Internet a technologie 09

Bezpečnostní týmy CERT/CSIRT

Andrea Kropáčová

CESNET, z. s. p. o.

4. 6. 2009

CSIRT/CERT

- **CERT** (**C**omputer **E**mergency **R**esponse **T**eam)
- **CSIRT** (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam)
- Poskytuje služby a podporu v oblasti bezpečnosti počítačových sítí a služeb a to především v oblasti ***řešení bezpečnostních incidentů***
- Tvoří **infrastrukturu**, která umožňuje
  - Spolupráci a koordinaci
    - Rychlejší a efektivnější reakci při řešení BI
  - Prevenci BI

Vznik CSIRT/CERT

- Identifikace
  - Zřizovatel, provozovatel
  - Členové týmu, kontaktní informace
- Pole působnosti (definice sítě)
- Poskytované služby
  - Minimem je ***řešení incidentů*** (RESPONSE)
  - Reaktivní, proaktivní, osvětové
- Zázemí:
  - Organizační, technické, adiministrativní

CSIRT/CERT

- Modely:
  - interní
  - koordinační
  - vendor
  - *národní, vládní (tzv. **vrcholové** týmy)*
- Zřizovatel CERT/CSIRT definuje:
  - Model (roli)
  - Pole působnosti
  - **Zodpovědnost a pravomoc**
  - Služby

Incident handling

CESNET2

Ipv4 svět
RIRs

Delegovaný adresový blok
LIR (ISP)

CSIRT

Delegovaný adresový blok
Organizace

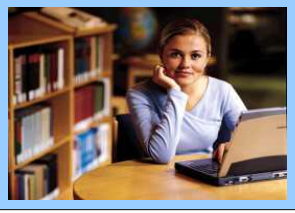
ČVUT

CUNI

Koncová síť
(kolej, laboratoř, učebna)

Kolejní síť STRAHOV

MFF UK



Karlín

Incident handling

CESNET2

Ipv4 svět
RIRs

Delegovaný adresový blok
LIR (ISP)

Delegovaný adresový blok
Organizace

Koncová síť
(kolej, laboratoř, učebna)

CSIRT

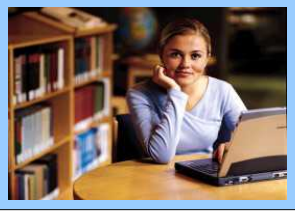
ČVUT

CUNI

Kolejní síť STRAHOV

MFF UK

Karlín



Kdy je tým CERT/CSIRT?

- Když tým uznají již existující CERT/CSIRT týmy
  - FIRST
  - TERENA (TI, TF-CSIRT)
- Čím je zaručena důvěryhodnost CERT/CSIRT?:
  - Důraz kladen na komunikaci a spolupráci
  - Musí být plně transparentní
  - Musí mít konzistentní vystupování
  - Otevřenost ke komunitě CSIRTů

Platformy pro spolupráci

- **FIRST** (http://www.first.org/)
  - 197 týmů
  - Získává se ***členství***
  - Pořádá:
    - Výroční konference (2008 v Kyoto, Japonsko)
    - Školení, konference, semináře

Platformy pro spolupráci

- **TERENA** (http://www.terena.org/)
  - CSIRT Training
  - TI (Trusted Introducer, http://www.trusted-introducer.org)
    - → **Listed status**
      - → **Accredited status**
        - → ***Certified (maturity)***

