Pressemitteilung

Immer mehr Cyberangriffe auf Krankenhäuser

Betreiber brauchen präventive, performante IT-Security-Konzepte

18. Mai 2021 – Cyberangriffe auf Krankenhäuser steigen. Die Bundesregierung registrierte 2020 bis Anfang November 43 erfolgreiche Angriffe auf Gesundheitsdienstleister – mehr als doppelt so viele wie im Vorjahr. Das zeigt: Krankenhäuser müssen ihre IT Security effizienter aufstellen. „Ein angegriffenes medizintechnisches Gerät, beispielsweise ein Operationsroboter, kann das Netzwerk eines ganzen Krankenhauses stilllegen. Um diese Gefahr einzudämmen, ist ein ausgeklügeltes Sicherheitskonzept notwendig“, sagt Jürgen Busch, Consultant der xevIT GmbH, Mitglied des Digitalisierungsverbunds Innovation Alliance.

Vier Stufen für mehr IoMT-Sicherheit

Ein Krankenhaus mit 1.000 Betten hat im Durchschnitt 4.000 vernetzte medizintechnische Geräte im Einsatz. Bei Angriffen auf Gesundheitseinrichtungen nutzen Cyberkriminelle diese Internet of Medical Things (IoMT)-Geräte als Brückenköpfe, um IT-Infrastrukturen zu kontrollieren. Um Cyberattacken (inklusive schwerwiegende Folgen wie Datendiebstahl und Erpressung) abzuwehren, sind aktive Präventions-, Detektions- und Reaktionsmaßnahmen notwendig:

- **Stufe 1: Erkennung von Geräten und Kommunikation:** Mithilfe eines passiven Scanverfahrens wird festgestellt, welche Medizingeräte in dem Netzwerk miteinander kommunizieren, und wo es Sicherheitslücken gibt.
- **Stufe 2: Netzwerksegmentierung:** Netzwerke werden in „Zonen“ isoliert, um eine effektive Netzwerkzugangskontrolle zu ermöglichen. Ziel ist es, Angriffsflächen zu verkleinern und die Verbreitung von Angriffen so einzuschränken.
- **Stufe 3: Erkennung von Bedrohungen und Bekämpfung:** Eine wesentliche Schutzmaßnahme ist es, bekannte und unbekannte Bedrohungen im Unternehmensnetzwerk mit Hilfe erprobter Verfahren wie Viren-Scanner und Mustererkennung zu entdecken. Cyberkriminelle gestalten Angriffe mittlerweile oft so, dass sie erst zu einem späteren Zeitpunkt ein schädliches Verhalten zeigen. Auf Sicherheitsvorfälle schnell zu reagieren,

stellt besondere Anforderungen an die IT-Verantwortlichen in Krankenhäusern.

- **Stufe 4: IT & IoMT zur präventiven und laufenden Überwachung:** Die IT-Sicherheitsvorfälle werden gespeichert und ausgewertet, um sich auf künftige Bedrohungen vorzubereiten. Eine ganzheitliche Übersicht ermöglicht zudem eine schnelle Reaktion und Behebung bei Angriffen.

Krankenhäuser haben Nachholbedarf

Hans-Martin Kuhn, Account Manager der SWS Computersysteme AG, sagt: „Den Chancen der vielen vernetzten medizintechnischen Geräte stehen hohe IT-Sicherheitsrisiken entgegen, die performante IT-Sicherheitsstrategien erfordern. Dazu zählt auch ein sehr gutes Passwortmanagement." So setzen die Hersteller der Geräte oft Standard-Passwörter, die aber von den Gerätenutzern nicht verändert werden. SWS Computersysteme ist wie xevIT Mitglied der Innovation Alliance. Die Innovation Alliance ist ein Kompetenzverbund aus mehreren Unternehmen der IT-Branche. Als Ansprechpartner zum Thema Digitalisierung berät sie Krankenhäuser zu IT-Sicherheitskonzepten und begleitet bei der präventiven und fortlaufenden Überwachung und Bekämpfung von Cyber-Attacken. Zu dem umfangreichen Lösungsportfolio zählen Security Assessments, externe Penetration Tests, DNS Traffic Analysen, Beratung zur Security Architecture, Vulnerability Scans der medizintechnischen Geräte sowie ein SOC, das Security Services anbietet.

