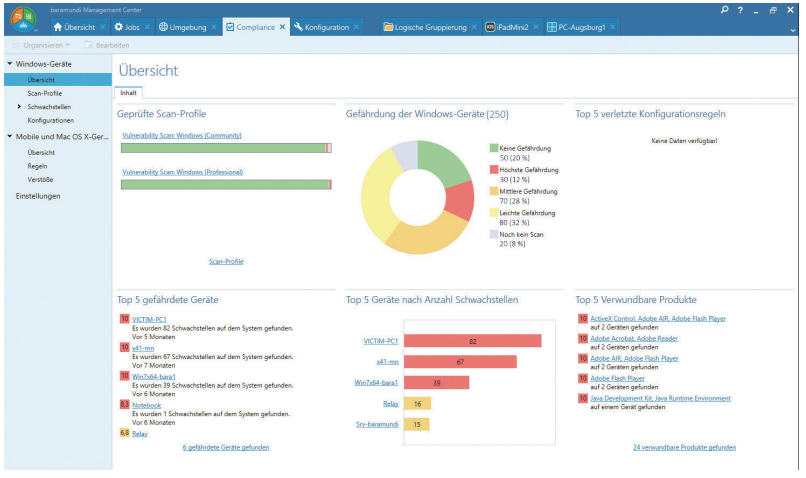
PRÄVENTION MIT SCHWACHSTELLENMANAGEMENT

Spätestens WannaCry und NotPetya haben die Wahrnehmung von IT-Sicherheit verändert. Nach Angabe der Krankenhausstudie 2017 vom Beratungsunternehmen Roland Berger sind 64 % deutscher Krankenhäuser bereits Opfer eines Hackerangriffs geworden. Grund hierfür ist u. a. der Einsatz veralteter Technologien. Nach Statistiken der National Vulnerability Database von US-CERT werden jede Woche hundert neue Schwachstellen bekannt. Schutz bietet ein automatisiertes Schwachstellenmanagement.



Mit der baramundi Management Suite erkennen Sie alle Schwachstellen in ihrer Infrastruktur und können diese schnell schließen.

Sicherheitslücken in Software

Inmitten von Millionen Zeilen Programmcodes sind rein statistisch Schwachstellen zu erwarten. Solange diese nicht bekannt sind, ist das Risiko eines Schadens gering. Microsoft oder Google engagieren zur Prävention White Hat Hacker. Ihre Aufgabe: Schwachstellen finden und melden. Die Unternehmen stellen dann den entsprechenden Patch zum Schließen der Sicherheitslücke zur Verfügung. Sobald Black Hat Hacker von dem Patch erfahren, setzen sie alles daran, die Schwachstelle zu finden und einen entsprechenden Exploit zu erstellen. Exploits setzen Kriminelle ein, um einen Payload in das System einzuschleusen, der Daten ausspäht, löscht oder gar den Client zum Teil eines Botnets macht. Solange der Patch nicht auf allen betroffenen Geräten eingespielt wurde, sind Angriffe möglich. Die IT-Administration muss zu jeder Zeit die Krankenhaus-IT schützen. Ohne den Einsatz eines automatisierten Schwachstellenmanagements müsste der Administrator kontinuierlich Datenbanken auf Schwachstellen manuell durchsuchen und bewerten. Im nächsten Schritt müsste er die eigenen Rechner überprüfen und die nötigen Updates paketieren, testen und verteilen. Diese Vorgehensweise ist angesichts der Komplexität und Menge nicht praktikabel.

Sicherheit durch Automatisierung

Bündelt man jedoch sicherheitsrelevante Werkzeuge in einer einzigen Suite, so können diese wichtigen Aufgaben automatisiert werden. Mit einer Unified-Endpoint-Management (UEM)-Lösung verwalten IT-Administratoren alle in der Klinik befindlichen Endpoints zentral und einheitlich. Nur wer einen Überblick über alle Endpoints und deren Abhängigkeiten hat, kann diese auch schützen. Eine Schnittschnelle zu regelmäßig aktualisierten, anerkannten Schwachstellendatenbanken bietet zusätzlichen Schutz. Schwachstellen können dann auf Basis der Datenbanken automatisiert erkannt und durch die Verteilung von Patches behoben werden. Die IT-Administration spart dadurch wertvolle Zeit.

Mensch und IT als Einheit

IT-Administratoren müssen täglich zeitnah Entscheidungen treffen und handeln, weshalb sie Managementlösungen benötigen, die sie entlasten. Eine Kombination aus Know-how und einem automatisierten Patch-Management sorgt für die nötige Effizienz und Sicherheit. Wie beim Menschen auch, ist Vorsorge für die (IT-)Gesundheit die halbe Miete.

Franz Braun
PR-Manager
baramundi software AG, Augsburg
Tel.: 0821/567080
presse@baramundi.de
www.baramundi.de

Armin Koch
Senior Manager Digital & PR
AxiCom GmbH, München
Tel.: 089/80090818
armin.koch@axicom.com
www.axicom.de