ROHDE&SCHWARZ
Cybersecurity

presse INFORMATION

20.12. 2016

Neue Paradigmen in der IT-Sicherheit sind unabdingbar

Cyber-Attacken nehmen zu, werden raffinierter und kosten Unternehmen inzwischen Milliarden. Herkömmliche Sicherheitskonzepte sind zunehmend machtlos. Die Digitalisierung vieler Branchen sowie die Themen Internet of Things und Industrie 4.0 verschärfen die Notwendigkeit nach wirksamen und praktikablen Sicherheitslösungen. Wer sich schützen will muss umdenken…

Autor: Peter Rost, Director Marketing Rohde & Schwarz Cybersecurity

51 Milliarden Euro – so hoch ist laut BITKOM der Schaden, der deutschen Unternehmen durch Plagiate und den Verlust der Wettbewerbsfähigkeit in Folge von Cyber-Angriffen in einem einzigen Jahr entstanden ist. Cybercrime ist inzwischen ein lukratives Geschäftsmodell und in seiner finanziellen Dimension vergleichbar mit dem weltweiten Drogenhandel. Die Zahl der Angriffe steigt stetig – eine manuelle Bewältigung ist unmöglich. Volkswagen beispielweise beziffert die Cyber-Attacken auf sein IT-Netz mit rund 6.000 pro Tag.

360.000 neue Viren pro Tag

Die Angriffe sind deshalb so gefährlich, weil auch die Anzahl der vernetzten Geräte weiter steigt. Das liegt nicht zuletzt am „Internet of Things“ (IoT), das heißt der zunehmenden Vernetzung von Geräten, Sensoren etc. über IP-Netze. Das birgt enorme Sicherheitsrisiken und nur eine einzige Schwachstelle reicht aus, um für hohe Verluste im gesamten Netz zu sorgen. Bösartige Absender von Mails beispielsweise werden von Mitarbeitern nicht immer erkannt – die Malware lädt bereits auf den Rechner. Die Infizierung eines Rechners kann sich auf das ganze Unternehmen ausweiten. Täglich werden rund 360.000 neue Viren entdeckt.

Das Erschreckende: 27 Prozent der Malware bleibt in den ersten drei Tagen nach dem Fund unentdeckt. Bevor Angreifer überhaupt entdeckt und gestoppt werden, können sie unzählige Geräte infizieren. Sogenannte „Zero-Day Exploits“ nutzen gezielt Lücken in der Sicherheit aus, bevor diese entdeckt und geschlossen werden können. Für herkömmliche Anti-Virensoftware besteht keine Möglichkeit, solche Angriffe abzuwehren. Noch perfider sind so genannte Botnetze: Mit dem Internet verbundene Geräte werden gehackt und dann erst einmal „schlafen“ gelegt. Nach einer Weile werden sie dann bspw. für kriminelle Zwecke, etwa für Erpressungen, genutzt.

Proaktiv statt reaktiv

Firewalls und herkömmliche Antiviren-Software alleine reichen nicht mehr aus, um Unternehmen lückenlos zu schützen. „Anti-Virus is dead“ – dieser Leitsatz eines Branchenexperten unterstreicht die Notwendigkeit eines Paradigmenwechsels in der Cybersicherheit. Das ähnelt der Entwicklung der Sicherheit beim Auto: Mit einem Airbag alleine geben wir uns nicht mehr zufrieden. Wir kaufen Autos mit Electronic Stability Control (ESP), um aktiv Unfälle zu verhindern statt sie nur zu lindern, wenn sie schon eingetreten sind.

Dieser Wechsel von reaktiven hin zu proaktiven Lösungen ist auch in der Cybersicherheit unabdingbar. Ein Beispiel ist der Endpoint-Schutz. Rund 70 Prozent der Malware dringen über den Browser in das Netzwerk ein. Proaktive Endpoint-Lösungen arbeiten mit dem Prinzip der Separierung: Der Browser wird im PC virtualisiert und von allen anderen Daten und Anwendungen in Endpoint und Intranet hermetisch getrennt. Das verkleinert die Angriffsfläche für Windows- und Linux-Malware enorm, und Unternehmensdaten sind für Angreifer wie etwa Ransomware unsichtbar. Das Prinzip kann auch auf Smartphones und Tablets umfassenden Schutz bieten.

