**MEDIENINFORMATION**

Zürich, 13. Dezember 2019

**Hackerangriffe via Microsoft Office an der Tagesordnung**

**Laut WatchGuards Internet Security Report Q3/2019 ist die von E-Mail-Anhängen ausgehende Gefahr präsenter denn je**

**Wie der aktuell veröffentlichte WatchGuard Internet Security Report für das dritte Quartal 2019 belegt, sollte bei per E-Mail eingehenden Word-, RTF- oder anderen Office-Dokumenten weiterhin besondere Vorsicht gelten. Diesmal haben es gleich zwei einschlägige Malware-Varianten in die Top 10 geschafft. Die Nase vorn hat dabei ein Angriffsversuch, der auf einer Schwachstelle des Word-Formeleditors basiert. Dieser ermöglicht es Hackern beliebigen Code auszuführen, sobald das manipulierte Dokument geöffnet wird. Sowohl hinsichtlich der Gesamtmenge als auch der Verbreitung solch Office-basierter Übergriffe wurden dabei im dritten Quartal neue Bestmarken erreicht: Neben der Anzahl entsprechender Attacken verdoppelte sich auch der Adressatenkreis im Vergleich zum Vorquartal. Die Übermittlung erfolgte in der Mehrzahl aller Fälle per E-Mail. Daher wird es gerade für Unternehmen immer wichtiger, ihre Mitarbeitenden gezielt zu sensibilisieren. Schulungen und Aufklärungsinitiativen können dazu beitragen, dass Anwender solche und andere Übergriffe sowie Phishing-Versuche besser erkennen.**

Die Ergebnisse des WatchGuard Internet Security Reports basieren auf anonymisierten Firebox-Feed-Daten von knapp 37.000 aktiven WatchGuard UTM-Appliances weltweit, deren Anwender dem Daten-Sharing zugestimmt haben. Insgesamt blockierten diese im dritten Quartal dieses Jahres über 23 Millionen Malware-Varianten (623 pro Gerät) und rund 2,4 Millionen Netzwerkangriffe (65 pro Gerät).

**Malware-Attacken und Netzwerkangriffe nehmen zu**

Neben der generellen Verschärfung der Bedrohungslage im Hinblick auf die Häufigkeit von Malware und Netzwerkangriffen fällt vor allem die Zunahme der sogenannten Zero-Day-Malware auf, die auf bisher unbekannte und somit ungepatchte Sicherheitslücken in Softwareanwendungen setzt. Nachdem sich der Anteil solcher Malware-Varianten in den letzten Quartalen bei 38 Prozent eingependelt hatte, stieg er diesmal auf 50 Prozent an. Traditionelle, signaturbasierte Sicherheitslösungen bieten in dem Zusammenhang keinerlei Abwehrmöglichkeiten. Gerade vor dem Hintergrund des signifikanten Anstiegs dieser Gefahr wird die Notwendigkeit von mehrschichtigen Sicherheitsdiensten deutlich. Nur so kann fortgeschrittenen, sich ständig weiterentwickelnden Bedrohungen Einhalt geboten werden.

"Unsere neuesten Erkenntnisse belegen, dass die Spielwiese der Hacker immer grösser wird. Ihre Methoden sind von zunehmend mehr Raffinesse geprägt. Von bekannten Erfolgskonzepten bei Angriffen bis hin zu trickreichen neuen Malware-Kampagnen – Cyberkriminelle nutzen jede sich bietende Gelegenheit. Im Fokus stehen dabei insbesondere Anwendungen oder Domains, die wir tagtäglich nutzen, und Angreifer setzen alles daran, diese für ihre Zwecke zu instrumentalisieren“, so Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies. "Da sich die Taktiken immer wieder ändern, können wir Unternehmen nur raten, sich selbst, ihre Kunden und Partner mit modernen, mehrschichtigen Sicherheitsdiensten zu schützen. Das Security-Konzept sollte dabei ganzheitlich aufgesetzt sein und alle Aspekte beachten – vom Kernnetzwerk über die Endpunkte bis hin zu den Benutzern selbst."

IT-Profis bietet der Report eine detaillierte Analyse der wichtigsten Trends in Bezug auf Malware- und Netzwerkangriffe sowie stichhaltige Übersichten zu Malware-lastigen Domains, kompromittierten Webseiten und Phishing-Links. So wird beispielsweise auch auf Apache Struts-Schwachstellen aufmerksam gemacht, die es im Zuge des Equifax-Vorfalls in jüngster Vergangenheit in die Schlagzeilen geschafft haben. Ergänzt wird diese Aufarbeitung wie immer von zahlreichen Tipps und Best-Practices, die Unternehmen dabei helfen, sich gegenüber der aktuellen Bedrohungslage effektiv abzusichern.

Last but not least wirft das WatchGuard Threat Lab einen genauen Blick auf die HTTPS-Entschlüsselungskampagne von Kasachstan und ähnliche Initiativen anderer Länder zur Überwachung des Datenverkehrs. In dem Zusammenhang werden nicht nur die Besonderheiten der HTTPS-Verschlüsselung und -Entschlüsselung im Detail erläutert. Auch die Bedeutung der HTTPS-Verschlüsselung für die Sicherheit von Unternehmensnetzwerken arbeiten die WatchGuard Security-Experten klar heraus – inklusive spezifischer Handlungsempfehlungen.

Der vollständige Bericht steht hier zum Download zur Verfügung: <https://www.watchguard.com/wgrd-resource-center/security-report-q3-2019>

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 GmbH  Paul Moll – Field Marketing Manager Central Europe  Wendenstr. 379, 20537 Hamburg  Tel.: +49 152 31795040  paul.moll@watchguard.com  www.watchguard.de | Presse- und Öffentlichkeitsarbeit:  Press'n'Relations GmbH, c/o Medianovis AG  Rebecca Horn  Schaffhauser. 91, 8057 Zürich  Tel.: +49 731 962 87 15  rh@press-n-relations.de  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.