SECURITY LIFECYCLE REVIEW

ACME

Berichtzeitraum: 7 Days
Beginn: Wed, Nov 23, 2016
Ende: Wed, Nov 30, 2016

Erstellt von:
Test
Palo Alto Networks

www.paloaltonetworks.com

COMPANYNAME
INSERT YOUR TAGLINE HERE

paloalto NETWORKS®

Kurzfassung Acme

Haupterkenntnisse:

- Es sind insgesamt **305** Anwendungen in Verwendung, die ein potenzielles Geschäfts- und Sicherheitsrisiko bergen. Sobald sich wichtige Funktionen nicht mehr unter der Kontrolle einer Organisation befinden, besteht nicht nur das Risiko der Nutzung nicht arbeitsbezogener Anwendungen durch die Mitarbeiter, sondern auch das Risiko, dass Cyberkriminelle diese Anwendungen für Bedrohungen und Datendiebstahl nutzen.
- Es wurden **98** Hochrisikoanwendungen erkannt, einschließlich derer, die für schädliche Aktivitäten genutzt werden oder diese verbergen können, die Dateien aus dem Netzwerk stehlen oder die nicht genehmigte Verbindungen aufbauen.
- Es wurden insgesamt **458,514** Bedrohungen in Ihrem Netzwerk gefunden, einschließlich Sicherheitslücken, bekannter und unbekannter Malware und ausgehender Befehls- und Steuerungsaktivitäten.

Das Security Lifecycle Review liefert einen Überblick über die Geschäfts- und Sicherheitsrisiken von **Acme**. Die Daten für diese Analyse wurden von Palo Alto Networks während des Berichtzeitraums erfasst. Der Bericht bietet verwertbare Informationen in Bezug auf Anwendungen, URL-Traffic, Inhaltstypen und Bedrohungen, die sich im Netzwerk befinden, und spricht Empfehlungen zur Reduzierung des Gesamtrisikos der Organisation aus.

305
APPLICATIONS IN USE

98
HIGH RISK APPLICATIONS

458,514
TOTAL THREATS

405,610
VULNERABILITY EXPLOITS

41,562
KNOWN MALWARE

11,342
UNKNOWN MALWARE

Report Period: 7 Days
Start: Wed, Nov 23, 2016
End: Wed, Nov 30, 2016

Anwendungen auf einen Blick

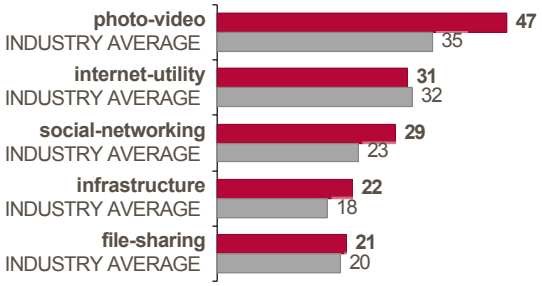
Anwendungen können Risiken bergen: So dienen sie etwa als Zugang für Bedrohungen, stehlen Daten aus dem Netzwerk, ermöglichen den unautorisierten Zugriff, senken die Produktivität oder verbrauchen einen Teil der Netzwerkbandbreite des Unternehmens. In diesem Abschnitt erhalten Sie einen Überblick über die derzeit genutzten Anwendungen, damit Sie potenzielle Risiken und Geschäftsvorteile fundiert gegeneinander abwägen können.

Haupterkenntnisse:

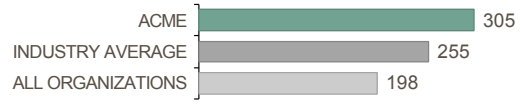
- Im Netzwerk wurden Hochrisikoanwendungen wie **photo-video, internet-utility und social-networking** erkannt. Diese sollten aufgrund ihres Schadenspotenzials untersucht werden.
- Im Netzwerk befinden sich insgesamt **305** Anwendungen verteilt auf **27** Unterkategorien, im Vergleich zum Branchendurchschnitt von insgesamt **255** Anwendungen in Organisationen aus dem Bereich **High Technology**.
- Es wurden **410.91GB** von allen Anwendungen genutzt, einschließlich **general-internet** mit **221.83GB**. Der Branchendurchschnitt in vergleichbaren Organisationen liegt bei **660.03GB**.

Hochrisikoanwendungen

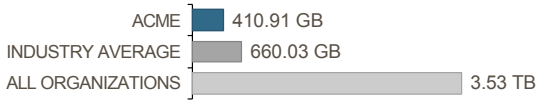
Der erste Schritt zur Verwaltung des Sicherheits- und Geschäftsrisikos ist das Ermitteln der Anwendungen mit dem höchsten Schadenspotenzial. Wir empfehlen, Anwendungen aus diesen Kategorien sorgfältig zu analysieren, um sicherzustellen, dass diese keine unnötigen Compliance-, Betriebs- oder Cybersicherheitsrisiken bergen.



Anzahl von Anwendungen im Netzwerk

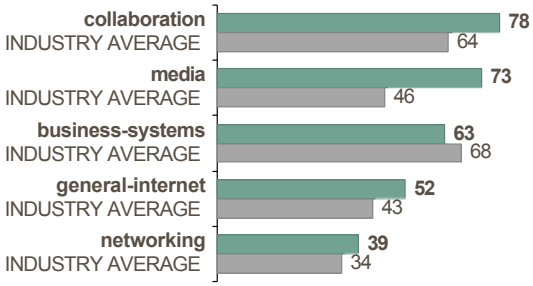


Durch Anwendungen genutzte Bandbreite



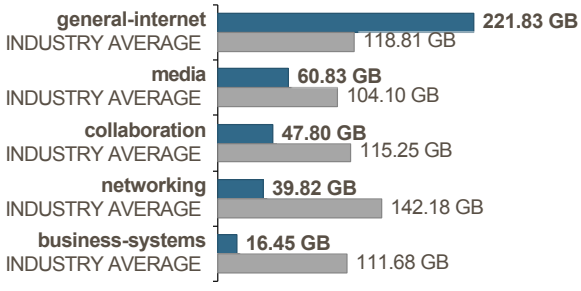
Kategorien mit den meisten Anwendungen

Die folgenden Kategorien besitzen die meisten Anwendungsvarianten und sollten auf ihre geschäftliche Relevanz hin geprüft werden.



Kategorien mit dem höchsten Bandbreitenverbrauch

Die nach Anwendungskategorie verbrauchte Bandbreite zeigt, wo Anwendungen am stärksten genutzt werden und wo Betriebsressourcen eingespart werden können.



Risikobehaftete Anwendungen

Nachfolgend werden die Topverbraucher (nach Bandbreitenverbrauch sortiert) je Anwendungsunterkategorie aufgeführt, die Risiken bergen, einschließlich Branchen-Benchmarks bezüglich der Anzahl von Anwendungsvarianten in anderen Organisationen aus dem Bereich **High Technology**. Mithilfe dieser Daten können Sie effektiver entscheiden, auf welche Anwendungen Sie sich zuerst fokussieren sollten.

RISK LEVEL

5
4
3
2
1

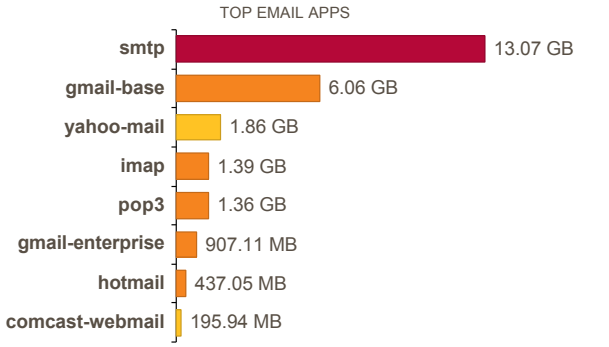
Haupterkenntnisse:

- In Ihrer Organisation wurden insgesamt **305** Anwendungen erkannt. Der Branchendurchschnitt liegt bei **255** in anderen Organisationen aus dem Bereich **High Technology**.
- Am häufigsten kommen die folgenden Typen von Anwendungsunterkategorien vor: **photo-video, internet-utility und social-networking**.
- Die folgenden Anwendungsunterkategorien weisen den höchsten Bandbreitenverbrauch auf: **internet-utility, file-sharing und photo-video**.

