Potřebujeme kybernetickou bezpečnost? Jak chráníme informační aktiva?

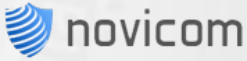
Ing. Jiří Sedláček
Chief of Security Experts
jiri.sedlacek@nsmcluster.com

24.9.2015
Kybernetická bezpečnost III

Kdo jsme…

NSM NETWORK SECURITY MONITORING CLUSTER

- Kooperační odvětvové uskupení 19 firem se specializací na bezpečnost v ICT.



Potřebujeme kybernetickou bezpečnost?

NSM
NETWORK SECURITY MONITORING CLUSTER

- Informační technologie, na kterých jsme dnes bezprostředně závislí, spolu komunikují v digitálním prostředí – kybernetickém prostoru.

Definice:

- **Kybernetický prostor**

  Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací1).

- **Kybernetická bezpečnost**

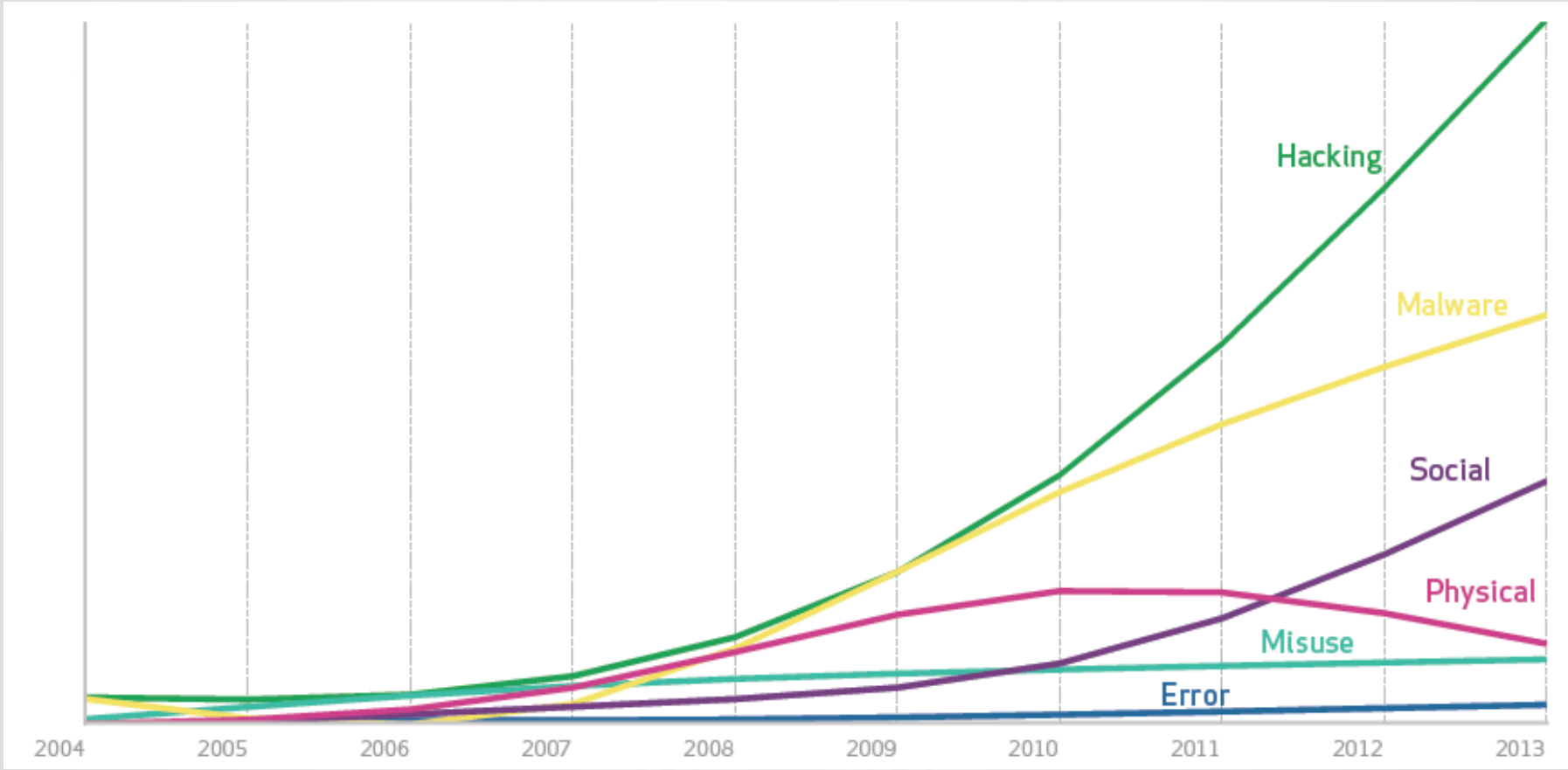
  Souhrn právních, organizačních, technických a vzdělávacích **prostředků** k zajištění ochrany kybernetického prostoru.

