



Nejlepší přítel správce sítě!

Řešení bezpečnosti Vaší sítě v Cloudu

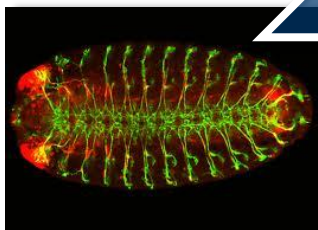
Pavel Minařík
CTO, AdvalCT,a.s.

ADVAiCT

- ▶ IT infrastruktura hraje roli nervové soustavy organizace



Ve vysoce dynamickém prostředí, kde vše je služba a služba je vše, stabilní a odolná infrastruktura je to, co dělá rozdíl mezi fungujícím a nefungujícím světem



...

2005

2010

2012

...



Úvod

Přehled technologií



Eurostat report (Feb 2011)

- 84% počítačů je chráněno anti-malware nástrojem
- 31% počítačů je infikovaných nežádoucím kódem



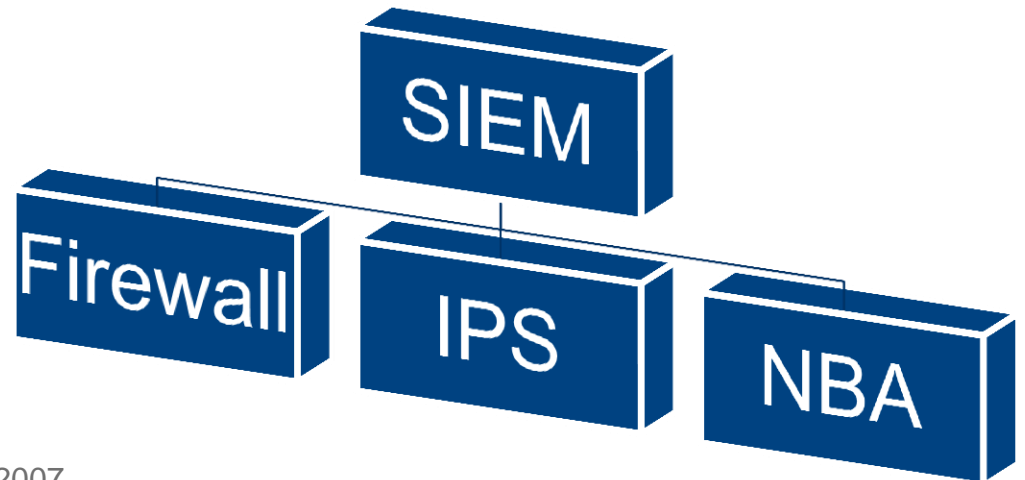
21/2011 - 7 February 2011

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

- ▶ Jasně definovaný segment trhu
- ▶ Bezpečná síť = Firewall + IPS + NBA
 - Poté, co úspěšně nasadíte firewall a systém detekce průniků, zvažte nasazení technologie NBA, která je schopná rozpoznat hrozby a chování neodhalitelné jinými systémy.



Network Behavior Analysis Update, November , 2007

Network Behavior Analysis: Protecting by Predicting and Preventing, Aberdeen Research Group, November, 2009