Email - 25.42GB

16 11

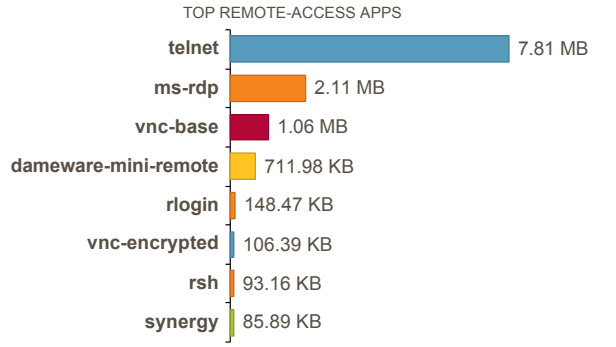
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Remote-Access - 12.1MB

8 7

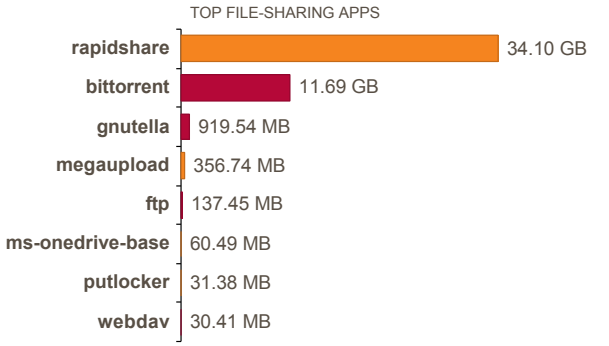
APPLICATION VARIANTS VS INDUSTRY AVERAGE



File-Sharing - 47.36GB

21 17

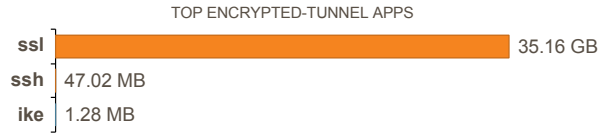
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Encrypted-Tunnel - 35.2GB

3 5

APPLICATION VARIANTS VS INDUSTRY AVERAGE

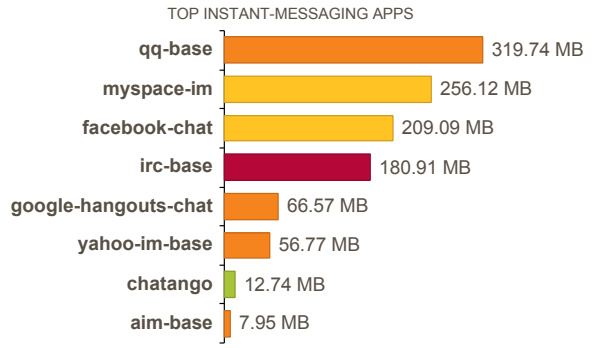


Risikobehaftete Anwendungen (Fortsetzung)

Instant-Messaging - 1.09GB

15 | 10

APPLICATION VARIANTS VS INDUSTRY AVERAGE



Social-Networking - 9.92GB

29 | 20

APPLICATION VARIANTS VS INDUSTRY AVERAGE

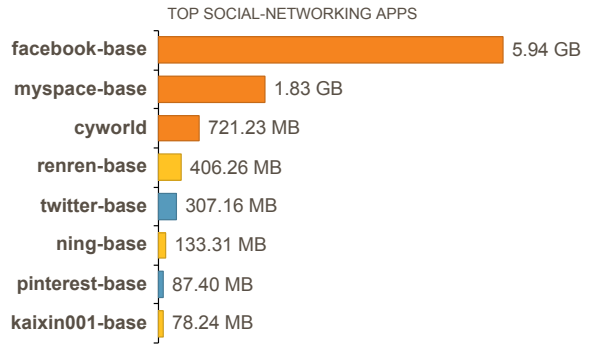
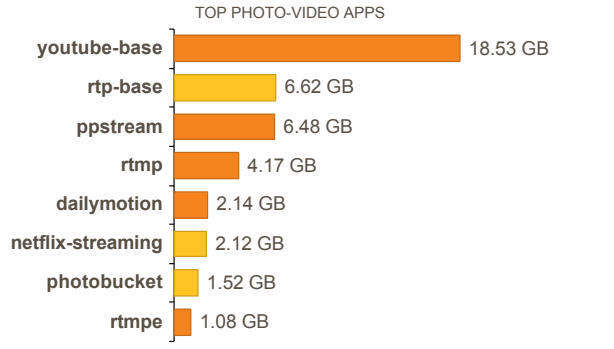


Photo-Video - 46.58GB

47 | 30

APPLICATION VARIANTS VS INDUSTRY AVERAGE



Proxy - 103.55MB

1 | 1

APPLICATION VARIANTS VS INDUSTRY AVERAGE

Risikobehaftete Anwendungen – Details

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
5	smtp	collaboration	email	client-server	13.07GB	231499
4	gmail-base	collaboration	email	browser-based	6.06GB	93296
3	yahoo-mail	collaboration	email	browser-based	1.86GB	71975
4	imap	collaboration	email	client-server	1.39GB	17122
4	pop3	collaboration	email	client-server	1.36GB	16869
4	gmail-enterprise	collaboration	email	browser-based	907.11MB	18624
4	hotmail	collaboration	email	browser-based	437.05MB	28308
3	comcast-webmail	collaboration	email	browser-based	195.94MB	6488
4	ssl	networking	encrypted-tunnel	browser-based	35.16GB	1757342
4	ssh	networking	encrypted-tunnel	client-server	47.02MB	452
2	ike	networking	encrypted-tunnel	client-server	1.28MB	1230
4	rapidshare	general-internet	file-sharing	browser-based	34.1GB	988
5	bittorrent	general-internet	file-sharing	peer-to-peer	11.69GB	1662379
5	gnutella	general-internet	file-sharing	peer-to-peer	919.54MB	124240
4	megaupload	general-internet	file-sharing	browser-based	356.74MB	989
5	ftp	general-internet	file-sharing	client-server	137.45MB	34339
4	ms-onedrive-base	general-internet	file-sharing	client-server	60.49MB	4013
4	putlocker	general-internet	file-sharing	browser-based	31.38MB	182
5	webdav	general-internet	file-sharing	browser-based	30.41MB	3232
4	qq-base	collaboration	instant-messaging	client-server	319.74MB	120135
3	myspace-im	collaboration	instant-messaging	client-server	256.12MB	9094
3	facebook-chat	collaboration	instant-messaging	browser-based	209.09MB	27925
5	irc-base	collaboration	instant-messaging	client-server	180.91MB	11475
4	google-hangouts-chat	collaboration	instant-messaging	browser-based	66.57MB	7142
4	yahoo-im-base	collaboration	instant-messaging	client-server	56.77MB	22070

