Moderní technologie pro bezpečný cloud

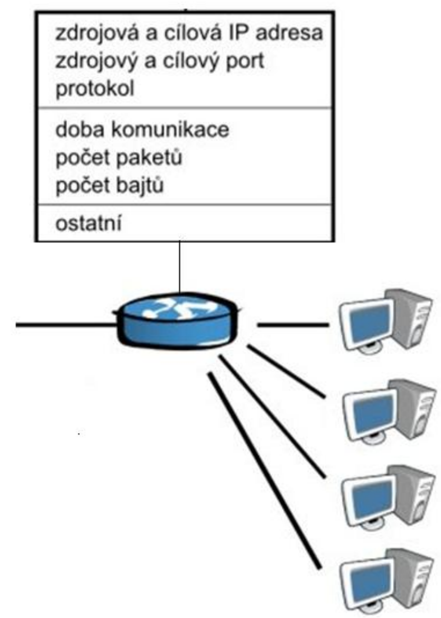
Pavel Minařík, INVEA-TECH

Trendy v oblasti bezpečnosti

- Tradiční pojetí bezpečného perimetru skončilo
  - Všecho „as a service“
  - Služby a aplikace v cloudu
  - Využívání vlastních zařízení (BYOD)
  - Zvyšující se míra šifrované komunikace
- Kybernetická kriminalita jako business
  - Pokročilé útoky a hrozby
  - Malware na míru

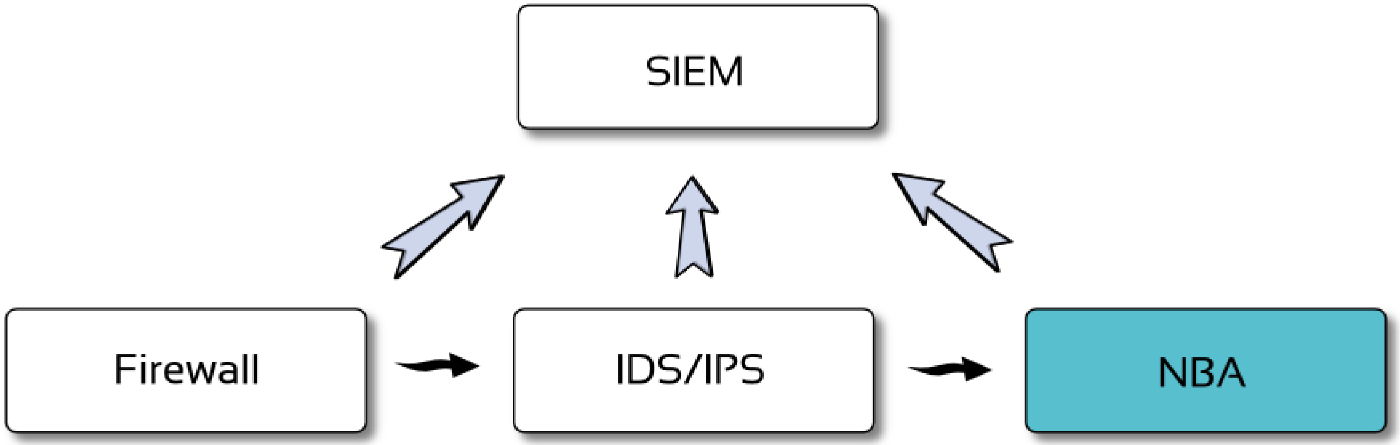
Trendy v oblasti bezpečnosti

- Prosazení technologie monitorování a analýzy provozu datové sítě
  - Flow Monitoring (průmyslový standard NetFlow)
  - Network Behavior Analysis (NBA)



