Sicherheit braucht Endpoint-Schutz – und gute Hardware

Um Datendiebstahl oder anderen unerlaubten Datenabfluss aus Unternehmen auch in Zeiten von Cloud-Diensten oder mobilen Endgeräten zu verhindern, sind Endpoint-Security-Lösungen nötig, die direkt auf den Clients für die Durchsetzung von Sicherheitsrichtlinien sorgen. Das Beispiel Endpoint Protector zeigt, wie ein zuverlässiger Hardware-Partner dabei helfen kann, skalierbare Lösungen auch für fünfstellige Nutzerzahlen zu finden.

Bedrohungen für die IT im Unternehmen kommen nicht nur von außen, sondern auch von innen. Zu den größten Gefahren gehört die unberechtigte Weitergabe oder Veröffentlichung von vertraulichen Daten. Oft ist es nicht einmal böse Absicht, wenn Mitarbeiter den Umgang mit sensiblen Dokumenten etwas locker nehmen. Richtlinien und Schulungen helfen nur begrenzt, wenn die technischen Mittel fehlen, um sie umzusetzen und zu überwachen. Software zur Data Loss Prevention (DLP), also der Schutz vor Datenverlust, Datendiebstahl oder anderen Insider-Bedrohungen wird deshalb für viele Firmen oder Organisationen immer wichtiger. In bestimmten Branchen, wie etwa dem Gesundheitswesen, sind Maßnahmen gegen Datenabfluss obligatorisch.

Durch die Trends zu immer mehr mobilen Endgeräten, Nutzung von Cloud-Diensten für den Upload von Daten und BYOD wird es aber nahezu unmöglich, zentrale Unternehmens-Gateways dafür zu verwenden. Deshalb setzt Endpoint Protection an den Endgeräten an und überwacht und blockiert dort anhand von zentralen Richtlinien die Datenweitergabe.

Software dieser Art ist komplex und muss eine Reihe von Anforderungen erfüllen. Es genügt nicht, dass sie die unerlaubte Weitergabe schützenswerter Daten verhindert. Wichtig ist auch, dass sich dem Nutzer bei der täglichen Arbeit keine Hindernisse in den Weg legt, einfach zu administrieren ist und sich auf einer Vielzahl von Endgeräten verwenden lässt. Ein zusätzlicher Aspekt ist die Einhaltung von Datenschutz-Richtlinien und Arbeitnehmer-Rechten, beispielsweise bei der Protokollierung der Zugriffe und der Auswertung der Protokolle.

Als eine der besten Lösungen am Markt gilt der Endpoint Protector von CoSoSys. Er bietet Schutz gegen unerlaubten Transfer von Daten per E-Mail, Webmail, Cloud-Diensten sowie tragbarer Datenspeicher wie USB-Sticks. Er schützt PCs mit Microsoft-Systemen von Windows

XP bis Windows 10, Ubuntu- oder OpenSUSE-Linux, Apple-Computer mit Mac OS X sowie mobile Geräte mit iOS und Android.

Auch wenn die eigentliche Sicherheitsüberprüfung auf dem Endgerät stattfindet, sind zuverlässige Server für die Konfiguration, Steuerung und Protokollierung der Daten unerlässlich. Endpoint Protector arbeitet deshalb im Hardware-Bereich schon lange Zeit mit Thomas-Krenn zusammen. Derzeit testet Endpoint Protector auf Thomas-Krenn-Hardware Systeme mit virtuellen Appliances für den Einsatz mit bis zu 20.000 Endgeräten.

Denn in vielen Fällen ist der Einsatz einer dedizierten Hardware-Appliance die beste Lösung, da sie sich schnell in Betrieb nehmen lässt. Bei besonders dynamischen, schnell wachsenden Firmen oder großen Organisationen mit Tausenden von Nutzern kann aber auch der Einsatz virtueller Appliances sinnvoll sein. Damit lassen sich Workloads besser skalieren und schnell auf sich ändernde Anforderungen anpassen.