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
1	chatango	collaboration	instant-messaging	client-server	12.74MB	4634
4	aim-base	collaboration	instant-messaging	client-server	7.95MB	1228
4	youtube-base	media	photo-video	browser-based	18.53GB	12653
3	rtp-base	media	photo-video	client-server	6.62GB	208
4	ppstream	media	photo-video	peer-to-peer	6.48GB	159928
4	rtmp	media	photo-video	browser-based	4.17GB	2686
4	dailymotion	media	photo-video	browser-based	2.14GB	2666
3	netflix-streaming	media	photo-video	browser-based	2.12GB	1781
3	photobucket	media	photo-video	browser-based	1.52GB	22016
4	rtmpe	media	photo-video	browser-based	1.08GB	1141
5	http-proxy	networking	proxy	browser-based	103.55MB	7330
2	telnet	networking	remote-access	client-server	7.81MB	7509
4	ms-rdp	networking	remote-access	client-server	2.11MB	564
5	vnc-base	networking	remote-access	client-server	1.06MB	153
3	dameware-mini-remote	networking	remote-access	client-server	711.98KB	90
4	rlogin	networking	remote-access	client-server	148.47KB	259
2	vnc-encrypted	networking	remote-access	client-server	106.39KB	144
4	rsh	networking	remote-access	client-server	93.16KB	63
1	synergy	networking	remote-access	client-server	85.89KB	90
4	facebook-base	collaboration	social-networking	browser-based	5.94GB	450448
4	myspace-base	collaboration	social-networking	browser-based	1.83GB	90390
4	cyworld	collaboration	social-networking	browser-based	721.23MB	14207
3	renren-base	collaboration	social-networking	browser-based	406.26MB	27440
2	twitter-base	collaboration	social-networking	browser-based	307.16MB	58355
3	ning-base	collaboration	social-networking	browser-based	133.31MB	722

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	pinterest-base	collaboration	social-networking	browser-based	87.4MB	9336
3	kaixin001-base	collaboration	social-networking	browser-based	78.24MB	9275

Notes:

SaaS-Anwendungen

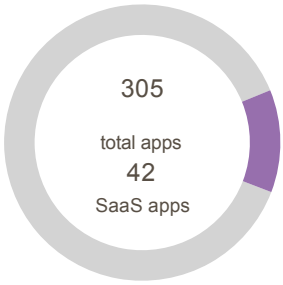
Durch SaaS-basierte Anwendungsservices befindet sich der Umfang des Netzwerkes stetig im Wandel. Oftmals als „Schatten-IT“ bezeichnet werden die meisten dieser Services direkt von einzelnen Benutzern, Unternehmensteams oder sogar gesamten Abteilungen genutzt. Um Datensicherheitsrisiken zu minimieren, sind Transparenz und geeignete Richtlinien für SaaS-Anwendungen notwendig.

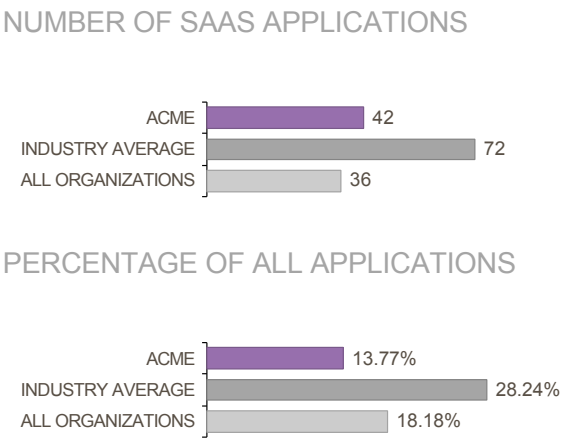
Haupterkenntnisse:

- Sie nutzen im Durchschnitt mehr SaaS Anwendungen als andere Organisationen aus Ihrem Industriezweig und mehr als die meisten Palo Alto Networks Kunden.
- Die meisten SaaS Applikationen gehören zur Unterkategorie **Email**.
- Bezogen auf den Datentransfer wird die SaaS Applikation **rapidshare** in Ihrem Unternehmen am häufigsten genutzt.

SaaS Applikationen in Zahlen

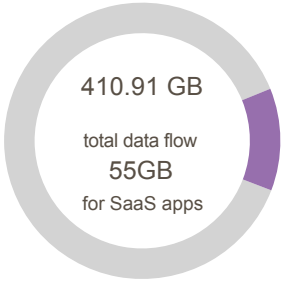
Überprüfen Sie die genutzten Applikationen in Ihrer Organisation. Um eine entsprechende administrative Kontrolle durzusetzen, sollten Sie nur SaaS Applikationen freigeben, welche durch Ihr IT-Team verwaltet und gebilligt sind.

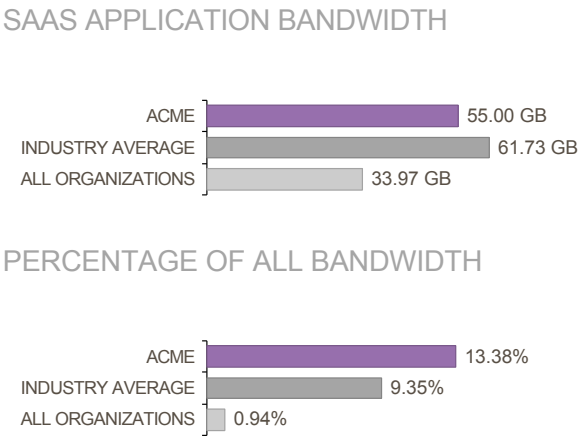




Bandbreitennutzung der SaaS Applikationen

Überwachen Sie das ein und ausgehende Datenvolumen Ihrer SaaS Applikationen. Verstehen Sie die Art der Anwendungen und wie sie genutzt werden.

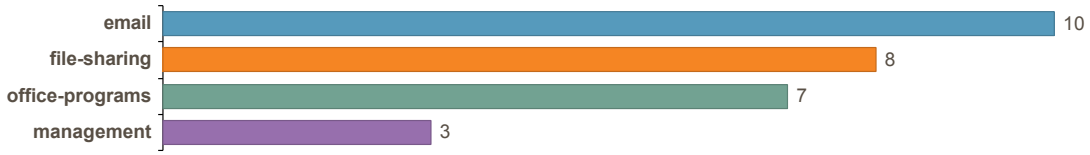




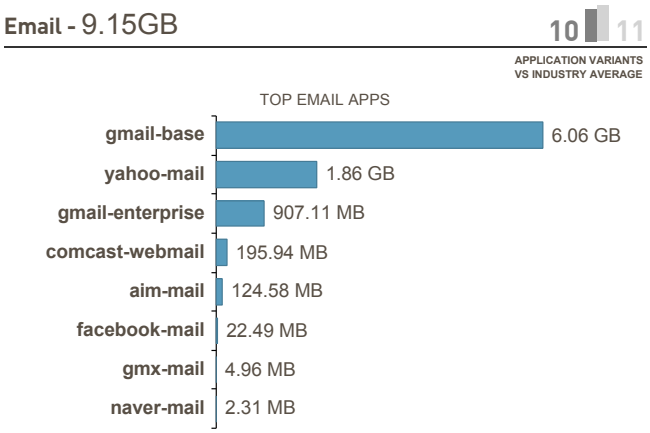
SaaS Anwendungen Unterkategorien

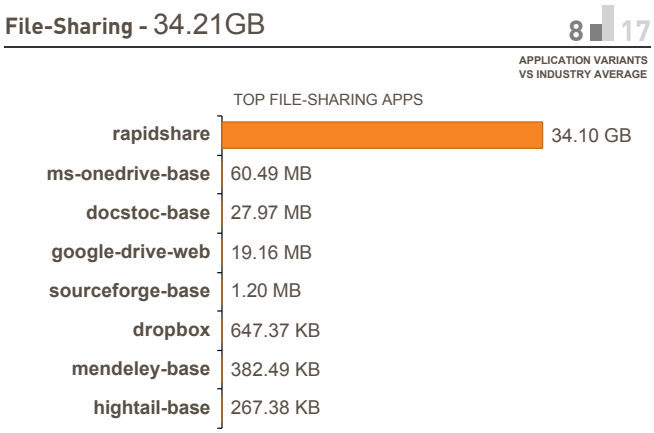
Nachfolgend werden die Anzahl von Applikation pro Unterkategorie dargestellt. Dies erlaubt die am meisten benutzten Anwendungen im Unternehmen zu erkennen.

