Bezpečnost lidských zdrojů

Ing. Jiří Sedláček
NSMC, TP-KB

NSMC, TPKB

NSM
NETWORK SECURITY MONITORING CLUSTER

Sdružení českých firem a expertů zabývajících se kybernetickou bezpečností.

Znalostní platforma zaměřená na evangelizaci problematiky počítačové bezpečnosti.

Komplexní zajištění KB v organizaci.

Sídlo

- Brno – CERIT MU
- Jundrov

Řídící výbor

Ladislav Chodák

Lukáš Přibyl

Jiří Sedláček

Založení

2010

SSPS
Smíchovská střední průmyslová škola

Střední škola informatiky, poštovnictví a finančnictví Brno

NSMC portfolio služeb

NETWORK SECURITY MONITORING CLUSTER

IMPLEMENTACE

- ANALÝZY, GAP ANALÝZY, POSOUZENÍ SOULADU
- STUDIE PROVEDITELNOSTI
- ANALÝZY RIZIK Z POHLEDU LEGISLATIVY A STANDARDŮ (ISMS, ZoKB, GDPR)
- IMPLEMENTACE PRINCIPŮ A POLITIK V SOULADU SE ZoKB A ISMS ISO 27K
  - ORGANIZAČNÍ A TECHNICKÁ OPATŘENÍ
- PENETRAČNÍ TESTY

EDUKACE

- VZDĚLÁVACÍ KURZY PRO IT A NE IT PRACOVNÍKY A MANAGEMENT
- VZDĚLÁVACÍ KURZY PRO SŠ (ŘEDITELÉ A UČITELÉ)
- ZAVEDENÍ VÝUKY KB DO VZDĚLÁVACÍHO SYSTÉMU STŘEDNÍHO ŠKOLSTVÍ (PILOT V BRNĚ A PRAZE)

PORADENSKÉ SLUŽBY

- PRO ORGANIZACE V RÁMCI ČR, I V ZAHRANIČÍ

Proč se zabývat vzděláváním v oblasti KB?

NSM
NETWORK SECURITY MONITORING CLUSTER

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020

„Český model vzdělávání a výchovy v oblasti kybernetické bezpečnosti neodpovídá v současné podobě aktuálním požadavkům a trendům. Z tohoto důvodu pak nedostatečně vzdělává a vychovává na základním a středním stupni žáky a také v nedostatečné míře nabízí vysokoškolské programy, které by vytvářely odborníky na kybernetickou bezpečnost.
Poptávka po těchto odbornících je přitom vysoká.“

Admini strátor

Manažer KB

Operátor

Architekt KB

DPO

Auditor KB

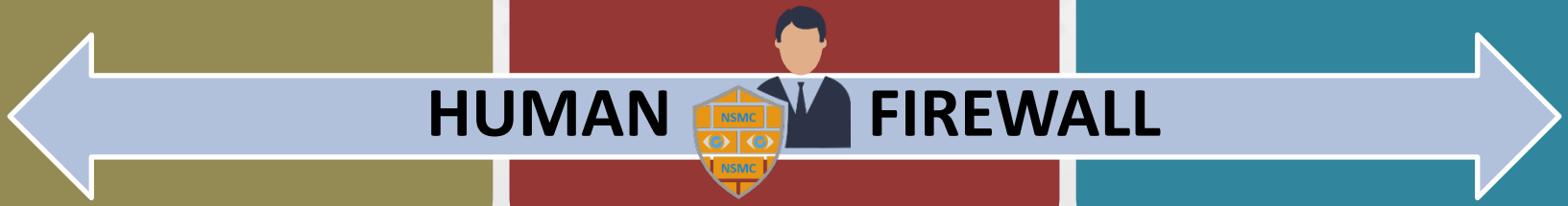
Proč tedy vzdělávat?