    } Proces začlenění do komunity evropských CERT/CSIRT týmů

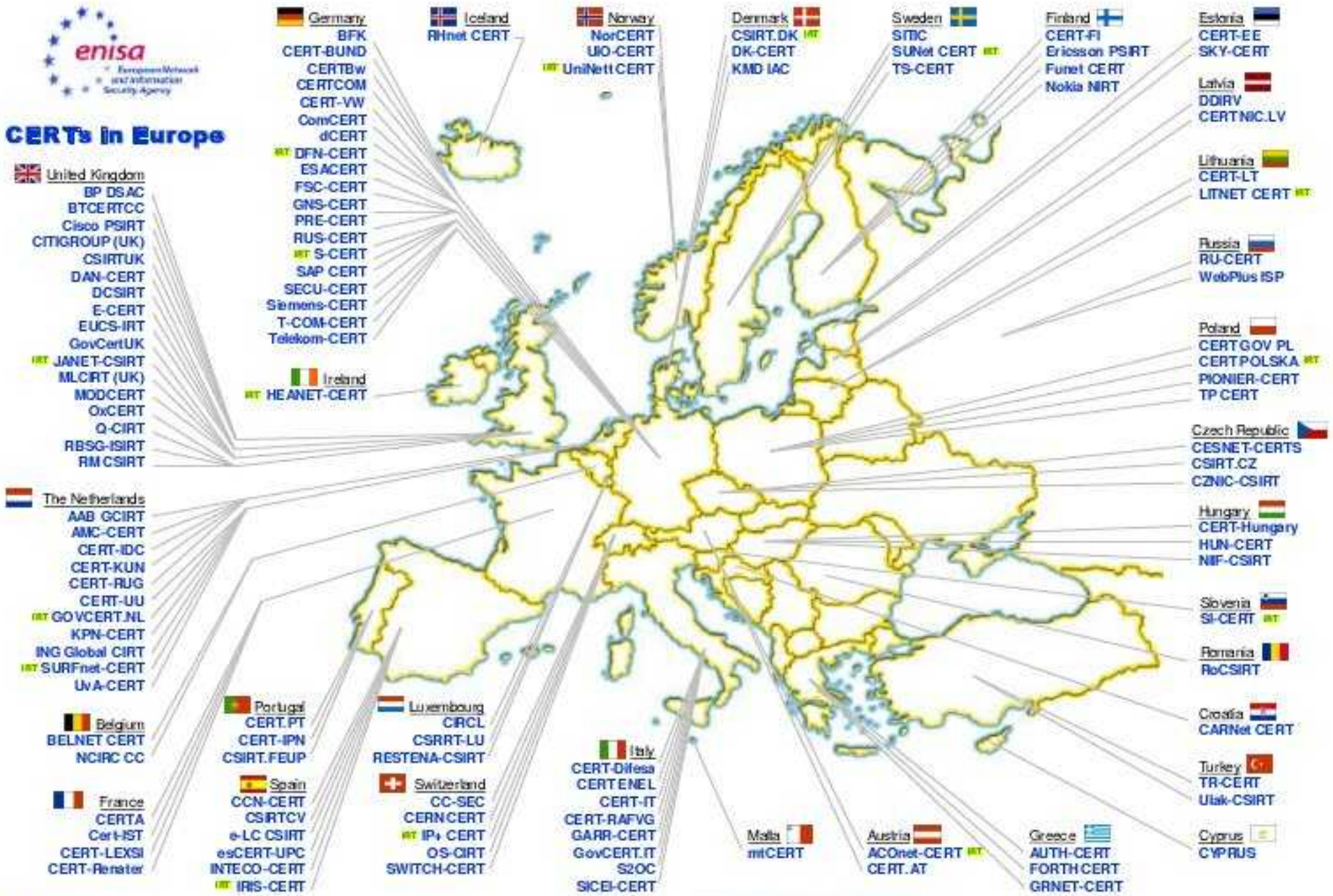
  - TF-CSIRT (Task Force for CSIRT teams)
    - 144 týmů
    - Setkání 3x ročně
    - Projekty – organizační, technické, legislativní