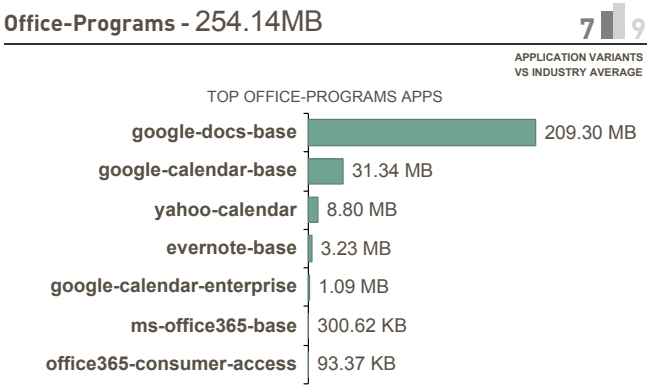
Top SaaS Anwendungs-Unterkategorien nach Anzahl von Anwendungen

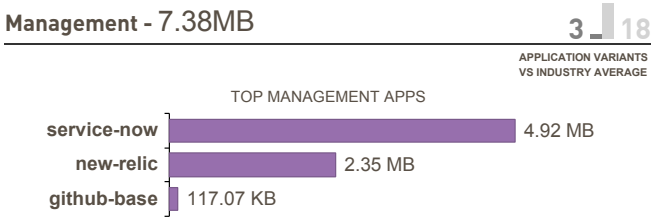


Folgenden Grafiken zeigen die Top Applikationen pro Unterkategorie. Sortiert sind die Anwendungen nach Transfervolumen.





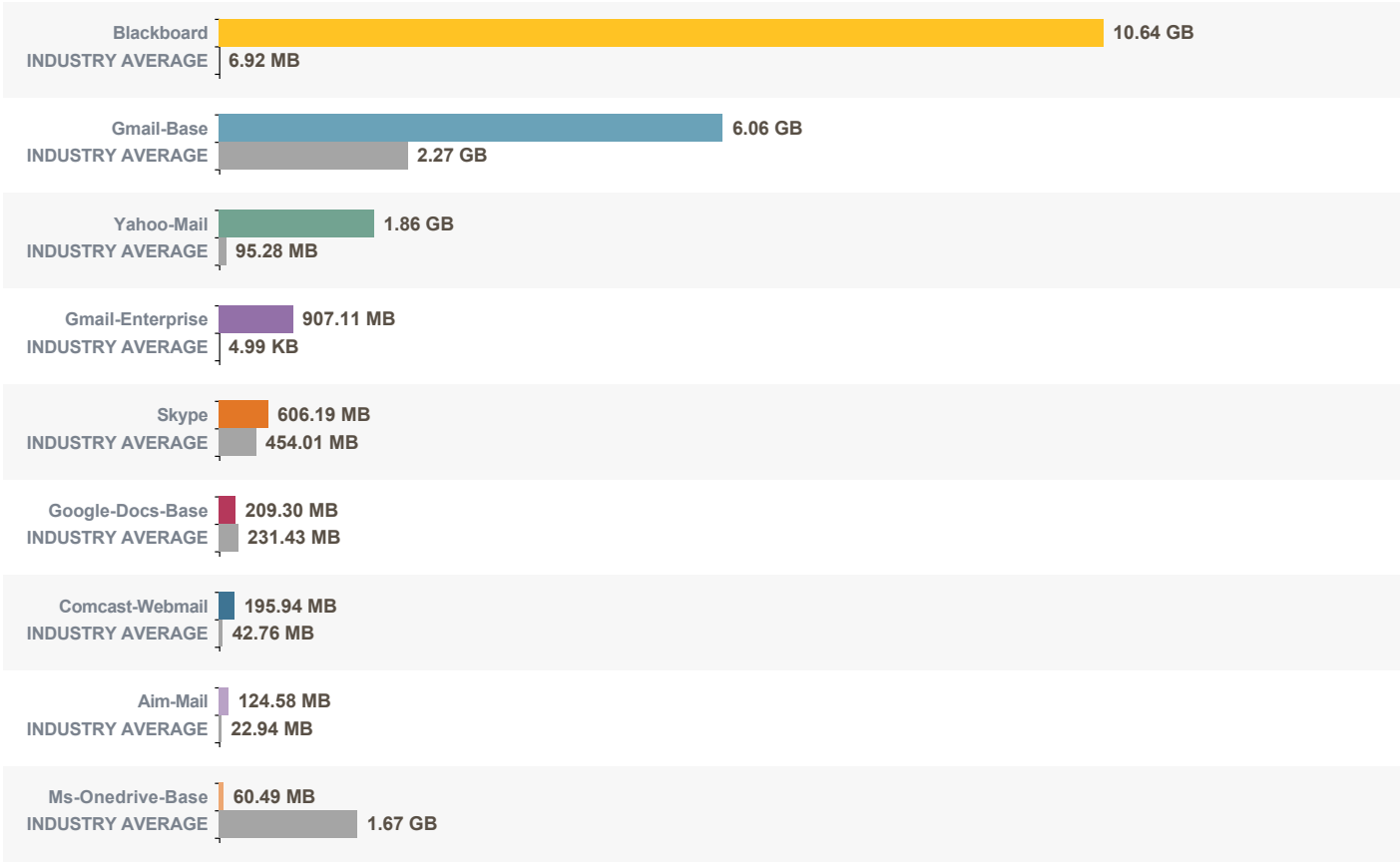




SAAS Applikationen

Im folgenden werden die 10 in Ihrem Unternehmen am häufigsten benutzten SaaS Anwendungen, Branchen-Benchmarks vergleichbarer Unternehmen sowie aller Palo Alto Networks Kunden dargestellt.

Top SaaS Anwendungen nach Datendurchsatz



URL-Aktivität

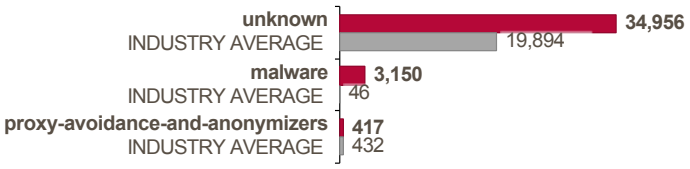
Unkontrolliertes Surfen im Internet setzt Organisationen Sicherheits- und Geschäftsrisiken aus, einschließlich der Verbreitung potenzieller Bedrohungen, Datenverlust oder Compliance-Verstößen. Die am häufigsten von Benutzern im Netzwerk besuchten URL-Kategorien werden unten aufgeführt.

Haupterkenntnisse:

- Es wurden Hochrisiko-URL-Kategorien im Netzwerk erfasst, wie **und educational-institutions**.
- Benutzer haben während des Berichtzeitraums insgesamt **4,250,738** URLs in **58** Kategorien besucht.
- Die Web-Aktivität setzte sich aus einer Mischung aus persönlichen und arbeitsbezogenen Aktivitäten zusammen, einschließlich Besuchen auf potenziell risikobehafteten Websites.

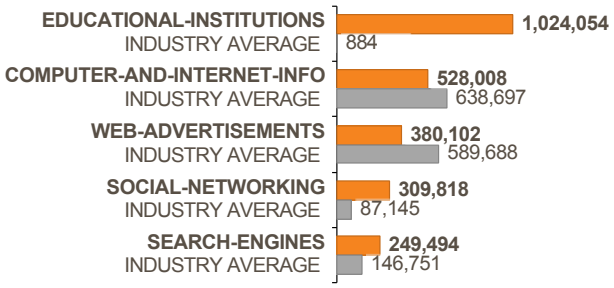
Hochrisiko-URL-Kategorien

Angreifer nutzen das Internet als primären Infektionsvektor. Dabei stellen Hochrisiko-URL-Kategorien ein äußerst hohes Risiko für die Organisation dar. Lösungen sollten ein schnelles Sperren unerwünschter oder schädlicher Websites sowie eine rasche Kategorisierung und Untersuchung unbekannter Websites ermöglichen.