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

Proč se zabývat KB?

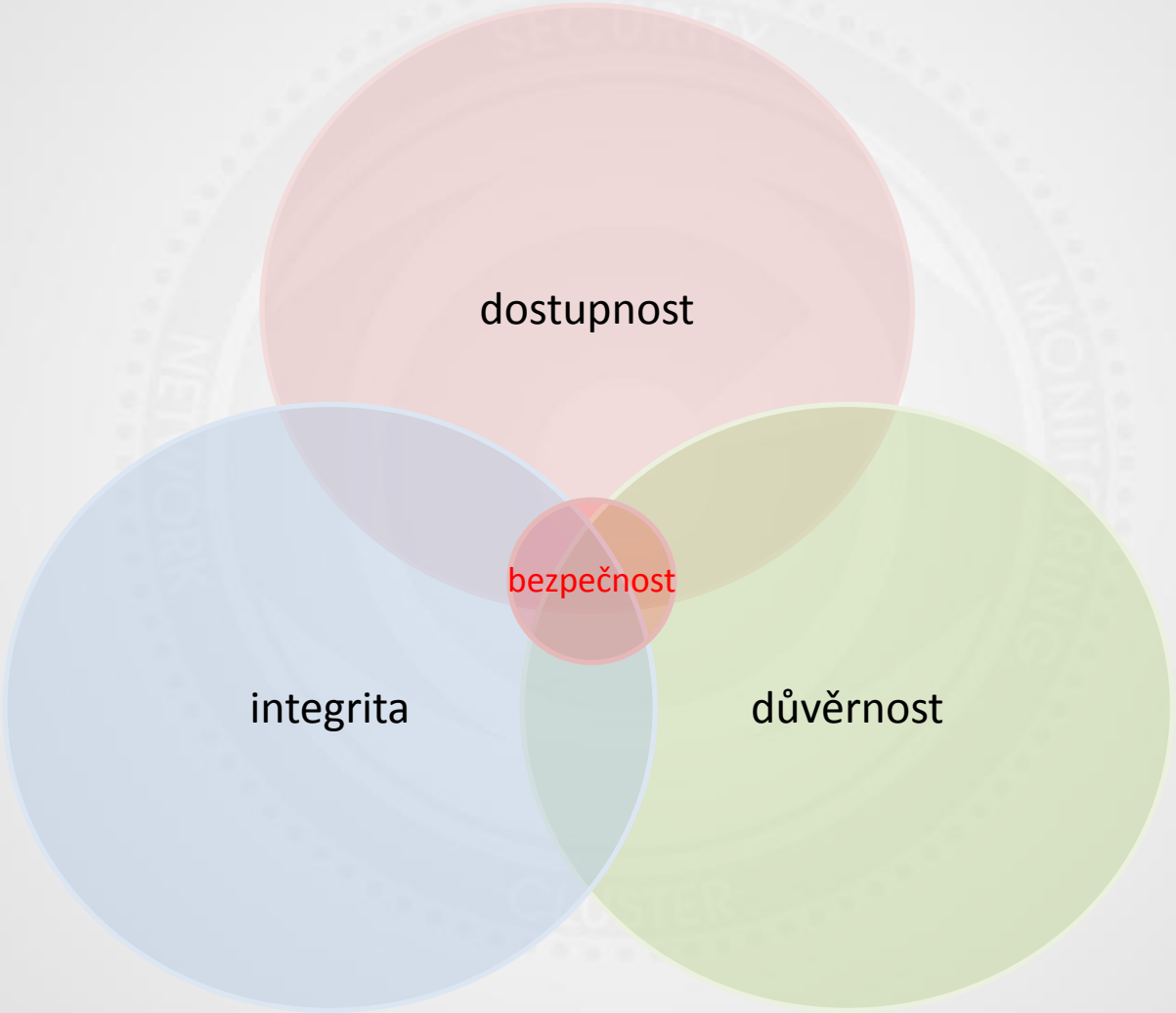
NSM
NETWORK SECURITY MONITORING CLUSTER

Nárůst kybernetických útoků (období 2004 – 2013)



Zdroj: Verizon 2014 data breach investigations report

Co je to bezpečná informace?



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
ISMS ISO/IEC 27002
BCMS ISO 2301
BCMS ISO 2313

Podpora managementu

Interní směrnice

Překážky v prosazování KB

NSM
NETWORK SECURITY MONITORING CLUSTER

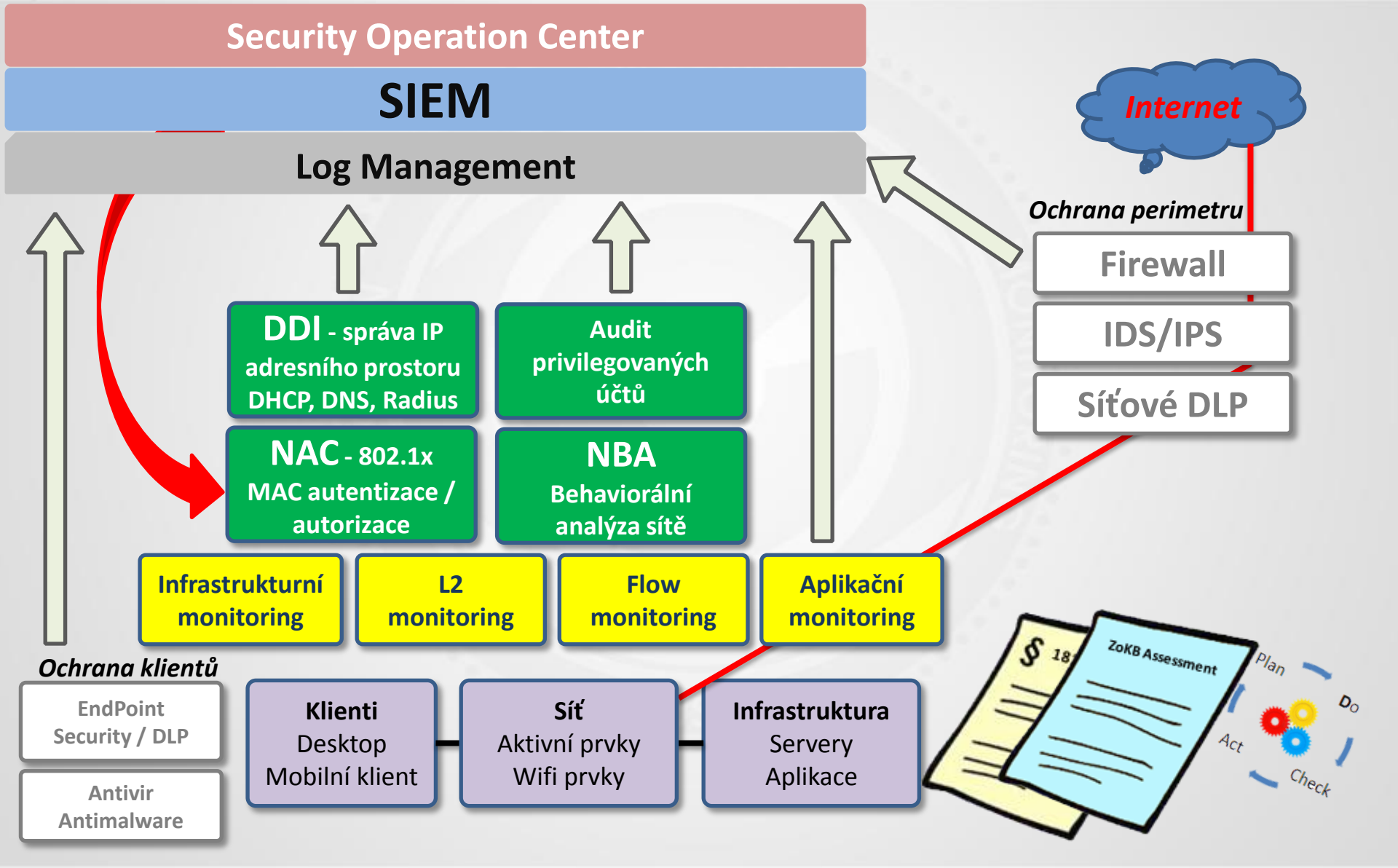
- **Nedostatečná evidence aktiv, chybějící klasifikace a kategorizace aktiv**
- **Chybějící analýza rizik a absence řízení rizik**
- **Nízké povědomí**
  - bagatelizace – „doposud se nic nestalo…“,
  - podceňování – „ono to nebude tak horké…“,
  - ignorance a vyhýbání se zodpovědnosti – „to řeší IT…“.
- **Peníze**
  - **Organizace chtějí poskytovat vyšší úroveň služeb a současně mají tendenci snižovat náklady**
- **Nekvalifikovaní IT zaměstnanci**,
  - špatná politika HR v otázce vzdělávání v oblasti ICT a KB,
  - omezený budget na vzdělávání,
  - souběh pracovních rolí.
- **Nedostatečná pravomoc manažera KB**,
  - nezajištění podpory managementu (manažer KB je podřízen FŘ).
- **Vazba manažera KB na IT**,
  - manažer KB je současně vedoucím IT.

