ECTA - ACME Inc.

Report Date: May 13, 2017 16:56

Table of Contents

Grundlegende Informationen und Methodologie

Dieses Dokument präsentiert die Resultate aus der kürzlich in Ihrem Netzwerk vorgenommenen Messung. In diesem Dokument fassen wir einzelne Statistiken und Werte zusammen und geben Empfehlungen um festgestellte Bedrohungsszenarien zu adressieren. Weder der Report noch unsere Empfehlungen sind abschliessend sondern dienen als Grundlage für die weitere Betrachtung und den Ausbau Ihrer Cyber-Sicherheit.

Der Report wurde aufgrund folgender Charakteristiken erstellt:

Firmendetails

Firmenname: ACME Inc.
Standort: Münster
Branche: Handel
Firmengröße: 300 Mitarbeiter

Details der Messung

Startdatum: DD.MM.YYYY
Enddatum: DD.MM.YYY
Analyse Equipment: ECTA-300D
Analyse Version: 5.4.1
Analysiertes Netzwerk: Produktionsnetzwerk
Bemerkung:

Aufbau und Methode der Messung

Ihr Netzwerk-Datenverkehr wurde mit einer ECTA-300D analysiert. Dazu wurden der Analyseappliance über einen SPAN-Port Ihrer Switch-Infrastruktur die nötigen Daten zur Verfügung gestellt. Die Analyse fand am Perimeter-Gateway statt, d.h. es wurde der ein- und ausgehende Datenverkehr vor Ihrer Firewall (vom internen Netz aus betrachtet) analysiert.

Neben dem Aufzeichnen der typischen Sessioninformationen erfolgt auf der ECTA Appliance auch eine "Deep Packet Inspection". Dadurch sind wir in der Lage den Datenverkehr auf weitere Bedrohungen zu analysieren. Zu den verwendteten Techniken gehören unter anderem Intrusion Detection (IDS), Anti-Virus, sowie WEB- und Applikationsmonitoring.

Aus dem analysierten Datenverkehr wurden entsprechende Log-Files erzeugt und in das Datacenter der Exclusive Networks Deutschland GmbH übermittelt. Dort werden die Logfiles zentral und sicher aufbewahrt und nach Abschluss des Messzeitraums entsprechend ausgewertet um diesen Report zu erstellen. Eine Löschung der aufgezeichneten Logfiles erfolgt automatisch nach Abschluss der Analyse.

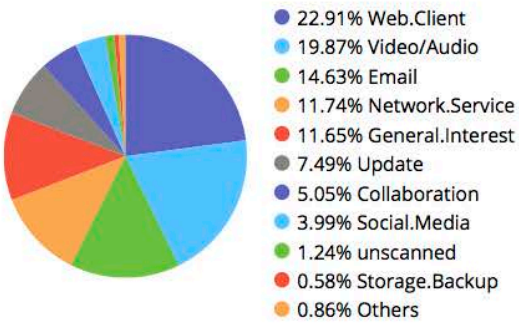
Zusammenfassung

Sicherheit und Bedrohungsabwehr

Malicious & Phishing Sites	54
Critical & High Intrusion Attack	8
Malware & Botnet C&C	4

Applikationskategorien

Das Exclusive Networks Team kategorisiert Applikationen in unterschiedliche Kategorien, welche aufgrund ihres normalen Verhaltens, deren genutzen Technologien und deren Auswirkungen auf das Netzwerk erstellt werden. Eine solche Kategorisierung erlaubt ein besseres Management der Sicherheitsinfrastruktur und dient vor allem der Übersichtlichkeit von Reports und Regeln.



Empfohlene Maßnahmen

Botnet und Malware Infektionen: 63

Bots können genutzt werden um Denial-of-Service (DOS oder DDOS) Angriffe zu starten, bzw. Spam, Spyware, Viren und anderen Code zu verteilen. Weiterhin werden Bots und Botnetze auch dafür genutzt, gefährlichen Code zu verteilen oder Daten aus dem Unternehmen zu sammeln und zu versenden. Dies kann ernsthafte finanzielle und rechtliche Konsequenzen nach sich ziehen. Botnet Infektionen sollten ernst genommen und umgehend weiter untersucht werden. Infizierte PCs sollten identifiziert und schnellstmöglich vom Netz genommen werden um eine weitere Analyse zu ermöglichen, bzw. diese von den Infektionen durch schadhaften Code zu bereinigen. Die o.g. Anzahl ist die Summe aller erkannten Botnetzverbindungen und Malware wie z.B. Viren oder Trojaner.

