Jak by měl vedoucí pracovník prosazovat zásady kybernetické bezpečnosti

Ing. Jiří Sedláček
Chief of Security Experts
jiri.sedlacek@nsmcluster.com

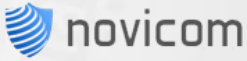
IDET 2015

NSM NETWORK SECURITY MONITORING CLUSTER | Our Vision Your Security

Kdo jsme…

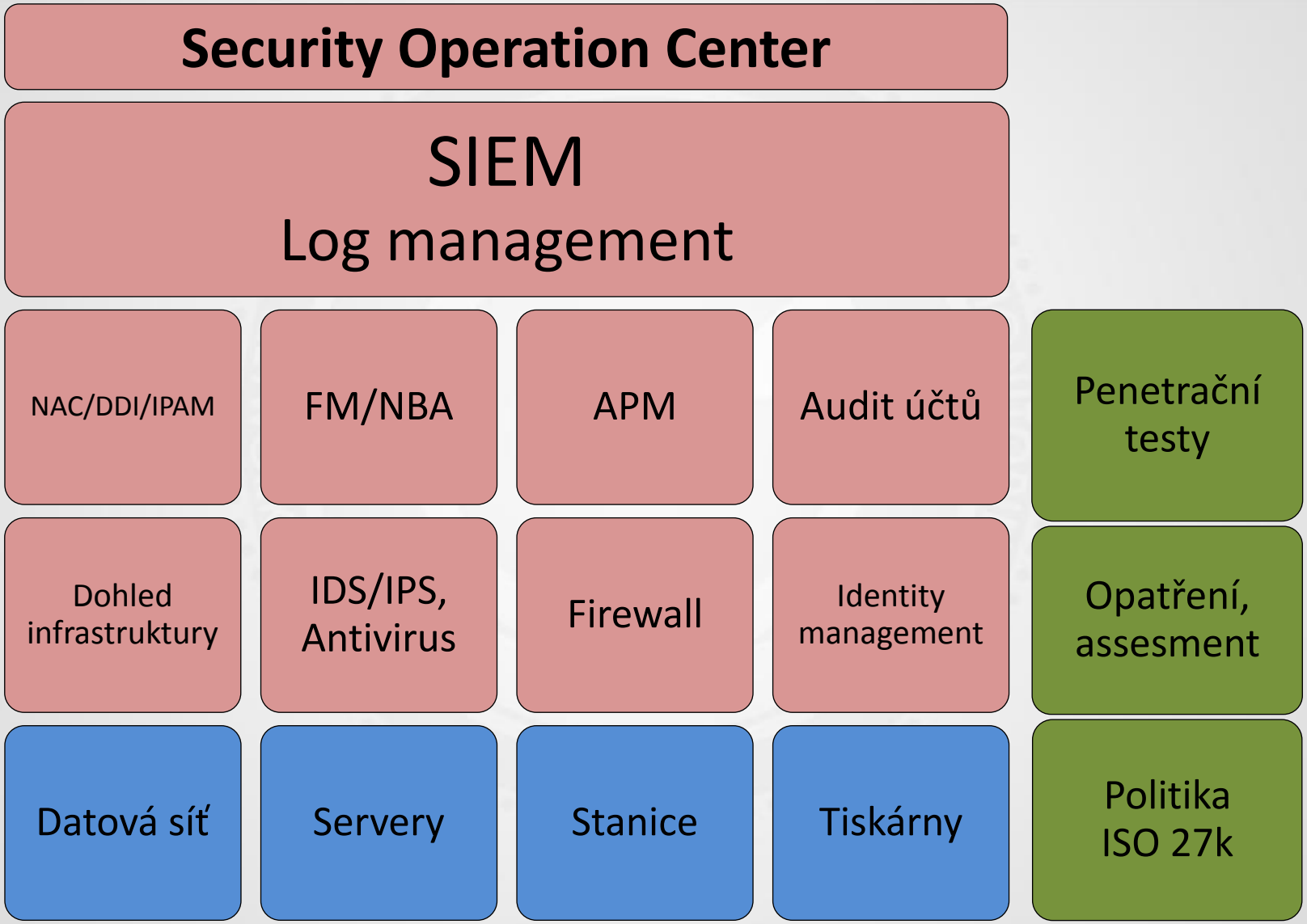
NSM
NETWORK SECURITY MONITORING CLUSTER

- Kooperační odvětvové uskupení 19 firem se specializací na bezpečnost v ICT,
- firmy s vlastními produkty, ale i integrátoři komplexních řešení.