Network Behavior Analysis

Principy fungování



Detekce chování



Detekce signatur



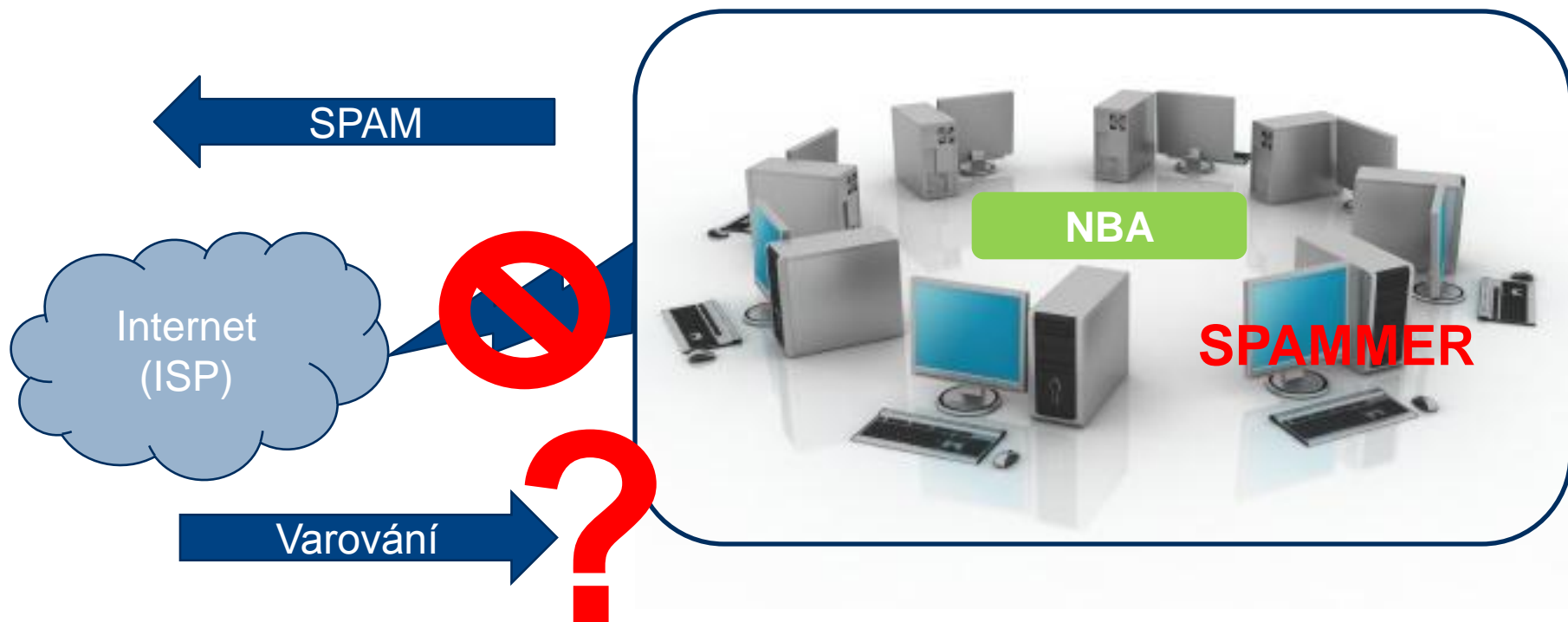
Na úrovni sítě



Na úrovni stanic



Odchozí SPAM



Network Behavior Analysis

Dostupnost řešení

	České řešení	Zahraniční řešení
Malý podnik do cca 100 PC	???	není
Střední podnik 100-500 PC	AdvaICT FlowMon ADS 275.000+ Kč	50.000+ USD
Velký podnik 500+ PC	AdvaICT FlowMon ADS 800.000+ Kč	100.000+ USD



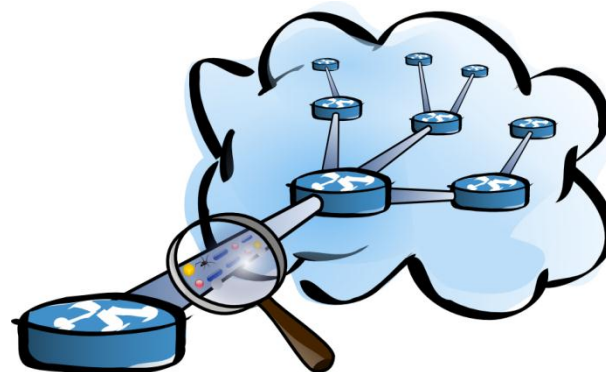
FlowMon ADS v Cloudu

Služba NetHound

- ▶ Celé appliance řešení je přesunuto do infrastruktury poskytovatele
- ▶ Minimalizace počáteční investice (HW/SW vybavení)
- ▶ Eliminace nároků na expertní znalosti na straně uživatele
- ▶ Dostupnost 24/7 prostřednictvím webu odkudkoliv



- ▶ Detekce nežádoucích vzorů chování
 - ▶ Vnitřní i vnější útoky
 - ▶ Nežádoucí služby a aplikace
 - ▶ Provozní a konfigurační problémy
- ▶ Behaviorální analýza
 - ▶ Profily chování
 - ▶ Detekce anomálií
 - ▶ Sběr statistik
- ▶ Přehledné uživatelské rozhraní
 - ▶ Dashboard s okamžitou indikací problémů a top statistik
 - ▶ Interaktivní vizualizace událostí
 - ▶ Integrace informací ze služeb DNS, WHOIS, geolokační služby
- ▶ Alerting a reporting
 - ▶ Upozornění na nežádoucí aktivity mailem
 - ▶ Souhrnné a manažerské reporty



