CYBER RESILIENCE: KLINISCHE IT-INFRASTRUKTUR WIDERSTANDSFÄHIG MACHEN

GREENBONE Angriffsflächen mit Schwachstellenmanagement minimieren

In den vergangenen Jahren gab es weltweit bereits zahlreiche Angriffe auf Gesundheitseinrichtungen. Sie geben einen Vorgeschmack darauf, was noch kommen wird. Denn Cyberkriminelle sind heute gut organisiert. Ihr Ziel: Mit Hackerangriffen möglichst großen Profit zu erzielen. Die WannaCry-Offensive im Mai 2017, die besonders den National Health Service (NHS) in Großbritannien traf, ist der bisher wohl bekannteste Fall. Insgesamt mussten dadurch 6 912 Termine verschoben werden – darunter auch zahlreiche Operationen.

Angesichts der akuten – und vermutlich weiter steigenden – Bedrohungslage müssen sich Krankenhäuser und andere Gesundheitseinrichtungen effektiv gegen Cyberangriffe schützen. Reaktive IT-Schutzmaßnahmen reichen jedoch längst nicht mehr aus. Stattdessen müssen Einrichtungen einen Zustand der Sustainable Cyber Resilience erreichen: der nachhaltigen Widerstandsfähigkeit. Ziel ist es, den klinischen Betrieb auch im Falle eines Angriffs aufrechtzuerhalten. Ein umfassender Cyber-Resilience-Ansatz setzt sich dabei aus zahlreichen Komponenten zusammen. So gilt es etwa, die physische Sicherheit der Geräte zu gewährleisten und Mitarbeiter für Risiken zu sensibilisieren. Die Basis bildet jedoch ein effektives Schwachstellenmanagement. Denn letztlich nutzen Hacker meist Sicherheitslücken im System, um sich Zugang zu Daten und Geräten zu verschaffen.

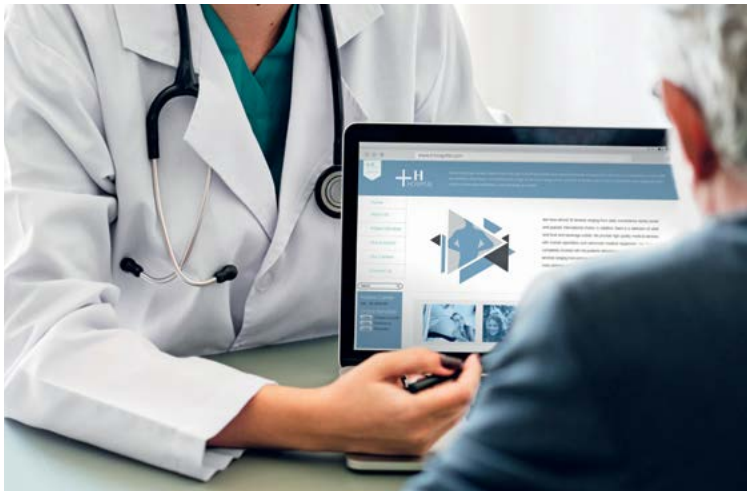
KOMPLEXE IT-INFRASTRUKTUREN ÜBERBLICKEN

Um Schwachstellenmanagement wirkungsvoll umzusetzen, sollten sich Verantwortliche zunächst einen Überblick sowohl über die eingesetzte Unternehmens-IT als auch die medizinische IT verschaffen. Zu den gängigen Systemen und Anwendungen im medizinischen Umfeld gehören zum Beispiel Patienten-Management-Systeme (PMS) für die Aufnahme und Administration. Nicht zu vergessen sind aber auch Systeme der Gebäudetechnik wie die zentralen Klimaanlagen. Auch hier könnten Hacker durch eine Manipulation den Krankenhausbetrieb erheblich beeinträchtigen.

Im nächsten Schritt gilt es, Sicherheitsvorgaben zu entwickeln, die festlegen, welche Systeme wie intensiv geschützt werden müssen. Ein Schwachstellenmanagement-Tool wie der Greenbone Security Manager (GSM) kann dann alle an das IT-Netzwerk angeschlossenen Geräte scannen und auf mögliche Schwachstellen prüfen. Anschließend bewertet er das Risiko der Sicherheitslücken, priorisiert diese und stößt Prozesse an, um sie zu beseitigen.

RISIKEN ABWÄGEN UND MANAGEN

Die Fähigkeit, Schwachstellen zeitnah aufzufinden, zu priorisieren und zu beseitigen, ermöglicht es Unternehmen, ihre IT-Systeme kontinuierlich sicherer zu machen und die Angriffsfläche zu reduzieren. Dies ist ein laufender Prozess, der niemals abgeschlossen sein darf. Denn Risiken lassen sich nicht komplett ausschalten – vielmehr geht es darum, das richtige Maß an Sicherheit und Risikobereitschaft abzuwägen.



Mehr Informationen dazu, wie Sie Ihre klinische IT-Infrastruktur mithilfe von Cyber Resilience schützen können, finden Sie im Greenbone Whitepaper:
www.greenbone.net/whitepaper/gesundheit

Greenbone

Greenbone Networks GmbH
Neumarkt 12, 49074 Osnabrück
Tel.: +49-(0)541-760278-0
E-Mail: info@greenbone.net
www.greenbone.net