Warum Security ohne SaaS nicht mehr machbar ist

On-Premises oder Software-as-a-Service? Vor dieser Frage stehen Unternehmen auch bei ihrer Security. Es gibt viele gute Gründe, auf die Cloud zu setzen. Der wichtigste: Ohne SaaS wird es künftig kaum noch möglich sein, Bedrohungen schnell genug zu erkennen und abzuwehren.

Die Modernisierung des Rechenzentrums schreitet immer weiter voran. Zunehmend verlagern Unternehmen IT-Infrastrukturen in die Cloud, um Hardware einzusparen, Aufwand zu reduzieren und besser zu skalieren. Bei ihren Sicherheits-Systemen halten viele aber noch an traditionellen On-Premises-Modellen fest. Dadurch hinkt die Security hinterher, während die Angriffsfläche wächst und Cyberkriminelle immer aggressiver und professioneller vorgehen. Ein grosses Problem bei On-Premises-Systemen sind zu lange Update-Zyklen. Viele IT-Abteilungen aktualisieren ihre Security-Software nur alle drei Jahre im Rahmen ihrer gängigen Wartungs-Abfolgen. Doch das kann gravierende Folgen haben, denn Security ist immer ein Wettlauf zwischen Angreifern und Verteidigern. Cyberkriminelle entwickeln ihre Angriffstechniken rasant weiter. Wer seine Security-Technologie nicht auf dem neuesten Stand hält, verliert.

Gefährliche Bremsklötze

Dabei wird auch der Fachkräftemangel immer mehr zum Bremsklotz. Viele haben schlichtweg nicht genug Kapazitäten, um ihre Security-Software richtig zu pflegen. Dazu kommt, dass die Zahl der Systeme, die gewartet werden müssen, mit wachsender Komplexität der Infrastruktur zunimmt. So haben es viele IT-Teams mit einem Flickenteppich an Einzellösungen zu tun, die sie individuell managen müssen. Nicht nur verursacht das einen immensen Aufwand, auch die Transparenz leidet darunter. Denn wenn Daten in Silos liegen, wird es schwer, Zusammenhänge herzustellen. Genau das aber ist wichtig, um Bedrohungen schnell zu erkennen. Professionelle Cyberangriffe erstrecken sich heute häufig über einen längeren Zeitraum und viele verschiedene IT-Vektoren. Sie

The Art of Cybersecurity. Quelle: Trend Micro/Stefanie Posavec

sind gut getarnt und segeln unter dem Radar herkömmlicher Security-Systeme. Erst indem man Daten über alle Ebenen hinweg korreliert und analysiert, wird eine komplexe Attacke sichtbar.

Zeit und Transparenz als kritische Faktoren

Mehr denn je zählen in der Security heute Geschwindigkeit und Transparenz. Das verdeutlicht auch die wachsende Zahl an Zero-Day-Exploits, die die Sicherheitsforscher von Trend Micro 2021 entdeckt haben. Für 2022 prognostizieren sie einen weiteren Anstieg. Je schneller Cyberkriminelle in der Lage sind, neue Schwachstellen auszunutzen, umso wichtiger wird es, Sicherheitslücken möglichst früh zu schliessen und Angriffe zeitnah zu erkennen. SaaS bringt Unternehmen dabei einen wertvollen Zeitvorsprung. Wenn sie ihre Security-Software als Cloud-Service beziehen, kümmert sich der Hersteller um Patches und Updates. Dadurch, dass das Security-Management über einen Web-Service erfolgt, reduziert sich der Aufwand für das IT-Team erheblich.

SaaS wird zum Schlüssel für mehr Sicherheit

Um sich vor der wachsenden Gefahr durch Cyberangriffe zu schützen, brauchen Unternehmen die neuesten Security-Funktionen und aktuellste Threat Intelligence. Sie müssen ihr Security-Management vereinfachen, Silos aufbrechen und Transparenz in der gesamten IT-Umgebung gewinnen. All das gelingt am besten mit SaaS-Lösungen, die automatisch immer auf dem neuesten Stand sind und ein zentrales Security-Management bieten. Die Zukunft liegt in einer Cloud-nativen Security-Plattform, die wichtige Sicherheitsfunktionen einheitlich On-Premises und in der Cloud bereitstellt. Ergänzt wird sie durch XDR-basierte Threat Defense. So hält die Security mit der Digitalisierung Schritt, ist auch gegen neueste Angriffe gewappnet und ermöglicht Sicherheit in der gesamten hybriden IT-Umgebung. ■

Trend Micro (Schweiz) GmbH
CH-8304 Wallisellen
marketing_alps@trendmicro.com
www.trendmicro.com