Cyber-Sicherheit

Isolation statt Detektion

[31.07.2019] Gefälschte E-Mails und Malware sind weiterhin das Haupteinfallstor für Cyber-Angreifer. Insbesondere neue Schad-Software können die herkömmlichen Sicherheitslösungen nicht immer erkennen. Die Micro-Virtualisierung kann hier eine sinnvolle Ergänzung sein.

Gefälschte E-Mails und bösartige Downloads bleiben die Hauptwege von Cyber-Angriffen. „Mit klassischen Sicherheitslösungen wie Firewalls, Web- und E-Mail-Filtern oder Antivirenprogrammen lassen sich die durch E-Mails und Downloads bestehenden Gefahren nicht vollständig in den Griff bekommen“, sagt Jochen Koehler, Regional VP Sales Europe beim Software-Anbieter Bromium. „Das Problem dieser Lösungen ist, dass sie auf die Malware-Erkennung angewiesen sind und bisher unbekannte Schad-Software wie einen neuen Virus in einem E-Mail-Anhang nicht zu 100 Prozent aufspüren können.“ Eine sinnvolle Schutzmaßnahme könne stattdessen eine Lösung bieten, die auf Isolation statt Detektion setze. „Und die effektivste Variante für eine solche Isolation ist die Nutzung der Virtualisierungstechnologie.“
Wie Bromium mitteilt, wird bei der so genannten Micro-Virtualisierung jede riskante Anwenderaktivität wie das Öffnen eines E-Mail-Anhangs oder das Downloaden eines Dokuments in einer eigenen Micro-VM (Virtual Machine) gekapselt. Eine mögliche Schädigung durch ein Schadprogramm bleibe dadurch immer auf die jeweilige Micro-VM beschränkt, die nach Beendigung einer Aktivität ohnehin automatisch gelöscht werde. Überflüssig würden die herkömmlichen Sicherheitslösungen durch die Micro-Virtualisierung allerdings nicht. Antiviren-Tools für die Erkennung bekannter Schad-Software bleiben laut Unternehmen elementarer Bestandteil jeder Sicherheitsarchitektur. „Aber das Entscheidende ist, dass diese Lösungen letztlich nur eine komplementäre Ergänzung darstellen, und zwar von Lösungen, die einen gezielten Schutz auch vor unbekannter Malware bieten“, sagt Koehler.

(ve)

Stichwörter: IT-Sicherheit, Bromium, Micro-Virtualisierung