Příklady výstupů

FlowMon ADS 105 - Dashboard

- Home
- Dashboard
- Events
- Profiles**
- Network
- Events
 - Simple list
 - By hosts
 - By topology
 - SSH attacks
- Profiles
 - Hosts
 - Client/Server lookup
 - Host properties
 - Statistics
- Reports
 - General report
- Configuration
 - General configuration
 - NetFlow sources
 - Filters
 - Methods
 - Perspectives
 - Event categories
 - Topology
 - Event reporting
 - False positives
- About

FlowMon ADS 105 - Dashboard

- Domů
- Dashboard
- Události
- Profilý**
- Síť
- Události
 - Jednoduchý přehled
 - Dle zařízení
 - Dle topologie
 - SSH útoky
- Profilý
 - Zařízení v síti
 - Vyhledávání dle klient/server
 - Vlastnosti zařízení v síti
 - Statistiky
- Reporty
 - Obecný report
- Konfigurace
 - Obecná nastavení
 - Zdroje NetFlow dat
 - Filtry
 - Detekční metody
 - Perspektivy
 - Kategorie událostí
 - Topologie sítě
 - Reporty událostí
 - False positives
 - O aplikaci

Top 10 IPs by data volume (all traffic)

#	IP Address	SUM (MB)	IN (MB)	OUT (MB)
1	192.168.3.108	1,749	1,091	658
2	192.168.3.110	1,207	50	1,157
3	192.168.3.106	706	683	23
4	192.168.3.105	151	150	1
5	192.168.3.123	72	61	11
6	192.168.3.118	43	34	10
7	192.168.32.1	38	38	0
8	192.168.3.114	30	28	2
9	192.168.32.198	20	0	20
10	192.168.3.100	16	14	2
11	Others	51	15	36
Top 10 sum		4,034	2,149	1,884
Total sum		4,085	2,165	1,920

Top 10 IPs by connection count



- 192.168.3.110 (46.2%)
- 192.168.3.106 (11.5%)
- 192.168.3.123 (6.1%)
- 192.168.3.254 (5%)
- 192.168.3.118 (4.4%)
- 192.168.3.102 (3.3%)
- 192.168.3.114 (3.3%)
- 192.168.3.116 (2.4%)
- 192.168.3.120 (2.3%)
- 192.168.3.108 (1.6%)
- Others (14%)

Events

8.122

#	Type	Details	Timestamp	Event targets
1	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 16:39:50	24.5
2	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 16:13:42	24.5
3	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 15:59:44	24.5

Interactive event visualization

Type	Timestamp	Event source	Detail	Probability	NetFlow source	False positive
TCP Scans (SCANS)	2010-04-29 07:37:48	10.0.1.4	chaotic TCP SYN scan (attempts: 1176, targets: 2, port list: 24, 22)	100 %	LAN	No

100% Freeze

Event evidence

Type: DIVCOM
 Timestamp: 2010-05-12 09:20:31
 Event source: 10.0.1.78
 Detail: distinct destination IPs: 70, distinct destination ports: 70
 Targets:

