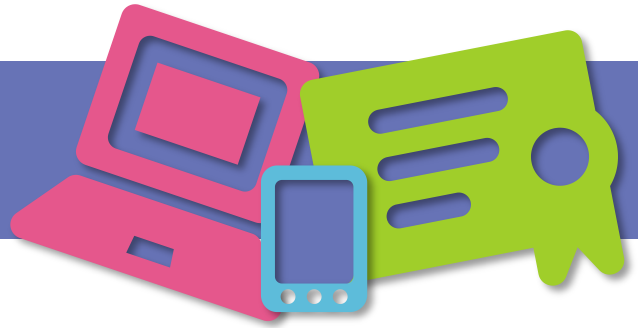
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Případová studie: zavedení FlowMon v HCI

Maroš Barabas, AEC

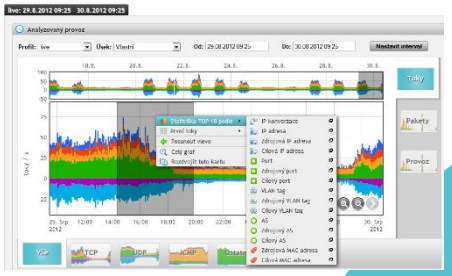
Zdeněk Vrbka, INVEA-TECH

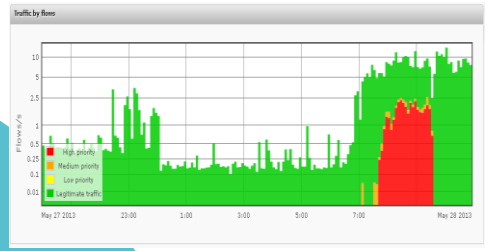
Obsah

- Technologie monitorování a analýzy provozu datových sítí
- Nasazení FlowMon v HCI (z pohledu AEC)
- Poučení, závěry