NSMC
NETWORK SECURITY MONITORING CLUSTER

Orientace v dnešním kybernetickém světě

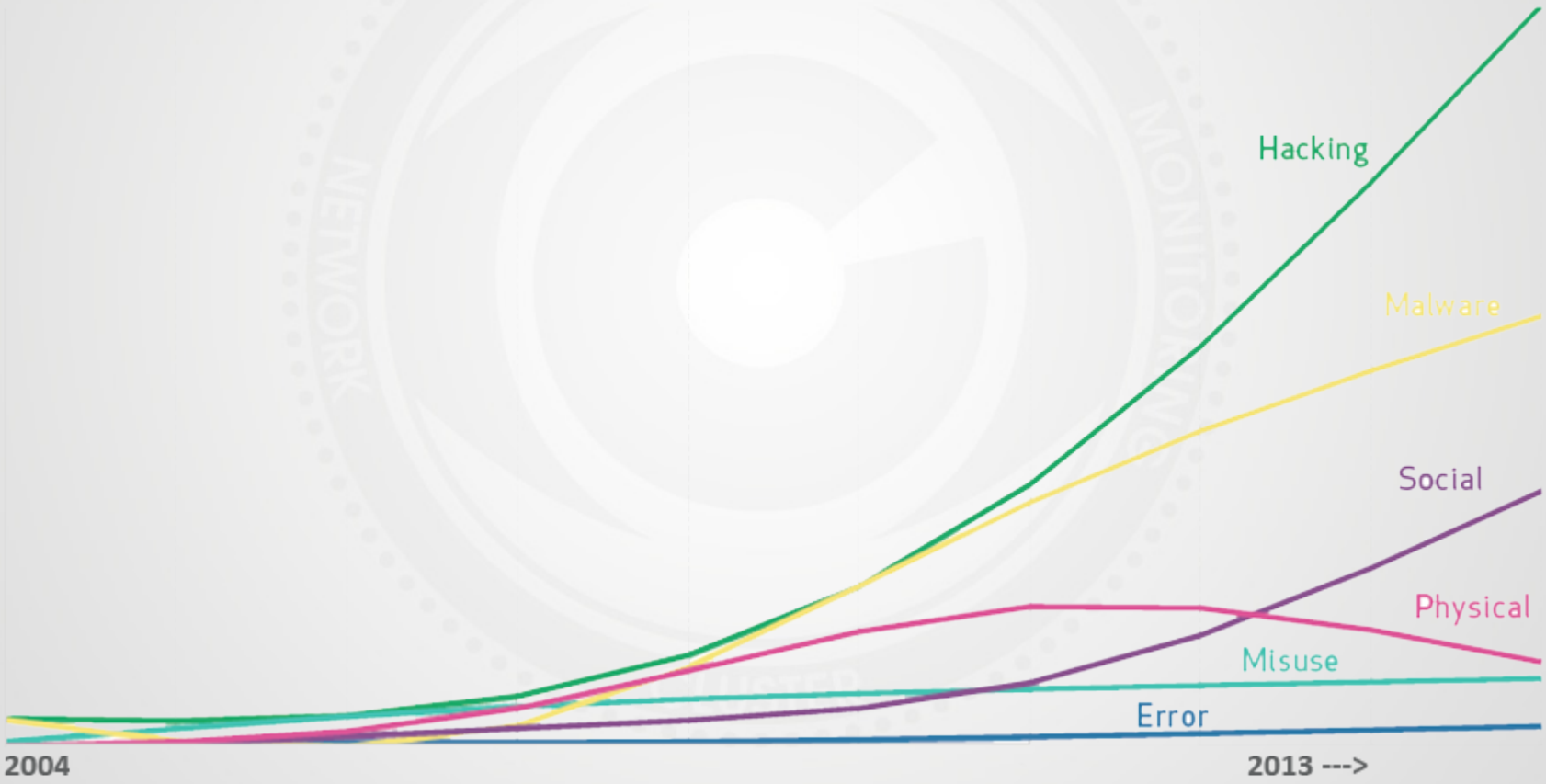
Orientace v právní problematice KB

Správná terminologie



Nárůst kybernetických útoků

NSM
NETWORK SECURITY MONITORING CLUSTER



Zdroj: Verizon data breach investigations report

Kybernetická bezpečnost

NSM
NETWORK SECURITY MONITORING CLUSTER

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

Aktiva z pohledu VyKB §2

NSM
NETWORK SECURITY MONITORING CLUSTER

Primární

- Informace nebo služba (kterou zpracovává nebo poskytuje informační a komunikační systém)

