**MEDIENINFORMATION**

Zürich, 26. Juni 2019

**Ohne Rundumverteidigung kein zuverlässiger Schutz**

**WatchGuard Internet Security Report Q1/2019 konstatiert eine Zunahme bei Mac-Malware, bösartigen Office-Dokumenten und Web Application Exploits**

**62 Prozent mehr Malware im Vergleich zum Vorquartal und Cyberkriminelle, die zunehmend verschiedene Angriffstechniken kombinieren – der vierteljährliche Internet Security Report von WatchGuard für das erste Quartal 2019 zeichnet ein klares Bild der aktuellen Bedrohungssituation. In den ersten drei Monaten dieses Jahres verdoppelten die Angreifer ihre Anstrengungen, um über bösartige Microsoft Office-Dokumente, Mac-Malware und Web-Anwendungs-Exploits an Daten für Identitäten und Netzwerkzugänge zu kommen. Dies spiegelt eine Entwicklung, auf die Unternehmen reagieren sollten.**

„Die wichtigsten Ergebnisse des letzten Berichts heben deutlich die Notwendigkeit eines mehrschichtigen Sicherheitskonzepts hervor“, so Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies. „Angesichts der Bedrohungslandschaft müssen Unternehmen eine Rundumverteidigung etablieren – angefangen bei DNS-Filtern, um Verbindungen zu bösartigen Websites und Phishing-Versuche zu blockieren, über Intrusion Prevention Services (IPS) zur Abwehr von Angriffen auf Webanwendungen bis zur Multifaktor-Authentifizierung, um persönliche Anmeldeinformationen zu schützen. Es ist notwendig, der Vielzahl verschiedener Angriffsmethoden und -vektoren eine einheitliche Sicherheitsplattform mit entsprechenden Sicherheitsdiensten entgegenzusetzen."

Die Erkenntnisse, Forschungsergebnisse und Sicherheits-Best-Practices im vierteljährlichen Internet Security Report helfen mittelständischen Unternehmen ebenso wie grossen, dezentral aufgestellten Organisationen dabei, einen Überblick zur aktuellen Cyber-Sicherheitslandschaft zu geben. In Folge können sie sich selbst, ihre Partner und Kunden vor Bedrohungen besser schützen. Zu den wichtigsten Ergebnissen des Berichts zum ersten Quartal 2019 gehören:

* **Angreifer bevorzugen weiterhin bösartige Office-Dokumente** – Im ersten Quartal 2019 blockierten über 17 Prozent der Firebox-Appliances kompromittierte Office-Dokumente. Zwei Bedrohungen aus dieser Kategorie schafften es sogar in die Liste der am weitesten verbreiteten Malware-Varianten sowie in die mit den zehn häufigsten Angriffen nach Volumen. Mehr als die Hälfte wurden in der EMEA-Region blockiert, vor allem in Osteuropa. Benutzer sollten die Interaktion mit verdächtigen Office-Dokumenten auf jeden Fall vermeiden und alle Anhänge, die Makros aktivieren wollen, als Bedrohung betrachten.
* **Mac OS-Malware weiter auf dem Vormarsch** – Mac-Malware erschien erstmals im dritten Quartal 2018 in der Top-10-Malware-Übersicht von WatchGuard. In den ersten drei Monaten dieses Jahres haben sich sogar zwei Varianten weit genug verbreitet, um es auf die Liste zu schaffen. Diese Zunahme von Mac-basierter Malware entkräftet den Mythos, dass Apple-Rechner immun gegen Viren und Malware sind. Umso wichtiger ist es, den Bedrohungsschutz auf alle Geräte und Systeme im Unternehmen auszuweiten.
* **Web-Anwendungs-Exploits nehmen zu** – Trotz eines Rückgangs des Gesamtvolumens an Netzwerkattacken im ersten Quartal nahmen die Angriffe auf Webanwendungen deutlich zu. Das IPS-Modul von WatchGuard hat Angreifer dabei ertappt, wie sie Schwachstellen mittels Cross-Site-Scripting (XSS) und SQL-Injection (SQLI) ausnutzen – beides beliebte Methoden für den Diebstahl von Zugangsdaten. Zwei SQLI-Angriffe schafften es in die Top-10-Netzwerkangriffsliste, ein spezifischer Web-XSS-Angriff machte sogar mehr als 10 Prozent der Netzwerkangriffe insgesamt aus.
* **DNS-Filter blockieren mehr als fünf Millionen bösartige Websites** – Der WatchGuard-Dienst DNSWatch verhinderte erfolgreich 5.192.883 Aufrufversuche schädlicher Webseiten. Darüber hinaus blockierte er über eine halbe Million Verbindungen zu bekannten Malware-Hosting-Domänen, 187.101 zu kompromittierten Websites und 61.096 zu bekannten Phishing-Sites. Bösartige Websites können vom Anwender alleine schwer zu identifizieren sein. Aus diesem Grund ist die Filterung auf DNS-Ebene entscheidend. Sie verhindert, dass Benutzer unwissentlich ein Opfer von Malware-Infektionen, Identitätsdiebstahl oder Command-and-Control-Systemen für Botnets werden.
* **Fileless Malware behauptet sich** – Fileless-Bedrohungen finden sich sowohl in der Top 10 für Malware als auch in der für Netzwerkangriffe. Auf der Malware-Seite wurde im ersten Quartal erstmals ein PowerShell-basierter Code-Injection-Angriff verzeichnet, während das beliebte dateilose Backdoor-Tool Meterpreter sein Debüt bei den Netzwerkangriffen feierte. Dieser Trend zeigt erneut: Für Cyberkriminelle sind diese Angriffsarten weiterhin ein probates Mittel.
* **„Mimikatz“-Malware nimmt um 73 Prozent zu und bleibt die grösste Gefahr** – Mit 20,6 Prozent aller im ersten Quartal gefundenen Malware wird dieses beliebte Open-Source-Tool häufig für den Diebstahl von Passwörtern und anschliessende Netzwerkinfiltrationen eingesetzt. Mimikatz ist ein Dauerkandidat auf der Top-10-Malware-Liste. Das unterstreicht die Bedeutung zur Verwendung langer und komplexer Passwörter, die für jedes einzelne Konto einzigartig sind. Angesichts der fortgesetzten Fokussierung von Cyberkriminellen auf den Diebstahl von Identitäten sollten Unternehmen – gleich welcher Grösse – die Einführung von Multifaktor-Authentifizierungslösungen in Betracht ziehen. Nur auf diese Weise können Benutzerkonten wirksam geschützt werden.