Flow listing

#	IP source	Destination IP	Start	Duration	Protocol	Source port	Destination port	Transferred	Packets	Flags	TOS
1	10.0.1.78	224.0.0.22	2010-05-12 09:20:31.880	22.391	IGMP	0	137	648	16	---	0
2	10.0.1.78	10.0.1.255	2010-05-12 09:20:31.891	62.82	UDP	137	137	4410	51	---	0
3	10.0.1.78	239.256.256.250	2010-05-12 09:20:31.984	0	UDP	56464	1900	161	1	---	0
4	10.0.1.78	224.0.0.252	2010-05-12 09:20:32.007	0.99	UDP	56464	5305	112	2	---	0
5	10.0.1.78	83.228.111.72	2010-05-12 09:20:34.426	137	UDP	45869	4905	170	3	---	0
6	83.228.111.72	10.0.1.78	2010-05-12 09:20:34.400	134	UDP	4905	45969	202	3	---	0
7	10.0.1.78	94.113.209.167	2010-05-12 09:20:34.662	0	UDP	45869	58396	53	1	---	0
8	94.113.209.167	10.0.1.78	2010-05-12 09:20:34.662	0	UDP	58396	45869	79	1	---	0
9	10.0.1.78	89.102.186.142	2010-05-12 09:20:34.775	0	UDP	45869	39952	62	1	---	0
10	89.102.186.142	10.0.1.78	2010-05-12 09:20:34.794	0	UDP	39952	45869	79	1	---	0
11	10.0.1.78	94.45.168.205	2010-05-12 09:20:34.802	0	UDP	45869	47135	52	1	---	0
12	94.45.168.205	10.0.1.78	2010-05-12 09:20:35.043	0	UDP	47135	45869	79	1	---	0
13	10.0.1.78	94.138.102.112	2010-05-12 09:20:35.044	0	UDP	45869	33426	62	1	---	0
14	94.138.102.112	10.0.1.78	2010-05-12 09:20:35.091	0	UDP	33426	45869	79	1	---	0
15	10.0.1.78	87.126.192.96	2010-05-12 09:20:35.092	0	UDP	45869	10288	50	1	---	0
16	87.126.192.96	10.0.1.78	2010-05-12 09:20:35.153	0	UDP	10288	45869	79	1	---	0
17	10.0.1.78	78.92.118.89	2010-05-12 09:20:35.166	0	UDP	45869	15563	56	1	---	0

- ▶ Potenciální únik firemních dat
 - ▶ Ukládání dat na veřejné servery

Events

#	Event source	Type	Detail	Timestamp	NetFlow source	Japan 🇯🇵	Targets
1	10.0.1.79	UPLOAD	Uploaded: 11.52 MB, downloaded: 0.26 MB, ports: 443	2011-06-10 09:50:14	localhost	150.70.178.112	(inboundmx.safesync.com)
2	10.0.1.79	UPLOAD	Uploaded: 30.95 MB, downloaded: 0.85 MB, ports: 443	2011-06-10 09:46:12	localhost	150.70.178.112	(inboundmx.safesync.com)
3	10.0.1.79	UPLOAD	Uploaded: 21.79 MB, downloaded: 0.44 MB, ports: 443	2011-06-10 09:34:46	localhost	150.70.178.112	(inboundmx.safesync.com)

- ▶ Odesílání soukromé pošty

Events

#	Event source	Type	Detail	Timestamp	NetFlow source	Targets
1	10.0.1.74	UPLOAD	Uploaded: 1.4 MiB, downloaded: 0.08 MiB, ports: 80	2011-06-15 16:46:47	localhost	77.75.76.6 (email.seznam.cz)

▶ Útoky

- ▶ Skenování portů, slovníkové útoky, DoS
- ▶ Detekce infikovaných stanic

Events

#	Event source	Type	Detail	Timestamp	NetFlow source	Targets
1	████████.71	SCANS	Horizontal Scan (attempts: 136 targets: ██████.1, ██████.2, ██████.3, ██████.4, ██████.5 port list: 139, 445)	2010-04-29 07:37:48	localhost	████████.1, ██████.2 ██████.3 ██████.4 ██████.5

▶ Šíření SPAMu

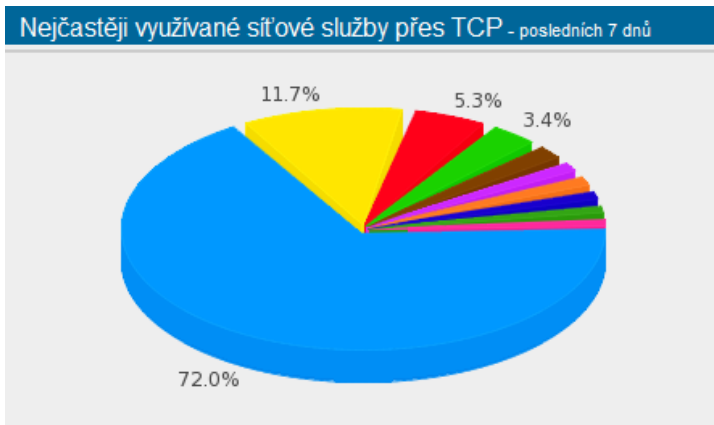
- ▶ Pokusy o odeslání pošty přes velké množství poštovních serverů