Technologie monitorování a analýzy provozu datových sítí

Bezpečnost sítě





LAN visibility & security

Perimeter security

End point security

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

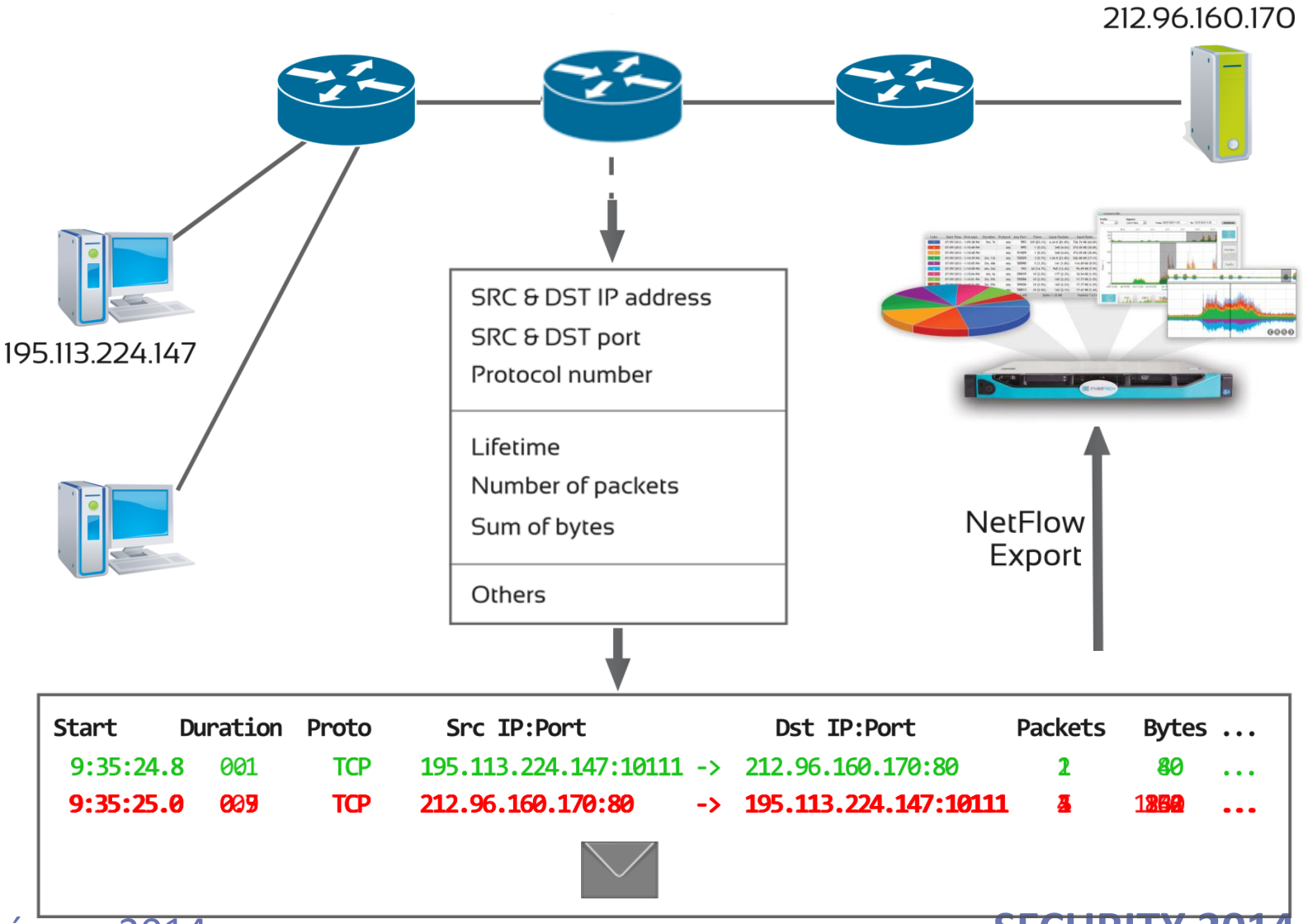
21/2011 - 7 February 2011

8 February 2011: Safer Internet Day

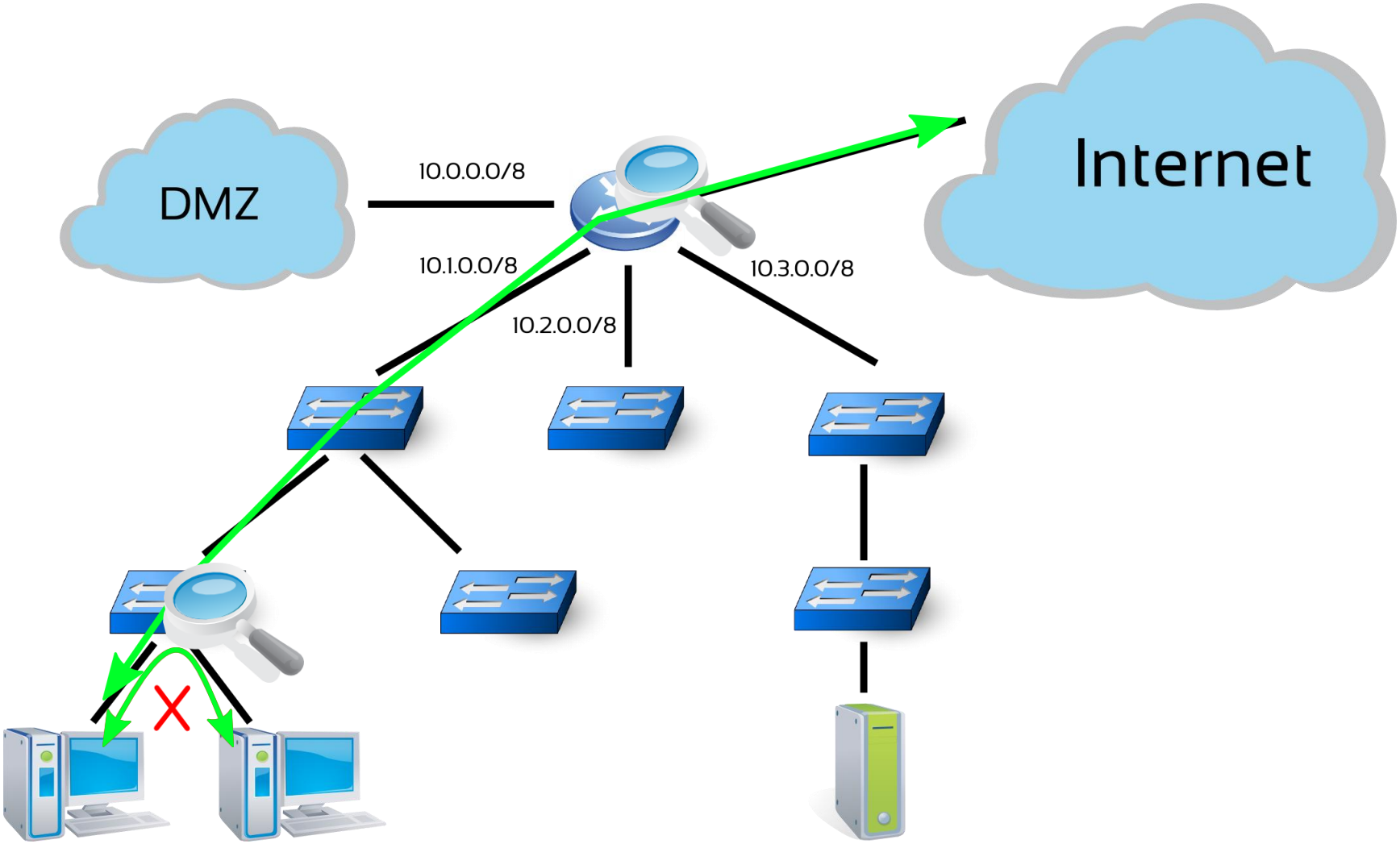
Nearly one third of internet users in the EU27 caught a computer virus