Podpůrná

- Technická
  - Technické vybavení
  - Komunikační prostředky
  - Programové vybavení
  - Objekty, ve kterých jsou umístěny IS a KS
- Zaměstnanci
- Dodavatelé ICT

Jako aktivum označujeme cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu.
Výkladový slovník KB

Vybrané hrozby dle VyKB

NSM NETWORK SECURITY MONITORING CLUSTER

Hrozby (nechtěné události)

- porušení **bezpečnostní politiky**, provedení **neoprávněných činností**, zneužití **oprávnění** ze strany uživatelů a administrátorů,
- poškození nebo selhání **technického anebo programového vybavení**,
- zneužití i**dentity**,
- užívání programového vybavení **v rozporu** s licenčními podmínkami,
- škodlivý **kód** (například viry, spyware, trojské koně),
- narušení **fyzické** bezpečnosti,
- přerušení poskytování služeb **elektronických komunikací** nebo dodávek **elektrické energie**,
- zneužití nebo neoprávněná **modifikace údajů**,
- ztráta, odcizení nebo poškození **aktiva**,
- nedodržení smluvního závazku ze strany **dodavatele**,
- pochybení ze strany **zaměstnanců**,
- zneužití vnitřních prostředků, **sabotáž**,
- **dlouhodobé** přerušení poskytování služeb **elektronických komunikací**, dodávky **elektrické energie** nebo jiných důležitých služeb,
- nedostatek **zaměstnanců** s potřebnou odbornou úrovní,
- cílený kybernetický útok pomocí **sociálního inženýrství**, použití špionážních technik,
- zneužití **vyměnitelných** technických **nosičů dat**,
- napadení **elektronické komunikace** (odposlech, modifikace).

Vybrané zranitelnosti dle VyKB

NSM
NETWORK SECURITY MONITORING CLUSTER

Zranitelnosti (slabá místa, nedostatky)

- nedostatečná **údržba** informačního a komunikačního systému,
- **zastaralost** informačního a komunikačního systému
- nedostatečná **ochrana** vnějšího perimetru,
- nedostatečné **bezpečnostní povědomí** uživatelů a administrátorů,
- nevhodné **nastavení přístupových oprávnění,**
- nedostatečné **postupy** při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- nedostatečné **monitorování** činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
- nedostatečné **stanovení bezpečnostních pravidel**, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
- nedostatečná **ochrana aktiv**,
- nevhodná **bezpečnostní architektura**,
- nedostatečná **míra nezávislé kontroly**,
- neschopnost **včasného** odhalení pochybení ze strany zaměstnanců.

Spasí nás technologie?

NSMC
NETWORK SECURITY MONITORING CLUSTER

- Velká část bezpečnostních incidentů je způsobena lidským faktorem (cca 59%),
- vedoucí pracovníci se tradičně zaměřují na vyřešení bezpečnostních problémů investováním do technologií, nikoli do lidí,
- investování výhradně do technologií neřeší hlavní příčinu incidentů: chování zaměstnanců,
- technologie je pouze nástroj.

Lidský faktor…

NSM
NETWORK SECURITY MONITORING CLUSTER

Katastrofa je přisuzována špatné konstrukci reaktoru, jeho kontraintuitivním vlastnostem, **nedodržení podmínek**, na které byl plánovaný pokus připraven, a **obecnému nedostatku bezpečnostní kultury.** Stejně jako v Three Mile Island byl druhotným faktorem přispívajícím k havárii fakt, že **elektrárenští operátoři nebyli dostatečně vyškoleni a obeznámeni s mnoha charakteristikami reaktoru.**

ZoKB - VyKB §9 Bezpečnost lidských zdrojů

NSM
NETWORK SECURITY MONITORING CLUSTER

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení bezpečnosti lidských zdrojů

a) stanoví plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a určí osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny,

b) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,

c) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a

d) zajistí vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.

