SECURITY LIFECYCLE REVIEW

tenzing - Dr. Müller & Partner GmbH IT-Solutions

Erstellt von:
Hèctor Gaspar Humet
tenzing - Dr. Müller & Partner GmbH IT-Solutions
www.tenzing.de

Die Security Lifecycle Review umfasst Unternehmens- und Sicherheitsrisiken von **tenzing - Dr. Müller & Partner GmbH IT-Solutions** und Kunden, die ihr Netzwerk nutzen. Palo Alto Networks erfasste die für diese Analyse verwendeten Daten während des Berichtszeitraums. Der Bericht enthält verwertbare Handlungsgrundlagen und eine Risikobewertung von Anwendungen, URL-Traffic und Content-Arten, die über das **tenzing - Dr. Müller & Partner GmbH IT-Solutions** -Netzwerk ausgetauscht werden, sowie Umfang und Arten von Bedrohungen und Schwachstellen, die im Verlauf beobachtet wurden. Es werden Empfehlungen ausgesprochen, die zur Verringerung der allgemeinen Risikolage für Netzwerkbetreiber und ihre Kunden eingesetzt werden können.

Berichtzeitraum: 8 DAYS
Tue, Sep 03, 2019 - Tue, Sep 10, 2019

TABLE OF CONTENTS

Kurzfassung tenzing - Dr. Müller & Partner GmbH IT-Solutions

Das Security Lifecycle Review liefert einen Überblick über die Geschäfts- und Sicherheitsrisiken von **tenzing - Dr. Müller & Partner GmbH IT-Solutions**. 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.

Vertrauliche Informationen – Nicht zur Weitergabe bestimmt

WICHTIGSTE ERGEBNISSE

170

BENUTZTE ANWENDUNGEN

Es sind insgesamt **170** 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.

34

HOCHRISKANTE ANWENDUNGEN

Es wurden **34** 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.

41

SAAS-ANWENDUNGEN

41 SaaS-Anwendungen wurden in Ihrem Netzwerk gefunden. Um die administrative Kontrolle zu behalten, sollten Ihre SaaS-Anwendungen von Ihrem IT-Team verwaltet werden.

59

AUSNUTZEN VON SICHERHEITSLÜCKEN

Es wurden insgesamt **59** Schwachstellen in Ihrer Organisation entdeckt, einschließlich der Schwachstellenkategorien **brute-force, info-leak und code-execution**.

63

BEDROHUNGEN INSGESAMT

Es wurden insgesamt **63** Bedrohungen in Ihrem Netzwerk gefunden, einschließlich Sicherheitslücken, bekannter und unbekannter Malware und ausgehender Befehls- und Steuerungsaktivitäten.

Anwendungen auf einen Blick

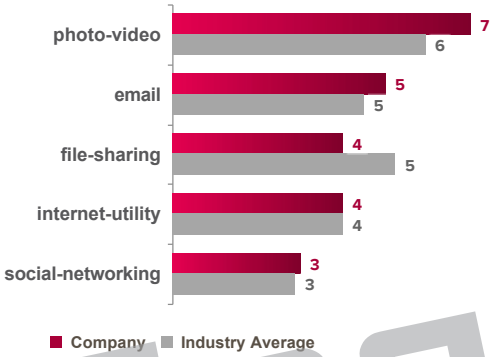
Anwendungen können Risiken bergen: So dienen sie etwa als Zugang für Bedrohungen, stehlen Daten aus dem Netzwerk, ermöglichen den unautorisierten Zugriff, senken die Produktivität oder verbrauchen einen Teil der Netzwerkbandbreite des Unternehmens. In diesem Abschnitt erhalten Sie einen Überblick über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

WICHTIGSTE ERGEBNISSE

- Im Netzwerk wurden Hochrisikoanwendungen wie **photo-video, email und file-sharing** erkannt. Diese sollten aufgrund ihres Schadenspotenzials untersucht werden.
- Im Netzwerk befinden sich insgesamt **170** Anwendungen verteilt auf **28** Unterkategorien, im Vergleich zum Branchendurchschnitt von insgesamt **191** Anwendungen in Organisationen aus dem Bereich **High Technology**.
- Es wurden **220.25 GB** von allen Anwendungen genutzt, einschließlich **business-systems** mit **110.4 GB**. Der Branchendurchschnitt in vergleichbaren Organisationen liegt bei **6.01 TB**.

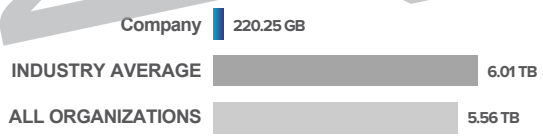
HOCHRISIKOANWENDUNGEN

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.



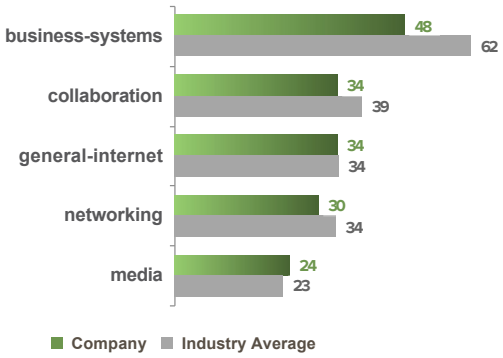
ANZAHL VON ANWENDUNGEN IM NETZWERK

DURCH ANWENDUNGEN GENUTZTE BANDBREITE



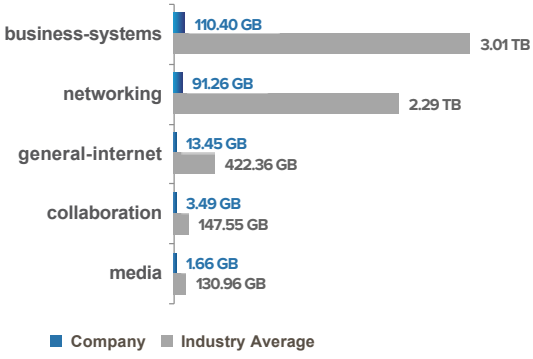
KATEGORIEN MIT DEN MEISTEN ANWENDUNGEN

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.