Standardní topologie

Běžně je bezpečnost ICT řešena pouze na úrovni perimetru.

NSMC koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury

NSM
NETWORK SECURITY MONITORING CLUSTER



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)

Myslíme to s kybernetickou bezpečností vážně?

- 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.

Školení kybernetické bezpečnosti

- 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 … 2-denní
  - Manažerské … 1-denní

NSM
NETWORK SECURITY MONITORING CLUSTER

FlowMon

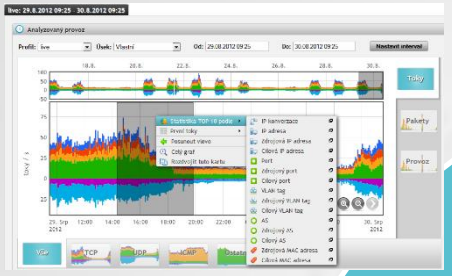
Vaše síť pod kontrolou!

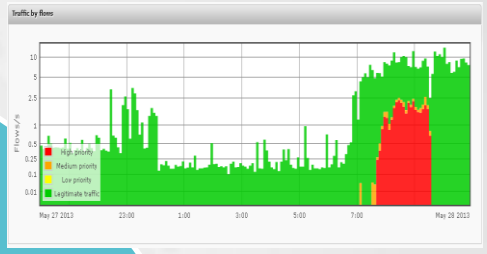
inveaTECH

Jiří Sedláček
jiri.sedlacek@nsmcluster.com

Zaměření produktu

NSM
NETWORK SECURITY MONITORING CLUSTER





Network visibility & security

Perimeter security

End point security

Gartner

Gartner last year stated that flow analysis should be done 80% of the time and that packet capture with probes should be done 20% of the time.

Recommendations

- Implement the use of advanced flow-based data sources to allow better measurement of the user experience.
- Implement flow-based monitoring technologies extensively, and leverage probes where detail is needed. Using a single platform for both makes management easier.

