Aktivity NBÚ při zajišťování kybernetické bezpečnosti

Jaroslav Šmíd
Tel.: 420 257 283 333

e-mail: J.Smid@nbu.cz

Zákon o kybernetické bezpečnosti

Kritická informační infrastruktura

Věcný záměr zákona o kybernetické bezpečnosti

Usnesení vlády ze dne 30. května 2012 č. 382 k návrhu věcného záměru zákona o kybernetické bezpečnosti.

- ukládá řediteli Národního bezpečnostního úřadu zpracovat na základě věcného záměru zákona uvedeného v bodě I tohoto usnesení a předložit vládě do 31. července 2013 návrh zákona o kybernetické bezpečnosti.

Hlavní zásady a pilíře návrhu zákona

- minimalizace zásahů do práv soukromoprávních subjektů
- individuální odpovědnost za bezpečnost vlastní sítě
- bezpečnostní opatření (standardizace)
- hlášení kybernetických bezpečnostních incidentů
- protiopatření

Zákon o kybernetické bezpečnosti (ZKB)

Předmět úpravy § 1

- Předmětem je úprava práv a povinností orgánů veřejné moci, fyzických a právnických osob, stanovení působnost orgánů státní správy a jejich vzájemná spolupráce v oblasti kybernetické bezpečnosti.
- Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.
- Výjimka zohledňující specifika činnosti zpravodajských služeb České republiky v § 24.

Pojmy ZKB

Kybernetický prostor § 2 písm. a)

Kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.

Pojmy ZKB

Kybernetická bezpečnost § 2 písm. b)

Kybernetickou bezpečností se rozumí souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění nerušeného a bezvadného fungování kybernetického prostoru.

Pojmy ZKB
Kritická informační infrastruktura

§ 2 písm. c)

Kritickou informační infrastrukturou se rozumí kritická infrastruktura v odvětví komunikační a informační systémy určená Národním bezpečnostním úřadem.

Povinné osoby ZKB

§ 3 písm. a) a b)

Povinnými osobami v oblasti kybernetické bezpečnosti jsou

a) poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací,

b) poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací spravující páteřní sítě, pokud nespadají pod písmeno c),

Povinné osoby ZKB

Kritická informační infrastruktura § 3 písm. c) a d)
Významný IS § 3 písm. e)

Povinnými osobami v oblasti kybernetické bezpečnosti jsou

c) správci komunikačních systémů zařazených do kritické informační infrastruktury,

d) správci informačních systémů zařazených do kritické informační infrastruktury a

e) správci významných informačních systémů. Správcem se rozumí u informačních systémů ten subjekt, který určuje účel zpracování informací a podmínky jeho provozování, komunikačních systémů ten subjekt, který určuje účel KS a podmínky jeho provozování.

Systém k zajištění kybernetické bezpečnosti

§ 4

Systém zajištění kybernetické bezpečnosti tvoří:

- bezpečnostní opatření,
- hlášení kybernetických bezpečnostních incidentů,
- protiopatření,
- oznamování kontaktních údajů a
- činnost dohledových pracovišť.

Systém k zajištění kybernetické bezpečnosti

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

§ 8 až § 12

- Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
- Kybernetickým bezpečnostním incidentem je událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
- Stanovena povinnost detekce a hlášení kybernetických bezpečnostních incidentů.

Systém k zajištění kybernetické bezpečnosti
Dohledová pracoviště

§ 19 až § 23

Národní CERT - soukromoprávní subjekt – právnická osoba.

Vládní CERT - provozuje Úřad.