(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona vede o školení podle odstavce 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

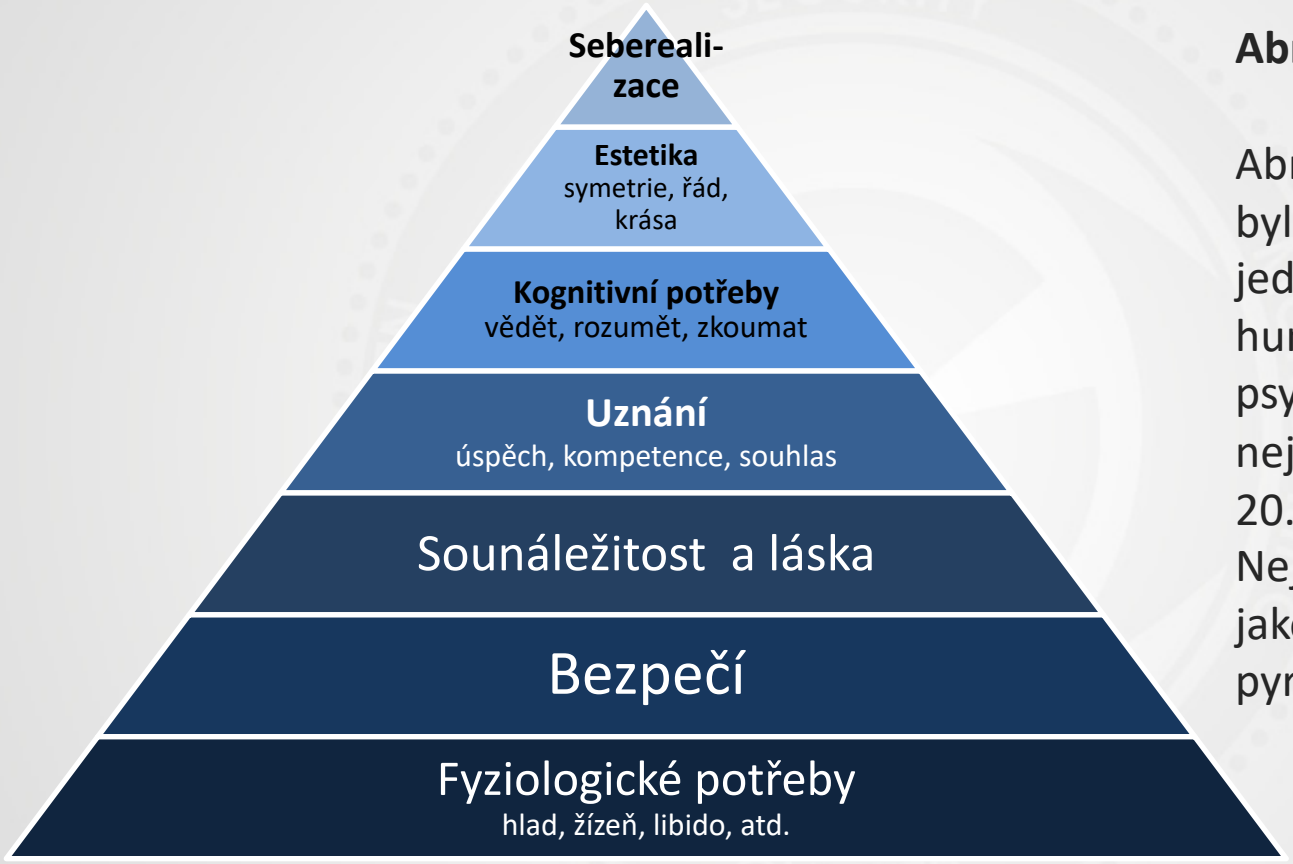
a) stanoví pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů,

b) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí,

c) určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a

d) zajistí změnu přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.