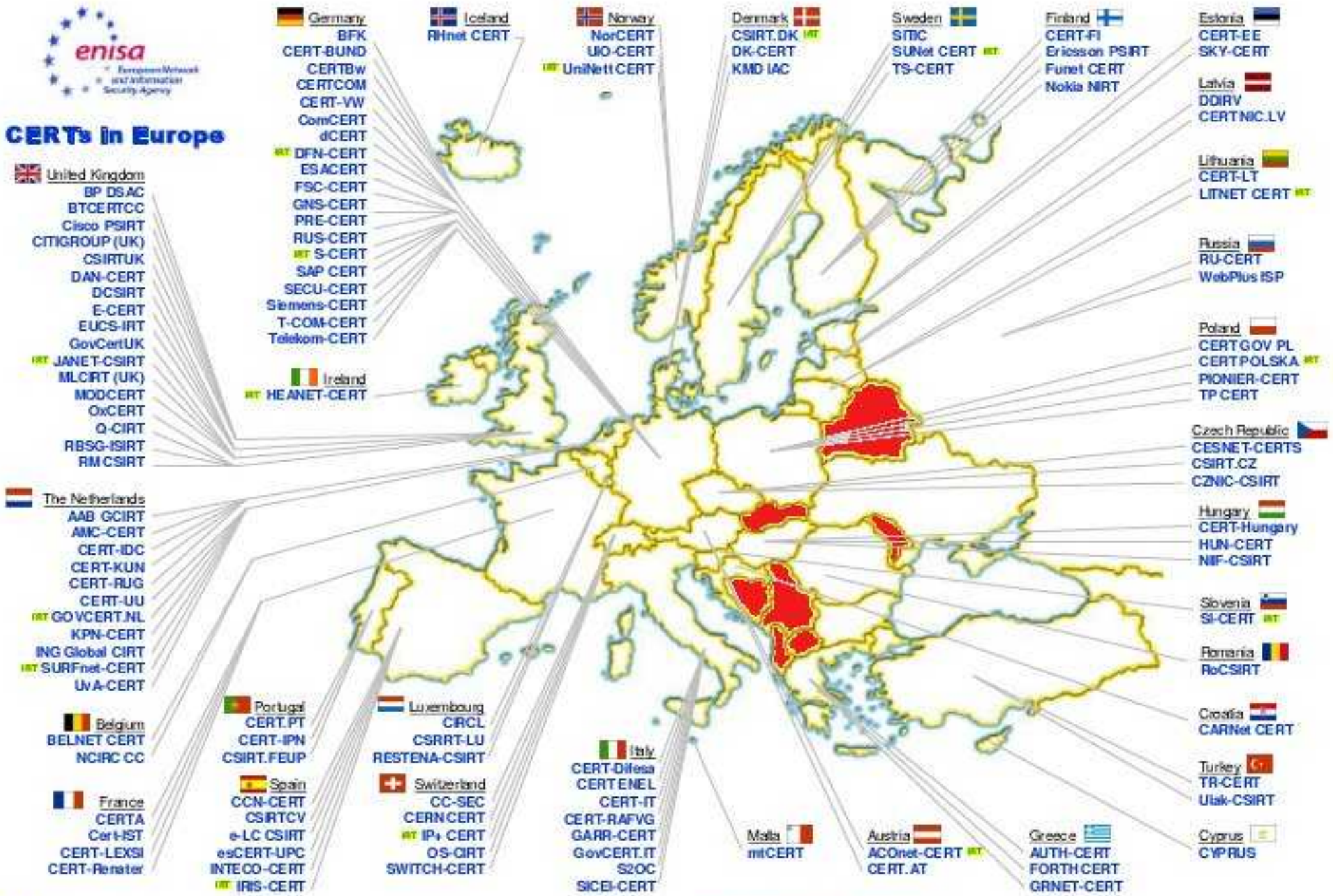
Platformy pro spolupráci

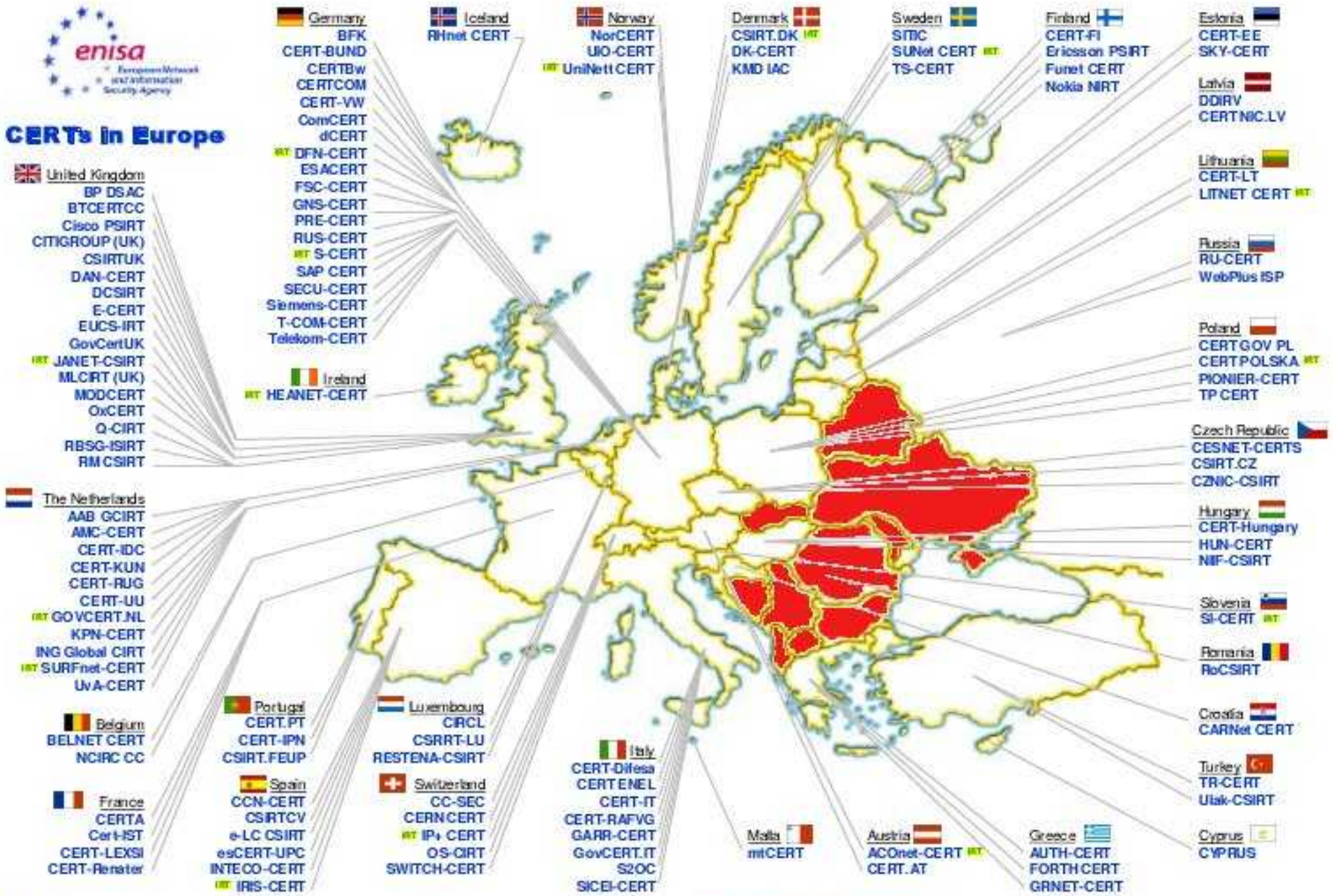
- **ENISA** (http://www.enisa.eu/)
  - Konference a školení pořádané CERT/CSIRT týmy
  - CHIHT (Clearing House for Incident Handling Tools)
- **GÉANT** (http://www.dante.net/geant)
  - Konsorcium realizující projekt evropské sítě GN2
  - Sdružuje 30 provozovatelů národních akademických sítí v Evropě
- **CLOSER** projekt
  - Podpora vzniku CERT/CSIRT v zemích bývalého Sovětského svazu

ENISA inventory in CERT activities in Europe

- Následující 3 slajdy zobrazují (ne) existenci CERT/CSIRT týmů v evropských zemích:
- V zemích vybarvených červenou barvou neexistuje ani jeden tým typu CERT/CSIRT:
  - 1. slajd = (ne)existence CERT/CSIRT týmů v Evropě
  - 2. slajd = stav v roce 2009 (květen)
  - 3. slajd = stav v roce 2008 (říjen)
- Mapa (obrázek) je převzat ze stránek organizace ENISA:
  - http://www.enisa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf


enisa
European Network and Information Security Agency
CERTs in Europe
United Kingdom
BP DSAC
BTCERTCC
Cisco PSIRT
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
EUCS-IRT
GovCertUK
IRT JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RM CSIRT
The Netherlands
AAB GCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
IRT GOVCERT.NL
KPN-CERT
ING Global CIRT
IRT SURFnet-CERT
UvA-CERT
Belgium
BELNET CERT
NCIRC CC
France
CERTA
Cert-IST
CERT-LEXSI
CERT-Renater
Germany
BFK
CERT-BUND
CERTBw
CERTCOM
CERT-VW
ComCERT
dCERT
IRT DFN-CERT
ESACERT
FSC-CERT
GNS-CERT
PRE-CERT
RUS-CERT
IRT S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
T-COM-CERT
Telekom-CERT
Ireland
IRT HEANET-CERT
Portugal
CERT.PT
CERT-IPN
CSIRT.FEUP
Spain
CCN-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
INTECO-CERT
IRT IRIS-CERT
Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT
Switzerland
CC-SEC
CERN CERT
IRT IP+ CERT
OS-CIRT
SWITCH-CERT
Iceland
RHnet CERT
Norway
NorCERT
UIO-CERT
IRT UniNett CERT
Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT
Malta
mtCERT
Denmark
CSIRT.DK IRT
DK-CERT
KMD IAC
Sweden
SITIC
SUNet CERT IRT
TS-CERT
Austria
ACOnet-CERT IRT
CERT.AT
Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
Greece
AUTH-CERT
FORTH CERT
GRNET-CERT
Estonia
CERT-EE
SKY-CERT
Latvia
DDIRV
CERT NIC.LV
Lithuania
CERT-LT
LITNET CERT IRT
Russia
RU-CERT
WebPlus ISP
Poland
CERT GOV PL
CERT POLSKA IRT
PIONIER-CERT
TP CERT
Czech Republic
CESNET-CERTS
CSIRT.CZ
CZNIC-CSIRT
Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT
Slovenia
SI-CERT IRT
Romania
RoCSIRT
Croatia
CARNet CERT
Turkey
TR-CERT
Ulak-CSIRT
Cyprus
CYPRUS
IRT - teams using their RIPE IRT object for networks they serve
CERTS in Europe map, Oct. 2008 v1.7 www.enisa.europa.eu/cert_inventory/
© European Network and Information Security Agency (ENISA)


enisa
European Network and Information Security Agency
CERTs in Europe
United Kingdom
BP DSAC
BTCERTCC
Cisco PSIRT
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
EUCS-IRT
GovCertUK
IRT JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RM CSIRT
The Netherlands
AAB GCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
IRT GOVCERT.NL
KPN-CERT
ING Global CIRT
IRT SURFnet-CERT
UvA-CERT
Belgium
BELNET CERT
NCIRC CC
France
CERTA
Cert-IST
CERT-LEXSI
CERT-Renater
Germany
BFK
CERT-BUND
CERTBw
CERTCOM
CERT-VW
ComCERT
dCERT
IRT DFN-CERT
ESACERT
FSC-CERT
GNS-CERT
PRE-CERT
RUS-CERT
IRT S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
T-COM-CERT
Telekom-CERT
Ireland
IRT HEANET-CERT
Portugal
CERT.PT
CERT-IPN
CSIRT.FEUP
Spain
CCN-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
INTECO-CERT
IRT IRIS-CERT
Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT
Switzerland
CC-SEC
CERN CERT
IRT IP+ CERT
OS-CIRT
SWITCH-CERT
Iceland
RHnet CERT
Norway
NorCERT
UIO-CERT
IRT UniNett CERT
Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT
Malta
mtCERT
Denmark
CSIRT.DK IRT
DK-CERT
KMD IAC
Sweden
SITIC
SUNet CERT IRT
TS-CERT
Austria
ACOnet-CERT IRT
CERT.AT
Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
Greece
AUTH-CERT
FORTH CERT
GRNET-CERT
Estonia
CERT-EE
SKY-CERT
Latvia
DDIRV
CERT NIC.LV
Lithuania
CERT-LT
LITNET CERT IRT
Russia
RU-CERT
WebPlus ISP
Poland
CERT GOV PL
CERT POLSKA IRT
PIONIER-CERT
TP CERT
Czech Republic
CESNET-CERTS
CSIRT.CZ
CZNIC-CSIRT
Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT
Slovenia
SI-CERT IRT
Romania
RoCSIRT
Croatia
CARNet CERT
Turkey
TR-CERT
Ulak-CSIRT
Cyprus
CYPRUS
IRT - teams using their RIPE IRT object for networks they serve
CERTS in Europe map, Oct. 2008 v1.7 www.enisa.europa.eu/cert_inventory/
© European Network and Information Security Agency (ENISA)