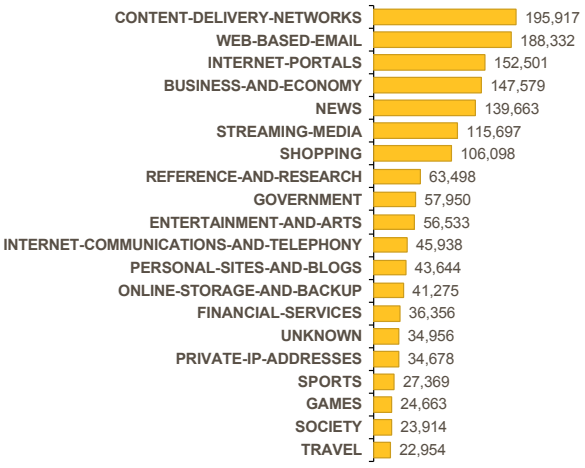
Traffic-starke URL-Kategorien

Nachfolgend werden die fünf am häufigsten besuchten URL-Kategorien sowie Branchen-Benchmarks vergleichbarer Unternehmen



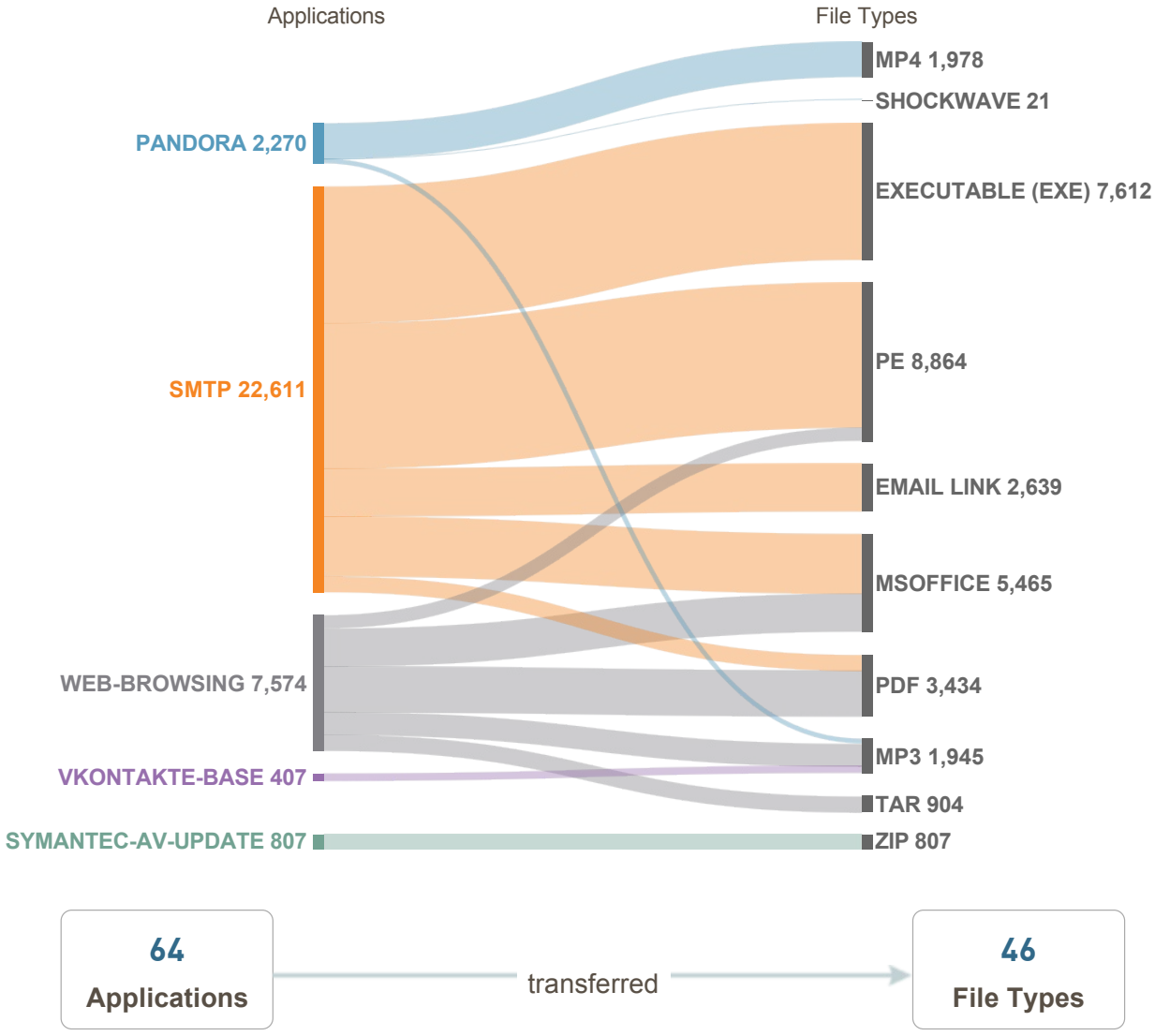
Häufig besuchte URL-Kategorien

Nachfolgend werden die 20 am häufigsten besuchten URL-Kategorien aufgeführt.



Dateiübertragungsanalyse

Anwendungen zur Dateiübertragung haben eine wichtige geschäftliche Funktion. Allerdings besteht auch das Risiko, dass sensible Daten über diese Anwendungen das Netzwerk verlassen oder Cyberbedrohungen durch sie übertragen werden. In Ihrer Organisation wurden insgesamt **46** verschiedene Dateitypen erfasst, die mit Hilfe von **64** verschiedenen Anwendungen übertragen wurden. Im Bild unten werden die am häufigsten für Dateiübertragungen verwendeten Anwendungen mit den häufigsten Datei- und Inhaltstypen korreliert.