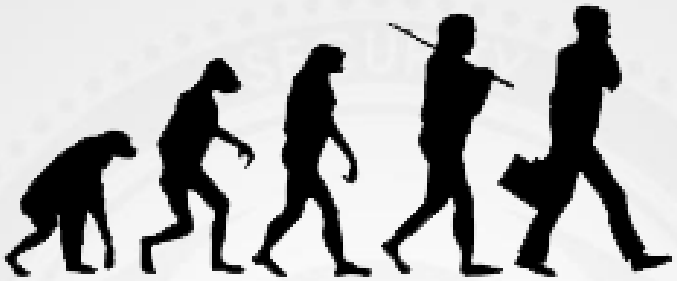
Portfolio NSMC

NSM
NETWORK SECURITY MONITORING CLUSTER



Malé ohlédnutí

NSM
NETWORK SECURITY MONITORING CLUSTER



sálové počítače	první PC	www	mobilní zařízení
1960…	1970…	1980…	současnost

chytré spotřebiče

Základní pojmy

NSM
NETWORK SECURITY MONITORING CLUSTER

Kybernetická bezpečnost

Souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru.

Kybernetický prostor

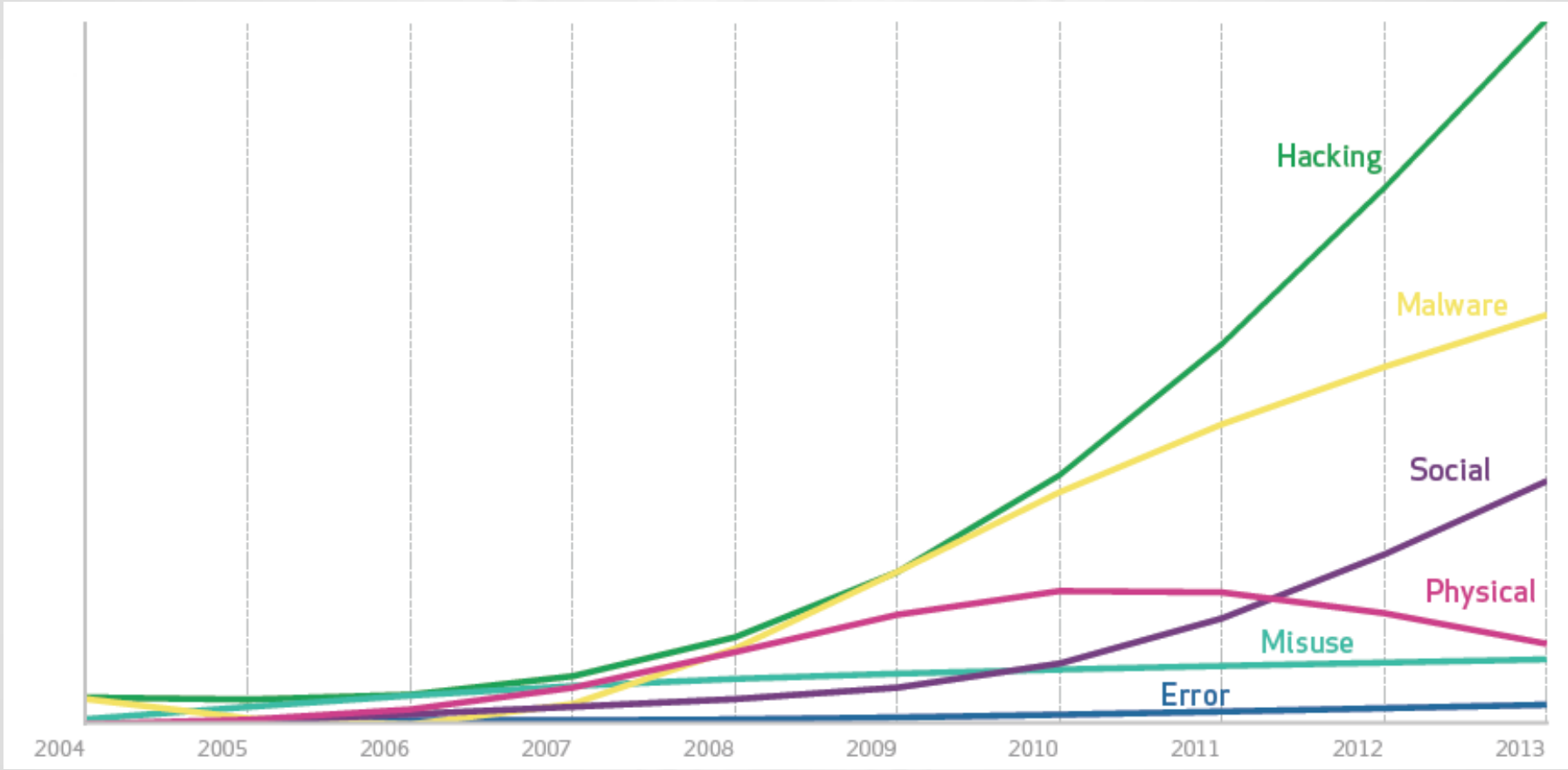
Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací[1)].