enisa
European Network and Information Security Agency
CERTs in Europe
United Kingdom
BP DSAC
BTCERTCC
Cisco PSIRT
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
EUCS-IRT
GovCertUK
IRT JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RM CSIRT
The Netherlands
AAB GCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
IRT GOVCERT.NL
KPN-CERT
ING Global CIRT
IRT SURFnet-CERT
UvA-CERT
Belgium
BELNET CERT
NCIRC CC
France
CERTA
Cert-IST
CERT-LEXSI
CERT-Renater
Germany
BFK
CERT-BUND
CERTBw
CERTCOM
CERT-VW
ComCERT
dCERT
IRT DFN-CERT
ESACERT
FSC-CERT
GNS-CERT
PRE-CERT
RUS-CERT
IRT S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
T-COM-CERT
Telekom-CERT
Ireland
IRT HEANET-CERT
Portugal
CERT.PT
CERT-IPN
CSIRT.FEUP
Spain
CCN-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
INTECO-CERT
IRT IRIS-CERT
Iceland
RHnet CERT
Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT
Switzerland
CC-SEC
CERN CERT
IRT IP+ CERT
OS-CIRT
SWITCH-CERT
Norway
NorCERT
UIO-CERT
IRT UniNett CERT
Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT
Malta
mtCERT
Denmark
CSIRT.DK IRT
DK-CERT
KMD IAC
Sweden
SITIC
SUNet CERT IRT
TS-CERT
Austria
ACOnet-CERT IRT
CERT.AT
Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
Greece
AUTH-CERT
FORTH CERT
GRNET-CERT
Estonia
CERT-EE
SKY-CERT
Latvia
DDIRV
CERT NIC.LV
Lithuania
CERT-LT
LITNET CERT IRT
Russia
RU-CERT
WebPlus ISP
Poland
CERT GOV PL
CERT POLSKA IRT
PIONIER-CERT
TP CERT
Czech Republic
CESNET-CERTS
CSIRT.CZ
CZNIC-CSIRT
Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT
Slovenia
SI-CERT IRT
Romania
RoCSIRT
Croatia
CARNet CERT
Turkey
TR-CERT
Ulak-CSIRT
Cyprus
CYPRUS
IRT - teams using their RIPE IRT object for networks they serve
CERTS in Europe map, Oct. 2008 v1.7 www.enisa.europa.eu/cert_inventory/
© European Network and Information Security Agency (ENISA)

CERT/CSIRT v ČR

- CESNET-CERTS (http://www.cesnet.cz/)
  - Provozován sdružením CESNET
  - *Accredited* od ledna 2008 (*listed* od ledna 2004)
- CSIRT.CZ (http://www.csirt.cz/)
  - Součást projektu “Kybernetické hrozby” (grant MV ČR)
  - *Listed* od června 2008 (provoz spuštěn 3. dubna 2008)
- CZ.NIC-CSIRT (http://www.nic.cz/)
  - Provozován sdružením CZ.NIC
  - *Listed* od září 2008

CSIRT.CZ

- Modelové pracoviště typu CSIRT
- Spuštěno 3. dubna 2008
- Úkol v rámci projektu “Problematika kybernetických hrozeb z hlediska bezp. zájmů ČR” (MV ČR)
- Založeno a vedeno CESNET-CERTS
- Role “**poslední záchrany**” pro hlášení BI v ČR
  - Obsluhuje všechny adresové rozsahy přidělené do ČR
  - Kontakt - abuse@csirt.cz (a “master” adresy csirt.cz)
  - Negarantuje úspěch, ale udělá pro něj maximum

Ipv4 svět
RIRs

Delegovaný adresový blok
LIR (ISP)

Delegovaný adresový blok
Organizace

Koncová síť
(kolej, laboratoř, učebna)

CESNET-CERTS

ČVUT

Kolejní síť STRAHOV

CSIRT.CZ

Ipv4 svět
RIRs

Delegovaný adresový blok
LIR (ISP)

CESNET-CERTS

Delegovaný adresový blok
Organizace

ČVUT

Koncová síť
(kolej, laboratoř, učebna)

Kolejní síť STRAHOV

CSIRT.CZ

Ipv4 svět
RIRs

Delegovaný adresový blok
LIR (ISP)