Events

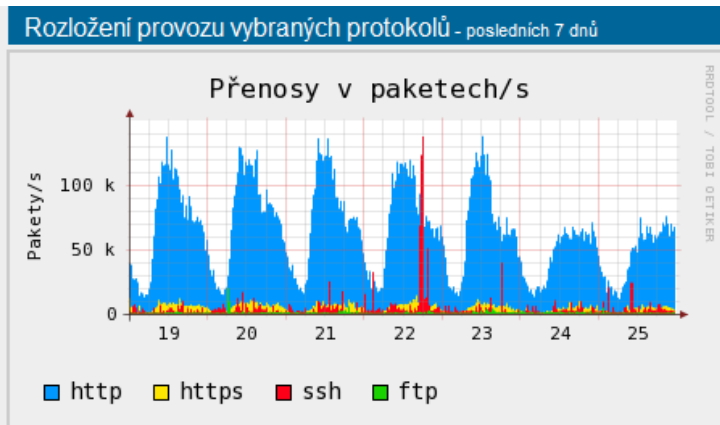
#	Event source	Type	Details	Timestamp	Data source	Event targets
1	████████.67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 7)	2009-09-24 19:23:00	PřF	62.3.131.181, 69.7.167.23, 146.201.3.234, 194.109.24.132, 209.145.5.10, 210.101.199.231, 213.232.0.195
2	████████.67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 65)	2009-09-24 19:17:45	PřF	62.3.131.181, 63.101.151.1, 64.18.4.11, 64.18.5.10, 64.18.6.10, 64.18.6.14, 64.18.7.13, 64.191.223.42, 65.55.88.22, 65.172.13.10, ...
3	████████.67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 75)	2009-09-24 19:16:00	PřF	62.12.136.97, 63.166.155.140, 64.18.6.10, 64.18.6.11, 64.18.7.11, 64.26.60.153, 64.88.167.155, 64.118.228.132, 65.55.88.22, 65.61.115.199, ...

► Manažerské reporty

- Dostupné přes web nebo rozesílané v PDF do e-mailu



		Port	Přeneseno
1.	http	http	25.88 TiB
2.	smtp	smtp	4.19 TiB
3.	irdmi	irdmi	1.90 TiB
4.	https	https	1.21 TiB
5.	rsync	rsync	692.61 GiB
6.	cvd	cvd	489.17 GiB
7.	ssh	ssh	465.60 GiB
8.	macromedia-fcs	macromedia-fcs	395.73 GiB
9.	6904	6904	388.83 GiB
10.	oms	oms	379.24 GiB

