Controlware Security Day 2016

„Sind die Hausaufgaben gemacht, bleiben Schäden überschaubar“

Mehr als 300 Besucher haben sich auf den Weg zum Controlware Security Day 2016 gemacht. Security-Experten, IT-Leiter und technische Spezialisten hatten an zwei Tagen Gelegenheit, sich in mehr als 30 Vorträgen und persönlichen Gesprächen über aktuelle Bedrohungen, zukünftige Risiken und innovative Lösungsansätze rund um IT-Sicherheit zu informieren.

„Viele Unternehmen gehen ihre IT-Security nach wie vor punktuell und reaktiv an. Sie analysieren, von welcher Seite ihnen Gefahr droht – und reagieren dann mit Einzellösungen, die sie vor diesem Angriff schützen. Aber spätestens bei mehrstufigen Threats, die ihre Vektoren immer wieder ändern – wie Locky & Co. – stößt dieser Ansatz an seine Grenzen“, warnt Bernd Schwefing, Geschäftsführer (CEO) von Controlware. „Als Security-Dienstleister betonen wir daher seit Jahren die Bedeutung einer systematischen, proaktiven Vorgehensweise zum Aufbau und Management von Sicherheitsarchitekturen.“ Die Unternehmen müssten ein ganzheitliches Fundament schaffen, um neue IT-Lösungen schnell, nahtlos und sicher integrieren und managen zu können. Wie die Planung und Umsetzung solcher systematischen Ansätze gelingen kann – darauf lag der Fokus des Controlware Security Day 2016.

Bernd Schwefing, Geschäftsführer von Controlware, bei der Eröffnungs-Keynote des Security Day. Quelle: Controlware

Am Vortag des Security Day stand Schwefing, zusammen mit Security-Experten von Herstellern wie Check Point, RSA/EMC, Fortinet, Palo Alto Networks, Radware, Symantec und Zscaler, den Fachjournalisten Rede und Antwort. Dabei waren sich die Experten einig: Man werde es niemals verhindern können, dass nicht doch ein Mitarbeiter auf eine Mail mit einem „Ransomware-Anhang“ klickt. „Doch wenn ein Unternehmen seine Security-Hausaufgaben gemacht hat“, ist sich Schwefing sicher, „dann bleiben die negativen Auswirkungen überschaubar“.

Zu diesen Hausaufgaben zählt Schwefing zeitnahe Backups, die nicht online gehalten werden dürfen, eine Segmentierung der Unternehmensnetzwerke sowie eine mehrstufige Sicherheitsarchitektur, die von aktuell gehaltenen Security Policies sekundiert wird. Allerdings müssten Unternehmen dafür einiges an Aufwand betreiben, so dass vor allem kleine und mittlere Unternehmen mit einem geringeren Security-Budget – aber auch Organisationen aus dem Gesundheitswesen – von Ransomware stark betroffen sind.

Im Mittelpunkt des Security Days standen mehr als 30 Vorträge aus allen Bereichen der IT-Security – von A wie „Antivirus“ bis Z wie „Zentralisierte Security-Policy“. Dabei hatten die Besucher die Wahl aus Themen-Tracks wie:

- Threat Prevention & Response: Frühzeitige Erkennung von Ransomware & Co. sowie wirkungsvolle Gegenmaßnahmen.
- Endpoint Security: Wie Sie Ihre Endgeräte dank neuer Detection & Response-Technologien effektiv schützen können.
- Cloud Security: Mehr Flexibilität für Ihre IT-Prozesse durch die sichere Integration von Cloud Security Services.
- Security Operations: Rechtzeitige Anomalie-Erkennung, Aufbau von SOC-Teams und Incident-Response-Prozessen.
- Lösungen zum Schutz Kritischer Infrastrukturen (KRITIS): IT-Sicherheitsgesetz, kritische Infrastrukturen und die Unterstützung durch Managed Security Services.
- Infrastructure Security: Angriffsvektoren und Abwehrmethoden in zunehmend vernetzten Infrastrukturen.

In der begleitenden Ausstellung hatten die Besucher noch die Möglichkeit, mit Security-Spezialisten der 25 vertretenden Hersteller Gespräche zu führen. **Rainer Huttenloher** ■