Stav kybernetického nebezpečí

§ 25

- Stav mimořádný, speciální oproti mimořádným stavům vyhlašovaným podle ústavního zákona č. 110/1998 Sb. o bezpečnosti České republiky nebo podle krizového zákona č. 240/2000 Sb.
- Možno vyhlásit pokud je ve velkém rozsahu ohrožena bezpečnost informací v IS, bezpečnost služeb nebo sítí elektronických komunikací a tím dojde k ohrožení nebo porušení zájmu České republiky.
- Stav KN vyhlašuje předseda vlády na návrh ředitele NBÚ.
- Musí jej schválit vláda do 24 hod jinak jej zruší.
- Vyhlašován na dobu nejdéle 7 dnů – prodloužení jen se souhlasem vlády.

Účinnost

§ 37

Předpokládaná účinnost je dnem 1. ledna 2015.

Metody ochrany před kybernetickými hrozbami a útoky

- individuální odpovědnost – individuální ochrana
    - outsourcing specializovanými společnostmi
- CERT/CSIRT

Computer Emergency Response Team – CERT

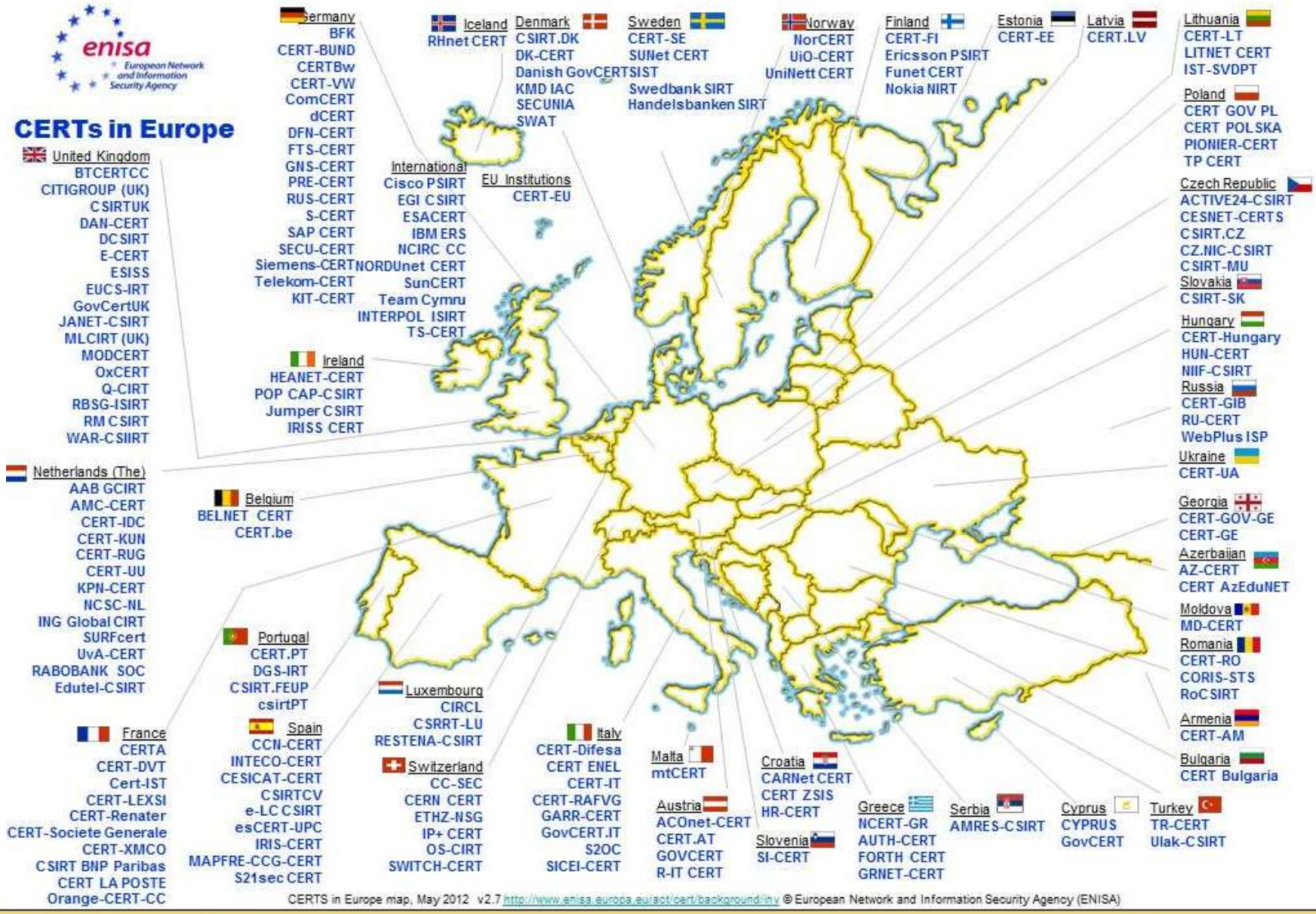
• 3.11.1988 – první významné napadení Internetu škodlivým programem tzv. Morrisovým červem