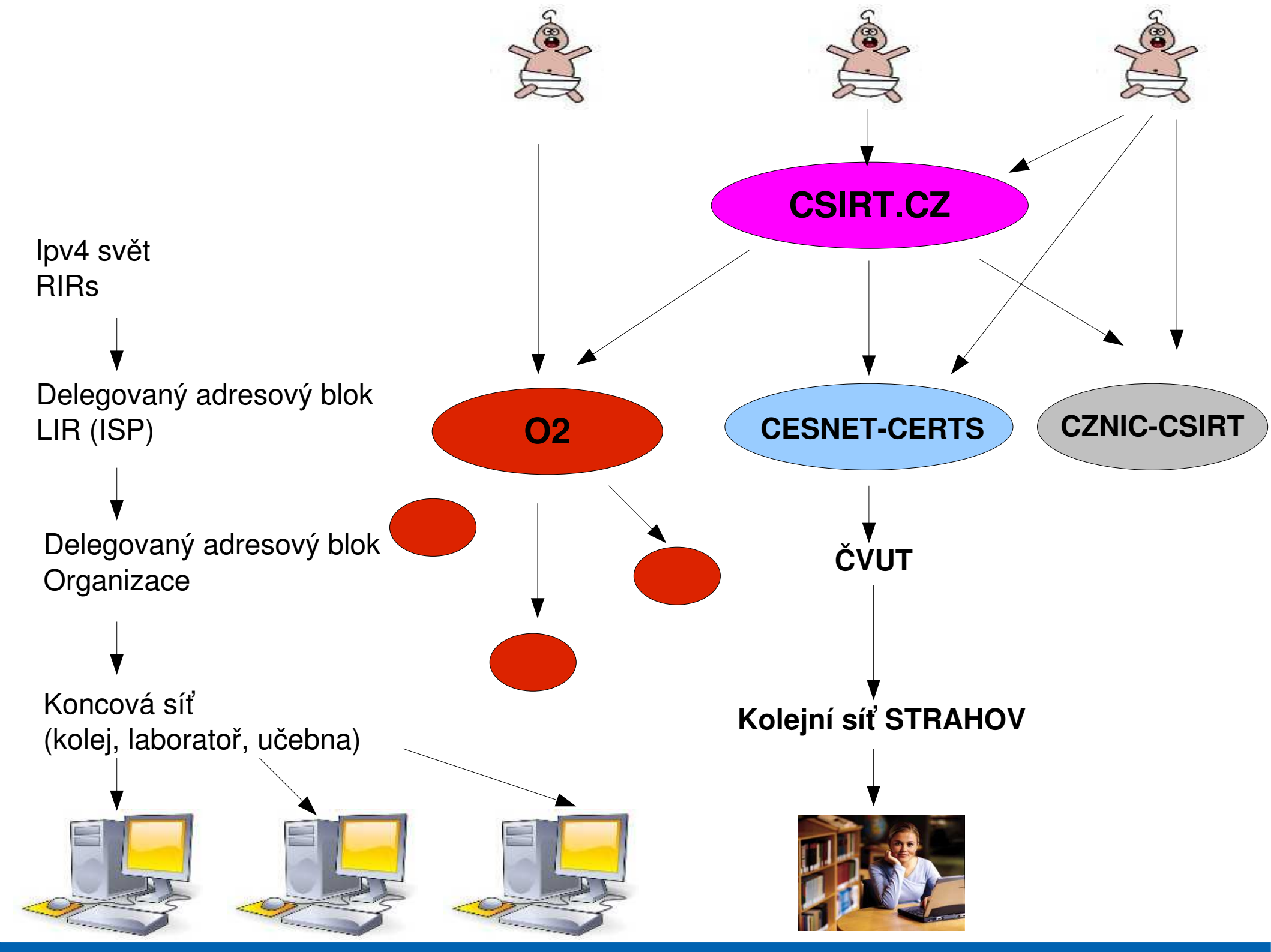
CESNET-CERTS

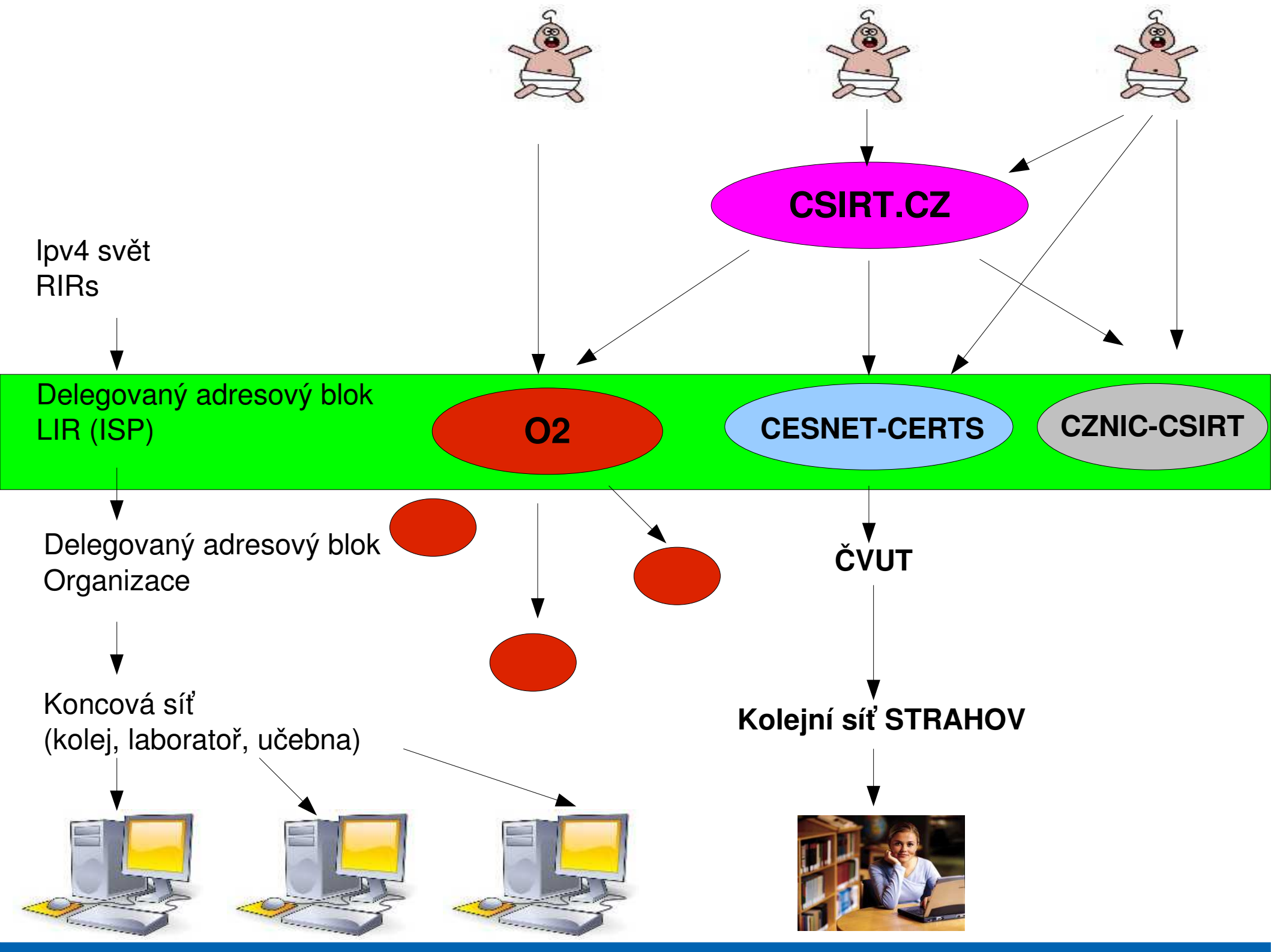
Delegovaný adresový blok
Organizace

ČVUT

Koncová síť
(kolej, laboratoř, učebna)

Kolejní síť STRAHOV


CSIRT.CZ
Ipv4 svět
RIRs
Delegovaný adresový blok
LIR (ISP)
O2
CESNET-CERTS
CZNIC-CSIRT
Delegovaný adresový blok
Organizace
ČVUT
Koncová síť
(kolej, laboratoř, učebna)
Kolejní síť STRAHOV


CSIRT.CZ
Ipv4 svět
RIRs
Delegovaný adresový blok
LIR (ISP)
O2
CESNET-CERTS
CZNIC-CSIRT
Delegovaný adresový blok
Organizace
ČVUT
Koncová síť
(kolej, laboratoř, učebna)
Kolejní síť STRAHOV

Problémy při řešení BI z pohledu CSIRT.CZ

- Nemožnost kontaktovat zodpovědnou osobu:
  - Adresy abuse@, postmaster@, hostmaster@:
    - Neexistují
    - Existují, ale neexistují koncoví příjemci (osoby)
  - Nedostupný mailer, nesprávná antispamová ochrana
  - Chybné údaje v databázích
    - RIRů (RIPE, ARIN, APNIC, AFRINIC, LACNIC)
    - Národních TLD
- Personální – málo správců, špatná zástupnost
- Technické – nepřipravenost, neschopnost reagovat

CSIRT/CERT

- Nástroj ke zvyšování bezpečnosti síťové infrastruktury
- Edukační – pro provozovatele sítí, poskytovatele obsahu i uživatele
- **CSIRT není nástrojem ani prostředkem represe, kontroly a regulace!**

Dotazy?

Děkuji za pozornost.

Andrea Kropáčová