NBA v kontextu IT bezpečnosti

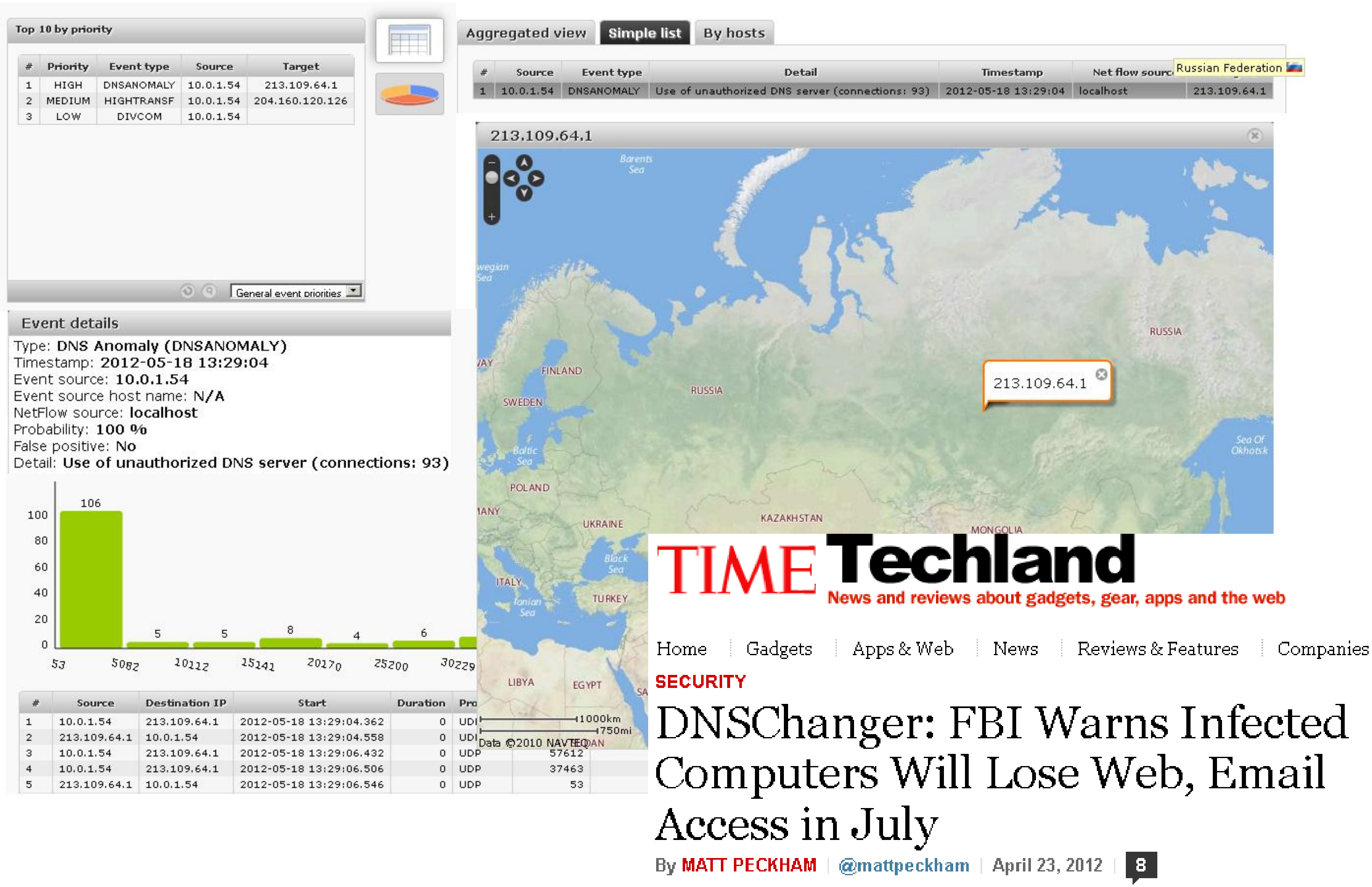
- Doporučený koncept bezpečné infrastruktury
  - Gartner: Network Behavior Analysis Update, November 2007
  - Aberdeen Group: Network Behavior Analysis – Protecting by Predicting and Preventing, November 2009



NBA v korporátních sítích

- Všechna zařízení pod dohledem a kontrolou
- Vyšší bezpečnost a spolehlivost datové sítě
  - Odhalování nežádoucích aktivit a úniků dat
  - Odhalování malware
- Identifikace a odstraňování příčin provozních problémů