Tunnel Applikationen: 3

Proxy- oder Tunnelapplikationen werden häufig genutzt um existierende Sicherheitsmaßnahmen zu umgehen. Dies hat Auswirkungen auf Ihr Unternhemen sowie auf die Sicherheit. Entsprechende Sicherheitsregeln auf Firewalls und interne Policies, die die Nutzung solcher Applikationen regeln sollten implementiert werden.

P2P Applikationen: 2

P2P Applikationen können dazu genutzt werden existierende Inhaltskontrollen am Perimeter zu umgehen. Dadurch entsteht das Risiko des unkontrollierten Transports von Daten aus dem Unternehmensnetzwerk hinaus. Entsprechende Sicherheitsregeln auf Firewalls und interne Policies, die die Nutzung solcher Applikationen regeln sollten implementiert werden.

Stark bandbreitenintensive Applikationen: 65

Bandbreitenintensive Applikationen können den normalen Geschäftsablauf und die Performance der unternehmeskritischen Anwendungen negativ beeinflussen. Entsprechende Regeln auf dem Perimeter sollten evaluiert werden. Dazu zählen zeitliche Beschränkungen, komplette Sperrungen aber auch Bandbreiteneinschränkungen durch QoS.

Sicherheit und Bedrohungsabwehr

Definition Applikationsrisiko

Applikationen wird basierend auf ihrem Verhalten und den möglichen Auswirkungen eine Risikobewertung von 1 bis 5 zugewiesen. Diese Unterteilung erlaubt es Administratoren risikobehaftete Applikationen schnell zu erkennen und Reports entsprechend zu strukturieren.

Riskobewertung	Charakteristisches Verhalten	Beispiele
5 Kritisch	Bösartige Applikationen oder solche, die dazu genutzt werden können, diverse Sicherheitsmaßnahmen zu umgehen.	Botnet oder Proxy Applikationen
4 Hoch	Applikationen, die Malwareinfektionen oder "Data Leakage" verursachen können. Solche Applikationen sind häufig persönliche / private file-sharing Applikationen oder solche, die Datenverkehr tunneln um Sicherheitsmaßnahmen zu umgehen.	P2P oder Remote Access Applikationen
3 Erhöht	Applikationen, die der persönlichen / privaten Kommunikation dienen oder bekannte Schwachstellen haben.	IM, Email, Storage oder Backup Applikationen
2 Überwacht	Applikationen, die oft eine erhöhte Bandbreitennutzung nach sich ziehen oder die Effektivität beeinflussen können.	Spiele, Social Media, Video/Audio Applikationen
1 Niedrig	Geschäftliche Applikationen oder Software Update Mechanismen.	Update oder Business Applikationen

Risikobehaftete Applikationskategorien

Bei der Messung in Ihrem Netzwerk wurden folgende potentiell risikobehaftete Applikationskategorien ermittelt:

Remote.Access	8
Proxy	7
P2P	2
Botnet	1

#	Risiko	Applikation	Kategorie	Technologie	Benutzer	Bandbreite	Verbindungen
1	5	Proxy.HTTP	Proxy	Network-Protocol	21	11.55 MB	857
2	5	Tor	Proxy	Client-Server	1	5.36 MB	86
3	5	Zeroaccess.Botnet	Botnet	Client-Server	1	864 B	54
4	5	Peer2me	Proxy	Client-Server	1	1.17 MB	6
5	5	OKHTTP.Library.VPN	Proxy	Client-Server	1	5.74 KB	6
6	5	Tor2web	Proxy	Browser-Based	1	483 B	4
7	5	SOCKS4	Proxy	Network-Protocol	1	28 B	2
8	5	DNS.TXT.Records.Tunneling	Proxy	Client-Server	1	11.87 KB	1
9	4	AnyDesk	Remote.Access	Client-Server	48	613.15 MB	157,851
10	4	TeamViewer	Remote.Access	Client-Server	48	115.53 MB	9,786
11	4	Citrix.Receiver	Remote.Access	Client-Server	31	84.25 MB	8,497
12	4	RDP	Remote.Access	Client-Server	17	25.29 MB	209
13	4	Bitcomet.HTTP.Seed	P2P	Peer-to-Peer	23	2.53 KB	162
14	4	TeamViewer_CallRequest	Remote.Access	Client-Server	14	254.73 MB	117
15	4	BitTorrent			59	6.71 KB	77
16	4	TeamViewer_CallReceive	Remote.Access	Client-Server	5	17.18 MB	14
17	4	VNC	Remote.Access	Client-Server	2	5.78 MB	11
18	4	MS.Netlogon	Remote.Access	Client-Server	4	36.69 KB	6