[1)] Zákon č. 127/2005 Sb., o elektronických komunikacích.

Proč se zabývat KB?

NSM
NETWORK SECURITY MONITORING CLUSTER

Nárůst kybernetických útoků (období 2004 – 2013)



Zdroj: Verizon 2014 data breach investigations report

Překážky v prosazování KB

NSM
NETWORK SECURITY MONITORING CLUSTER

- Nízké povědomí
  - bagatelizace – „doposud se nic nestalo…“,
  - podceňování.
- Peníze.
- Nekvalifikovaní IT zaměstnanci,
  - souběh pracovních rolí.
- Nedostatečná pravomoc manažera KB,
  - nezajištění podpory managementu.
- Vazba manažera KB na IT,
  - manažer KB je současně vedoucím IT.

Jak na kybernetickou bezpečnost?

NSM
NETWORK SECURITY MONITORING CLUSTER

Právní předpisy

Normy a metodiky

Odborníci, know-how

Evangelizace

Technologie

40/2009 Sb.
101/2000 Sb.
365/2000 Sb.
181/2014 Sb.
315/2014 Sb.
316/2014 Sb.
317/2014 Sb.

ITIL
COBIT
CRAMM
ISMS ISO/IEC 27001:2014
ISMS ISO/IEC 27002:2014
BCMS ISO 2301:2014
BCMS ISO 2313:2014.