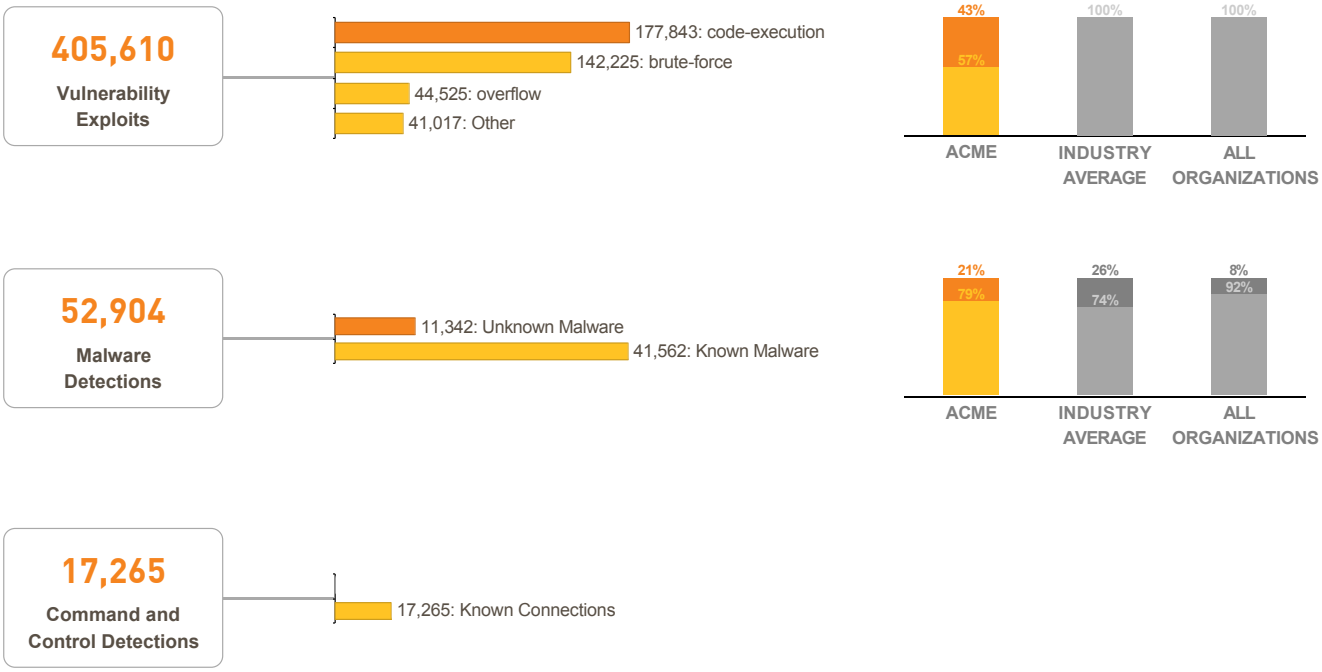


Bedrohungen auf einen Blick

Um zu verstehen, welchem Risiko Sie ausgesetzt sind und wie Sie Angriffe mithilfe Ihrer Sicherheitsinfrastruktur vermeiden, benötigen Sie Informationen über die Art und Anzahl der Bedrohungen, vor denen Sie Ihr Unternehmen schützen müssen. In diesem Abschnitt werden Anwendungsschwachstellen, bekannte und unbekannte Malware sowie die in Ihrem Netzwerk beobachteten Befehls- und Steuerungsaktivitäten aufgeführt.

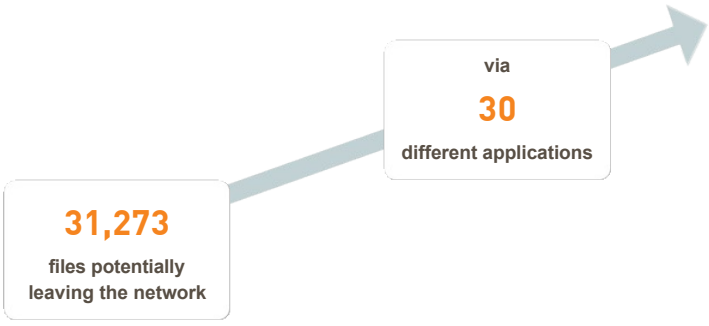
Haupterkenntnisse:

- Es wurden insgesamt **405,610** Schwachstellen in Ihrer Organisation entdeckt, einschließlich der Schwachstellenkategorien **code-execution, brute-force und overflow**.
- Es wurden **52,904** Malware-Ereignisse entdeckt. Der Branchendurchschnitt für vergleichbare Unternehmen liegt bei **7,515**.
- Es wurden insgesamt **17,265** ausgehende Befehls- und Steuerungsanfragen ermittelt. Diese weisen darauf hin, dass Malware versucht hat, mit externen Angreifern zu kommunizieren, um zusätzliche Malware herunterzuladen, Anweisungen zu erhalten oder Daten aus dem Netzwerk zu stehlen.



Potenziell das Netzwerk verlassende Dateien

Die Übertragung von Dateien ist ein notwendiger und gängiger Bestandteil von Geschäftsabläufen. Allerdings müssen Sie wissen, welche Inhalte das Netzwerk über welche Anwendung verlassen, um das Datenverlustrisiko des Unternehmens zu mindern.



Analyse von schädlichen und Hochrisikodateitypen

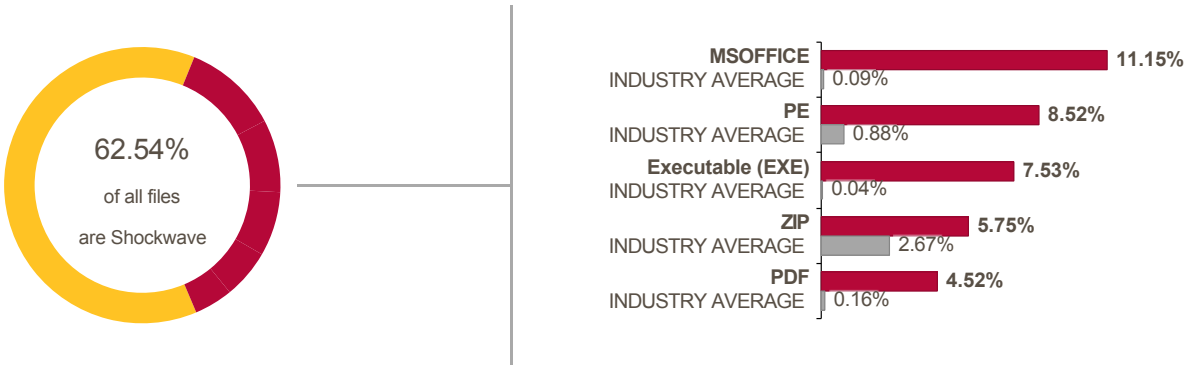
Cyberangreifer nutzen heutzutage die verschiedensten Dateitypen, um Malware und Exploits zu übermitteln. Dabei konzentrieren sie sich vor allem auf die Inhalte gängiger Geschäftsanwendungen. Der Großteil herkömmlicher Bedrohungen wird mit ausführbaren Dateien übertragen, während gezieltere und ausgeklügeltere Angriffe oft andere Inhalte nutzen, um Netzwerke zu schädigen.

Haupterkenntnisse:

- Da für die Übertragung von Bedrohungen verschiedene Dateitypen verwendet wurden, sollten die Präventionsstrategien alle gängigen Dateitypen umfassen.
- Sie können Ihre Angriffsfläche verkleinern, indem Sie verhindern, dass Hochrisikodateitypen wie ausführbare Dateien aus dem Internet heruntergeladen werden können, oder indem Sie RTF- oder LNK-Dateien, die nicht im Unternehmensalltag benötigt werden, sperren.

Hochrisikodateitypen

Die aufgeführten Dateitypen stellen ein erhöhtes Risiko dar, das sich aus der Entdeckung neuer Schwachstellen, bestehender und nicht gepatchter Mängel sowie der Verwendungshäufigkeit bei Angriffen ergibt.



Dateien, die unbekannte Malware übertragen

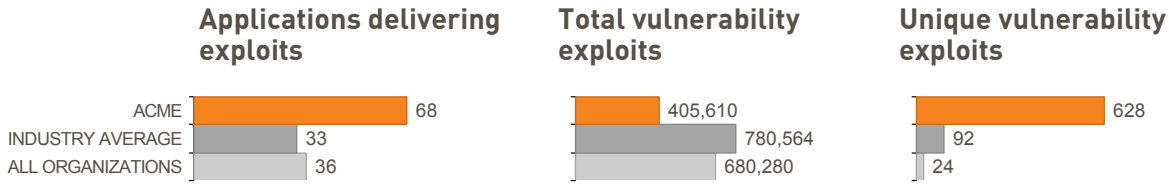
Wir empfehlen, die Dateien, mit denen Bedrohungen potenziell übertragen werden, sowohl innerhalb Ihres Unternehmens als auch innerhalb Ihrer Vergleichsgruppe zu untersuchen. Mithilfe dieser Trends können Sie Präventionsmaßnahmen ergreifen und beispielsweise Hochrisikodateitypen für unterschiedliche Benutzergruppen sperren.

Anwendungsschwachstellen

Anwendungsschwachstellen in verletzbaren, oftmals nicht gepatchten, Anwendungen werden häufig von Angreifern ausgenutzt, um Systeme zu infizieren. Dies stellt meistens den ersten Schritt einer Attacke dar. Auf dieser Seite werden die fünf Schwachstellen aufgeführt, die Angreifer am häufigsten auszunutzen versuchten. So erkennen Sie, welche Anwendungen den größten Angriffsspielraum besitzen.