Angriffe

Erkannte Angriffe

#	Attack Name	Severity	CVE-ID	Counts
1	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Critical		630
2	ASUS.Router.infosvr.UDP.Broadcast.Command.Execution	Critical	CVE-2014-9583	112
3	Obfuscated.Flash.Exploit	Critical		3
4	MS.WinVerifyTrust.Signature.Validation.Remote.Code.Execution	Critical	CVE-2012-0151	2
5	Sundown.Exploit.Kit	Critical		1
6	IP.Bad.Header	Critical		1
7	Worm.Slammer	high	CVE-2002-0649	387
8	MS.Exchange.Mail.Calender.Buffer.Overflow	high	CVE-2006-0027	1
9	BlackNurse.ICMP.Type.3.Code.3.Flood.DoS	medium		6
10	SIPVicious.SIP.Scanner	low		717
11	PHP.Remote.File.Inclusion	low		246
12	Port.Scanning	low		11
13	MS.Windows.TCP.Timestamp.Remote.Code.Execution	low	CVE-2009-1925	1

Angriffsziele

#	Attack Victim	Counts (Critical / High / Medium)	Percent of Total Attacks
1		78	6.86%
2		76	6.68%
3		75	6.60%
4		74	6.51%
5		73	6.42%
6		72	6.33%
7		71	6.24%
8		70	6.16%
9		70	6.16%
10		70	6.16%
11	de	69	6.07%
12		69	6.07%
13		68	5.98%
14		67	5.89%
15		64	5.63%
16		63	5.54%
17		3	0.26%
18		3	0.26%
19		1	0.09%
20		1	0.09%

Angriffsquellen

#	Attack Source	Counts (Critical / High / Medium)	Percent of Total Attacks
1		245	28.76%
2		87	10.21%
3		64	7.51%
4		64	7.51%
5		45	5.28%
6		33	3.87%
7		32	3.76%
8		32	3.76%
9		32	3.76%
10		32	3.76%
11		30	3.52%
12		24	2.82%
13		19	2.23%
14		18	2.11%
15		17	2.00%
16		17	2.00%
17		17	2.00%
18		16	1.88%
19		14	1.64%
20		14	1.64%

Malware, Botnetze, Spyware/Adware

Erkannte Malware

#	Malware Name	Malware Type	Counts
1	EICAR_TEST_FILE	Virus	7
2	JS/IFRAME.CNT!tr	Virus	1
3	W32/Kryptik.FSBJ!tr	Virus	1

Malware Ziele

#	Victim Name (or IP)	Counts
1	IPv4-39156	7
2	IPv4-28266	1
3	IPv4-51756	1

Malware Quellen

#	Malware Source	Hostname (or IP)	Counts
1	IPv4-39156		7
2	IPv4-28266		1
3	IPv4-51756		1

Erkannte Botnetze

#	Botnet Name	Counts
1	Zeroaccess.Botnet	54

Botnet Ziele

#	Victim Name (or IP)	Counts
1	IPv4-33281	54

Botnet Quellen

#	C&C IP	Hostname	Counts
1	IPv4-23257		4
2	IPv4-27544		4
3	IPv4-53995		4
4	IPv4-23310		4
5	IPv4-52772		4
6	IPv4-40640		4
7	IPv4-27215		3
8	IPv4-58147		3
9	IPv4-65202		3
10	IPv4-53114		3
11	IPv4-54197		3
12	IPv4-2915		3
13	IPv4-57981		3
14	IPv4-65516		3
15	IPv4-15349		3
16	IPv4-44630		3

Gefährdete Nutzer und Geräte

Die Reputationsbewertung erlaubt es Administratoren anhand der im Netzwerk verkehrenden Daten risikobehaftetes Verhalten sowohl für Nutzer als auch für Geräte im LAN zu erkennen. Jeder Nutzer und jedes Gerät haben zu Beginn der Bewertung einen Wert von „0" welcher durch unterschiedlichste Bedrohungsvektoren erhöht wird. Zu den Bedrohungsvektoren zählen u.a. Verbindungen zu Botnetzen, Nutzung potenziell gefährlicher Anwendungen und heruntergeladene oder verschickte Malware.