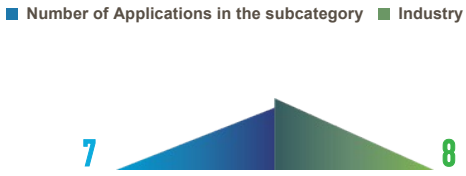
Risikobehaftete Anwendungen

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

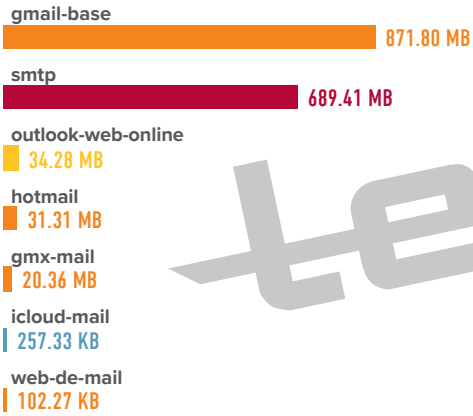
WICHTIGSTE ERGEBNISSE

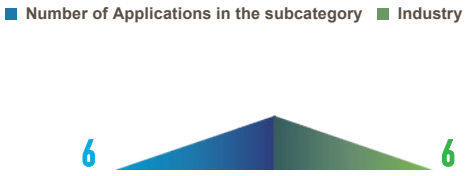
- In Ihrer Organisation wurden insgesamt **170** Anwendungen erkannt. Der Branchendurchschnitt liegt bei **191** in anderen Organisationen aus dem Bereich **High Technology**.
- Am häufigsten kommen die folgenden Typen von Anwendungsunterkategorien vor: **internet-utility, infrastructure und photo-video**.
- Die folgenden Anwendungsunterkategorien weisen den höchsten Bandbreitenverbrauch auf: **encrypted-tunnel, storage-backup und software-update**.



Email 1.65 GB

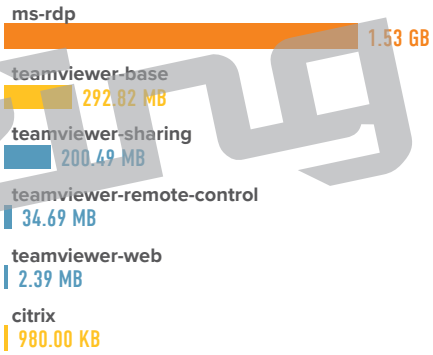
TOP EMAIL APPS





Remote-Access 2.06 GB

TOP REMOTE-ACCESS APPS



Number of Applications in the subcategory | Industry Average

File-Sharing 88.98 MB

TOP FILE-SHARING APPS

- whatsapp-file-transfer 33.04 MB
- dropbox-base 32.65 MB
- ms-onedrive-base 19.99 MB
- google-cloud-storage-download 2.46 MB
- ftp 452.36 KB
- adobe-cloud 172.40 KB
- slideshare-base 88.36 KB
- sourceforge-base 65.74 KB

Number of Applications in the subcategory | Industry Average

Encrypted-Tunnel 78.94 GB

TOP ENCRYPTED-TUNNEL APPS

- ssl 78.69 GB
- ssh 167.77 MB
- open-vpn 78.76 MB
- ipsec-esp-udp 1.14 MB
- ike 199.18 KB

Number of Applications in the subcategory | Industry Average

Instant-Messaging 57.04 MB

TOP INSTANT-MESSAGING APPS

- ms-lync-online 19.48 MB
- whatsapp-web 18.37 MB
- whatsapp-base 10.39 MB
- facebook-chat 7.04 MB
- jabber 928.85 KB
- telegram 709.16 KB
- snapchat 69.86 KB
- boldchat-logmein 42.62 KB

Number of Applications in the subcategory | Industry Average

Social-Networking 1.78 GB

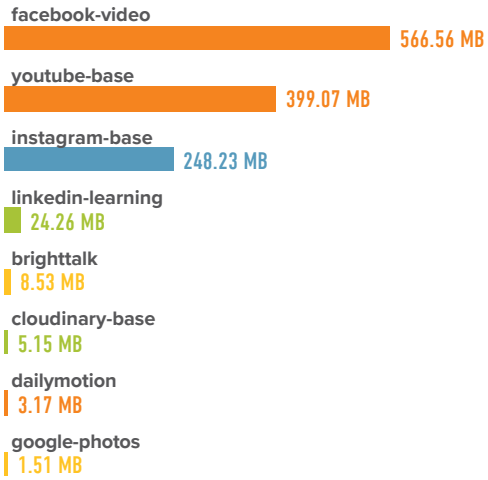
TOP SOCIAL-NETWORKING APPS

- facebook-base 942.41 MB
- linkedin-base 723.54 MB
- xing 56.70 MB
- twitter-base 38.66 MB
- reddit-base 9.45 MB
- pinterest-base 7.49 MB
- quora-base 283.45 KB
- mail.ru-base 137.22 KB