• jako reakce na tuto událost byl na zakázku vlády USA na univerzitě Carnegie Mellon vybudovám první **CERT**

• od roku 1994 se CERTy začaly budovat nejen v akademické sféře

• začala vznikat různá sdružení CERTů, např. EGC – Europeam Governmet CERT group, FIRST – Forum of Incident Response and Security Teams, TERENA – Trans-European Research and Education Networking Association,…

• CERT/CSIRT (Computer Security Incident Response Team)

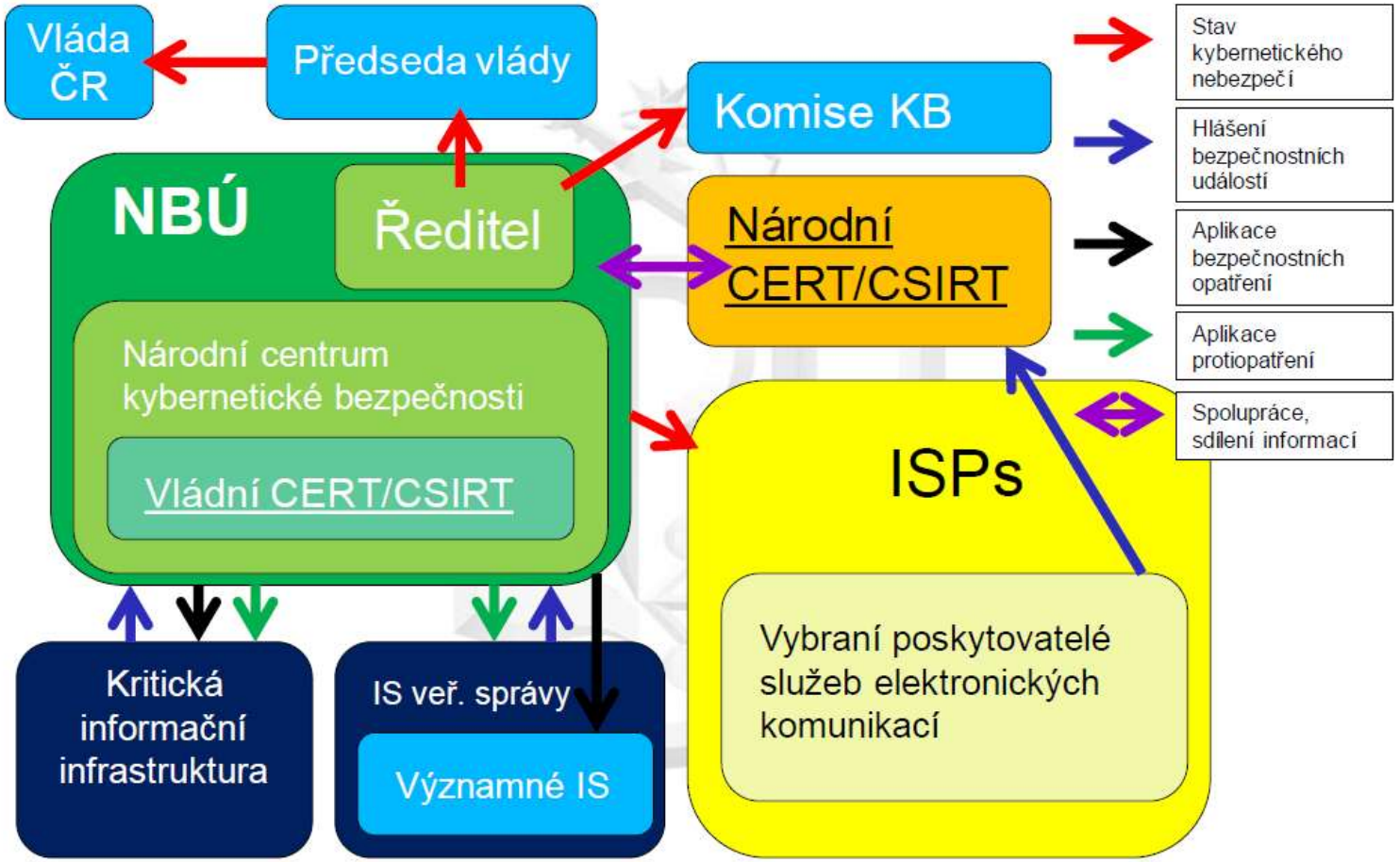

enisa
European Network and Information Security Agency
CERTs in Europe
United Kingdom
BTCERTCC
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
ESISS
EUCS-IRT
GovCertUK
JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RMCSIRT
WAR-CSIIRT
Netherlands (The)
AABGCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
KPN-CERT
NCSC-NL
ING Global CIRT
SURFcert
UvA-CERT
RABOBANK SOC
Edutel-CSIRT
France
CERTA
CERT-DVT
Cert-IST
CERT-LEXSI
CERT-Renater
CERT-Societe Generale
CERT-XMCO
CSIRT BNP Paribas
CERT LA POSTE
Orange-CERT-CC
Germany
BFK
CERT-BUND
CERTBw
CERT-VW
ComCERT
dCERT
DFN-CERT
FTS-CERT
GNS-CERT
PRE-CERT
RUS-CERT
S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
Telekom-CERT
KIT-CERT
Ireland
HEANET-CERT
POP CAP-CSIRT
Jumper CSIRT
IRISS CERT
Belgium
BELNET CERT
CERT.be
Portugal
CERT.PT
DGS-IRT
CSIRT.FEUP
csirtPT
Spain
CCN-CERT
INTECO-CERT
CESICAT-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
IRIS-CERT
