Endgerätesicherheit zeitgemäß gestalten

> Früher konnte man sich für den Schutz von Endgeräten weitestgehend auf Windows-basierte Systeme fokussieren und hier waren auch noch klassische Technologien wie „Musteranalysen“, die zur Erkennung bzw. Abwehr von Schadsoftware eingesetzt wurden, ausreichend. Heute treffen wir auf eine Vielzahl von Betriebssystemen bzw. Embbeded Systems und eine große Bandbreite von Anwendungsfällen.

Michael Huber,
Consultant bei der PROFI Engineering Systems AG

Ein zeitgemäßer Management-Ansatz sollte zum Ziel haben, ganzheitlich zu agieren, und zwar sowohl was das Auffinden von Auffälligkeiten betrifft als auch die Bekämpfung/Eindämmung dieser.

Was es jedoch zu beachten gilt, ist, dass eine „Endpoint Detection & Response“- oder auch „Xtended Detection & Response“-Lösung nur so gut ist wie die Daten, die sie von den beteiligten Endpoints erhält. Nur so kann gewährleistet werden, dass ein Unternehmen Einblick in bzw. Informationen über etwaige Sicherheitsvorkommnisse bekommt und eine umgehende Schadensanalyse möglich ist.

Der Anspruch an ein umfassendes Endpoint-Security-Konzept sollte sein, dass es eine nahezu vollständige Übersicht über alle Teilnehmer/Endpoints und deren Aktivitäten im Netzwerk bietet, die vorhandenen fortschrittlichen Abwehrfunktionen nutzt und Routineaufgaben automatisiert.

Nur in einer ausgewogenen Kombination zwischen Tools und entsprechend ausgebildetem Personal kann die Grundlage zur effektiven Bekämpfung komplexer Cyberangriffe und damit zur Aufrechterhaltung des Geschäftszweckes geschaffen werden. Was wiederum dafür sorgt, dass Unternehmen in die Lage versetzt werden, ihre knappen Ressourcen gezielt einzusetzen und sich auf ihre eigentlichen Kernthemen zu fokussieren – ohne sich Sorgen um den Schutz ihrer IT machen zu müssen. <

Im Internet: www.profi-ag.de

PROFI
Wir entwickeln mehr als IT