Number of Applications in the subcategory | Industry Average

Photo-Video 1.26 GB

TOP PHOTO-VIDEO APPS



Number of Applications in the subcategory | Industry Average

Proxy 13.43 KB

TOP PROXY APPS

Risikobehaftete Anwendungen – Details

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
4	gmail-base	collaboration	email	browser-based	871.8 MB	84
5	smtp	collaboration	email	client-server	689.41 MB	24387
3	outlook-web-online	collaboration	email	browser-based	34.28 MB	1395
4	hotmail	collaboration	email	browser-based	31.31 MB	123
4	gmx-mail	collaboration	email	browser-based	20.36 MB	619
2	icloud-mail	collaboration	email	client-server	257.33 KB	19
4	web-de-mail	collaboration	email	browser-based	102.27 KB	10
4	ssl	networking	encrypted-tunnel	browser-based	78.69 GB	603367
4	ssh	networking	encrypted-tunnel	client-server	167.77 MB	36898
3	open-vpn	networking	encrypted-tunnel	client-server	78.76 MB	8
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	1.14 MB	152
2	ike	networking	encrypted-tunnel	client-server	199.18 KB	154
3	whatsapp-file-transfer	general-internet	file-sharing	client-server	33.04 MB	35
4	dropbox-base	general-internet	file-sharing	client-server	32.65 MB	511
4	ms-onedrive-base	general-internet	file-sharing	client-server	19.99 MB	355
2	google-cloud-storage-download	general-internet	file-sharing	browser-based	2.46 MB	38
5	ftp	general-internet	file-sharing	client-server	452.36 KB	8
2	adobe-cloud	general-internet	file-sharing	browser-based	172.4 KB	26
3	slideshare-base	general-internet	file-sharing	browser-based	88.36 KB	3
2	sourceforge-base	general-internet	file-sharing	client-server	65.74 KB	6
3	ms-lync-online	collaboration	instant-messaging	client-server	19.48 MB	506
2	whatsapp-web	collaboration	instant-messaging	browser-based	18.37 MB	131
1	whatsapp-base	collaboration	instant-messaging	client-server	10.39 MB	425
3	facebook-chat	collaboration	instant-messaging	browser-based	7.04 MB	93
5	jabber	collaboration	instant-messaging	client-server	928.85 KB	1

Notes:

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
2	telegram	collaboration	instant-messaging	client-server	709.16 KB	48
2	snapchat	collaboration	instant-messaging	client-server	69.86 KB	6
4	boldchat-logmein	collaboration	instant-messaging	browser-based	42.62 KB	3
4	facebook-video	media	photo-video	browser-based	566.56 MB	164
4	youtube-base	media	photo-video	browser-based	399.07 MB	255
2	instagram-base	media	photo-video	client-server	248.23 MB	477
1	linkedin-learning	media	photo-video	browser-based	24.26 MB	14
3	brighttalk	media	photo-video	browser-based	8.53 MB	47
1	cloudinary-base	media	photo-video	client-server	5.15 MB	12
4	dailymotion	media	photo-video	browser-based	3.17 MB	43
3	google-photos	media	photo-video	browser-based	1.51 MB	7
5	http-proxy	networking	proxy	browser-based	6.91 KB	9
5	socks	networking	proxy	network-protocol	6.52 KB	11
4	ms-rdp	networking	remote-access	client-server	1.53 GB	597
3	teamviewer-base	networking	remote-access	client-server	292.82 MB	429
2	teamviewer-sharing	networking	remote-access	client-server	200.49 MB	25
2	teamviewer-remote-control	networking	remote-access	client-server	34.69 MB	29
2	teamviewer-web	networking	remote-access	browser-based	2.39 MB	49
3	citrix	networking	remote-access	client-server	980 KB	169
4	facebook-base	collaboration	social-networking	browser-based	942.41 MB	4156
3	linkedin-base	collaboration	social-networking	browser-based	723.54 MB	1053
3	xing	collaboration	social-networking	browser-based	56.7 MB	834
3	twitter-base	collaboration	social-networking	browser-based	38.66 MB	835
1	reddit-base	collaboration	social-networking	browser-based	9.45 MB	57
2	pinterest-base	collaboration	social-networking	browser-based	7.49 MB	128

Notes:

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
1	quora-base	collaboration	social-networking	browser-based	283.45 KB	40
4	mail.ru-base	collaboration	social-networking	browser-based	137.22 KB	23

Notes:

SAAS-ANWENDUNGEN

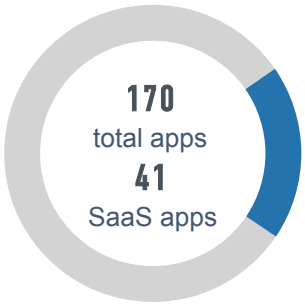
SaaS-Anwendungsdienste sind aus dem Netzwerkperimeter nicht mehr wegzudenken. Viele dieser auch als „Schatten-IT“ bezeichneten Dienste werden von Einzelnutzern, Geschäftsteams oder sogar ganzen Abteilungen direkt genutzt. Sie müssen unbedingt die volle Kontrolle über die in Ihrem Netzwerk verwendeten SaaS-Anwendungen haben, um die Sicherheit Ihrer Daten nicht zu gefährden.

WICHTIGSTE ERGEBNISSE

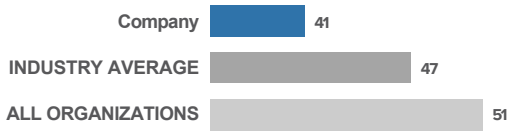
- **File-Sharing** enthält die höchste Anzahl unterschiedlicher SaaS-Anwendungen.
- Bezüglich der übertragenen Daten ist **gmail-base** die am meisten genutzte SaaS-Anwendung in Ihrem Unternehmen.