84% of internet users use IT security software for protection

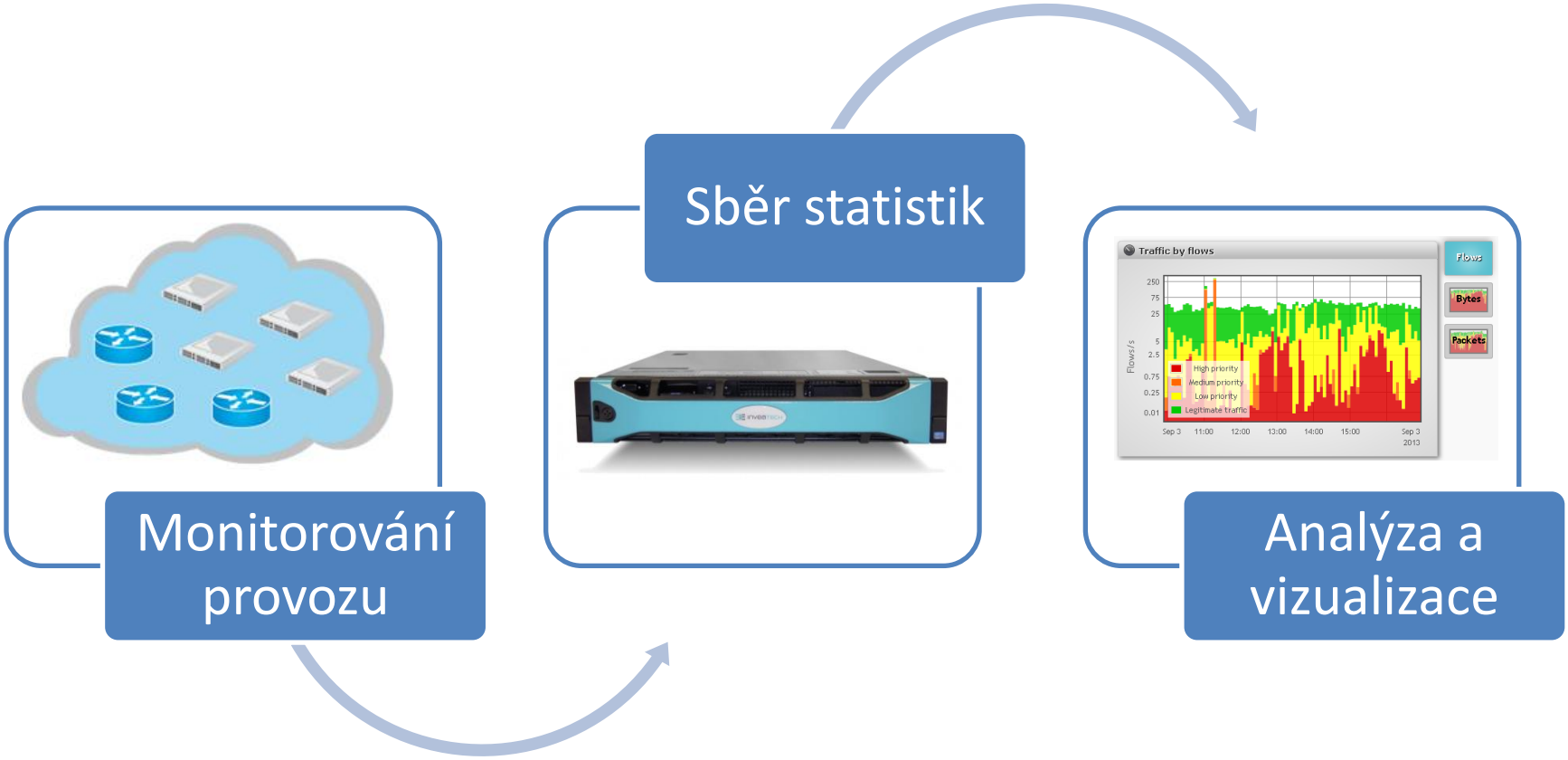
Monitorování provozu



Umístění v síti



Monitoring nové generace



Z pohledu uživatele

- Monitorování provozu v síti (NetFlow/IPFIX)
  - Kompletní viditelnost do dění v síti
  - Real-time a historická data pro LAN & WAN & komunikaci do Internetu
  - Optimalizace správy a provozu sítě
  - Efektivní troubleshooting

- Bezpečnost interní sítě (Network Behavior Analysis, NBA)
  - Jediný způsob, jak detekovat pokročilé hrozby
  - Založeno na behaviorální analýze
  - Detekce pokročilého malware, zero-day útoků, podezřelých přenosů dat, změn chování a dalších incidentů

Nasazení FlowMon v HCI
(z pohledu AEC)

Motivace HCI

- Standardní bezpečnostní nástroje a politiky nasazeny
  - Firewall
  - IDS/IPS
  - …
- Chybějící nástroj na detekci anomálií v síti
- Pilotní projekt FlowMon
  - Ověření přidané hodnoty řešení ve vlastní síti

Průběh PoC

- Instalace sondy na SPAN porty
- Instalace kolektoru formu virtuálního appliance
- Sběr flow dat z aktivních prvků
- Nízká časová náročnost
  - Instalace a konfigurace (0,5čld)
  - Ladění (0,5čld)
  - Prezentace výstupů (0,5čld)
- Výstupy
  - Potvrzeno doplnění stávajících systémů
  - Rozhodnuto o trvalém nasazení

Trvalé nasazení

- Připraveno z pilotního projektu
  - Pouze vygenerování permanentní licence ☺
- Provozní stav dosáhnut během několika dní
- Rozšíření záběru systému
  - Oproti původnímu záměru systém pokrývá i potřeby správců datové sítě
  - Přesah do rutinního provozu a správy datové sítě