Die Angriffsfläche entfernen

Der Schlüssel zur Vermeidung von Angriffen liegt in einem sicheren Betriebssystem. Deshalb basieren neue Sicherheitskonzepte auf dem technologischen Ansatz „Security by Design“. Die Sicherheit wird dabei direkt während der Entwicklung in das Betriebssystem integriert. Der Vorteil: Statt einer Analyse und Bekämpfung von sich stets weiterentwickelnden Angriffsformen wie zum Beispiel Zero day Exploits, wird die Angriffsfläche reduziert bzw. entfernt.

Der Paradigmenwechsel erfasst auch die Netzwerksicherheit. Beispiel Firewalls: Alte Firewall-Technologien sind reaktiv. Sie arbeiten nach schwarzen Listen („Black-Lists“): Datenpakete mit bekannten Angriffsmustern werden geblockt. Gegen neue und unbekannte Angriffe bleiben solche Mechanismen aber wirkungslos. Hier helfen neue Technologien, wie sie Next-Generation Firewalls umsetzen, bei denen Datenpakete proaktiv geprüft werden. Nur wenn diese sich als gutwillig identifizieren können, dürfen sie passieren. Alle anderen, auch die unbekannten, werden abgewiesen. Dieses als "Whitelisting" bezeichnete Verfahren bietet sich besonders im Intranet und für SCADA- und IoT-Netzwerke an.

Vertrauenswürdige Lösungen „Made in Germany“

Zu einem Paradigmenwechsel bei der IT-Sicherheit gehört auch die Einsicht, dass Unternehmen vertrauenswürdige Lösungen benötigen, die „Made in Germany“ sind. Denn der Standort Deutschland genießt ein hohes Vertrauen in der IT-Sicherheit: Nicht zuletzt durch jahrzehntelange Forschungsförderung sind deutsche Sicherheitstechnologien weltweit führend. Das hohe Sicherheitsbewusstsein deutscher Ingenieure und Entwickler spiegelt sich auch in ihren Lösungen wieder. Darüber hinaus existiert in Deutschland keine Verpflichtung, Hintertüren für den Staat

einzubauen – im Gegensatz zu anderen Ländern. Mehr noch: Die deutschen Anbieter haben sich verpflichtet auch freiwillig keine solchen Hintertüren einzubauen.

Presse-Ansprechpartner:
Eva Wagenbach, Tel.: +49 (0)221 801087 89, Fax: +49 (0)221 801087 77, E-Mail: ew@moeller-pr.de

Kontaktdaten:
Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15
81671 München
Tel.: + 49 (0) 30 65884 223
cybersecurity@rohde-schwarz.com
https://cybersecurity.rohde-schwarz.com/de

Rohde & Schwarz Cybersecurity

Das IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity schützt Unternehmen und öffentliche Institutionen weltweit vor Cyber-Angriffen. Mit hochsicheren Verschlüsselungslösungen, Next-Generation-Firewalls sowie Software für Netzwerkanalyse und Endpoint-Security entwickelt und produziert das Unternehmen technisch führende Lösungen für die Informations- und Netzwerksicherheit. Das Angebot der mehrfach ausgezeichneten IT-Sicherheitslösungen „Made in Germany“ reicht von kompakten All-in-one-Produkten bis zu individuellen Lösungen für kritische Infrastrukturen. Im Zentrum der Entwicklung von vertrauenswürdigen IT-Lösungen steht der Ansatz „Security by Design“, durch den Cyber-Angriffe proaktiv statt reaktiv verhindert werden. Knapp 400 Mitarbeiter sind an den derzeitigen Standorten Berlin, Bochum, Darmstadt, Hamburg, Leipzig, München und Saarbrücken tätig.

Rohde & Schwarz

Der Technologiekonzern Rohde & Schwarz bietet innovative Lösungen auf allen Feldern der drahtlosen Kommunikationstechnik. Außerdem sorgt er für Sicherheit in der Informationstechnik. Vor mehr als 80 Jahren gegründet, unterhält das selbstständige Unternehmen ein engmaschiges Vertriebs- und Servicenetz mit Niederlassungen und Vertretungen in mehr als 70 Ländern. Zum 30. Juni 2016 betrug die Zahl der Mitarbeiterinnen und Mitarbeiter rund 10.000. Der Konzern erwirtschaftete im Geschäftsjahr 2015/2016 (Juli bis Juni) einen Umsatz von rund 1,92 Milliarden Euro. Der Firmensitz ist in Deutschland (München), in Asien und Amerika steuern starke regionale Hubs die Geschäfte.

Alle Pressemitteilungen sind im Internet unter https://cybersecurity.rohde-schwarz.com/de unternehmen/neuigkeiten-presse abrufbar.

Dort steht auch Bildmaterial für Sie zum Download bereit.