Cyberoam Security Assessment Report

Prepared for: Alternetivo s.r.o.

Delivered on: May 06, 2015

Report Duration: May 05 - May 05, 2015

Cyberoam
A SOPHOS Company

Cyberoam Security Assessment Report

Cyberoam next-generation firewall was used to conduct a quick network risk assessment at Alternetivo s.r.o.. This report aims to provide visibility into potential application and web risks, risky users, intrusion risks and usage of applications within Alternetivo s.r.o.'s network, thereby highlighting security issues that need to be addressed by Alternetivo s.r.o.. This report helps organizations understand capabilities of Cyberoam NGFW to see threats and network usage that their existing Firewalls may not see.

Today's dynamic threat landscape requires organizations to re-consider security at their network perimeter every few years. As a result, the next-generation firewall deployment has begun taking over the mantle of network protection from the last generation of firewalls and security appliances. The truth is, previous generation firewalls are not equipped to identify modern day security threats and do not provide adequate protection, leaving organization networks vulnerable against the tide of new threat vectors and actors.

Cyberoam Next-Generation Firewalls (NGFW) with Layer 8 Identity-based technology offer actionable security intelligence and controls to enterprises that allow complete control over L2-L8 for future-ready security. Cyberoam NGFW integrates multiple features over a single platform, eliminating the need to manage multiple solutions and hence reduces complexity.

This report provides a high level overview of Alternetivo s.r.o.'s network that covers:

- Report Findings
- User Behavior
- Application Risks & Usage
- Web Risks & Usage
- Intrusion attacks

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Report Findings:

Key Observations

- Application Risks and Usage
  - Alternetivo s.r.o. is facing low Application risk with an App risk score of 0.50.
  - 15 risk-prone applications were found traversing the network of which 5 were very high risk applications and 10 were high risk applications.

Key observations on top risky applications:

Application Category	Number of "Risk-5 & Risk-4" Applications found
Proxy and Tunnel	3
Mobile Applications	2
General Internet	2
File Transfer	2
Remote Access	1
Social Networking	1
Streaming Media	1
Infrastructure	1
Instant Messenger	1
P2P	1

- Web Risks & Usage
  - 49 very high risk web domains were accessed that belonged to IPAddress (33 web domains), P2P (6 web domains), Porn (1 web domains), Spyware (9 web domains).
  - Top Web categories by data transferred include InformationTechnology, ImageBanks, IPAddress.

- Intrusion attacks
  - Overall 2232928 intrusion attacks with Moderate severity and above were found, that includes 26 attacks of critical severity , 1422 attacks of Major and 2231480 attacks of Moderate severity level.
  - Top attack categories include Web Services and Applications, Reconnaissance, Operating System and Services, Office Tools, Multimedia.

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

User Behavior

Studies have proved that users are the weakest link in the security chain and patterns of human behavior can be used to predict and prevent attacks. Also usage pattern can help understand how efficiently are corporate resources utilized and if user policies need to be fine-tuned.

Cyberoam Layer 8 Technology over its network security appliances treat user identity as the 8th layer or the "human layer" in the network protocol stack. This allows administrators to uniquely identify users, control Internet activity of these users in the network, and enable policy-setting and reporting by username.

Top Risky Users

Cyberoam's User Threat Quotient (UTQ) helps security administrators spot risky users within their network. The risk could be a result of unintended actions due to lack of security awareness or malware infected host or intended actions of a rogue user. Knowing the user and the activities that caused risk can help the Network Security administrator take required actions to avoid these risks.

Top Risky Users

Relative Risk Ranking	User	Relative Threat Score
No Record Found.		

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Application Risks & Usage Visibility

Today, it is crucial for an organization to be aware about the applications traversing the network and potential risk they pose to effectively manage related business risks. Cyberoam's Application Visibility & Control offers complete visibility on which applications are being accessed within the network irrespective of their ports and protocols. This stops sophisticated application-layer threats right at the network perimeter.

Application Risk Score

This risk calculator indicates the overall risk associated with the applications and is calculated on the basis of individual risk associated with the application and number of hits on that application.

Risk: 0.50

Top Risky Applications in use

The table below lists top 30 risky applications (risk rating 5 or 4 or 3 in this order) along with risk level, application category, characteristic and technology to help understand potential application risks faced by the network.