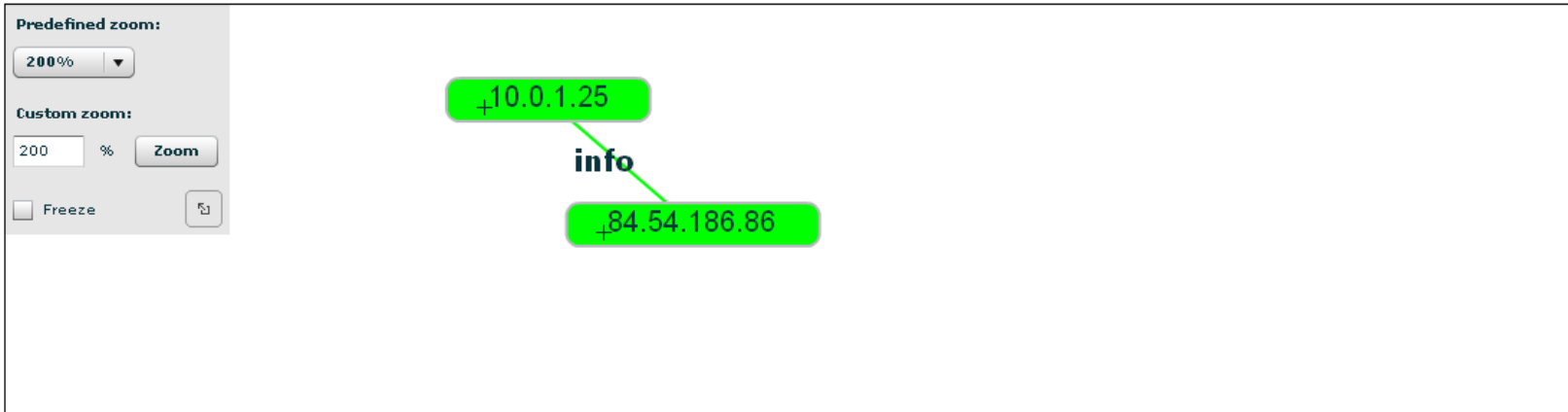


		Protokol	Přenosová rychlost
1.	http	http	377.13 Mb/s
2.	https	https	17.68 Mb/s
3.	ssh	ssh	6.63 Mb/s
4.	ftp	ftp	2.96 Mb/s

Příklady výstupů

Interactive event visualization

Type	Timestamp	Event source	Detail	Probability	NetFlow source	False positive
Instant Messaging (INSTMSG)	2011-01-18 16:50:29	10.0.1.25	Skype protocol, unique servers: 1	100 %	localhost	No



Details - 84.54.186.86 <-> 10.0.1.25									
Source IP 84.54.186.86					Destination IP 10.0.1.25				
Start	Duration	Protocol	Source port	Destination Port	Bytes	Packets	Flags	TOS	
2011-01-18 16:44:59.857	.02	TCP	37024	52556	106	2	.AP...	0	
2011-01-18 16:46:59.883	0	TCP	37024	52556	54	1	.AP...	0	
2011-01-18 16:48:29.069	.358	TCP	37024	52556	168	3	.AP...	0	
2011-01-18 16:50:29.525	.067	TCP	37024	52556	106	2	.AP...	0	
2011-01-18 16:52:29.513	1.035	TCP	37024	52556	106	2	.AP...	0	
2011-01-18 16:53:05.265	.562	TCP	37024	52556	300	4	.AP...	0	
2011-01-18 16:55:05.706	.457	TCP	37024	52556	106	2	.AP...	0	

Source IP 10.0.1.25					Destination IP 84.54.186.86				
Start	Duration	Protocol	Source port	Destination Port	Bytes	Packets	Flags	TOS	
2011-01-18 16:44:59.585	.292	TCP	52556	37024	106	2	.AP...	0	
2011-01-18 16:46:59.647	.236	TCP	52556	37024	106	2	.AP...	0	
2011-01-18 16:48:29.069	.093	TCP	52556	37024	160	3	.AP...	0	
2011-01-18 16:50:29.264	.328	TCP	52556	37024	106	2	.AP...	0	
2011-01-18 16:52:29.301	1.248	TCP	52556	37024	106	2	.AP...	0	
2011-01-18 16:53:05.266	.343	TCP	52556	37024	230	4	.AP...	0	
2011-01-18 16:55:05.426	.737	TCP	52556	37024	106	2	.AP...	0	

- ▶ Služba aktivně propagována od března 2011
 - ▶ Možnost vyzkoušet si 14 dní zdarma
 - ▶ K 31.5.2011 6 stálých uživatelů služby
 - ▶ Nejčastější model – NetHound Basic (5.000 Kč/měsíc)

- ▶ Statistika provozovaných instancí
 - ▶ Služba NetHound k 31.5.2011 zpracovala **130 milionů** datových toků
 - ▶ V průměru 300 tisíc toků denně na jednu instanci

Network Behavior Analysis

Dostupnost řešení

	České řešení	Zahraniční řešení
Malý podnik do cca 100 PC	AdvaICT NetHound 5.000+ Kč	není
Střední podnik 100-500 PC	AdvaICT FlowMon ADS 275.000+ Kč	50.000+ USD
Velký podnik 500+ PC	AdvaICT FlowMon ADS 800.000+ Kč	100.000+ USD



ITP Group Brno s.r.o.

NetHound

A rodina produktů AdvaICT



Analýza síťového provozu
Základní, a.s.

Anomálie a bezpečnostní rizika
Tato kapitola automaticky odhalí problémy a bezpečnostní problémy a obecné anomálie provozu datové sítě. Všechny údaje je vhodné na obsahení škodě a nežádoucích aktivit na datové síti, které mohou znamenat ohrožení počítačů nebo sítě jako celku. Pozornost je třeba věnovat průběhu provozu a všem přehledům sítě (IDS/IPS) a analyzované síti.