Podpora managementu

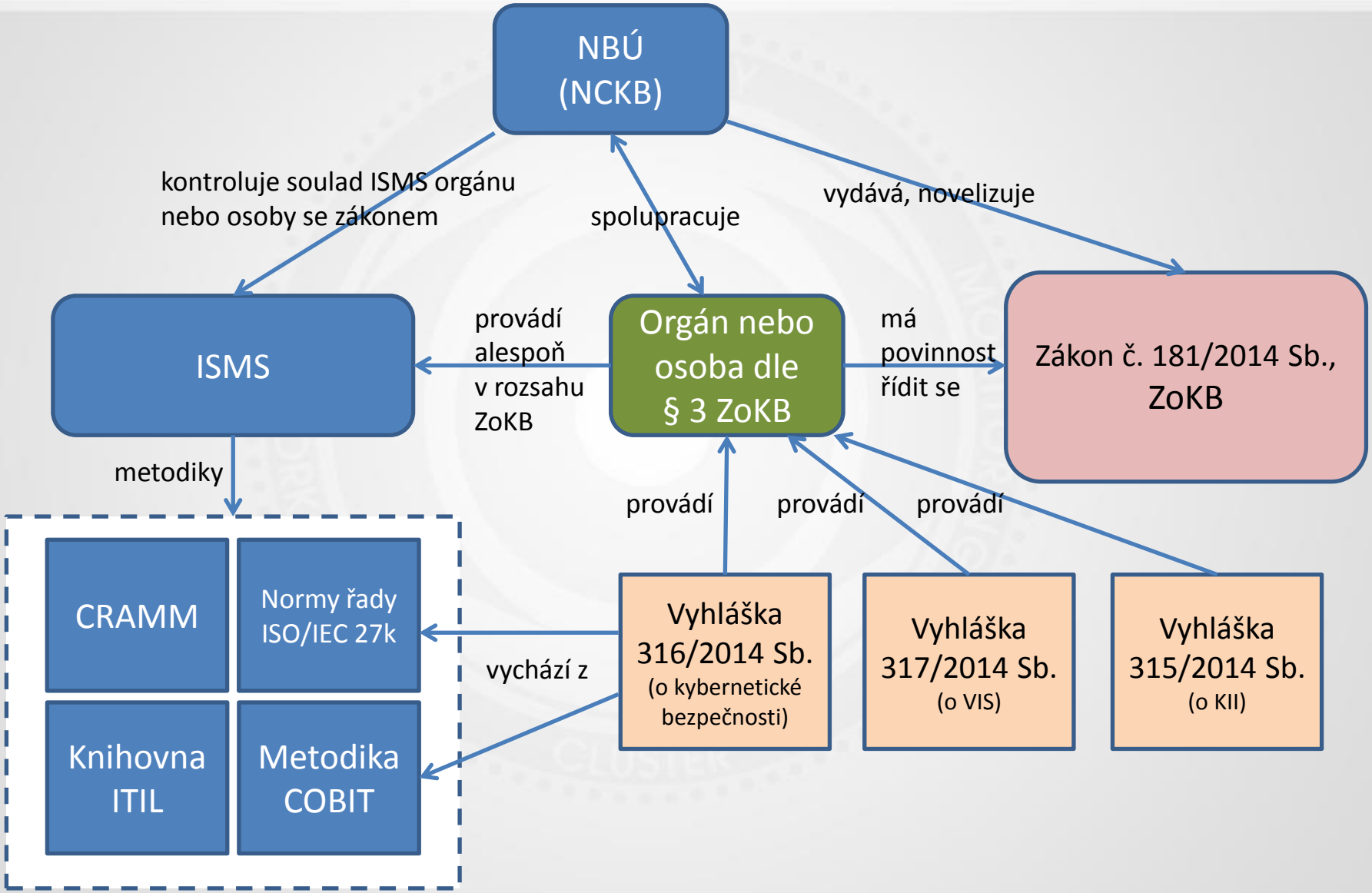
Interní směrnice

ZoKB

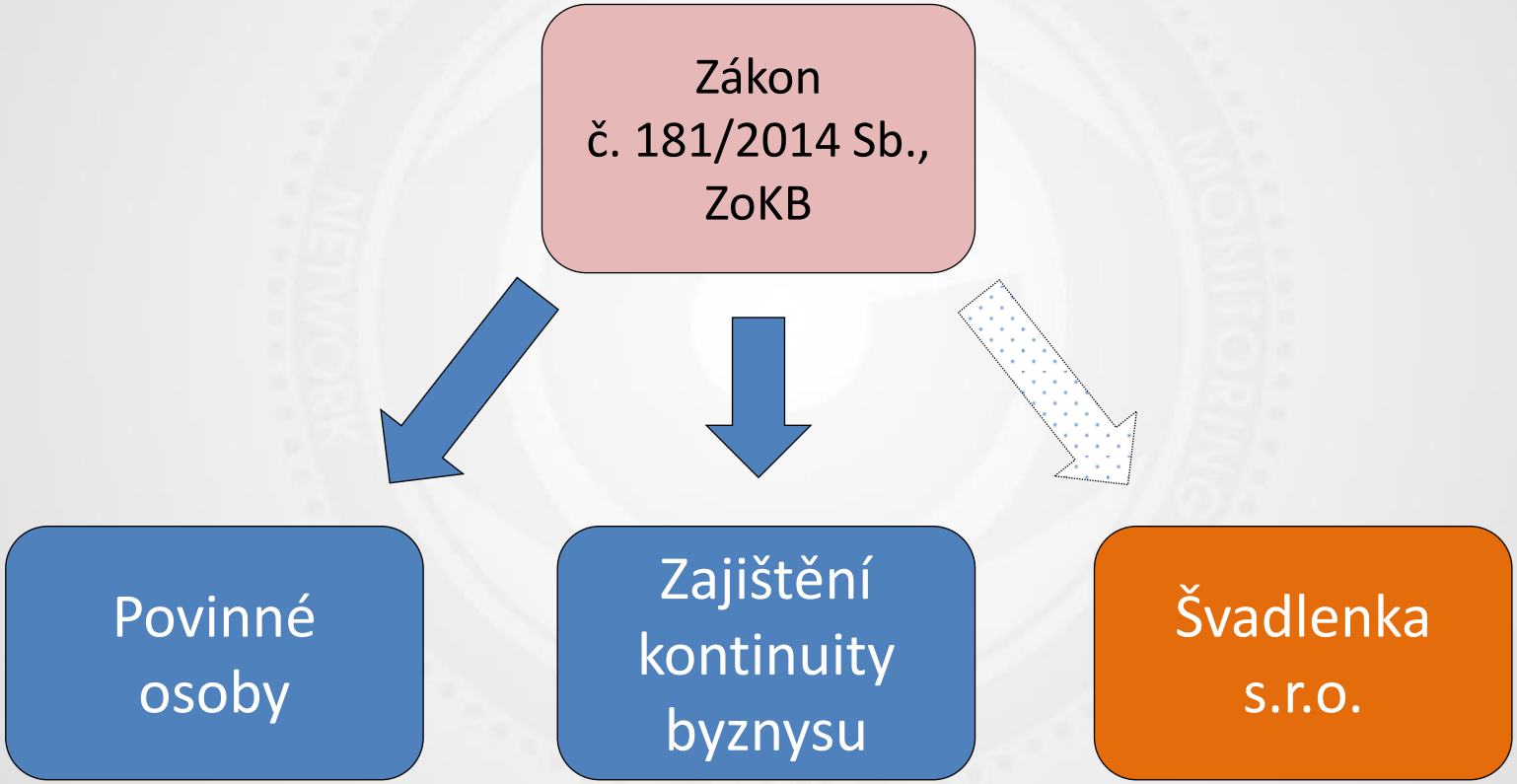
NSM
NETWORK SECURITY MONITORING CLUSTER

- Významný **milník** v české legislativě,
- krok k **vyšší bezpečnosti** v kybernetickém prostředí státních institucí i firem,
- významné **zvýšení standardu bezpečnosti** a dostupnosti služeb, které jsou v kyberprostoru občanům poskytovány.
- nezaměřuje se pouze na úzkou oblast problému, ale nabízí **kompletní návod**, jak postavit základy bezpečnosti ve společnosti a dále ji vylepšovat.