MAPFRE-CCG-CERT
S21sec CERT
Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT
Switzerland
CC-SEC
CERN CERT
ETHZ-NSG
IP+ CERT
OS-CIRT
SWITCH-CERT
Iceland
RHnet CERT
International
Cisco PSIRT
EGI CSIRT
ESACERT
IBM ERS
NCIRC CC
NORDUnet CERT
SunCERT
Team Cymru
INTERPOL ISIRT
TS-CERT
EU Institutions
CERT-EU
Denmark
CSIRT.DK
DK-CERT
Danish GovCERT
KMD IAC
SECUNIA
SWAT
Sweden
CERT-SE
SUNet CERT
SISTSIST
Swedbank SIRT
Handelsbanken SIRT
Norway
NorCERT
UiO-CERT
UniNett CERT
Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
Estonia
CERT-EE
Latvia
CERT.LV
Lithuania
CERT-LT
LITNET CERT
IST-SVDPT
Poland
CERT GOV PL
CERT POLSKA
PIONIER-CERT
TP CERT
Czech Republic
ACTIVE24-CSIRT
CESNET-CERTS
CSIRT.CZ
CZ.NIC-CSIRT
CSIRT-MU
Slovakia
CSIRT-SK
Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT
Russia
CERT-GIB
RU-CERT
WebPlus ISP
Ukraine
CERT-UA
Georgia
CERT-GOV-GE
CERT-GE
Azerbaijan
AZ-CERT
CERT AzEduNET
Moldova
MD-CERT
Romania
CERT-RO
CORIS-STS
RoCSIRT
Armenia
CERT-AM
Bulgaria
CERT Bulgaria
Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT
Malta
mtCERT
Austria
ACOnet-CERT
CERT.AT
GOVCERT
R-IT CERT
Croatia
CARNet CERT
CERT ZSIS
HR-CERT
Slovenia
SI-CERT
Greece
NCERT-GR
AUTH-CERT
FORTH CERT
GRNET-CERT
Serbia
AMRES-CSIRT
Cyprus
CYPRUS
GovCERT
Turkey
TR-CERT
Ulak-CSIRT
CERTS in Europe map, May 2012 v2.7 http://www.enisa.europa.eu/act/cert/background/inv © European Network and Information Security Agency (ENISA)