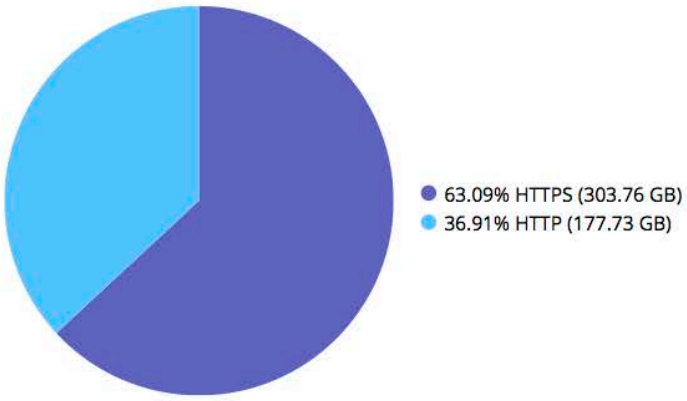
Top Geräte nach Reputation Scores

#	Device	Scores
1		35,975
2		8,735
3	m.cr	7,320
4		6,450
5		5,940
6		5,580
7		4,975
8		4,740
9		4,330
10		3,690
11		3,200
12		3,200
13		2,700
14		2,610
15		2,460
16		2,360
17		2,300
18		2,250
19		2,220
20		2,210

Nutzerproduktivität

Verhältnis HTTPS zu HTTP

HTTP SSL Ratio



Top Zielländer nach Zeit

#	Destination	Browsing Time(hh:mm:ss)	Bandwidth	Sent	Received
1	United Kingdom	332:20:01			1.12 GB
2	United States	241:26:06			58.27 GB
3	Ireland	217:22:23			2.61 GB
4	Netherlands	210:42:17			5.68 GB
5	Germany	158:40:59			13.62 GB
6	France	29:05:51			651.17 MB
7	Canada	09:26:05			829.15 MB
8	China	04:20:58			21.95 MB
9	Czech Republic	04:09:56			105.54 MB
10	Japan	03:47:31			16.92 MB

Top-Cloud-Anwendungen

#	Application	Action	Bandwidth	Session Count
1	Amazon.AWS_S3	Allowed	404.73 MB	6,611
2	Amazon.AWS	Allowed	369.84 MB	3,234
3	Fortiguard.Search	Allowed	121.45 MB	1,975,690
4	Microsoft.Azure	Allowed	31.37 MB	4,269
5	Godaddy	Allowed	18.73 MB	7,276
6	TrendMicro.WFBS	Allowed	1.06 MB	23
7	Google.Cloud.Platform	Allowed	585.12 KB	1
8	Twilio	Allowed	51.75 KB	1

Top-Fernzugriffsanwendungen

#	Application	Action	Bandwidth	Session Count
1	AnyDesk	Allowed	613.15 MB	157,851
2	TeamViewer_CallRequest	Allowed	254.73 MB	117
3	TeamViewer	Allowed	115.53 MB	9,786
4	Citrix.Receiver	Allowed	84.25 MB	8,497
5	RDP	Allowed	25.29 MB	209
6	TeamViewer_CallReceive	Allowed	17.18 MB	14
7	VNC	Allowed	5.78 MB	11
8	MS.Netlogon	Allowed	36.69 KB	6

Top-Proxy-Anwendungen

#	Application	Action	Bandwidth	Session Count
1	Proxy.HTTP	Allowed	11.55 MB	857
2	Tor	Allowed	5.36 MB	86
3	Peer2me	Allowed	1.17 MB	6
4	OpenVPN	Allowed	1.16 MB	22
5	PPTP	Allowed	483.90 KB	558
6	L2TP	Allowed	45.25 KB	433
7	DNS.TXT.Records.Tunneling	Allowed	11.87 KB	1
8	OKHTTP.Library.VPN	Allowed	5.74 KB	6
9	Tor2web	Allowed	483 B	4
10	SOCKS4	Allowed	28 B	2