NBA v korporátních sítích



NBA v korporátních sítích

Malware from Peru Reportedly was sending AutoCAD Drawings to China

by SUNITHBABU (ONLINE) on JUNE 26, 2012

Event details

Type: **Behavior Profiling - Country reputation (PRFCOUNTRY)**
Timestamp: **2013-01-25 14:43:23**
Event source: **192.168.3.149**
Event source host name: **N/A**
NetFlow source: [redacted]**cz**
Probability: **100 %**
False positive: **No**
Detail: **Unusual communication to the country Israel (device: upload: 1.01 MiB, download: 390.99 KiB, upload/download ratio: 2.63; network average: upload: 137.72 KiB, download: 263.57 KiB, upload/download ratio: 0.52).**

Targets (1) | Comments (0) | Event categories (0)

[redacted].77.198

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.1.1.84	UPLOAD	Uploaded: 38.83 MiB, downloaded: 0.57 MiB, ports: 80	2012-05-10 11:43:34	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
2	10.1.1.84	UPLOAD	Uploaded: 243.48 MiB, downloaded: 4.07 MiB, ports: 80	2012-05-10 11:37:19	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
3	10.1.1.84	UPLOAD	Uploaded: 199.97 MiB, downloaded: 4.49 MiB, ports: 80	2012-05-10 11:33:47	localhost	98.13 United States vip.ac4.yahoo.net)
4	10.1.1.84	UPLOAD	Uploaded: 232.03 MiB, downloaded: 4.38 MiB, ports: 80	2012-05-10 11:28:32	localhost	98.136. vip.ac4.yahoo.net)
5	10.1.1.84	UPLOAD	Uploaded: 197.11 MiB, downloaded: 3.74 MiB, ports: 80	2012-05-10 11:24:10	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)

NBA u poskytovatelů služeb/cloudu

- Vyšší bezpečnost a spolehlivost datové sítě
- Konkurenční výhoda
- Nová služba s přidanou hodnotou pro zákazníky
- Trendy v oblasti kybernetické bezpečnosti
  - Požadavky v oblasti CSIRT/CERT

NBA u poskytovatelů služeb/cloudu

- Útoky s cílem získat neoprávněný přístup
  - SSH, Telnet, RDP (stále častější)

NBA u poskytovatelů služeb/cloudu

- Infikované stanice a sítě Vašich zákazníků
  - Včasné varování, alerty, reporty

#	Source	Event type	Detail	Timestamp	Targets
1	7.1.35.22	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 173, targets: 173, port list: 445).	2013-02-14 13:20:44	13.17.144.40, 14.75.40.31, 17.99.236.100, 17.120.91.68, 18.10.215.19, 18.18.122.74, 18.28.146.125, 18.35.149.6, 18.43.142.46, 18.61.165.100, ...
2	7.1.35.22	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 220, targets: 220, port list: 445).	2013-02-14 13:15:28	14.1.20.62, 14.34.122.61, 14.68.95.123, 14.85.198.29, 14.86.80.104, 17.6.109.4, 17.7.147.6, 17.52.250.96, 17.57.161.61, 17.59.234.6, ...
3	7.1.35.22	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 203, targets: 203, port list: 445).	2013-02-14 13:10:35	14.1.56.58, 14.60.68.18, 14.68.44.97, 17.4.21.57, 17.10.110.30, 17.100.134.57, 18.0.237.64, 18.30.131.51, 18.34.186.56, 18.37.149.54, ...
4	7.1.35.22	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 194, targets: 194, port list: 445).	2013-02-14 13:05:30	17.15.23.41, 17.59.45.50, 17.61.145.101, 17.99.224.113, 17.100.174.91, 18.9.10.104, 18.36.87.126, 18.68.176.96, 18.74.46.7, 18.105.145.100, ...
5	7.1.35.22	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 229, targets: 229, port list: 445).	2013-02-14 13:00:33	13.17.156.53, 14.54.28.76, 14.81.81.11, 14.84.134.85, 14.85.125.45, 14.90.89.98, 14.90.118.123, 17.40.73.92, 17.51.179.23, 17.53.189.29, ...
6	7.1.35.22	SCANS	horizontal TCP SYN scan (attempts with response: 1, attempts without response: 212, targets: 213, port list: 445).	2013-02-14 12:55:38	14.77.17.49, 14.89.94.28, 17.43.100.84, 17.114.145.127, 17.124.49.94, 18.41.240.95, 18.66.235.10, 18.68.139.49, 18.79.165.76, 18.99.2.32, ...
7	7.1.35.22	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 213, targets: 213, port list: 445).	2013-02-14 12:50:33	13.17.180.106, 14.49.210.76, 14.61.134.33, 14.69.35.18, 14.80.206.62, 14.84.22.108, 14.86.36.60, 17.3.7.32, 17.4.5.91, 17.9.198.115, ...