Computer Emergency Response Team – CERT
-
mezinárodní rámec

• Digitální agenda pro Evropu – květen 2010 navazuje na strategii Evropa 2020
•požaduje, kromě jiného, rychlejší Internet a přístup k němu pro všechny obyvatele do roku 2013
• zřizuje ENISA – European Network and Information Security Agency
• od roku 2012 předpokládá vybudování sítě funkčních **národních/vládních CERTů** a CERTů unijních institucí

• NATO uzavírá s členskými zeměmi memoranda o porozumění pro spolupráci v oblasti kybernetické obrany

Národní centrum kybernetické bezpečnosti - začlenění ve státní správě



Národní centrum kybernetické bezpečnosti - hlavní cíle

- poskytovat ochranu významným informačním systémům veřejné správy a kritické informační infrastruktury před kybernetickými útoky
- přispívat k poskytování bezpečného a spolehlivého prostředí pro občany a podnikatelské subjekty
- přispívat k ochraně soukromí a základních práv v kybernetickém prostoru ČR
- spolupracovat s partnerskými organizacemi na národní i mezinárodní úrovni

Národní centrum kybernetické bezpečnosti - organizační členění

národní centrum kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti

Vládní CERT

Analýza a vyhodnocení přijatých hlášení o incidentech
Zpracování incidentů
Systém včasného varování
Součinnost se správci KII, KKI a ISVS
Přijímání protiopatření
Mezinárodní spolupráce na provozní a pracovní úrovni
Koordinace řešení incidentů na národní i mezinárodní úrovni
Kybernetická cvičení