Top-Social-Media-Anwendungen

#	Application	Action	Bandwidth	Session Count
1	Facebook	Allowed	10.70 GB	84,854
2	Instagram	Allowed	6.15 GB	12,186
3	Tumblr	Allowed	1.90 GB	6,299
4	Twitter	Allowed	1.67 GB	22,010
5	DeviantArt	Allowed	367.91 MB	1,375
6	XING	Allowed	264.08 MB	3,621
7	LinkedIn	Allowed	101.10 MB	5,462
8	Pinterest	Allowed	28.27 MB	1,476
9	Tinder	Allowed	24.05 MB	99
10	Jodel	Allowed	12.81 MB	830
11	Yammer	Allowed	11.01 MB	1,724
12	Snapchat	Allowed	9.70 MB	961
13	Google.Plus	Allowed	3.43 MB	147
14	Ning	Allowed	1.43 MB	24
15	Google.Groups	Allowed	906.58 KB	1
16	Flickr	Allowed	318.45 KB	14
17	Foursquare	Allowed	173.66 KB	13
18	Vkontakte	Allowed	135.23 KB	27
19	Reddit	Allowed	60.28 KB	15
20	Tapatalk	Allowed	54.80 KB	2

Top-Video-/Audio-Streaming-Anwendungen

#	Application	Action	Bandwidth	Session Count
1	YouTube	Allowed	75.13 GB	68,039
2	HTTP.Video	Allowed	23.90 GB	2,683
3	Spotify	Allowed	3.29 GB	3,375
4	Dailymotion	Allowed	2.21 GB	556
5	iTunes_Select.Play	Allowed	580.75 MB	198
6	Vimeo	Allowed	273.48 MB	796
7	Ooyala	Allowed	197.83 MB	100
8	HTTP.Audio	Allowed	62.41 MB	44
9	Deezer	Allowed	52.31 MB	156
10	CNN.Video	Allowed	51.53 MB	11
11	Amazon.Video	Allowed	36.25 MB	2,771
12	SoundCloud	Allowed	17.99 MB	1,319
13	RTCP	Allowed	11.70 MB	519
14	Last.FM	Allowed	8.68 MB	372
15	Netflix	Allowed	6.48 MB	381
16	Flowplayer	Allowed	1.19 MB	18
17	RTMPE	Allowed	1,002.60 KB	5
18	Twitch	Allowed	843.37 KB	27
19	Zune	Allowed	674.74 KB	7
20	Shazam	Allowed	439.76 KB	28

Top-Spieleanwendungen

#	Application	Action	Bandwidth	Session Count
1	Steam	Allowed	38.69 MB	53
2	Clash.Of.Clans	Allowed	3.93 MB	32
3	Apple.Game.Center	Allowed	3.55 MB	662
4	Playstation.Network	Allowed	2.06 MB	2
5	Super.Mario.Run	Allowed	257.05 KB	47
6	Madden.NFL.Mobile	Allowed	80.60 KB	16
7	Valve.Games	Allowed	11.36 KB	170
8	Warcraft	Allowed	6.04 KB	34
9	Xbox	Allowed	2.72 KB	2

Top-Peer-to-Peer-Anwendungen

#	Application	Action	Bandwidth	Session Count
1	BitTorrent	Allowed	6.71 KB	77
2	Bitcomet.HTTP.Seed	Allowed	2.53 KB	162

Webnutzung

Top-Webkategorien

#	Category	Browsing Time(hh:mm:ss)
1	Information Technology	463:20:40
2	Search Engines and Portals	169:47:36
3	News and Media	123:28:16
4	Business	123:24:40
5	Information and Computer Security	78:11:13
6	Social Networking	45:42:40
7	Shopping	32:59:27
8	Reference	25:56:50
9	Real Estate	20:09:43
10	Games	17:39:54