NBA u poskytovatelů služeb/cloudu

- Rozesílání SPAMu
- Botnety

#	Detail	Timestamp	Net flow source	Targets
1	Mail count: 1270, network average: 414.50	2012-10-24 21:48:46		12.102.252.75, 17.172.36.33, 17.172.36.34, 24.71.223.11, 46.255.224.55, 64.8.71.15, 64.12.90.65, 64.12.90.66, 64.12.90.98, 64.12.138.161, , ...
2	Mail count: 1386, network average: 259.50	2012-10-24 21:38:52		12.102.252.75, 17.172.36.32, 24.71.223.11, 64.8.71.15, 64.12.90.34, 64.12.90.65, 64.12.90.66, 64.12.90.97, 64.12.138.161, 64.18.5.10, , ...
3	Mail count: 545, network average: 130.00	2012-10-24 21:23:41		12.102.252.75, 24.71.223.11, 64.8.71.15, 64.12.90.1, 64.12.90.34, 64.12.90.97, 64.1[illegible] 64 18.5.11, 64.59.134.8, 64.[illegible] Canada
4	Mail count: 2181, network a[illegible]	[illegible]	[illegible]	12.102.252.75, 17.172.36.32, 17.172.36.34, [illegible].11, 38.102.228.17, 62.211.72.32, [illegible]5, 64.12.90.1, 64.12.90.33, [illegible]34, , ...

Event details

Type: **Blacklist (BLACKLIST)**
Timestamp: **2012-10-27 19:41:41**
Event source: [redacted] ([redacted].cz)
Event source host name: **N/A**
NetFlow source:
Probability: **100 %**
False positive: **No**
Detail: **Custom black list, attempts: 2, uploaded: 0 MiB, downloaded: 0 MiB**

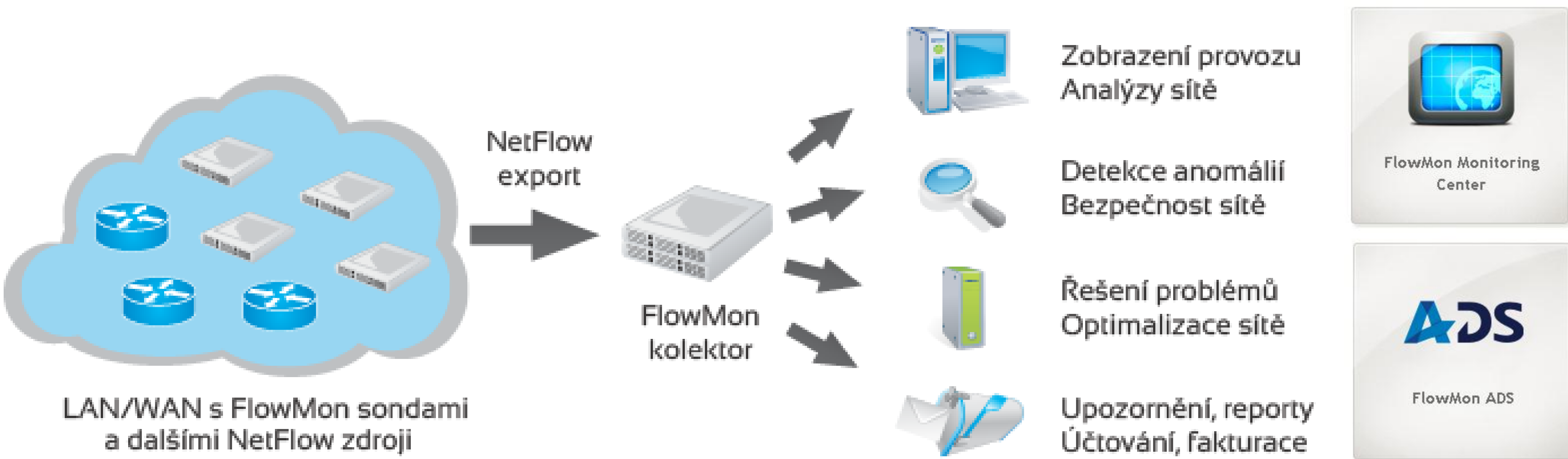
Targets (1) | Comments (0) | Event categories (0)