SAAS-ANWENDUNGEN IN ZAHLEN

Überprüfen Sie die in Ihrem Unternehmen genutzten Anwendungen. Im Unternehmen sollten nur SaaS-Anwendungen zum Einsatz kommen, die von Ihrem IT-Team verwaltet werden, damit Sie die volle Kontrolle über die genutzten Anwendungen behalten.



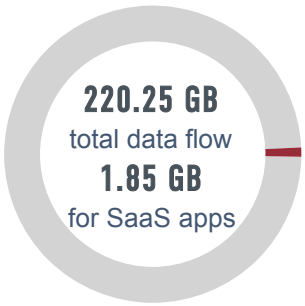
NUMBER OF SAAS APPLICATIONS



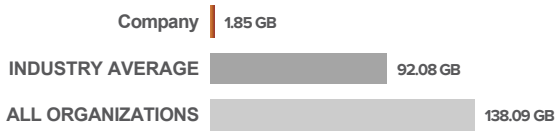
PERCENTAGE OF ALL APPLICATIONS

BANDBREITE DER SAAS-ANWENDUNGEN

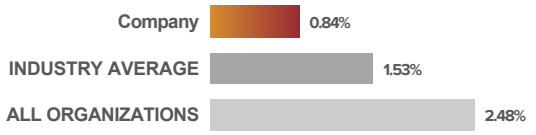
Hiermit können Sie die Menge der übertragenen Daten von und zu den SaaS-Anwendungen überwachen. So können Sie die Funktionsweise und Art der Nutzung nachvollziehen.



SAAS APPLICATION BANDWIDTH



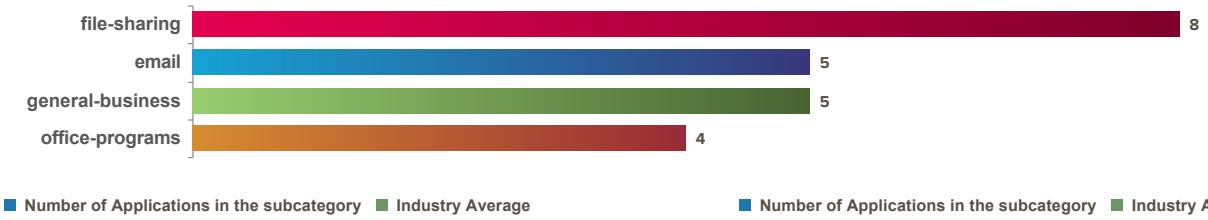
PERCENTAGE OF ALL BANDWIDTH



AM MEISTEN GENUTZTE SAAS-ANWENDUNGS-UNTERKATEGORIEN

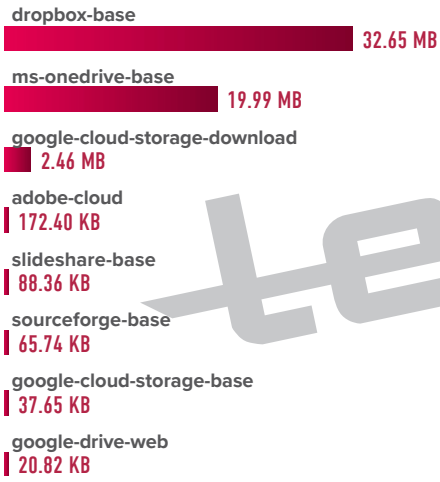
Die folgende Grafik zeigt die Anzahl der Anwendungen in den einzelnen Anwendungs-Unterkategorien. So können Sie nachvollziehen, welche Anwendungen in Ihrem Unternehmen am meisten genutzt werden. Am meisten genutzte SaaS-Anwendungs-Unterkategorien (gemessen an der Gesamtanzahl von Anwendungen) Die folgende Grafik zeigt die am meisten verwendeten Anwendungen (gemessen an den übertragenen Daten) in den unten angegebenen Unterkategorien.