Pressekontakt:

Innovation Alliance
Frank Dittmar: Presse/Marketing
Tel.: +49 6103 932114
dittmar@pandacom.de
www.innovationalliance.de

VOCATO public relations GmbH
Birgit Brabeck/Verena Schmorleiz
Tel.: +49 2234 60 198-18/-15
bbrabeck@vocato.com, vschmorleiz@vocato.com
www.vocato.com

Über die Innovation Alliance:

Die Innovation Alliance ist ein Kompetenzverbund aus mehreren Unternehmen der IT-Branche. Als Ansprechpartner zum Thema Digitalisierung im Mittelstand berät sie Unternehmen in Digitalisierungsfragen und begleitet bei der Umsetzung und dem Betrieb der Lösungen. Das Angebot der Innovation Alliance richtet sich an Unternehmen vor allem aus den Branchen Industrie, Produktion, Handel und Dienstleistungen sowie an Städte und Kommunen in Deutschland. Die Innovation Alliance wurde 2016 von Cisco, dem führenden Hersteller von Netzwerk-, Security- und Kommunikationslösungen, initiiert. Darüber hinaus zählen ausgewählte Digitalisierungsexperten aus dem Mittelstand – darunter Systemhäuser, Software-Entwickler, Managed Service Provider, Reseller und Berater – zu den Partnern des Kompetenzverbunds.

Die Partnerunternehmen der Innovation Alliance:
Cisco Systems GmbH, ENTIRETEC AG, Logicalis GmbH, Pan Dacom Networking AG, pco Personal Computer Organisation GmbH & Co. KG, Schweickert GmbH, SWS Computersysteme AG, xevIT GmbH. Mehr Infos unter: https://www.innovationalliance.de/

Bildmaterial:

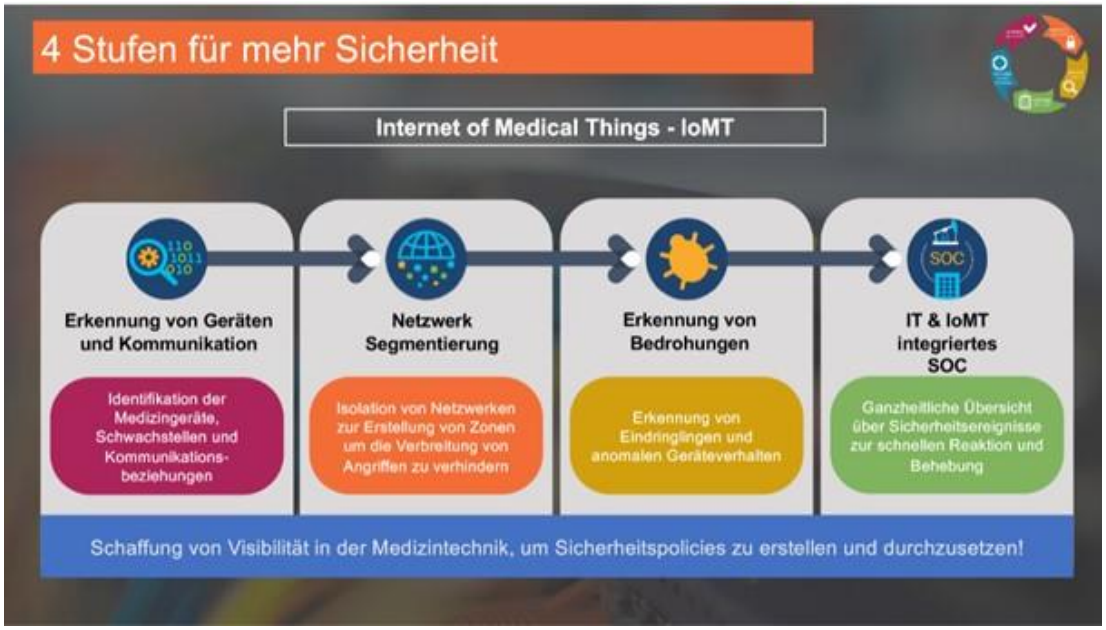

Bild: 4-Stufen-Plan für aktive Cybercrime-Abwehr, Quelle: xevIT GmbH