Dionaea: https://github.com/rep/dionaea

- ShadowServer: http://www.shadowserver.org/
- Team Cymru: https://www.team-cymru.org/
- UceProtect-Network: http://www.uceprotect.net/
- N6: http://www.cert.pl/news/5350/
- NCKB: http://www.govcert.cz/cs/

Obrázky převážně https://openclipart.org/, špatný vkus můj vlastní