Canada

131.253.18.12 (unknown)

Možnosti nasazení technologie NBA

- FlowMon sondy pro měření provozu a generování NetFlow statistik na jeden nebo více kolektorů
- FlowMon ADS pro automatickou detekci útoků a anomálií
- Kompatibilní s NetFlow technologiemi třetích stran
- Bez vlivu na stávající nástroje a infrastrukturu

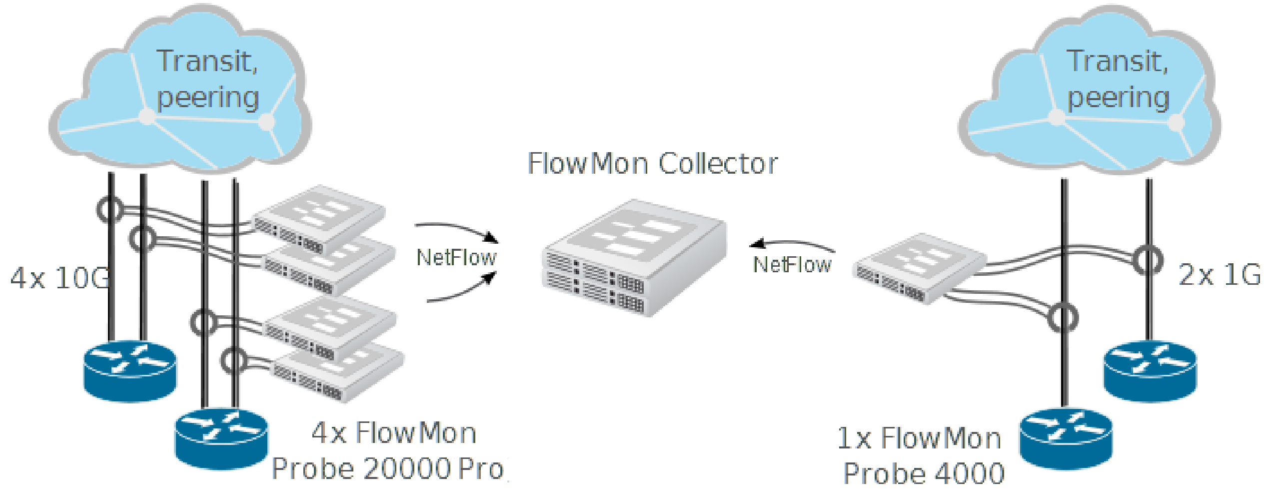


NBA – případová studie

Během prvních tří měsíců jsme díky FlowMon ADS odhalili infikované stanice a systematické útoky vedené z počítačů našich nic netušících zákazníků, komunikace botnet sítí nebo rozesílání nevyžádané pošty. Dnes nabízíme našim zákazníkům jako přidanou hodnotu automatické upozornění na podobné anomálie, čímž zajišťujeme vyšší bezpečnost a kvalitu našich ISP služeb.

ČD-Telematika

Ing. Mikuláš Labský, ředitel úseku Telekomunikační služby



Kontakt

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno
www.invea.cz

Výhradní zastoupení v SR

DV s.r.o.
Továrenská 1
018 41 Dubnica nad Váhem
www.dvsro.eu

Ďakujeme za pozornosť

eFOCUS