**PRESSEINFORMATION**

Zürich, 30. März 2017

**Zero Day Malware macht 30 Prozent aller Angriffe aus**

**Neuer „Internet Security Report“ von WatchGuard beleuchtet ab sofort vierteljährlich die aktuelle Gefahrenlage**

**Mit dem heute erstmals veröffentlichten „Internet Security Report“ läutet WatchGuard eine neue Berichtsserie ein. Künftig wird der Netzwerksicherheits-Spezialist viermal im Jahr fundierte Einblicke in weltweite Angriffsszenarien geben. Bereits die erste Ausgabe des Reports für die Monate Oktober bis Dezember 2016 zeichnet ein klares Bild: Danach lassen sich im betrachteten Zeitraum 30 Prozent aller global registrierten Malware-Vorfälle auf das „Zero Day“-Schema bzw. neue Angriffsmuster zurückführen. Eingesetzte Antivirus-Lösungen waren hier machtlos, was einmal mehr bestätigt, dass die AV-Anbieter im Umgang mit neuen Signaturen den Automatismen der Cyberkriminellen beim Restrukturieren und Verändern ihrer Malware kaum noch gewachsen sind. Ohne den Einsatz einer Sicherheitslösung, die zusätzlich auf modernen Erkennungs- und Abwehrtechniken basiert, hätten Unternehmen in 30 Prozent der Fälle das Nachsehen gehabt.**

Gleichzeitig sollte auch die Gefahr von Makro-basierter Malware nicht unterschätzt werden. Obwohl es sich hierbei um keinen ganz neuen Trick handelt, werden im Zuge des Spear-Fishings nach wie vor Dokumente mit bösartigen Makros eingesetzt. Zudem haben Angreifer auch Wege gefunden, das neue Dokumenten-Format von Microsoft zu kompromittieren. Darüber hinaus sind Webshells zur Infiltrierung von Webservern nach wie vor nicht aus der Mode – ganz im Gegenteil: Dank neuer Verschleierungsmethoden erleben PHP-Shells gerade ein unrühmliches Revival. Gleiches gilt für JavaScript: Die Auswertungen der Sicherheitsvorfälle an den WatchGuard-Fireboxen zeigen in diesem Zusammenhang einen deutlichen Malware-Anstieg – sowohl bei E-Mails als auch im Web. Generell lässt sich festhalten, dass bei der Mehrzahl der Netzwerkangriffe Webdienste und Browser im Fokus stehen: In 73 Prozent der einschlägigen Sicherheitsvorfälle konnte als Ursache ein Drive-by-Download verortet werden. Und last but not least zeigt die WatchGuard-Analyse ein klares Länderspiel: Einer der prägnantesten Angriffe via Wscript.shell Remote Code Execution konzentrierte sich zu 99 Prozent auf Deutschland (siehe Seite 13 des Internet Security Report).

**18,7 Millionen Malware-Varianten in Summe**

Alle Erkenntnisse des „Internet Security Reports“ lassen sich auf die anonymisierten Daten von über 24.000 WatchGuard-Appliances zurückführen, die weltweit im Einsatz sind. Insgesamt wehrten die UTM-Plattformen im Betrachtungszeitraum von Oktober bis Dezember 2016 über 18,7 Millionen Malware-Varianten ab. Zudem konnten drei Millionen Netzwerkübergriffe verhindert werden, im Durchschnitt hat jede einzelne beteiligte Appliance 123 Zugriffsversuche unterbunden.

**Sensibilisierung für die Bedrohung**

Im Report werden die wichtigsten Malware-Trends, Auffälligkeiten beim Web- und E-Mail-Verkehr sowie verortete Sicherheitsvorfälle im Detail aufgeschlüsselt. Die Darstellungen sollen in erster Linie dazu beitragen, dass insbesondere kleine und mittlere sowie dezentral aufgestellte Unternehmen im Hinblick auf die sich kontinuierlich verändernde Gefahrenlandschaft konkrete Einblicke erhalten und für einschlägige Bedrohungstrends sensibilisiert werden. Gleichzeitig hat das WatchGuard Threat Lab in Folge der rasanten Verbreitung des Mirai-Botnets ein weiteres Forschungsprojekt ins Leben gerufen, das sich konkret mit den Sicherheitslücken von IoT-Devices – in diesem Fall u.a. WLAN-Kameras und Fitness-Accessoires – auseinandersetzt. Die Erkenntnisse finden im aktuellen Report ebenfalls Niederschlag. So wurden Schwachstellen des WLAN-Kameramodells Amcrest IPM-721S intensiv beleuchtet (der Hersteller wurde informiert, die Sicherheitslücken sind bereits geschlossen) und es gibt praktische Hinweise, welche Schritte Anwender im Sinne der Absicherung von IoT-Geräten generell unternehmen sollten.

„Mit dem ‚Internet Security Report’ gehen wir einen weiteren wichtigen Schritt“, betont Corey Nachreiner, Chief Technology Officer bei WatchGuard. „Unsere Sicherheitsexperten im Threat Lab verfolgen bereits seit Jahren die vorherrschenden Trends im Security-Umfeld. In Kombination mit den Daten, die uns von den weltweit eingesetzten UTM-Plattformen in anonymisierter Form vorliegen, erhalten wir jetzt Einblicke aus erster Hand und können die Evolution der Cyber-Attacken gezielt mitverfolgen und genau im Auge behalten, wie sich die Angreifer verhalten. Ab sofort werden wir die Ergebnisse der spezifischen Untersuchungen zur allgemeinen Gefahrenlage kontinuierlich mit den Auswertungen unserer Appliances abgleichen. Auf diese Weise identifizieren wir die tatsächlichen Trends und können passgenaue Hinweise zur Abwehr der jeweiligen Bedrohung geben.“

Der vollständige Report steht hier zum Download bereit: www.watchguard.com/security-report

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Bild 1: Top 10 der von Firebox Gateway Antivirus registrierten Vorfälle im 4. Quartal 2016 | Bild 2: Verteilung aller von IPS registrierten Vorfälle im 4. Quartal 2016 nach Ländern | Bild 3: Verteilung von Wscript.shell(3) nach Ländern (4. Quartal 2016) |

Das Bildmaterial zum Download finden Sie in unserem Medienportal press-n-relations.amid-pr.com (Suchbegriff „Internet Security Report Q4/2016“).

|  |  |
| --- | --- |
| Kontakt:  WatchGuard Technologies GmbH  Michael Haas – Area Sales Director Central Europe  Wendenstr. 379, 20537 Hamburg  Tel.: +49 170 7727415  michael.haas@watchguard.com  www.watchguard.de | Presse- und Öffentlichkeitsarbeit:  Press'n'Relations GmbH  Markus Häfliger Hirslanderstr. 51, 8032 Zürich  Tel.: +41 43 344 58 65 [mh@press-n-relations.ch](mailto:mh@press-n-relations.ch) [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 bis hin zu Technologien für umfassenden WLAN-Schutz sowie weiteren spezifischen Produkten und Services rund ums Thema IT-Security. Mehr als 75.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen 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. Weitere Informationen, Updates und tagesaktuelle Inhalte sind auf Twitter @sichersein und auf [www.watchguard.de](http://www.watchguard.de) zu finden.