**PRESSEINFORMATION**

Hamburg, 17. September 2018

**Unzulänglichkeiten im Umgang mit Passwörtern sind die größte Gefahr**

**WatchGuard Internet Security Report Q2 2018: Cyberangriffe auf persönliche Login-Daten sowie Office-Dokumente mit Malware weiter an der Tagesordnung**

**Kleine und mittlere Unternehmen (KMU) sowie dezentral organisierte Firmen sahen sich auch im zweiten Quartal 2018 mit Angriffen aus unterschiedlichen Richtungen konfrontiert. Im Hauptfokus der Angreifer stand der Diebstahl persönlicher Anmeldeinformationen. Als Top-Bedrohung identifizierte das WatchGuard Threat Lab in diesem Zusammenhang eine auf Mimikatz basierende Malware. Außerdem wurde eine Zunahme von entsprechenden Brute-Force-Login-Angriffen auf Webanwendungen verzeichnet. Daraus folgt, dass Passwörter allein keinen ausreichenden Schutz mehr bieten. Unternehmen – unabhängig von ihrer Größe – können diesen nur über Multifaktor-Authentifizierungs-(MFA)-Lösungen gewährleisten.**

„Die sichere Authentifizierung des Anwenders ist einer der Security-Eckpfeiler in jedem Unternehmen. Angesichts der auf den Diebstahl von Passwörtern und Anmeldedaten gerichteten Bedrohungen im zweiten Quartal 2018 sehen wir dieses Thema besonders kritisch“, so Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies. „Aus unserer Sicht ist es unerheblich, ob bei den Angriffen eine fortschrittliche Malware-Variante oder die ‚Brechstangen-Methode‘ mittels Brute-Force-Login-Techniken zum Einsatz kommt: Auf der Agenda von Cyberkriminellen steht der Diebstahl von Anmeldedaten zum einfachen Zugriff auf das Unternehmensnetzwerk und sensible Daten ganz oben. Dieser Trend befeuert bei WatchGuard die Entwicklung moderner Abwehrmaßnahmen innerhalb unseres Produktportfolios. Mit AuthPoint bieten wir beispielsweise eine cloudbasierte Multifaktor-Authentifizierungslösung an. Unser KI-unterstützter IntelligentAV-Service nutzt zur Erkennung neuer Varianten von Schad-Software drei Malware-Engines – denn nur traditionelle signaturbasierte Antivirenprodukte sind hier chancenlos. Angesichts der Bedrohungssituation sollte jedes Unternehmen mehrschichtige Schutzmaßnahmen ergreifen, um den sich ständig weiterentwickelnden Angriffstechniken Paroli bieten zu können. Die WatchGuard-Vertriebspartner stehen dafür mit Rat und Tat zur Seite.“

Der vierteljährlich erscheinende Internet Security Report von WatchGuard informiert über aktuelle Entwicklungen und Forschungsergebnisse aus dem Bereich der Cyberkriminalität. Neben einem besseren Verständnis für die Thematik geben die Security-Best-Practices konkrete Hilfestellungen, mit denen Unternehmen den Schutz ihrer Daten und Systeme verbessern können. Die wichtigsten Ergebnisse des Q2-Berichts sind:

* **Rund die Hälfte der Passwörter von Mitarbeitern der US-Regierung und des US-Militärs sind schwach.** Das Threat Lab-Team von WatchGuard hat die Datensätze des LinkedIn-Datendumps von 2012 gründlich analysiert, um die Stärke der verwendeten Benutzerkennwörter festzustellen. Das Ergebnis: Bei nahezu der Hälfte aller Mail-Adressen mit einer Verbindung zu „.mil“- und „.gov“-Domains waren die Passwortphrasen objektiv schwach. Von 355.023 Passwörtern für Regierungs- und Militär-Accounts in der Datenbank konnten 178.580 in weniger als zwei Tagen geknackt werden. Kein Wunder, denn zu den gebräuchlichsten gehörten „123456“, „Passwort“, „linkedin“, „sunshine“ und „111111“. Umgekehrt stellte das Team fest, dass etwas mehr als 50 Prozent der zivilen Passwörter ebenfalls nicht aktuellen Anforderungen genügen. Diese Ergebnisse veranschaulichen klar die grundsätzliche Notwendigkeit stärkerer Passwörter für alle sowie einen generell höheren Sicherheitsstandard für Mitarbeiter im öffentlichen Dienst, die mit potenziell sensiblen Informationen umgehen. Zusätzlich zu besseren Passwortschulungen und -prozessen sollte jedes Unternehmen Multifaktor-Authentifizierungslösungen einsetzen, um das Risiko von Datenverstößen weiter zu reduzieren.
* **Die am weitesten verbreitete Malware-Variante im zweiten Quartal war Mimikatz.** Mit einem Anteil von 27,2 Prozent im letzten Quartal gehört sie zu den zehn wichtigsten Malware-Varianten. Mimikatz ist ein bereits seit Langem bekanntes Tool für den Diebstahl von Passwörtern und Berechtigungen. In den vergangenen Quartalen war es zwar beliebt, schaffte es jedoch nie in die Top-Liste. Die zunehmende Verwendung von Mimikatz deutet darauf hin, dass Authentifizierungsangriffe und Identitätsdiebstähle für Cyberkriminelle nach wie vor oberste Priorität haben. Diese Entwicklung ist ein weiterer Indikator dafür, dass Passwörter als Sicherheitskontrolle alleine nicht mehr ausreichen. Deren Schutz muss mit MFA-Lösungen untermauert werden. Nur dadurch kann Cyberkriminellen das Leben schwer gemacht werden, da sie zusätzliche Authentifizierungsfaktoren benötigen, um sich erfolgreich im Netzwerk anzumelden und darauf zuzugreifen.
* **Mehr als 75 Prozent der Malware-Angriffe werden über das Internet verbreitet.** Insgesamt 76 Prozent der Bedrohungen aus dem zweiten Quartal waren webbasiert. Das deutet darauf hin, dass Unternehmen ihre HTTP- und HTTPS-Verbindungen permanent überprüfen müssen. Denn dadurch lässt sich die überwiegende Mehrheit der Angriffe bereits im Ansatz verhindern. Die vierthäufigste Malware-Variante namens "WEB Brute Force Login -1.1021" ermöglicht es Angreifern etwa, eine massive Flut an Anmeldeversuchen auf Webanwendungen durchzuführen. Dabei wird eine endlose Reihe von Zufallskombinationen genutzt, um Benutzerpasswörter in kurzer Zeit zu knacken. Derartige Angriffe sind ein weiteres Beispiel für die zunehmende Konzentration von Cyberkriminellen auf den Identitätsdiebstahl. Er zeigt, wie wichtig nicht nur die Sicherheit und Komplexität von Passwörtern ist, sondern auch die Notwendigkeit von MFA-Lösungen als effektiver Präventionsmaßnahme.
* **Kryptowährungs-Miner sind erstmals in die Liste der Top-Malware-Variante vertreten.** Es zeichnete sich bereits ab: Die Verwendung von bösartigen Krypto-Minern als Hacking-Taktik erfreut sich steigender Beliebtheit – sie schaffte es im zweiten Quartal erstmals in die Top 10 der Malware-Liste. Anfang des Jahres stellte WatchGuard den ersten Krypto-Miner namens „Cryptominer.AY“ vor, der mit der JavaScript-Variante „Coinhive“ übereinstimmt. Dabei werden die Computerressourcen von Opfern genutzt, um die beliebte, auf Anonymität ausgerichtete Kryptowährung Monero (XRM) zu schürfen. Die Statistik zeigt, dass die Vereinigten Staaten in diesem Fall das wichtigste geografische Ziel für diesen Krypto-Miner waren und im Zuge dessen etwa 75 Prozent des gesamten Angriffsvolumens hier zu verzeichnen sind.
* **Cyberkriminelle setzen nach wie vor bösartige Office-Dokumente ein.** Seitens der Angreifer werden weiterhin modifizierte Office-Dokumente in Umlauf gebracht und alte Schwachstellen in beliebten Microsoft-Produkten ausgenutzt, um ahnungslose Opfer zu täuschen. Interessanterweise belegen gleich drei neue Office-Malware-Exploits die Top-10-Liste von WatchGuard. 75 Prozent der Angriffe hatten es auf europäische Ziele abgesehen, wobei schwerpunktmäßig deutsche Anwender attackiert wurden.

Der vollständige Internet Security Report enthält eine detaillierte Analyse der Schwachstelle rund um die EFail-Verschlüsselung sowie Einblicke zu den wichtigsten Angriffen im zweiten Quartal. Abwehrstrategien zeigen, wie kleine und mittlere Unternehmen ihre Sicherheitslage verbessern können. Die Ergebnisse im Report basieren auf den anonymisierten Firebox Feed-Daten von fast 40.000 aktiven WatchGuard UTM-Anwendungen weltweit. Im zweiten Quartal 2018 blockierten die Geräte fast 14 Millionen Malware-Varianten (449 pro Gerät) und mehr als eine Million Netzwerkangriffe (26 pro Gerät).

Für weitere Informationen können Sie den vollständigen Bericht hier herunterladen: https://www.watchguard.com/wgrd-resource-center/security-report

Das Datenvisualisierungstool [Threat Landscape](https://www.secplicity.org/threat-landscape/) von WatchGuard bietet darüber hinaus Echtzeitinformationen zu den unterschiedlichsten Bedrohungen. Über den neuen Podcast [„The 443 – Security Simplified“](https://www.secplicity.org/category/the-443/) liefert das Team ab sofort neben dem Internet Security Report und dem Secplicity.org-Blog wöchentlich weitere wichtige Einblicke zur aktuellen IT-Sicherheitslage.

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 GmbHRebecca HasertMagirusstr. 33, 89077 UlmTel.: +49 731 962 87 15 rh@press-n-relations.dewww.press-n-relations.de |

**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 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.

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.