Top-Webanwendungen

#	Risk	Web Application	Technology	User	Bandwidth	Session
1	3	HTTPS.BROWSER	Browser-Based	191	81.96 GB	1,877,833
2	3	Microsoft.Outlook	Browser-Based	119	76.94 GB	881,280
3	2	YouTube	Browser-Based	133	75.11 GB	67,400
4	2	MS.Windows.Update	Client-Server	115	31.66 GB	100,461
5	2	HTTP.Video	Browser-Based	46	23.90 GB	2,683
6	2	HTTP.Download.Accelerator	Browser-Based	96	21.44 GB	5,446
7	2	Microsoft.Portal	Browser-Based	148	18.88 GB	159,845
8	3	HTTP.BROWSER	Browser-Based	253	15.35 GB	639,361
9	2	Google.Services	Browser-Based	176	14.99 GB	287,163
10	2	HTTP.Segmented.Download	Browser-Based	122	14.28 GB	3,652
11	2	Apple.Services	Client-Server	86	13.39 GB	25,160
12	2	HTTP.BROWSER_Firefox	Browser-Based	81	12.23 GB	341,795
13	3	Facebook	Browser-Based	149	10.70 GB	84,854
14	2	HTTP.BROWSER_Chrome	Browser-Based	105	8.37 GB	193,315
15	2	Amazon.Services	Browser-Based	114	6.68 GB	103,195
16	2	Instagram	Client-Server	69	6.15 GB	12,186
17	3	SSL_TLSv1.2	Network-Protocol	110	4.57 GB	63,804
18	2	Microsoft.Office.Update	Client-Server	37	3.69 GB	3,519
19	3	Spotify	Client-Server	34	3.27 GB	3,094
20	1	Apple.Software.Update	Client-Server	27	2.80 GB	2,917

Meist besuchte Webdomänen

#	Website	Category	Requests
1	http.00.a.sophosxl.net	Information Technology	1,405,163
2	d1.sophosupd.com	Information and Computer Security	92,758
3	clients3.google.com	Search Engines and Portals	87,797
4	dci.sophosupd.com	Information Technology	77,005
5	http.00.s.sophosxl.net	Information and Computer Security	67,616
6	dci.sophosupd.net	Information Technology	64,848
7	resolver1.ast.ctmail.com	Information Technology	58,328
8	netsrv11.tlk.net	Domain Parking	57,330
9	d2.sophosupd.com	Information Technology	49,320
10	bilder.bild.de	News and Media	47,585
11	detectportal.firefox.com	Information Technology	46,383
12	citrixweb	Unrated	42,411
13	crl.microsoft.com	Information Technology	39,916
14	pagead2.googlesyndication.com	Advertising	33,251
15	10.8.1.235:3910	Unrated	28,816
16	www.exclusive-networks.com	Information Technology	27,048
17	ocsp.digicert.com	Information Technology	26,024
18	ww251.smartadserver.com	Advertising	25,268
19	officecdn.microsoft.com.edgesuite.net	Information Technology	24,372
20	ib.adnxs.com	Advertising	23,870

Meist besuchte Webdomänen nach Surfzeit

#	Sites	Category	Browsing Time(hh:mm:ss)
1	resolver1.ast.ctmail.com	Information Technology	308:09:48
2	http.00.a.sophosxl.net	Information Technology	199:02:30
3	detectportal.firefox.com	Information Technology	192:40:46
4	crl.microsoft.com	Information Technology	98:58:20
5	ocsp.digicert.com	Information Technology	89:52:12
6	www.microsoft.com	Information Technology	86:51:24
7	clients1.google.com	Search Engines and Portals	70:28:49
8	www.bild.de	News and Media	68:44:53
9	http.00.s.sophosxl.net	Information and Computer Security	60:15:10
10	crl.swisssign.net	Information Technology	55:39:35
11	ping.chartbeat.net	Information Technology	55:32:53
12	clients3.google.com	Search Engines and Portals	53:09:22
13	getgreenshot.org	Information Technology	50:24:39
14	ups.xplosion.de	Business	47:10:09
15	ss.symcd.com	Information Technology	43:32:25
16	wetter.bild.de	News and Media	39:26:07
17	cdn.content.prod.cms.msn.com	Search Engines and Portals	36:30:47
18	bilder.bild.de	News and Media	33:46:51
19	ocsp2.globalsign.com	Information Technology	30:09:51
20	odb.outbrain.com	Business	28:26:46