Top 30 risky applications

Risk Level	App Name	Category	Technology	Hits	Bytes
5	Skype Services	General Internet	Client Server	13611	3.28 MB
5	Facebook Graph API	Social Networking	Browser Based	60	1.16 MB
5	Psiphon Proxy	Proxy and Tunnel	Client Server	1211	1.14 MB
5	Freegate Proxy	Proxy and Tunnel	Client Server	125	233.86 KB
5	Torrent Clients P2P	P2P	P2P	8	22.28 KB
4	HTTP	General Internet	Browser Based	6324	3.09 GB
4	ZIP File Download	File Transfer	Browser Based	2	56.99 MB
4	FTP Base	Infrastructure	Client Server	69	35.06 MB
4	VNC Remote Access	Remote Access	Client Server	1	23.43 MB
4	Skype	Instant Messenger	P2P	197	5.32 MB
4	Gtalk Android	Mobile Applications	Client Server	86	1.85 MB
4	Multi Thread File Transfer	File Transfer	Client Server	1	1.34 MB
4	WhatsApp	Mobile Applications	Client Server	36	298.26 KB

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Risk Level	App Name	Category	Technology	Hits	Bytes
4	PPStream Streaming	Streaming Media	Client Server	8	170.46 KB
4	Manual Proxy Surfing	Proxy and Tunnel	Client Server	1	1.3 KB
3	Mpeg Streaming	Streaming Media	Browser Based	1	208.35 MB
3	Youtube Video Streaming	Streaming Media	Browser Based	179	119.16 MB
3	My SharePoint	General Business	Client Server	88	80.68 MB
3	WebEx	Conferencing	Browser Based	25	13.62 MB
3	Vimeo Streaming	Streaming Media	Browser Based	1	12.5 MB
3	Windows Remote Desktop	Remote Access	Client Server	5	11.58 MB
3	MS Essentials AV Update	Software Update	Client Server	3	9.29 MB
3	Facebook Website	Social Networking	Browser Based	142	8.12 MB
3	HTTP Resume FileTransfer	File Transfer	Browser Based	3	4.2 MB
3	SWF Streaming	Streaming Media	Browser Based	35	4.18 MB
3	Gmail WebMail	Web Mail	Browser Based	174	2.82 MB
3	Flickr Website	Social Networking	Browser Based	5	2.47 MB
3	Dropbox Download	Download Applications	Browser Based	114	2.3 MB
3	Twitter Website	Social Networking	Browser Based	66	1.97 MB
3	Google Plus Website	Social Networking	Browser Based	38	1.52 MB

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Top Application Categories & Applications

Knowing top app categories and applications help understand how efficiently are corporate resources utilized and also app filtering policies. These reports provide a snapshot of various application categories and applications accessed by users and amount of Internet traffic generated by them.

Top 15 Application Categories by Data Transfer

Application Category	Hits	Bytes
General Internet	20614	4.41 GB
Infrastructure	85776	546.06 MB
Streaming Media	474	352.41 MB
N/A	282986	311.67 MB
General Business	510	91.26 MB
File Transfer	178	63.6 MB
Network Services	1411	47.84 MB
Remote Access	6	35.01 MB
Social Networking	345	16.02 MB
Conferencing	26	13.76 MB
Software Update	66	11.65 MB
Instant Messenger	204	5.71 MB
N/A	4	5.43 MB
Mobile Applications	335	4.69 MB
Web Mail	195	3.27 MB

Top 20 Applications by Data Transfer

Application	Application Risk	Application Category	Hits	Bytes
HTTP	4	General Internet	6324	3.09 GB
OneDrive	2	General Internet	174	1.31 GB
Secure Socket Layer Protocol	1	Infrastructure	8725	256 MB
Mpeg Streaming	3	Streaming Media	1	208.35 MB
UDP:443	N/A	N/A	3433	130.54 MB
Youtube Video Streaming	3	Streaming Media	179	119.16 MB
BITS	2	Infrastructure	45	97.92 MB
SMTP	1	Infrastructure	541	87.87 MB
ICMP:0	N/A	N/A	180632	83.66 MB
My SharePoint	3	General Business	88	80.68 MB
ZIP File Download	4	File Transfer	2	56.99 MB
FTP Base	4	Infrastructure	69	35.06 MB
UDP:161	N/A	N/A	27814	28.8 MB
NetBIOS	1	Infrastructure	6327	26.06 MB
SNMP Monitor	1	Network Services	1290	24.26 MB
VNC Remote Access	4	Remote Access	1	23.43 MB

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Application	Application Risk	Application Category	Hits	Bytes
UDP:80	N/A	N/A	312	20.2 MB
DNS	1	Infrastructure	69829	19.7 MB
IMAPS	1	Network Services	81	19.15 MB
DCERPC	1	Infrastructure	159	14.22 MB

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Web Risks & Usage Visibility

Organizations need a strong security mechanism that blocks access to harmful websites, prevent malware, phishing, pharming attacks and undesirable content that could lead to legal liability & direct financial losses. Being able to do so also enables them to manage productivity of their users and helps achieve effective utilization of bandwidth.