TIME Techland
News and reviews about gadgets, gear, apps and the web

Home | Gadgets | Apps & Web | News | Reviews & Features | Companies

SECURITY

DNSChanger: FBI Warns Infected Computers Will Lose Web, Email Access in July

By MATT PECKHAM | @mattpeckham | April 23, 2012 | 8

63%
OF THE ORGANIZATIONS IN OUR RESEARCH ARE INFECTED WITH BOTS

CHECK POINT 2013 SECURITY REPORT

The DATACENTER Journal
Where IT, Facilities and Design Meet

Attaining Network Visibility in the Era of Big Risk and Big Data

Jason Echols | May 29, 2013 | 1 Comment »

eurostat newsrelease

21/2011 - 7 February 2011

8 February 2011: Safer Internet Day

Nearly one third of internet users in the EU27 caught a computer virus

84% of internet users use IT security software for protection

Hlavní oblasti

NSM
NETWORK SECURITY MONITORING CLUSTER

FlowMon

Monitorování datových toků

Bezpečnost (NBA)

Záznam komunikace v plném rozsahu

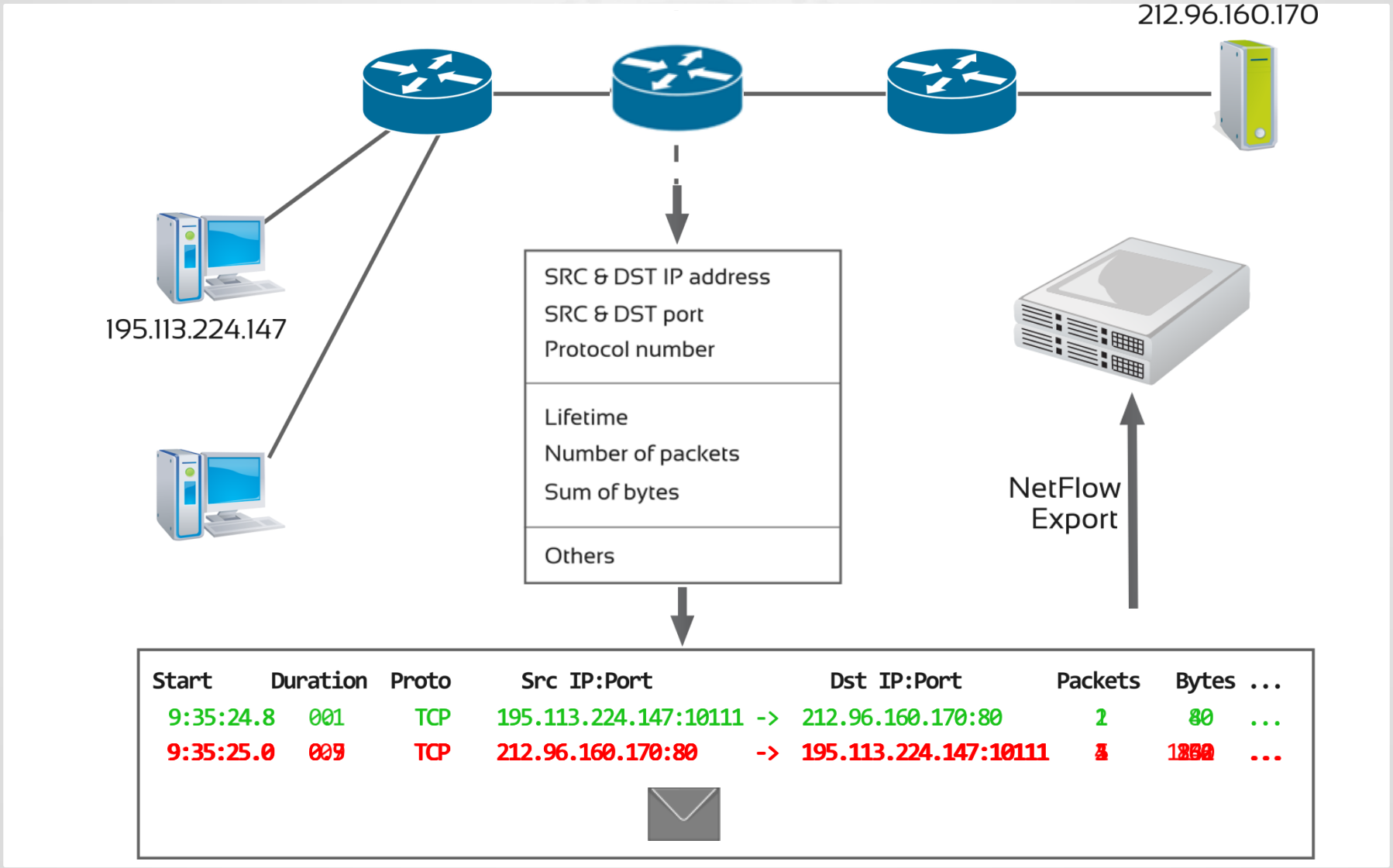
Měření odezvy sítě a aplikací

Ochrana před útoky typu DDoS

2013 2014 2015