Netzwerknutzung

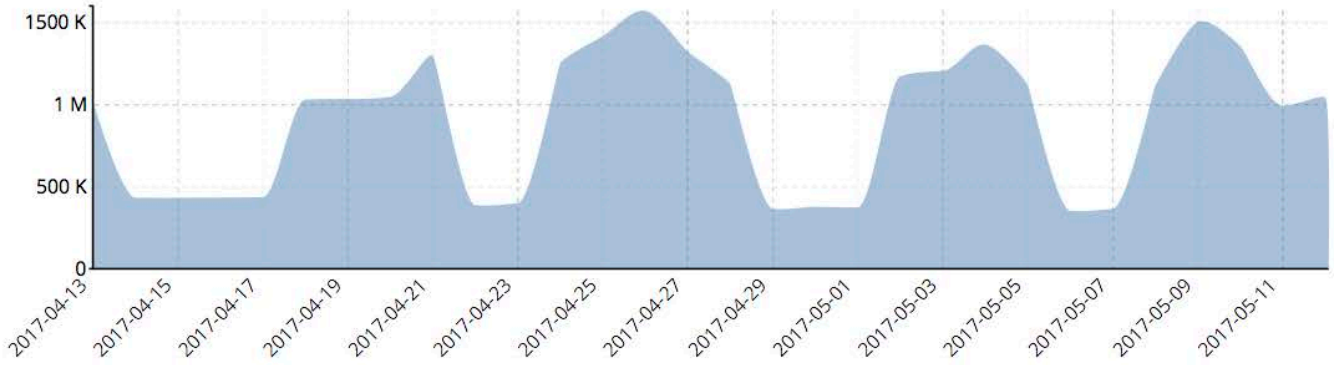
Nachfolgend zur Übersicht und zum besseren Verständis eine Übersicht des analysierten Datenverkehrs. Diese Daten sollen Sie insbesondere bei der Planung weiterer Maßnamen unterstützen, da sie wichtige Kriterien wie Anzahl der Sessions, Bandbreite, Anzahl der Benutzer, etc. aufzeigen.

#	Zusammenfassung	Werte
1	Total Sessions	27,328,903
2	Total Bytes Transferred	532.60GB
3	Most Active Date By Sessions	2017-04-26
4	Total Users	256,235
5	Total Applications	16,266
6	Total Destinations	59,636
7	Average Sessions Per Day	910,963
8	Average Bytes Per Day	17.75GB

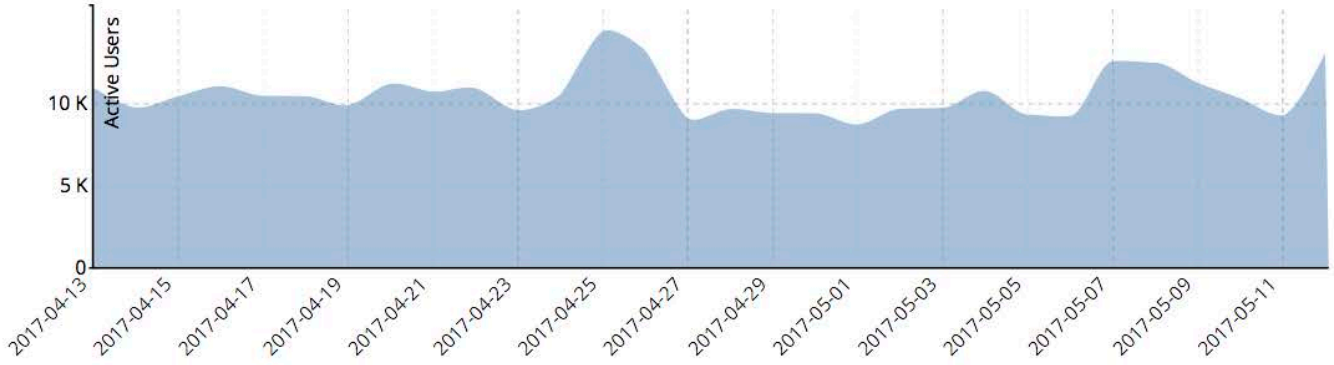
Bandbreitenerschöpfende-Top-Quellen/-Ziele

#	Hostname(or IP)	Bandwidth	Sent	Received	Sessions
1				41.10 GB	21,574
2	microsoft.com			15.71 GB	46,061
3	glomex.com			15.18 GB	2,022
4	apple.com			14.70 GB	7,590
5	windowsupdate.com			14.61 GB	6,519
6				11.40 GB	618,931
7				11.02 GB	102,628
8				9.80 GB	358
9				8.84 GB	17,171
10				4.77 GB	4,365,782
11	cloudfront.net			4.74 GB	1,722
12	edgesuite.net			4.03 GB	1,882
13				3.73 GB	637,408
14				3.37 GB	44,529
15				3.25 GB	157,073
16				3.22 GB	46,073
17				3.06 GB	37,915
18				3.04 GB	30,312
19				3.03 GB	36,651
20				3.03 GB	45,328

Übersicht über das Sessionaufkommen während des ECTAs



Aktive Benutzer



Appendix A

Devices

ECTA-FortiGate[ECTA]