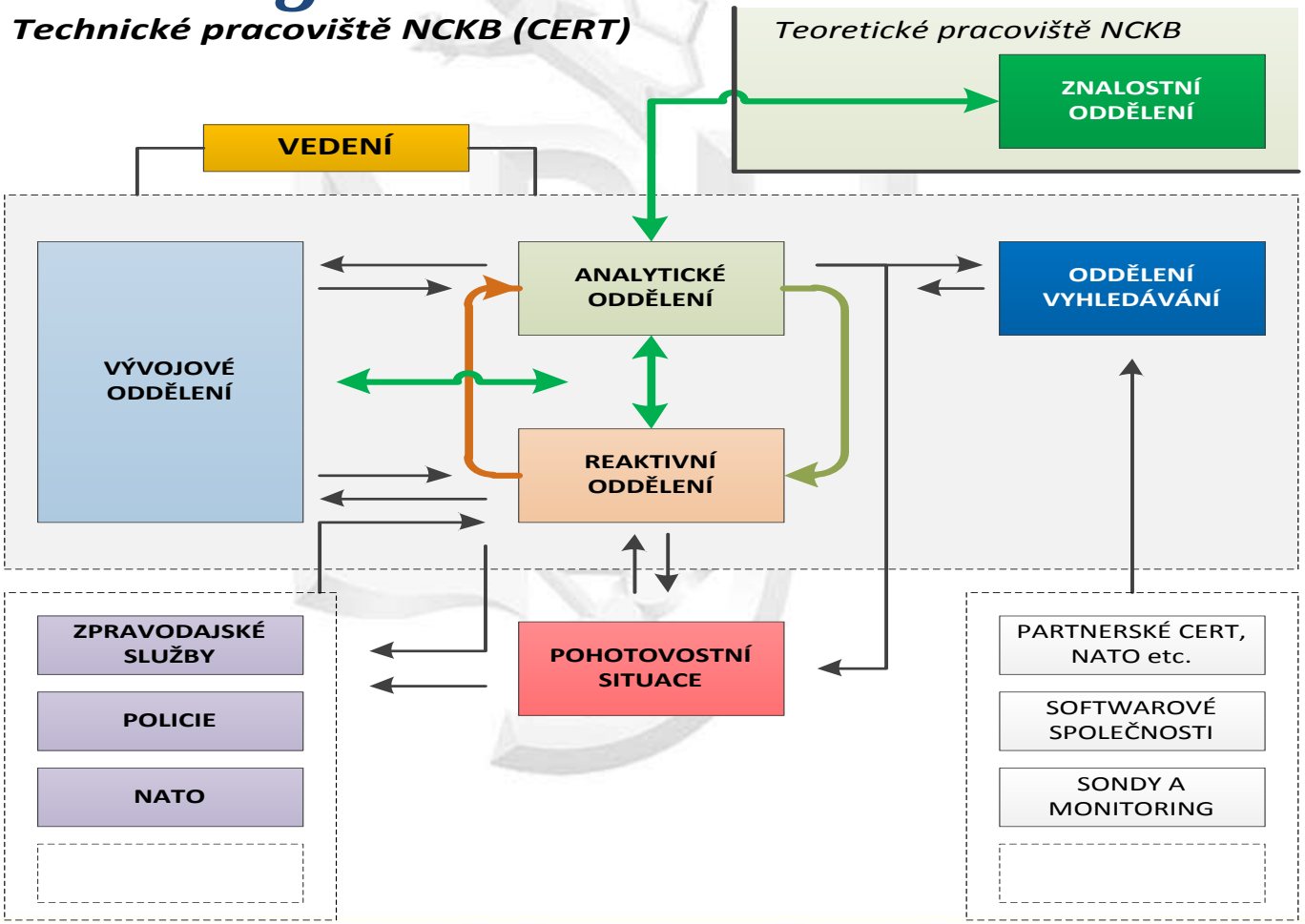
Ostatní činnosti

Tvorba standardů
Výzkum a vývoj
Analýza zranitelností a hrozeb
Prevence a vzdělávání
Kontrola
Spolupráce s ostatními NCKB a CERT pracovišti
Best practices
Školení
Mezinárodní spolupráce ve vybraných oblastech
Provozování webového portálu
Příprava scénářů pro kybernetická cvičení
Podpora vyšetřování kyber-kriminality a kyber-terorismu
Testování zranitelností

Ostatní útvary NBÚ

Legislativa
Státní dozor
Podpůrné činnosti
- -Sjednávání mezinárodních smluv
- -Materiálně technické zabezpečení
- -ICT
- -Provozní zabezpečení
- -Krypto

Vládní CERT
-
organizační struktura



národní centrum kybernetické bezpečnosti

Vládní CERT
-
technické a programové zabezpečení

- Spolehlivé dostatečně kapacitní napojení na Internet
- Linky pro příjem informací o incidentech
- Síť senzorů
- Incident handling systém
- Vývojové a testovací prostředí
- …

Děkuji za pozornost a případné dotazy rád zodpovím v diskusi.

Jaroslav Šmíd
Tel.: 420 257 283 333
e-mail: J.Smid@nbu.cz