Práce s výstupy

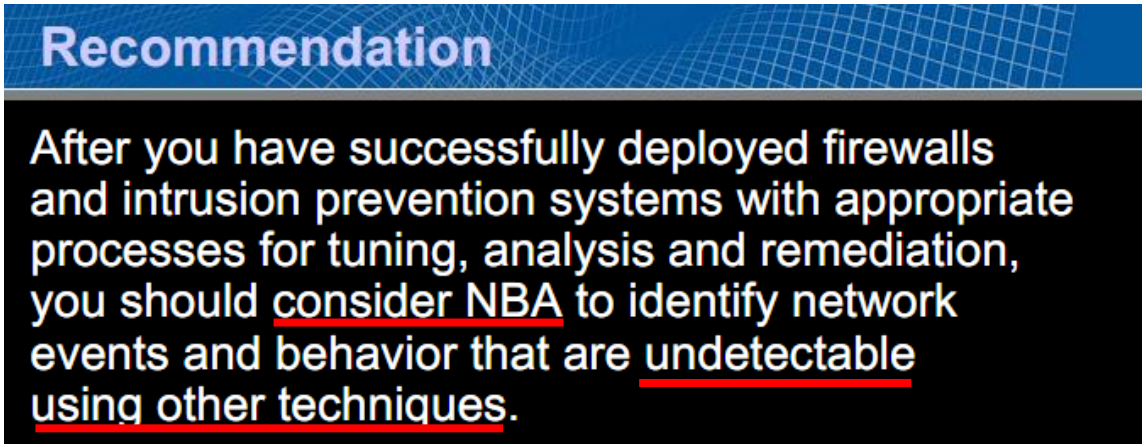
- Primárním uživatelem je tým bezpečnosti
- Výstupy dále využívá tým správy sítě
- Integrace do SIEM
  - Flow statistiky
  - Detekované události
- Přínosy především
  - Detekce anomálií na úrovni interní datové sítě
  - Reporting o objemech a struktuře provozu

Poučení, závěry

Gratulujeme k vítězství 5:3

Hodnocení technologie

- Monitorování sítě a behaviorální analýza jako důležitá součást správy a bezpečnosti sítě
  - Nejen doporučení Gartner



Network Behavior Analysis Update, Gartner

  - Praktické zkušenosti z projektů AEC

Hodnocení technologie 2

- IDS/IPS, SIEMy ani další nástroje monitorování sítě a behaviorální analýzu nenahradí
  - Lze vhodně integrovat, např. s QRadarem
    - Nižší cena SIEMu
    - Funkcionalita obou řešení
- Je v souladu s bezpečnostními trendy
  - Např. s Kybernetickým zákonem ČR

Výběr řešení

Klíčové vlastnosti	
Podpora verzí NetFlow	NetFlow v5 nestačí, požadujte v9 i IPFIX
Disková kapacita	Pro uložení provozu alespoň 1 rok zpětně
Úroveň detailu	Individuální toky, i pro historická data
Reporting & alerting	Na základě libovolných NetFlow atributů, uživatelsky definovatelné
Behaviorální analýza	Thresholdy nejsou behaviorální analýza, požadujte automatickou detekci incidentů
Sledování aktivních zařízení	Na úrovni přístupové vrstvy, sledování MAC-IP a podpora konceptu BYOD
Technické řešení	Preferujte appliance, prosté SW řešení nevyhoví požadavků enterprise segmentu

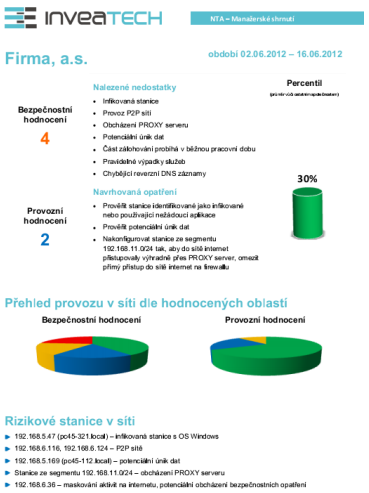
Reference INVEA-TECH FlowMon

AEC a FlowMon

Bezplatná zápůjčka řešení

vmware

Bezpečností analýza síťového provozu



Byli byste překvapeni, co se děje ve vaší síti!

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Maroš Barabas, AEC
maros.barabas@aec.cz

Zdeněk Vrbka, INVEA-TECH
vrbka@invea.com