Die Ergebnisse des Reports basieren auf anonymisierten Firebox-Feed-Daten von 42.372 aktiven WatchGuard UTM-Appliances weltweit, deren Anwender dem Daten-Sharing zugestimmt haben. Insgesamt blockierten diese im ersten Quartal 2019 23.884.979 Malware-Varianten (564 pro Gerät) und 989.759 Netzwerkangriffe (23 pro Gerät).

Der Bericht der Experten von WatchGuard hinterfragt die wirkungsvollsten Malware- und Angriffstrends aus dem ersten Quartal 2019 im Einzelnen. Darüber hinaus enthält er eine detaillierte Analyse des historischen 51 Prozent-Angriffs auf die Kryptowährung Ethereum Classic (ETC), der zu Verlusten in Höhe von 1,1 Millionen US-Dollar führte.

Für weitere Informationen können Sie den vollständigen Bericht [hier](https://www.watchguard.com/de/wgrd-resource-center/security-report-q1-2019) herunterladen.

Bildmaterial

|  |
| --- |
|   |
| Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies |

Das Bildmaterial zum Download finden Sie in unserem Medienportal press-n-relations.amid-pr.com (Suchbegriff „Corey Nachreiner"). Selbstverständlich schicke ich Ihnen die Datei auch gerne per E-Mail zu. Kontakt: rh@press-n-relations.de

|  |  |
| --- | --- |
| Kontakt:WatchGuard Technologies GmbHPaul Moll – Field Marketing Manager Central EuropeWendenstr. 379, 20537 HamburgTel.: +49 152 31795040paul.moll@watchguard.comwww.watchguard.de | Presse- und Öffentlichkeitsarbeit:Press'n'Relations GmbH, c/o Medianovis AGRebecca HasertSchaffhauser. 91, 8057 ZürichTel.: +49 731 962 87 15 rh@press-n-relations.de[www.press-n-relations.com](http://www.press-n-relations.com) |

**Über WatchGuard Technologies**

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Das umfangreiche Produktportfolio reicht von hochentwickelten UTM (Unified Threat Management)- und Next-Generation-Firewall-Plattformen über Multifaktor-Authen­tifizierung bis hin zu Technologien für umfassenden WLAN-Schutz sowie weiteren spezifischen Produkten und Services rund ums Thema IT-Security. Mehr als 80.000 Kunden weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung neben kleinen und mittelständischen Unternehmen nicht zuletzt auch grosse, dezentral aufgestellte Organisationen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Aktuelle Informationen, Aktionen und Updates finden Sie auch auf [Twitter](https://twitter.com/sichersein), [Facebook](https://de-de.facebook.com/WatchGuardSichersein/) oder [LinkedIn](https://de.linkedin.com/company/watchguardsichersein). Der WatchGuard InfoSec-Blog Secplicity berichtet darüber hinaus über die neuesten Bedrohungen und zeigt auf, wie man mit ihnen umgeht: [www.secplicity.org](http://www.secplicity.org/). Oder Sie abonnieren den 443 - Security Simplified Podcast bei [Secplicity.org](http://www.secplicity.org/) bzw. wo immer Sie Ihre Lieblings-Podcasts finden.