Haupterkenntnisse:

- Es wurden insgesamt **68** Anwendungen erkannt, die Exploits an Ihre Umgebung weitergeben.
- Es wurden insgesamt **405,610** Schwachstellen erkannt, und die drei häufigsten Kategorien lauten **web-browsing, ftp und smtp**.
- Die insgesamt erkannten Schwachstellen sind in **628** Schwachstellentypen aufgeteilt. Dies bedeutet, dass Angreifer immer wieder auf dieselben Schwachstellen zurückgriffen.



Vulnerability Exploits per Application (top 5 applications with most detections)

DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
213,947	**web-browsing**			
120,460	WordPress Login Brute Force Attempt	Critical	brute-force	
5,994	Upatre/Dyre Phishing Traffic Detection	Critical	code-execution	
1,535	Microsoft Internet Explorer Memory Corruption Vulnerability	Critical	code-execution	CVE-2015-0036
1,387	Microsoft Word RTF Object Parsing Vulnerability	Critical	code-execution	CVE-2008-4030
1,231	Windows Graphics Rendering Engine WMF SetAbortProc Code Execution	Critical	code-execution	CVE-2005-4560
566	Microsoft Office Access ActiveX Controls Remote Code Execution Vulnerability	Critical	overflow	CVE-2010-0814
556	Apache Tomcat JK Web Server Connector Long URL Stack Overflow	Critical		
536	Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability	Critical	code-execution	CVE-2009-2530
410	Microsoft Windows DirectShow MEPG2 ActiveX Remote Buffer Overflow Vulnerability	Critical	overflow	CVE-2008-0015
342	Microsoft Office PICT Filter Parsing Remote Code Execution Vulnerability	Critical	code-execution	CVE-2008-3021
43,533	**ftp**			
256	Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability	Critical	code-execution	CVE-2009-0075
253	Internet Explorer DirectAnimationPath Control KeyFrame Method Vulnerability	Critical	code-execution	CVE-2006-4777;CVE-2006-4446
145	FTP evasion attack	Critical	overflow	
142	Microsoft IIS FTPd NLST Remote Buffer Overflow Vulnerability	Critical	overflow	CVE-2009-3023
133	Microsoft Internet Explorer OBJECT Tag Buffer Overflow Vulnerability	Critical	code-execution	CVE-2003-0344
133	Microsoft Visual Studio MSDATGRD.OCX ActiveX Control Code Execution Vulnerability	Critical	code-execution	CVE-2008-4252
132	Internet Explorer DHTML Engine Race Condition Vulnerability	Critical	code-execution	CVE-2005-0553
131	Microsoft Internet Explorer Print Preview Cross Zone Script Injection Vulnerability	Critical	code-execution	CVE-2008-2259
131	Microsoft Visual Studio MSFLXGRD.OCX ActiveX Control Code Execution Vulnerability	Critical	code-execution	CVE-2008-4253
130	Microsoft Internet Explorer Source Name Buffer Overflow Vulnerability	Critical	code-execution	CVE-2008-4261

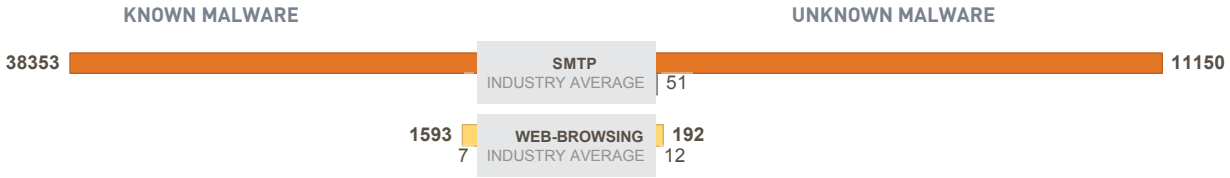
DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
38,137	**smtp**			
5,594	Microsoft Word RTF Object Parsing Vulnerability	Critical	code-execution	CVE-2008-4031
928	Windows Media Header Parsing Invalid Free Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-2498
774	Microsoft Windows GDI+ PNG Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-3126
738	Microsoft Windows GDI Remote Integer Overflow Vulnerability	Critical	overflow	CVE-2008-2249
730	Microsoft Word Memory Corruption Vulnerability	Critical	overflow	CVE-2008-4025
668	Microsoft Wordpad and Office Text Converters OLE Data Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-0087
587	Microsoft Office PowerPoint Memory Corruption Vulnerability	Critical	code-execution	CVE-2009-1128
567	Microsoft Office Memory Corruption Vulnerability	Critical	code-execution	CVE-2008-0118
551	Microsoft Windows Media Malformed AVI Header Parsing Heap Overflow Vulnerability	Critical	code-execution	CVE-2009-1545
392	Microsoft File Converter Buffer Overflow Vulnerability	Critical	code-execution	CVE-2009-1533
24,837	**imap**			
2,503	Microsoft Word RTF Object Parsing Vulnerability	Critical	code-execution	CVE-2008-4030
711	Windows Media Header Parsing Invalid Free Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-2498
523	Microsoft Windows GDI+ PNG Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-2501;CVE-2013-1331
506	Microsoft Windows GDI Remote Integer Overflow Vulnerability	Critical	overflow	CVE-2008-2249
503	Microsoft Word Memory Corruption Vulnerability	Critical	overflow	CVE-2008-4025
433	Microsoft Wordpad and Office Text Converters OLE Data Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-0087
400	Microsoft Office Memory Corruption Vulnerability	Critical	code-execution	CVE-2008-0118
381	Microsoft Office PowerPoint Memory Corruption Vulnerability	Critical	code-execution	CVE-2009-1129
279	Microsoft Office Excel Object Record Corruption Vulnerability	Critical	code-execution	CVE-2009-0557
278	Microsoft Windows Media Malformed AVI Header Parsing Heap Overflow Vulnerability	Critical	code-execution	CVE-2009-1545
24,631	**pop3**			
2,379	Microsoft Word RTF Object Parsing Vulnerability	Critical	code-execution	CVE-2008-4031
698	Windows Media Header Parsing Invalid Free Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-2498
519	Microsoft Windows GDI Remote Integer Overflow Vulnerability	Critical	overflow	CVE-2008-2249
490	Microsoft Windows GDI+ PNG Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-2501;CVE-2013-1331
488	Microsoft Word Memory Corruption Vulnerability	Critical	overflow	CVE-2008-4025
442	Microsoft Wordpad and Office Text Converters OLE Data Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-0087
422	Microsoft Office Memory Corruption Vulnerability	Critical	code-execution	CVE-2008-0118
388	Microsoft Office PowerPoint Memory Corruption Vulnerability	Critical	code-execution	CVE-2009-1129
282	Microsoft Windows Media Malformed AVI Header Parsing Heap Overflow Vulnerability	Critical	code-execution	CVE-2009-1545
268	Microsoft Windows Media Playback Memory Corruption Remote Code Execution Vulnerability	Critical	code-execution	CVE-2009-2499

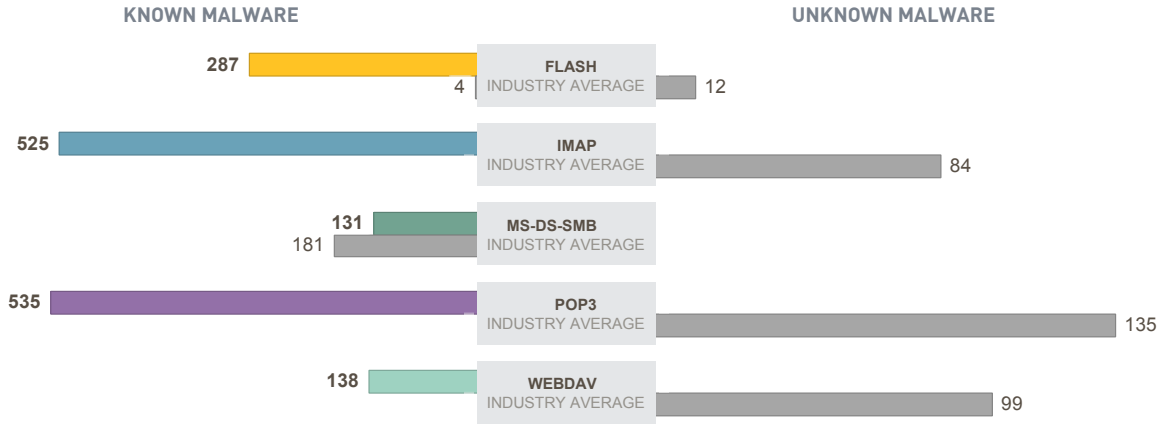
Bekannte und unbekannte Malware

Anwendungen dienen als primärer Vektor für die Übertragung und Infizierung von Organisationen, ausgehende Verbindungen oder gestohlene Daten. Die Taktik der Angreifer hat sich weiterentwickelt. Ziel werden immer häufiger Anwendungen im Netzwerk, in die herkömmliche Sicherheitslösungen kaum oder keinen Einblick haben.

Haupterkenntnisse:

- Es wurden insgesamt **7** Anwendungen von insgesamt **305** Anwendungen im Netzwerk erkannt, die Malware an Ihre Organisation übertragen.
- Viele der Anwendungen, die Malware übertragen, werden für den Geschäftsbetrieb benötigt. Dies bedeutet, dass Sie eine Lösung benötigen, die einerseits Bedrohungen verhindert und dennoch die Anwendungsnutzung nicht einschränkt.
- Während der Großteil der Malware mittels HTTP oder SMTP übertragen wird, nutzen fortschrittlichere Angriffe oft andere Anwendungen, die sich auf nicht standardmäßigen Ports befinden, oder andere Umgehungsstrategien.





7

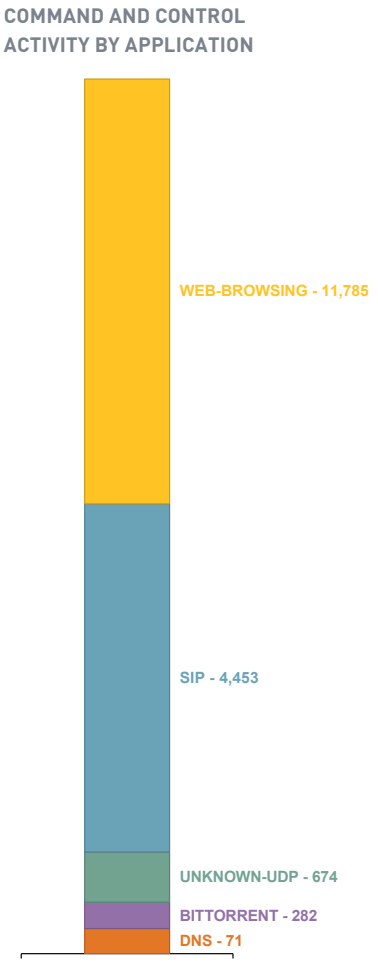
applications found delivering malware

Befehls- und Steuerungsanalyse

Die Befehls- und Steuerungsaktivität weist auf einen Host im Netzwerk hin, der von Malware infiziert wurde und versucht, sich außerhalb des Netzwerks mit Schadquellen zu verbinden. Diese Aktivität zu erkennen und zu verhindern ist äußerst wichtig, da Angreifer Befehls- und Steuerungsaktivitäten nutzen, um weitere Malware zu übertragen, Anweisungen zu geben oder Daten zu stehlen.

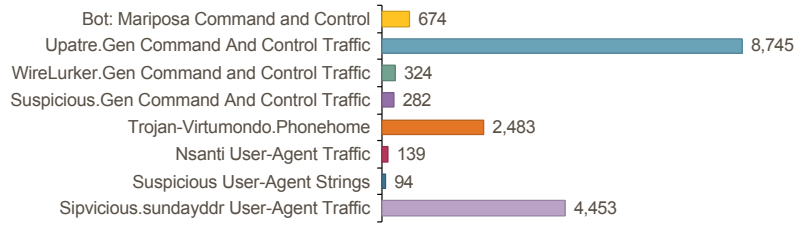
Haupterkenntnisse:

- Es wurden insgesamt **5** Anwendungen für die Befehls- und Steuerungskommunikation genutzt.
- Es wurden insgesamt **17,265** Befehls- und Steuerungsanfragen aus Ihrem Netzwerk erkannt.
- Es wurden insgesamt **71** verdächtige DNS-Abfragen erkannt.



Spyware-„Phone Home“ 17,194

Die nachstehende Abbildung zeigt die betroffenen Hosts, die versuchen, sich mit schädlichen externen Befehls- und Steuerungsservern zu verbinden.



Verdächtige DNS-Abfragen 71

DNS ist nicht nur eine häufige und notwendige Anwendungen, sondern wird oftmals auch dazu genutzt, die ausgehende Befehls- und Steuerungskommunikation zu verbergen, wie im unten stehenden Diagramm zu sehen ist.

Zusammenfassung Acme

Die Analyse hat ergeben, dass sich eine große Anzahl von Anwendungen und Cyberangriffen im Netzwerk befanden. Neben dem potenziellen Geschäfts- und Sicherheitsrisiko für **Acme** bergen diese Aktivitäten auch die Chance, sichere Anwendungsrichtlinien zu implementieren, die nicht nur zum Unternehmenswachstum beitragen, sondern auch das gesamte Risikopotenzial der Organisation senken.

Die wichtigsten Erkenntnisse:

- Im Netzwerk wurden Hochrisikoanwendungen wie **photo-video, internet-utility und social-networking** erkannt. Diese sollten aufgrund ihres Schadenspotenzials untersucht werden.
- Im Netzwerk befinden sich insgesamt **305** Anwendungen verteilt auf **27** Kategorien im Vergleich zum Branchendurchschnitt von insgesamt **255** Anwendungen in Organisationen aus dem Bereich **High Technology**.
- Es wurden insgesamt **405,610** Schwachstellen erkannt, und die drei häufigsten Kategorien lauten **web-browsing, ftp und smtp**.
- Es wurden **52,904** Malware-Ereignisse entdeckt. Der Branchendurchschnitt für vergleichbare Unternehmen liegt bei **7,515**.
- Es wurden insgesamt **5** Anwendungen für die Befehls- und Steuerungskommunikation genutzt.

305
APPLICATIONS IN USE

98
HIGH RISK APPLICATIONS

458,514
TOTAL THREATS

405,610
VULNERABILITY EXPLOITS

41,562
KNOWN MALWARE

11,342
UNKNOWN MALWARE

Empfehlungen:

- Implementierung sicherer Anwendungsrichtlinien, die nur geschäftskritische Anwendungen erlauben und eine umfassende Kontrolle aller anderen Anwendungen ermöglichen
- Untersuchung von Hochrisikoanwendungen mit Schadpotenzial, wie Remote-Zugriff, Datenaustausch oder verschlüsselte Tunnel
- Bereitstellung einer Sicherheitslösung, die sowohl bekannte als auch unbekannte Bedrohungen erkennen und verhindern kann, um das von Angreifern ausgehende Risiko zu senken
- Verwendung einer Lösung, die sich automatisch umprogrammieren kann, um neue Schutzmaßnahmen für aufkommende Bedrohungen zu ergreifen, die von einer globalen Gemeinschaft aus anderen Unternehmensanwendern genutzt wird