TOP SAAS ANWENDUNGS-UNTERKATEGORIEN NACH ANZAHL VON ANWENDUNGEN



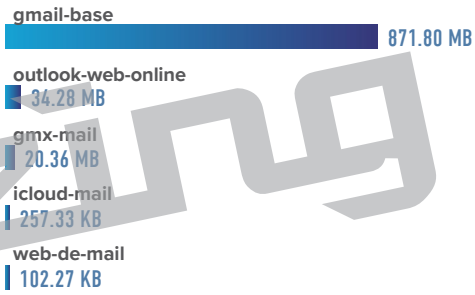
File-Sharing 55.48 MB

TOP FILE-SHARING APPS



Email 926.81 MB

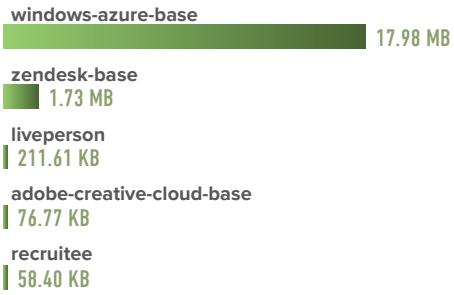
TOP EMAIL APPS



Number of Applications in the subcategory | Industry Average

General-Business 20.06 MB

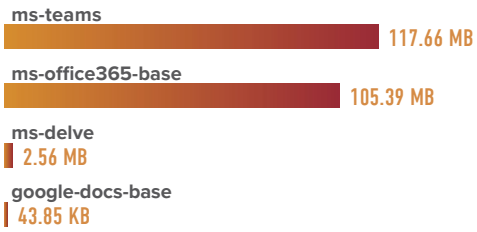
TOP GENERAL-BUSINESS APPS



Number of Applications in the subcategory | Industry Average

Office-Programs 225.65 MB

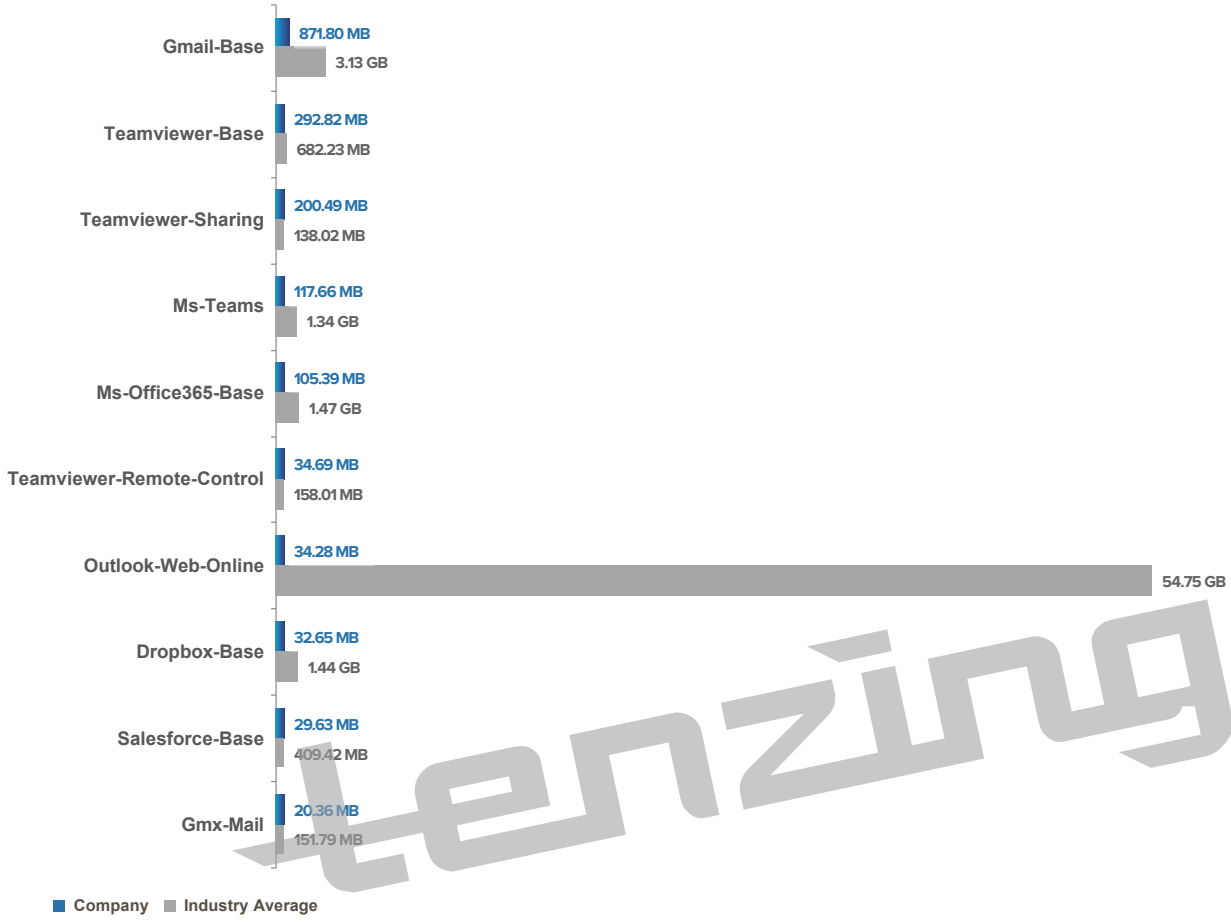
TOP OFFICE-PROGRAMS APPS



AM MEISTEN GENUTZTE SAAS-ANWENDUNGEN

Die folgende Grafik zeigt die zehn in Ihrem Unternehmen am häufigsten genutzten SaaS-Anwendungen sowie die Anwendungsnutzung in Ihrem Unternehmen im Vergleich zu ähnlichen Unternehmen und allen anderen Kunden von Palo Alto Networks.

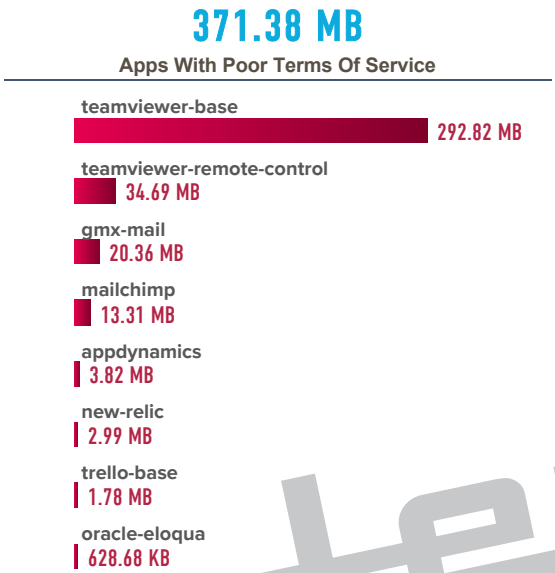
TOP SAAS ANWENDUNGEN NACH DATENDURCHSATZ

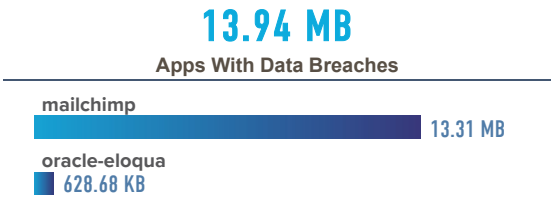


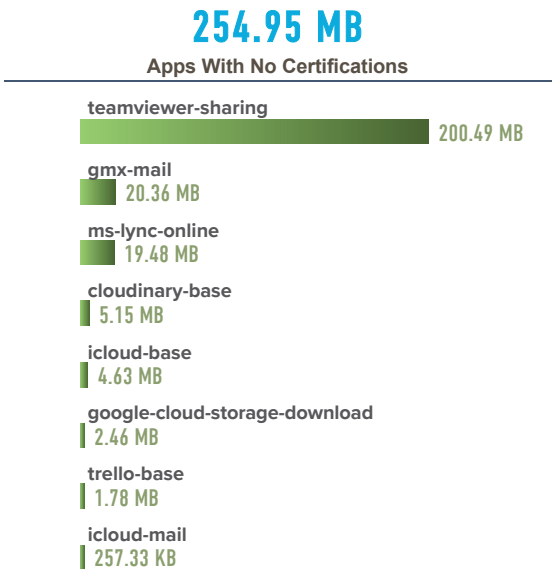
SAAS-ANWENDUNGEN NACH HOSTING-RISIKO

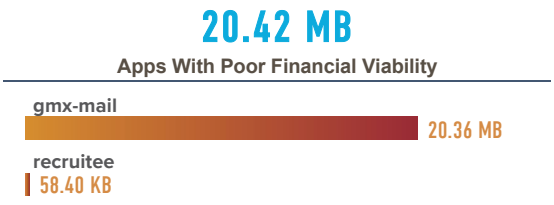
Im Rahmen Ihrer SaaS-Nutzung ist es unbedingt erforderlich, regelmäßig zu überprüfen, auf welche SaaS-Anwendungen zugegriffen wird, wer darauf zugreift und wie diese Anwendungen verwendet werden.
Im folgenden Diagramm ist die Anzahl der Anwendungen, aufgeschlüsselt nach Hosting-Risiko, zu sehen.

In den folgenden Diagrammen werden für jedes Hosting-Risiko die Anwendungen mit der größten Bandbreite angezeigt.









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.

WICHTIGSTE ERGEBNISSE

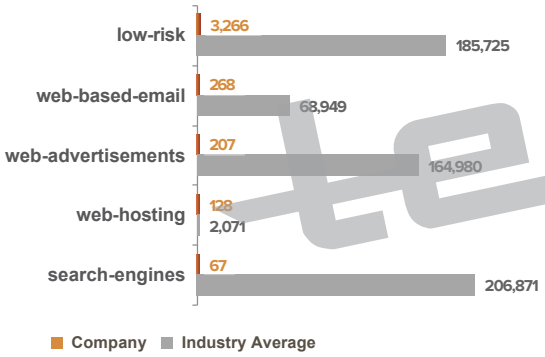
- Es wurden Hochrisiko-URL-Kategorien im Netzwerk erfasst, wie **low-risk, web-based-email und web-advertisements**.
- Benutzer haben während des Berichtzeitraums insgesamt **4,166** URLs in **21** Kategorien besucht.
- Die Web-Aktivität setzte sich aus einer Mischung aus persönlichen und arbeitsbezogenen 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.

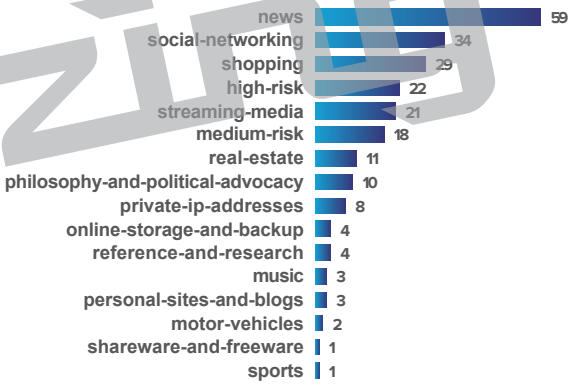
TRAFFIC-STARKE URL-KATEGORIEN

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



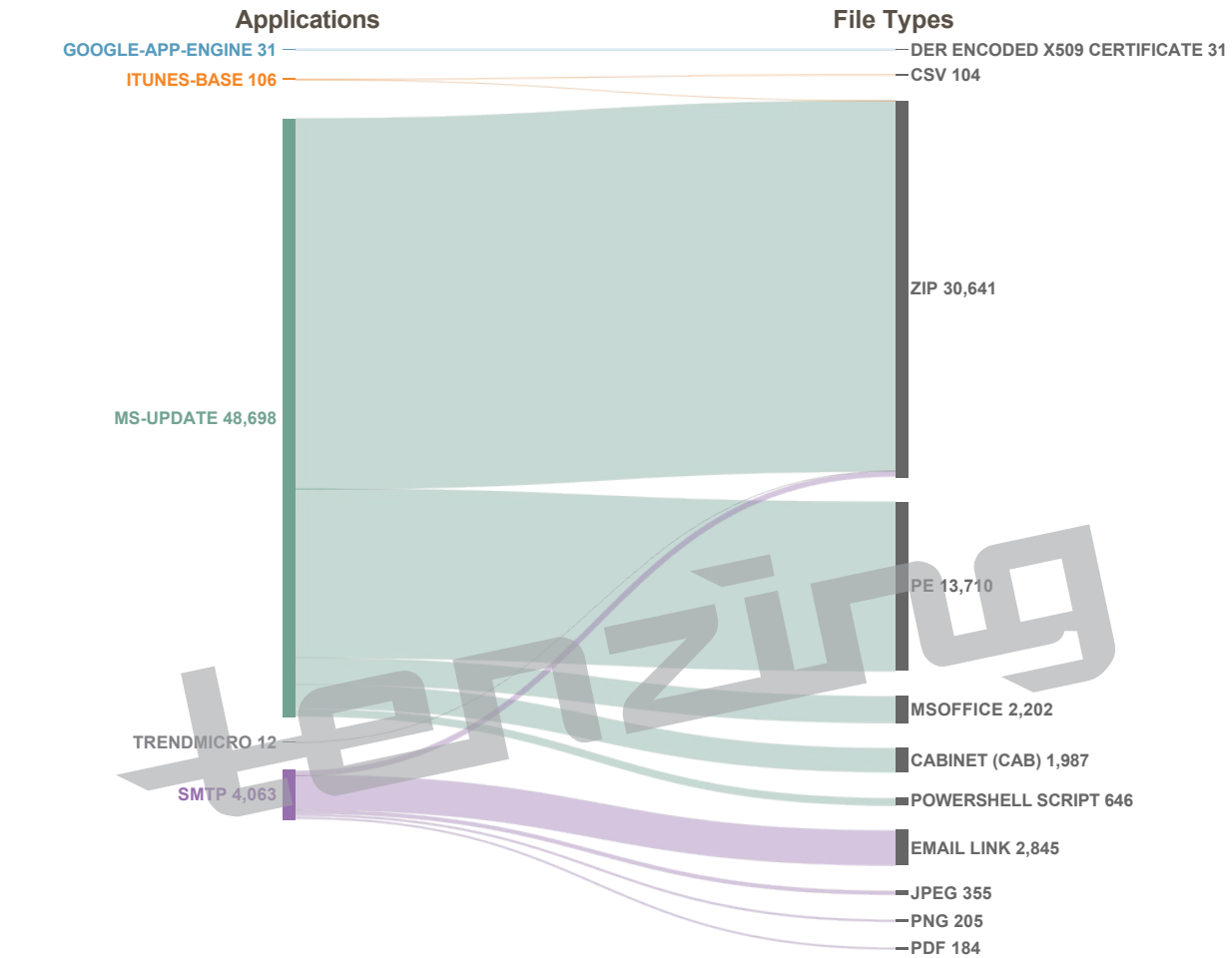
HÄUFIG BESUCHTE URL-KATEGORIEN

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 **32** verschiedene Dateitypen erfasst, die mit Hilfe von **13** verschiedenen Anwendungen übertragen wurden. Im Bild unten werden die am häufigsten für Dateiübertragungen verwendeten Anwendungen mit den häufigsten Datei- und Inhaltstypen korreliert.



13 Application(s) — transferred → **32** File Type(s)

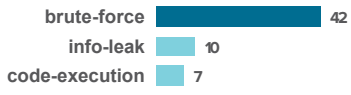
Bedrohungen auf einen Blick

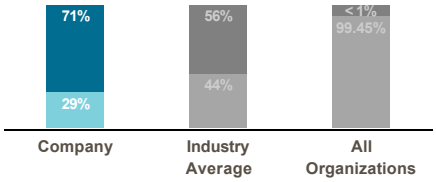
Um zu verstehen, welchem Risiko Sie ausgesetzt sind und wie Sie Angriffe mithilfe Ihrer Sicherheitsinfrastruktur vermeiden, benötigen Sie Informationen über die Art und Anzahl der Bedrohungen, vor denen Sie Ihr Unternehmen schützen müssen. In diesem Abschnitt werden Anwendungsschwachstellen, bekannte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

WICHTIGSTE ERGEBNISSE

- Es wurden insgesamt **59** Schwachstellen in Ihrer Organisation entdeckt, einschließlich der Schwachstellenkategorien **brute-force, info-leak und code-execution**.
- Es wurden **0** Malware-Ereignisse entdeckt. Der Branchendurchschnitt für vergleichbare Unternehmen liegt bei **95,276**.
- Es wurden insgesamt **4** 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.

59
Vulnerability Exploit(s)





4
Command and Control Detection(s)

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.

4,198
file(s) potentially leaving the network

via
12
different application(s)

Analyse von schädlichen und Hochrisikodateitypen

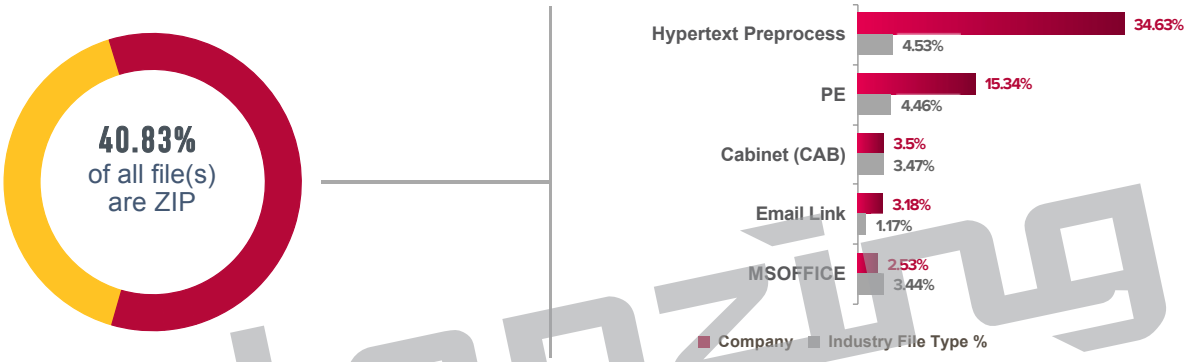
Cyberangreifer nutzen heutzutage die verschiedensten Dateitypen, um Malware und Exploits zu übermitteln. Dabei konzentrieren sie sich vor allem auf die Inhalte gängiger Geschäftsanwendungen. Der Großteil herkömmlicher Bedrohungen wird mit ausführbaren Dateien übertragen, während gezieltere und ausgeklügeltere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

WICHTIGSTE ERGEBNISSE

- 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. Wenn Host Prevention-Systeme sowohl lokale als auch Fernanalysen an diesen Dateitypen durchführen, werden die Endpunkte zusätzlich geschützt.

