**PRESSEINFORMATION**

Hamburg, 24. März 2020

**„Evasive Malware“ auf Rekordniveau**

**Internet Security Report Q4/2019 von WatchGuard: IT-Bedrohungen müssen auch und gerade in Zeiten von Corona im Auge behalten werden**

**IT-Abteilungen sind derzeit stärker gefordert denn je. Immer mehr Mitarbeiter arbeiten von zuhause und so gilt es, den Spagat zwischen Sicherheit und Produktivität bestmöglich zu bewältigen. Um Kräfte im Wettlauf mit den Cybergefahren besser bündeln zu können, sollten sich IT-Administratoren daher gezielt mit der Bedrohungslage auseinandersetzen. Studien wie der jüngst veröffentlichte Internet Security Report des Netzwerksicherheitsspezialisten WatchGuard Technologies liefern in dem Zusammenhang wichtige Erkenntnisse und zeigen, worauf besonderes Augenmerk liegen sollte. So konnte im vierten Quartal 2019 beispielsweise ein massiver Anstieg sogenannter „Evasive Malware“ festgestellt werden. Mehr als zwei Drittel des Gesamtvolumens an Malware wurden aufgrund ausgefeilter Tarnmöglichkeiten von klassischen, signaturbasierten Antivirenlösungen nicht erkannt. Vor diesem Hintergrund ist es Unternehmen jeder Art und Größe dringend angeraten, entsprechend nachzurüsten und auf moderne Antivirenlösungen umstellen, die in der Lage sind, auch solche Angriffe zu erkennen und zu blockieren.**

Die Ergebnisse des WatchGuard Internet Security Reports basieren auf anonymisierten Firebox-Feed-Daten von über 40.000 aktiven WatchGuard UTM-Appliances weltweit, deren Anwender dem Daten-Sharing zugestimmt haben. Insgesamt blockierten diese im vierten Quartal 2019 über 34 Millionen Malware-Varianten (859 pro Gerät) und rund 1,9 Millionen Netzwerkangriffe (47 pro Gerät).

**Tarnen und Täuschen ist nicht mehr die Ausnahme, sondern die Regel**

Gegenüber dem bisherigen Durchschnittswert von Evasive Malware im Jahr 2019 kommt der Anstieg auf 68 Prozent im vierten Quartal nahezu einer Verdopplung gleich. Zur Erläuterung: Bei der Malware-Erkennung kombinieren die WatchGuard UTM-Appliances insgesamt drei verschiedene Konzepte. Neben einem signaturbasierten Virenschutz kommen eine auf maschinellem Lernen basierende Erkennungstechnologie namens IntelligentAV und eine verhaltensbasierte Lösung namens APT Blocker zum Einsatz. Von Evasive Malware wird gesprochen, wenn diese den signaturbasierten Scanner überwindet und erst von einer der beiden anderen Technologien abgefangen wird.

**Cyberkriminelle setzen auf Corona-Angst**

Darüber hinaus verzeichneten die WatchGuard-Experten im letzten Quartal 2019 insbesondere in Deutschland, Großbritannien und Neuseeland weit verbreitete Phishing-Kampagnen, die auf einer bereits seit 2017 bekannten Microsoft Excel-Schwachstelle basieren. Über Makros lädt und installiert spezielle "Dropper"-Malware hierbei mehrere weitere Malware-Varianten auf Systeme der Opfer. Zum Einsatz kamen dabei unter anderem der Trojaner „Razy“ oder der Keylogger „Agent Tesla“. Letzterer wurde auch im Rahmen von Phishing-Angriffen im Februar 2020 genutzt, die gezielt mit der Angst vor dem Ausbruch des Coronavirus spielten.

**Mac Adware, SQL-Injection und Automatisierung bei der Malware-Verbreitung**

Der WatchGuard Internet Security Report Q4/2019 liefert aber noch weitere wichtige Erkenntnisse: So erfreute sich auch Mac Adware – also Mac-basierte Programme, die in Computersysteme eindringen und unerwünschte Werbung anzeigen – von Oktober bis Dezember 2019 großer Beliebtheit. Besonders hervor stach dabei „Bundlore“, eine Adware-Variante, die als Adobe Flash-Update anmutet. Dies deckt sich mit [den Ergebnissen der Studie von MalwareBytes](https://www.vox.com/recode/2020/2/12/21134681/mac-pc-virus-malware-malwarebytes) von Februar 2020, nach der Mac-Malware weiter im Kommen ist. Im Hinblick auf Netzwerkangriffe gab’s für WatchGuard im Jahr 2019 nur einen Sieger: SQL-Injections. Entsprechende Angriffe stiegen zwischen 2018 und 2019 um 8.000 Prozent an und sicherten sich damit klar die Spitzenposition. Einen weiteren Trend sehen die IT-Security-Forscher des WatchGuard Threat Labs in der zunehmenden Automatisierung bei der Verbreitung von Malware. Zahlreiche Angriffe trafen 70 bis 80 Prozent aller Fireboxen in einem Land, was zeigt, dass Hacker ihr Handwerk zunehmend zu automatisieren wissen.

„Die Ergebnisse des aktuellen Internet Security Reports untermauern aufs Neue, dass Cyberkriminelle ihre Angriffsmethoden konsequent weiterentwickeln“, so Corey Nachreiner, Chief Technology Officer bei WatchGuard. „Der hohe Anteil an Evasive Malware, die an signaturbasierten Abwehrmechanismen vorbeihuscht, und zahlreiche neuen Bedrohungen wie Mac Adware sind ein klares Indiz dafür, dass Unternehmen jeder Größenordnung in mehrschichtige Sicherheitslösungen investieren sollten. Der Einsatz künstlicher Intelligenz oder verhaltensbasierter Anti-Malware-Technologie sowie von DNS-Filtern und einem verlässlichen Phishing-Schutz ist dabei besonders wichtig.“

Der vollständige Bericht, der Unternehmen, IT-Sicherheitsdienstleister und Endkunden bei der Bewertung der aktuellen Bedrohungslage unterstützen soll, umfasst nicht zuletzt wichtige Tipps zur Abwehr all dieser Gefahren. Zudem bietet er auch eine detaillierte Analyse der MageCart JavaScript-Malware, die im Oktober 2019 genutzt wurde, um Kreditkartendaten von Kunden der größten Warenhauskette der USA – Macy's – zu stehlen.

Das Dokument in englischer Sprache steht hier zum Download zur Verfügung: <https://www.watchguard.com/wgrd-resource-center/security-report-q4-2019>

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 GmbHPaul Moll – Field Marketing Manager Central EuropeWendenstr. 379, 20537 HamburgTel.: +49 152 31795040paul.moll@watchguard.comwww.watchguard.de | Presse- und Öffentlichkeitsarbeit:Press'n'Relations Austria GmbHGeorg DutziLange Gasse 65/16, A-1080 WienTel.: +43 1 9076148-10gd@press-n-relations.atwww.press-n-relations.at |

**Über WatchGuard Technologies**

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich IT-Sicherheit. 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-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.