Cyberoam's Web Filtering offers one of the most comprehensive URL databases with millions of URLs grouped into 89+ categories providing Web Security, HTTPS Controls and comprehensive web & content filtering solution.

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Risky Web Categories & Domains being accessed

These reports help administrator monitor risky web categories and domains that can pose security and legal risks.

Top Risky Web Categories

Risky Category	No Of Domains	Bytes	Hits
IPAddress	33	1.1 GB	1856
Spyware	9	829 B	140
Gambling	6	586.73 KB	56
P2P	6	659.86 MB	16
Porn	1	8.14 KB	3
AlcoholandTobacco	1	18.15 KB	1

Top 20 Risky web domains

Risky Web Domain	Web Category	Bytes	Hits
80.188.78.193	IPAddress	949.62 MB	1615
ping.luckyorange.net	Spyware	0 B	100
89.233.129.131	IPAddress	0 B	52
www.livesport.cz	Gambling	530.58 KB	42
10.10.10.1	IPAddress	25.15 KB	39
10.77.77.236:8888	IPAddress	286.46 KB	31
10.0.0.237	IPAddress	0 B	25
secure-us.imrworldwide.com	Spyware	528 B	12
www.hellspy.cz	P2P	27.9 KB	11
sp.adbrn.com	Spyware	301 B	10
84.244.70.1:8888	IPAddress	198.18 KB	10
stats.g.doubleclick.net	Spyware	0 B	9
212.158.152.58	IPAddress	645.24 KB	9
d.livesport.cz	Gambling	9.04 KB	8
10.77.77.244	IPAddress	81.89 KB	7
62.240.165.163	IPAddress	138.14 KB	6
216.58.209.174	IPAddress	0 B	5
216.58.209.206	IPAddress	0 B	5
192.168.55.234:3910	IPAddress	5.7 KB	5
80.188.78.154	IPAddress	5.39 MB	5

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Top Web Categories & Domains visited

These reports can give an insight into the general user browsing habits that can help understand how efficiently corporate resources get utilized and efficacy of web filtering policies.
This Report displays a list of top categories along with the number of hits that generate the most traffic for various domains, users and contents.

Top 15 Web categories by Hits

Category	Bytes	Hits
InformationTechnology	3.16 GB	13902
Advertisements	24.83 MB	3978
BusinessAndEconomy	38.29 MB	3853
NewsAndMedia	89.67 MB	2368
None	30.45 MB	2239
Shopping	130.01 MB	2066
Portals	137.49 MB	1960
IPAddress	1.1 GB	1856
SearchEngines	5.39 MB	1222
HobbiesandRecreation	7.21 MB	903
Sports	8.02 MB	797
Vehicles	24.4 MB	717
EducationAndReferenceMaterial	27.44 MB	623
Finance	2.9 MB	422
Entertainment	75.12 MB	356

Top 15 Web categories by Data Transfer

Category	Hits	Bytes
InformationTechnology	13902	3.16 GB
ImageBanks	35	1.4 GB
IPAddress	1856	1.1 GB
PersonalStorage	13	793.87 MB
P2P	16	659.86 MB
Portals	1960	137.49 MB
Shopping	2066	130.01 MB
NewsAndMedia	2368	89.67 MB
Entertainment	356	75.12 MB
EducationalInstitutions	89	39.68 MB
BusinessAndEconomy	3853	38.29 MB
None	2239	30.45 MB
EducationAndReferenceMaterial	623	27.44 MB
Advertisements	3978	24.83 MB
Vehicles	717	24.4 MB

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Top 15 Web Domains by Hits

Web Domain	Web Category	Bytes	Hits
80.188.78.193	IPAddress	949.62 MB	1615
www.google-analytics.com	InformationTechnology	1.84 MB	1230
acsparta.srv-02.maxifi.net	HobbiesandRecreation	6.59 MB	825
api.expresfm.cz	None	0 B	700
h.imedia.cz	BusinessAndEconomy	92.08 KB	616
pixel.rubiconproject.com	InformationTechnology	24.76 KB	605
i.imedia.cz	BusinessAndEconomy	863.9 KB	549
app.huawei.com	InformationTechnology	1.92 MB	446
track.adform.net	Advertisements	223.13 KB	404
i.idnes.cz	NewsAndMedia	6.41 MB	389
cs-CZ.appex-rf.msn.com	Portals	0 B	374
www.google.com	SearchEngines	596.28 KB	355
www.novinky.cz	NewsAndMedia	156.34 KB	345
crl.microsoft.com	InformationTechnology	550 B	333
gidnes.cz	InformationTechnology	1.82 MB	311