Maslowowa pyramida



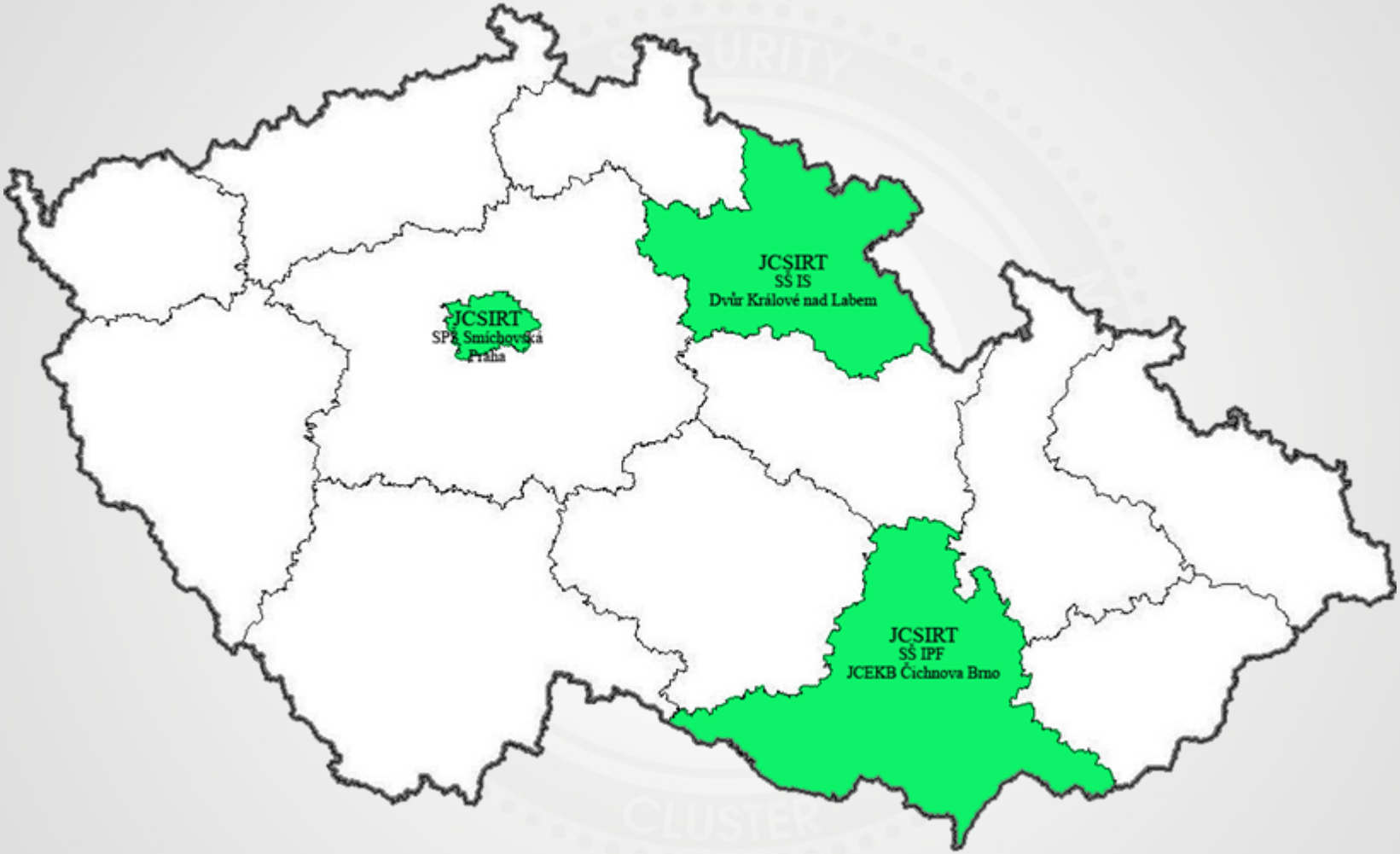
Abraham Harold Maslow

Abraham Harold Maslow byl americký psycholog, jeden ze zakladatelů humanistického proudu v psychologii, 10. nejcitovanější psycholog ve 20. století.
Nejčastěji bývá uváděn jako autor tzv. Maslowovy pyramidy lidských potřeb.

„Člověk je skládankou potřeb. Dej mu chybějící článek a on Ti dá cokoli…“ úryvek ze špionážního filmu z prostředí postsovětského Ruska