Útoky
Při této analýze byly detekovány různé útoky a problémy bezpečnosti. Přehled se skládá z IDS, DDoS, útoků na síť. Všechny tyto útoky, až na jednu výjimku, byly neúspěšné a typicky jim předcházela masivní síťová aktivita. Útoky na protokol Telnet byly detekovány. Dopravní údaje pro síť na IP adresu 192.168.1.100. Útoky byly vyvolány jako periodické spojení. Jedná se o síť z 201607-03 12:26:54 z IP adresy 208.115.230.125.

Nežádoucí aktivity
Všechny nežádoucí aktivity byly detekovány jako typy útoků a služby nebo útoků na síť. Všechny k obdržení sítě jsou zejména pouze aktivity, které mají původ v monitorované síti.

IP Adresa	Pr. útoků IP sítě na síť	Pr. útoků IP sítě na síť
192.168.1.100	10	0
192.168.1.100	10	0



ADVAiCT

▶ Matador Industries Dubnica nad Váhom



- ▶ Centralizovaná infrastruktura v jedné lokalitě
- ▶ Závislost výroby na IT infrastruktuře
- ▶ Outsourcing IT služeb
- ▶ Miroslav Mogora, IT manažer: *Vďaka tejto službe máme dnes kompletný prehľad o zaťažení a spôsobe využitia našej siete, čo nám umožňuje predchádzať prevádzkovým a bezpečnostným problémom*

▶ Liga vozíčkářů



- ▶ Celkem více než 50 počítačů v síti + 4 servery v DMZ
- ▶ Počítačová učebna a přístup k Internetu pro veřejnost
- ▶ Sběr statistik o provozu na síti prostřednictvím sondy FlowMon
- ▶ Zdeněk Škaroupka, ředitel: *V roce 2010 prošla naše IT infrastruktura kompletní modernizací, vyměnili jsme server, aktivní prvky a vůbec rozšířili služby poskytované na síti. Pomalu jsme se v tom začali ztrácet a hledali jsme řešení dohledu a především viditelnosti do sítě. Typická komerční řešení jsou pro naši organizaci nedosažitelná a možná právě proto jsme zkusili NetHound a musím říct, že to byla dobrá volba.*

FlowMon ADS

System pro analýzu a vyhodnocení provozu na síti. Automatické odhalení provozních problémů a bezpečnostních incidentů.

BVV



Veletrhy
Brno

Veletrhy Brno, a.s.

Jiří Heršálek, systémový administrátor:

“Díky řešení ADS od společnosti AdvaICT jsme schopni provoz na síti kompletně rozkrýt, odhalit problémy a útoky v reálném čase a tím pádem na ně pružně reagovat.”

Hlavní přínosy

- ▶ viditelnost do sítě, důraz na chování uživatelů a zařízení
- ▶ významné snížení nákladů na správu sítě
- ▶ automatizace procesů správy sítě a bezpečnosti
- ▶ vynikající poměr cena/výkon



Network Traffic Audit

Profesionální služba analýzy provozu datové sítě s cílem odhalit provozní a bezpečnostní problémy datové infrastruktury zákazníka.



Teplárny Brno, a.s.

Vladislav Kovář, asistent pro informatiku generálního ředitele společnosti:

“Implementace systému pro audit provozu datové sítě je velmi jednoduchá, rychlá, žádným způsobem neovlivňuje provoz na síti. Výsledky jsou prezentovány zdařilou formou přehledných grafů a tabulek.”

- ▶ Na stánku v předsálí čeká 10 poukazů na slevu 25%
 - ▶ Vysoká přidaná hodnota
 - ▶ Možnost vyzkoušet si prezentované řešení

Kontakt

AdvaICT, a. s.

Jundrovská 618/31, 624 00 Brno

tel.: +420 511 112 170,

info@advaict.com

www.advaict.com

www.nethound.eu

Pavel Minařík

Chief Technology Officer

tel.: +420 733 713 703

pavel.minarik@advaict.com



Správa IT infrastruktury:
lépe, snadněji, bezpečněji a levněji