ZoKB


NBÚ
(NCKB)
kontroluje soulad ISMS orgánu
nebo osoby se zákonem
spolupracuje
vydává, novelizuje
ISMS
provádí
alespoň
v rozsahu
ZoKB
Orgán nebo
osoba dle
§ 3 ZoKB
má
povinnost
řídit se
Zákon č. 181/2014 Sb.,
ZoKB
metodiky
provádí
provádí
provádí
CRAMM
Normy řady
ISO/IEC 27k
Knihovna
ITIL
Metodika
COBIT
vychází z
Vyhláška
316/2014 Sb.
(o kybernetické
bezpečnosti)
Vyhláška
317/2014 Sb.
(o VIS)
Vyhláška
315/2014 Sb.
(o KII)

Potřebuji ZoKB?



Jaká opatření nám ukládá ZoKB?

NSM
NETWORK SECURITY MONITORING CLUSTER

- Systém řízení bezpečnosti informací.
- Organizační bezpečnost.
- Řízení dodavatelů.
- Bezpečnost lidských zdrojů.
- Řízení provozu a komunikací.
- Řízení kontinuity činností.
- Řízení přístupu.
- Bezpečné chování uživatelů.

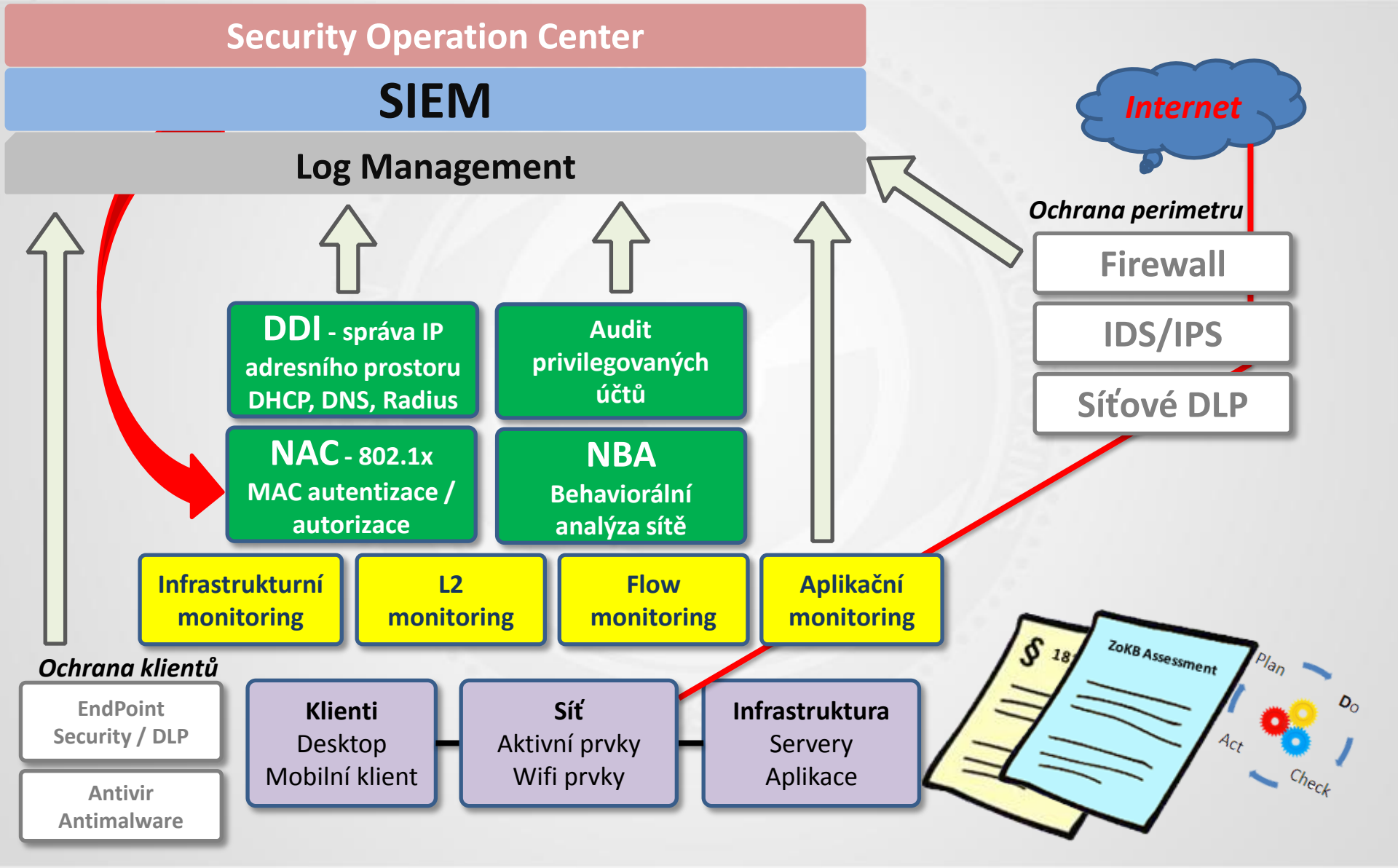
- Fyzická bezpečnost.
- Nástroj pro ochranu integrity komunikačních sítí.
- Nástroj pro ochranu před škodlivým kódem.
- Nástroj pro zaznamenávání činností IS, uživatelů, administrátorů.
- Nástroj pro detekci kybernetických bezpečnostních událostí.