NSMC koncept JCE IB v ČR

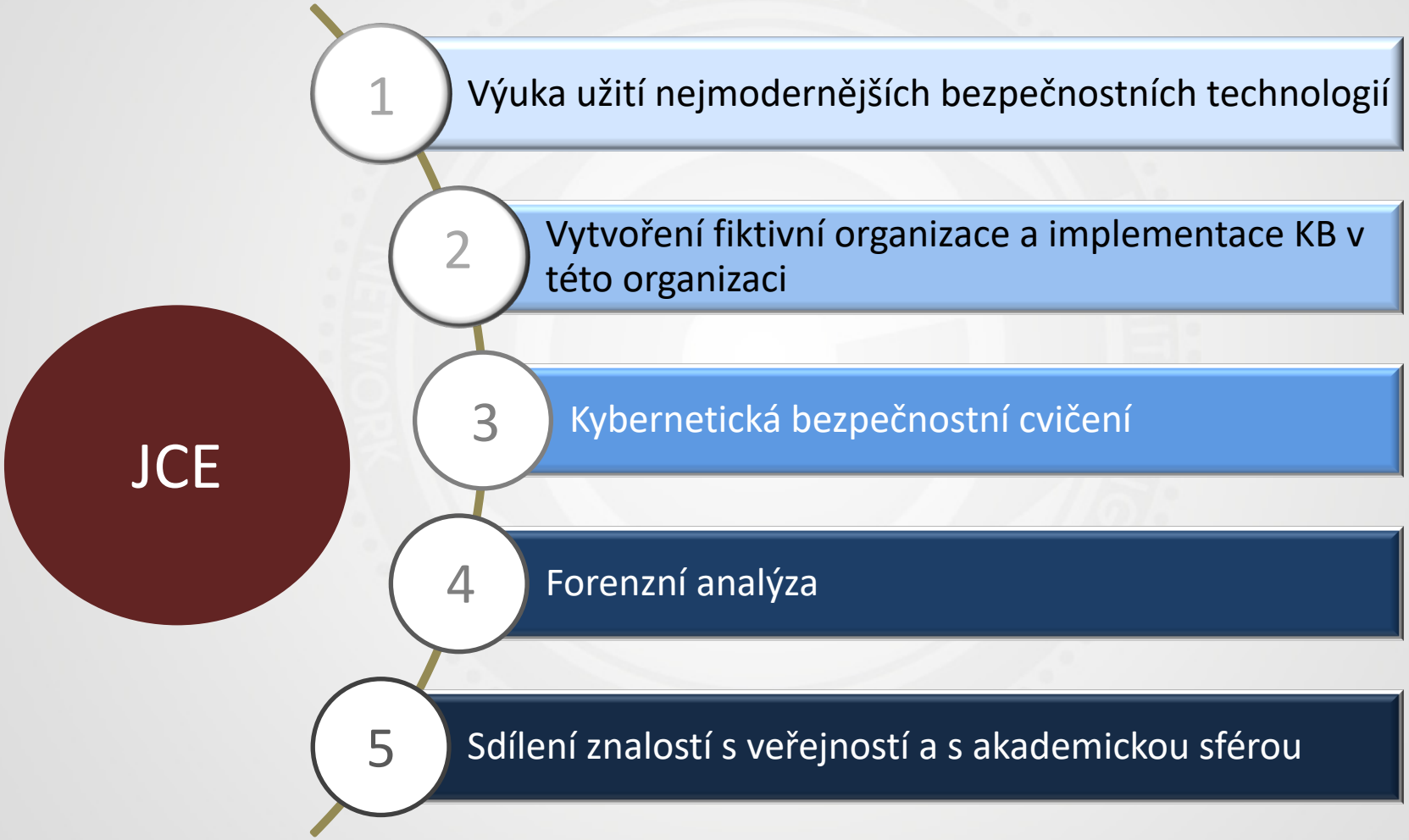
NSM
NETWORK SECURITY MONITORING CLUSTER



Motto: ***„Excelentním centrem nemůže být každá střední škola. Každá střední škola ale může (i s pomocí excelentních center) vyučovat informační bezpečnost.„***

Možnosti využití JCE

NSM
NETWORK SECURITY MONITORING CLUSTER



Cesta není úplně jednoduchá

NSMC
NETWORK SECURITY MONITORING CLUSTER

JCE KB Čichnova - vizualizace CYLAB

NSM
NETWORK SECURITY MONITORING CLUSTER

Děkuji za pozornost

NSMC
NETWORK SECURITY MONITORING CLUSTER

Network Security Monitoring Cluster
Jundrovská 618/31
Brno, 624 00, Czech Republic
info@nsmcluster.com
www.nsmcluster.com

Ing. Jiří Sedláček
NSMC CEO
jiri.sedlacek@nsmcluster.com