Princip technologie

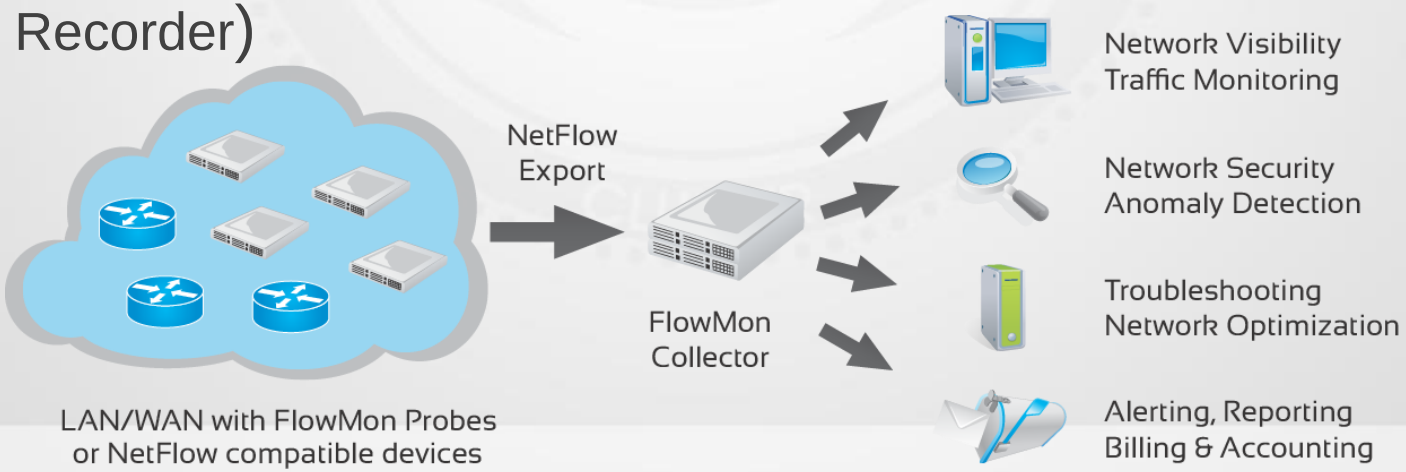
NSM
NETWORK SECURITY MONITORING CLUSTER



Architektura řešení

NSM
NETWORK SECURITY MONITORING CLUSTER

- FlowMon Sondy
  - Zdroje statistik o provozu datové sítě
- FlowMon Kolektory
  - Sběr, vizualizace a reporting statistik o provozu
- FlowMon plug-iny
  - ADS (Anomaly Detection System, behaviorální analýza)
  - APM (Application Performance Monitoring) , TR (Traffic Recorder)



Proč INVEA-TECH

NSM
NETWORK SECURITY MONITORING CLUSTER

- Původní české řešení, které se prosadilo na světových trzích v globální konkurenci
  - Pro české zákazníky lokální podpora přímo od výrobce
  - Stovky instalací v ČR i zahraničí
- Vynikající škálovatelnost a poměr cena/přínos
- Unikátní vlastnosti
  - Přináší funkcionality obvyklé pro nákladné technologie v jednom uceleném řešení od jednoho výrobce
  - Pasivní a transparentní monitoring datového provozu
  - Jediný evropský výrobce řešení pro behaviorální analýzu dle Gartner

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