Standardní topologie

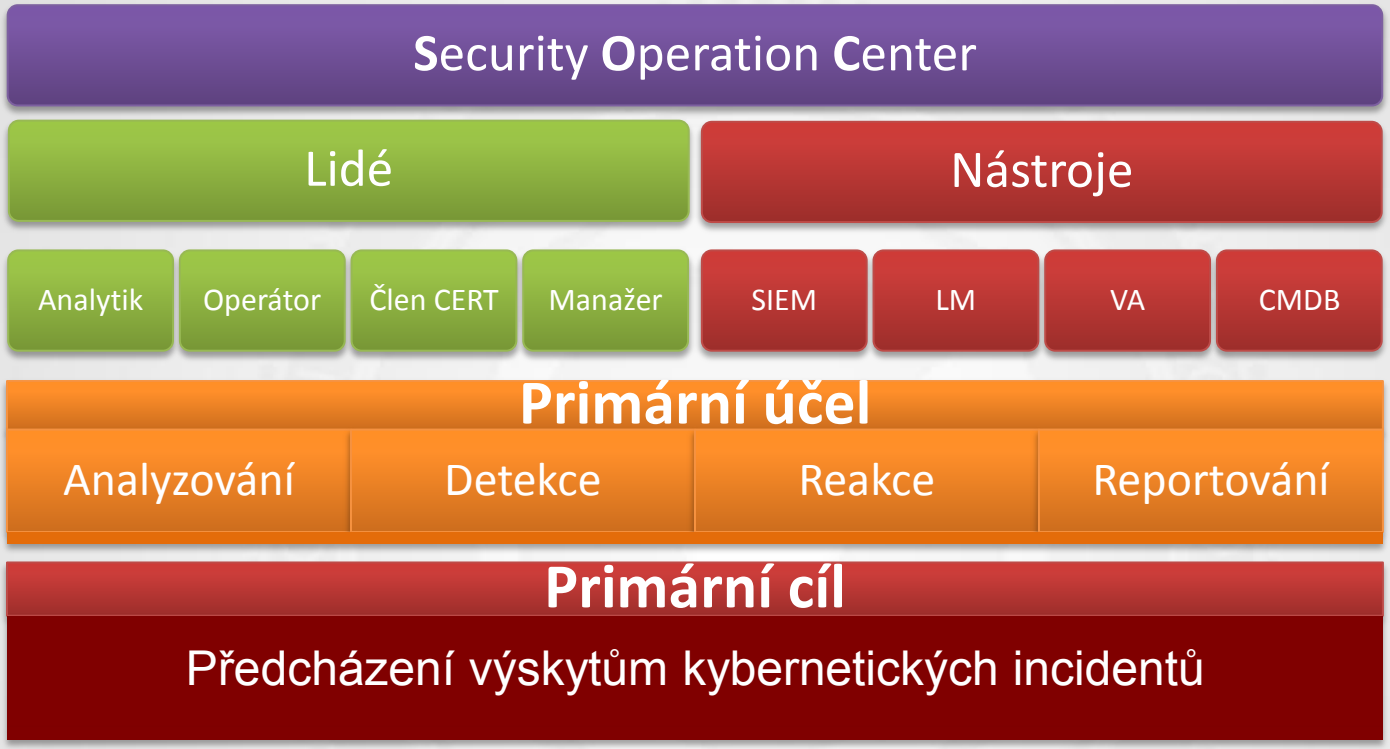
Běžně je bezpečnost ICT řešena pouze na úrovni perimetru.

NSMC koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury

NSM
NETWORK SECURITY MONITORING CLUSTER

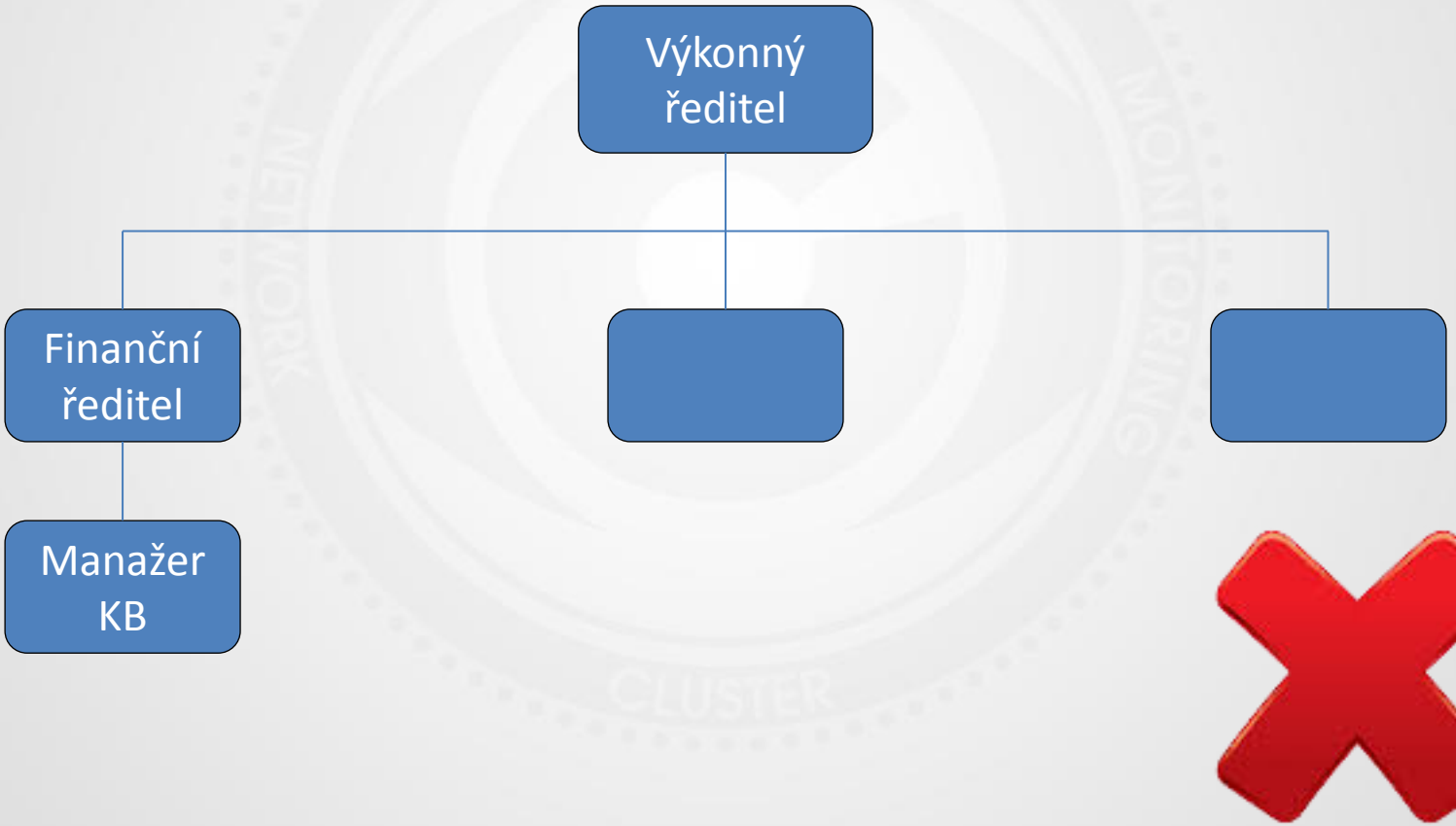


Security Operation Center

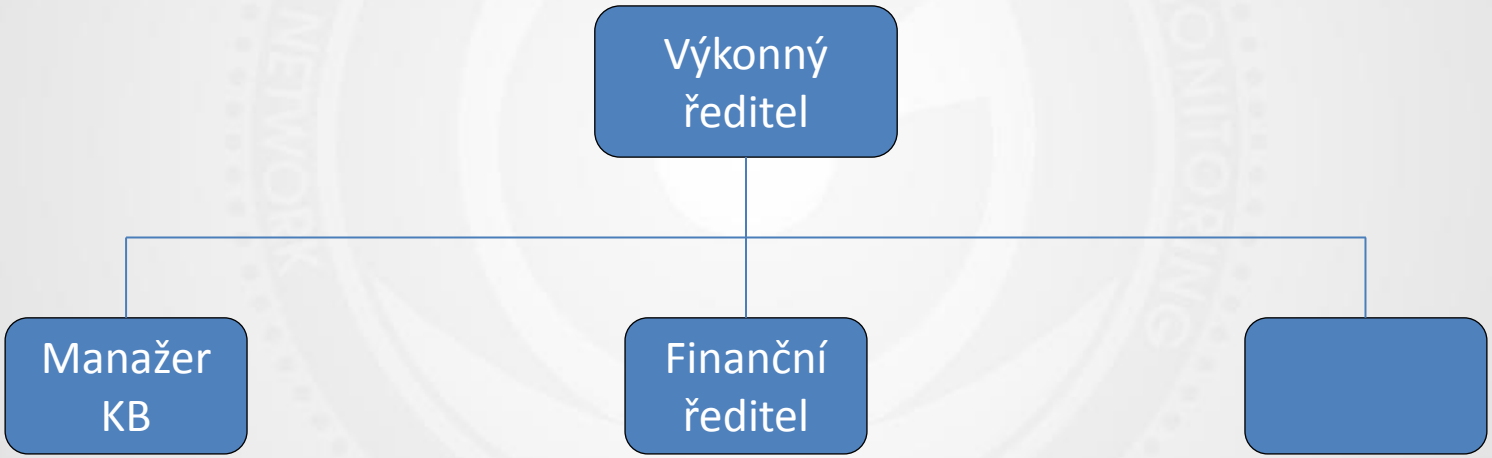


***SIEM** – **S**ecurity **I**nformation and **E**vent **M**anagement – Srdce SOC/KOC, nástroj na detekci bezpečnostní incidentů.*
***NBA** – **N**etwork **B**ehavior **A**nalysis - Vysoce Inteligentní systém na Detekci Anomálií.*
***VA** – **V**ulnerability **A**ssesment – Detekce zranitelností v IT infrastruktuře.*
***CMDB** – **C**onfiguration **M**anagement **D**ata**b**ase – Evidence všech aktiv z pohledu IT, spolu s jejich vztahy/závislosti.*
***LM** – **L**og **M**anagement*

Jak mohu prosazovat KB?



Jak mohu prosazovat KB?



Řízení lidských zdrojů

NSM
NETWORK SECURITY MONITORING CLUSTER

- Lidské zdroje se často označují pojmem "lidský kapitál„,
- jedná se o oblast strategického významu,
- zodpovědnost každého vedoucího pracovníka,
- lidský faktor je určujícím prvkem pro úspěšnost organizace.

"Systém je bezpečný tak, jak bezpečný je jeho nejslabší článek. Nejslabším článkem jsou lidé„. (Bruce Schneider)

„HW atakují pouze amatéři... Profesionálové se zaměřují na lidi...“. (Bruce Schneider)

Školení kybernetické bezpečnosti

NSM
NETWORK SECURITY MONITORING CLUSTER

- Vzdělávací kurz pro vedoucí pracovníky a management,
- evangelizace v oblasti KB,
- možnost reálné simulace a návrhu zabezpečení ICT jednotlivých účastníků (tedy jejich organizací), v souladu se ZoKB.

- Místo:
  - Brno,
  - Praha.
- Varianty
  - technické (2d, 5d),
  - manažerské (3h, 2d).

Kam dál?

NSM
NETWORK SECURITY MONITORING CLUSTER

- Informace o technologiích včetně živé ukázky ve vedlejším sále (INVEA-TECH a Novicom).

- FlowMon Friday – celodenní konference o technologiích Flow Monitoring, NBA, DDI.
- Vize, strategie, budoucnost technologie.
- Hosté – Novicom, CISCO, ČD-Telematika.
- Pátek 29.5, Konferenční Centrum City – Praha Pankrác.
- Registrace na registration@invea.com

Děkuji za pozornost

NSM
NETWORK SECURITY MONITORING CLUSTER

Ing. Jiří Sedláček
jiri.sedlacek@nsmcluster.com

Network Security Monitoring Cluster
CERIT Science Park, Botanická 68a
Brno, 602 00, Czech Republic
info@nsmcluster.com
www.nsmcluster.com