Top 15 Web Domains by Data Transfer

Web Domain	Web Category	Hits	Bytes
officecdn.microsoft.com	InformationTechnology	273	2.8 GB
freecache26-free.uloz.to	ImageBanks	1	1.4 GB
80.188.78.193	IPAddress	1615	949.62 MB
www118.uschovna.cz	PersonalStorage	1	698.42 MB
data19.helldata.com	P2P	1	659.82 MB
46.255.225.69	IPAddress	1	165.45 MB
h02c7.s11.cdn.szn.cz	Portals	2	128.22 MB
cdn1.evernote.com	PersonalStorage	1	94.8 MB
pdl.vimeocdn.com	Entertainment	2	71.88 MB
download.windowsupdate.com	InformationTechnology	84	64.35 MB
softwareupdate.vmware.com	InformationTechnology	1	61.1 MB
stream5.idnes.cz	NewsAndMedia	7	60.1 MB
a190.phobos.apple.com	Shopping	1	45.59 MB
ftp.prz.edu.pl	EducationalInstitutions	4	31.33 MB
get.geo.opera.com.global.prod.fastly.net	InformationTechnology	1	31.13 MB

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Intrusion Attacks

Detecting and protecting against network and application level attacks like intrusion attacks, malicious code transmission, backdoor activity is critical to protect network from hackers. Cyberoam's Intrusion Prevention System strengthens defenses against network-level and application-level attacks.

Top Intrusion Attacks

This Report fetches details for the top attacks that have hit the system with information of their severity level, category, platform, target and attack count.

Top 20 Intrusion attacks by Severity

Severity-level	Attack	Category	Platform	Target	Attack Count
Critical	IMAP PCT Client_Hello overflow attempt	Operating System and Services	Windows	Server	16
Critical	SHELLCODE x86 inc ebx NOOP	Misc	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Client,Server	2
Critical	DNS TCP inverse query overflow	DNS	BSD,Linux,Mac,Windows	Server	1
Critical	EXPLOIT ntpdx overflow attempt	Application and Software	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Client,Server	4
Critical	MS-SQL sp_start_job - program execution	Database Management System	Windows	Server	3
Major	Oracle Java Runtime Bytecode Verifier Cache Code Execution (Published Exploit)	Application and Software	Linux,Mac,Solaris, Windows	Client	2
Major	Microsoft Office TIFF Image Converter Heap Buffer Overflow	Office Tools	Windows	Client	6
Major	DNS Query Type ANY - isc.org	DNS	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	2
Major	Sipvicious User-Agent friendly-scanner	Reconnaissance	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	66
Major	Apache httpd Ranges Header Field Memory Exhaustion	Apache HTTP Server	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	4
Major	Novell ZENworks Configuration Management TFTPD Heap Buffer Overflow	Application and Software	Linux,Windows	Server	992
Major	RSA Authentication Agent for Web Buffer Overflow	Application and Software	Windows	Server	71
Major	DNS SPOOF query response with TTL of 1 min. and no authority	DNS	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	46
Major	HTTPS/SSL Renegotiation DoS	Web Services and Applications	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	7

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved

Severity-level	Attack	Category	Platform	Target	Attack Count
Major	Apache HTTP Server mod_rewrite RewriteLog Command Execution	Apache HTTP Server	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	79
Major	DNS named version attempt	Reconnaissance	BSD,Linux,Mac,Windows	Server	2
Major	DDOS TFN client command BE	Malware Communication	BSD,Linux,Other, Solaris,Unix	Client	9
Major	NMAP SCAN -sS window 1024	Reconnaissance	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	111
Major	SNMP missing community string attempt	Misc	BSD,Linux,Mac,Other,Solaris,Unix, Windows	Server	7
Major	Apple iTunes m3u Playlist Multiple Buffer Overflows	Multimedia	Mac,Windows	Client	18

Top attack categories

Attack Category	Variety of attacks	Attack Count
Reconnaissance	10	2231629
Browsers	1	15085
Application and Software	10	1823
Operating System and Services	6	167
Apache HTTP Server	3	154
DNS	3	49
Web Services and Applications	3	39
Multimedia	2	20
Malware Communication	1	9
Misc	2	9
N/A	1	7
Office Tools	1	6
Database Management System	1	3

© Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved