**MEDIENINFORMATION**

Zürich, 12. März 2018

**Bisherige Kür der Gefahrenabwehr mittlerweile Pflicht**

**Partner-Umfrage von WatchGuard unterstreicht Bedarf an erweiterter Funktionalität zur Malware-Abwehr, zeigt aber auch Unsicherheiten im Markt auf**

Firewall, Antivirus, Applikationskontrolle, URL-Filter, Spam Blocker: Diese grundlegenden Sicherheitstechnologien sind aus dem Alltag der IT-Abteilungen kaum noch wegzudenken. Jedoch ist es damit inzwischen bei weitem nicht mehr getan. Einzelne moderne Sicherheitsservices gewinnen zunehmend an Bedeutung, wie auch die jüngste Partnerbefragung von WatchGuard Technologies klar belegt. Danach ist vor allem die Abwehr der sogenannten Advanced Persistent Threats ein Thema, das die Reseller in Deutschland, Österreich und der Schweiz heute auf Schritt und Tritt begleitet. Die klare Mehrheit der Umfrageteilnehmer schätzt dabei die Möglichkeiten des Sandboxings – die sich bei WatchGuard hinter dem UTM-Dienst „APT Blocker“ verbergen – als unverzichtbar oder sehr wichtig ein.

Die WatchGuard-Befragung zeigt, dass nach wie vor insbesondere klassische Funktionen – wie signatur- und verhaltensbasierte Scans (Gateway AntiVirus), Intrusion Prevention oder URL-Filter (WebBlocker) sowie Spam-Blocker – einen hohen Stellenwert im Tagesgeschäft der IT-Häuser geniessen. Diese Dienste werden von nahezu jedem der über 100 Reseller, die sich bisher im Rahmen der Befragung äusserten, als wichtig bis unverzichtbar eingestuft. Länderspezifische Unterschiede zwischen Deutschland, Österreich und der Schweiz sind kaum zu verzeichnen, überall ergibt sich ein nahezu identisches Bild. Fast jeder teilnehmende Reseller bewertet gleichzeitig die Bedeutung der erweiterten Malware-Abwehr über die Sandboxing-Technologie von APT Blocker als extrem hoch. Einigkeit herrscht jedoch auch hinsichtlich der Bewertung weiterer Services, die WatchGuard im Rahmen seines UTM-Portfolios anbietet. Hier zeigen sich auffällig viele der antwortenden Partner unentschlossen bei der Frage, welchen Mehrwert die modernen UTM-Module „Data Loss Prevention (DLP)“, „Threat Detection and Response (TDR)“ oder „Access Portal“ aus dem WatchGuard-Programm für den Einsatz auf Kundenseite bereithalten.

„Hier ist es vor allem an uns, weitere Aufklärungsarbeit zu leisten. Immer mehr wichtige Funktionalitäten stehen dem Markt zur Verfügung, dadurch wächst natürlich die Komplexität des gesamten Themas“, wie Michael Haas, Area Sales Director Central Europe, berichtet. Die dadurch entstehenden Unsicherheiten auf Partner oder Kundenseite sollten jedoch nicht dazu führen, neue Technologien komplett zu ignorieren. „Letztendlich schliessen diese im IT-Security-Alltag situationsbedingt wichtige Lücken“, wie Haas unterstreicht. So stärke der UTM-Dienst „Threat Detection and Response“ in Kombination mit der Sandboxing-Funktionalität von APT Blocker beispielsweise den Schutz gegenüber komplexen Malware-Angriffen inklusive Ransomware enorm, wie Haas betont. Durch zusätzliche Bedrohungskorrelation und Priorisierung können Angriffe deutlich schneller aufgedeckt und abgewehrt werden.

Mehrschichtige Abwehr immer entscheidender

Da sich Angriffsszenarien immer diffiziler gestalten, muss auch die Abwehr auf Unternehmensseite mithalten und zusätzliche Komponenten integrieren. So entdeckt herkömmliche Antivirus-Software, die auf Signaturüberprüfung basiert, nachweislich nicht einmal die Hälfte der Malware, die Tag für Tag auf Organisationen jeder Grösse niederprasselt. Konsequenter Schutz erfordert verschiedenste Sicherheitstechnologien und mehrschichtige Verteidigungslinien. Der Umgang mit einer solch vielseitigen IT-Sicherheitsstrategie treibt jedoch gerade kleine und mittlere Unternehmen an die Grenze der Leistungsfähigkeit. „In diesem Zusammenhang sind modular aufgebaute UTM-Lösungen, die unterschiedlichste Sicherheitsfunktionalitäten gezielt über eine einheitliche Managementkonsole zusammenführen, im Markt gefragter denn je“, so Haas: „Der Anspruch von WatchGuard besteht ganz klar darin, mehr Licht in das Dickicht der Gefahren und Gegenmassnahmen zu bringen. Unter dem Schlagwort ‚Simplification‘ subsummieren wir unterschiedlichste Leistungsbausteine, die den Alltag der IT-Abteilungen erleichtern sollen – von intuitiven Visualisierungsmöglichkeiten bis hin zur zentralen Verwaltung aller Sicherheitsservices.“ Grundsätzlich ist Resellern daher angeraten, bei der Auswahl der passenden Lösung Weitsicht walten zu lassen. Welche Faktoren konkret ins Kalkül gezogen werden sollten, beleuchtet WatchGuard in einem UTM-Kaufberater für Händler, der zum Download zur Verfügung steht: https://www.watchguard.com/de/wgrd-resource-center/it-dream-team

Bildmaterial

|  |  |
| --- | --- |
|   |  |
| Michael Haas, Area Sales Director Central Europe | Passgenaue Visualisierung sorgt für mehr Durchblick und Kontrolle im Tagesgeschäft der IT-Sicherheit |

Das Bildmaterial zum Download finden Sie in unserem Medienportal press-n-relations.amid-pr.com (Suchbegriff „Partnerbefragung“). 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.com[www.watchguard.de](http://www.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 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.