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.

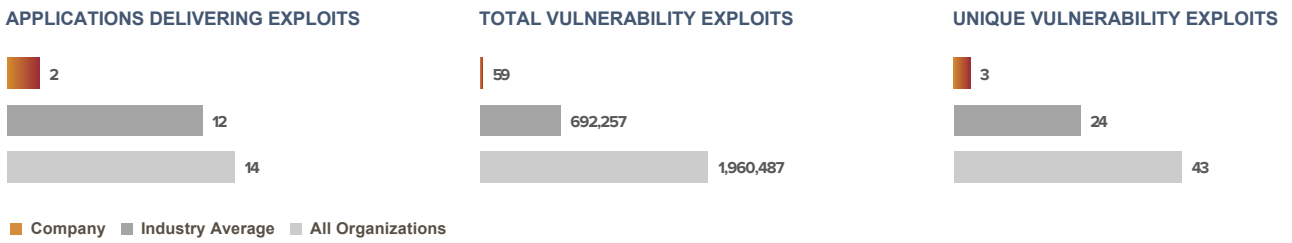


Anwendungsschwachstellen

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.

WICHTIGSTE ERGEBNISSE

- Es wurden insgesamt **2** Anwendungen erkannt, die Exploits an Ihre Umgebung weitergeben.
- Es wurden insgesamt **59** Schwachstellen erkannt, und die drei häufigsten Kategorien lauten **ssh und ms-ds-smbv3**.
- Die insgesamt erkannten Schwachstellen sind in **3** Schwachstellentypen aufgeteilt. Dies bedeutet, dass Angreifer immer wieder auf dieselben Schwachstellen zurückgriffen.



AUSGENUTZTE SICHERHEITSLÜCKEN NACH ANWENDUNG

(5 ANWENDUNGEN MIT DEN MEISTEN ANGRIFFEN)

DETECTIONS	EXPLOIT ID	SEVERITY	THREAT TYPE	CVE ID
42	Ssh			
42	SSH User Authentication Brute Force Attempt	HIGH	brute-force	
17	Ms-Ds-Smbv3			
7	Microsoft Windows System32 Write Access	MEDIUM	code-execution	
10	Windows Local Security Architect Isardelete access	LOW	info-leak	

Befehls- und Steuerungsanalyse

Command and Control (CnC)-Aktivitäten deuten häufig darauf hin, dass ein Host im Netzwerk mit Malware infiziert wurde, der von Malware infiziert wurde und versucht, sich außerhalb des Netzwerks mit Schadquellen zu verbinden. Detection and Response-Produkte können Aufschluss über die schädlichen Vorgänge im Netzwerk und auf dem Host geben, die durch die ermittelte Malware ausgelöst wurden.

WICHTIGSTE ERGEBNISSE

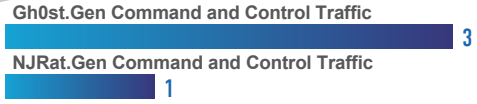
- Es wurden insgesamt **1** Anwendungen für die Befehls- und Steuerungskommunikation genutzt.
- Es wurden insgesamt **4** Befehls- und Steuerungsanfragen aus Ihrem Netzwerk erkannt.
- Es wurden insgesamt **0** verdächtige DNS-Abfragen erkannt.

unknown-tcp: 4

0 SUSPICIOUS DNS QUERIES

4 SPYWARE PHONE HOME

TOP 10



Zusammenfassung **tenzing - Dr. Müller & Partner GmbH IT-Solutions**

Die Analyse hat ergeben, dass sich eine große Anzahl von Anwendungen und Cyberangriffen im Netzwerk befanden. Neben dem potenziellen Geschäfts- und Sicherheitsrisiko für **tenzing - Dr. Müller & Partner GmbH IT-Solutions** 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, email und file-sharing** erkannt. Diese sollten aufgrund ihres Schadenspotenzials untersucht werden.
- Im Netzwerk befinden sich insgesamt **170** Anwendungen verteilt auf **28** Kategorien im Vergleich zum Branchendurchschnitt von insgesamt **191** Anwendungen in Organisationen aus dem Bereich **High Technology**.
- Es wurden insgesamt **59** Schwachstellen erkannt, und die drei häufigsten Kategorien lauten **ssh und ms-ds-smbv3**.
- Es wurden **0** Malware-Ereignisse entdeckt. Der Branchendurchschnitt für vergleichbare Unternehmen liegt bei **95,276**.
- Es wurden insgesamt **1** Anwendungen für die Befehls- und Steuerungskommunikation genutzt.

WICHTIGSTE ERGEBNISSE

170
BENUTZTE ANWENDUNGEN

34
HOCHRISKANTE ANWENDUNGEN

41
SAAS-ANWENDUNGEN

59
AUSNUTZEN VON SICHERHEITSLÜCKEN

63
BEDROHUNGEN INSGESAMT

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.
- Überwachen Sie die Command and Control-Kommunikation, indem sie die Host- oder Netzwerkquelle überprüfen. Detection and Response-Programme oder Logging Solutions könnten einen Hinweis dafür liefern, was genau vorgefallen ist.
- 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.