IST IHR IT-SYSTEM FÜR SÄMTLICHE ANGRIFFSWEGE GERÜSTET?

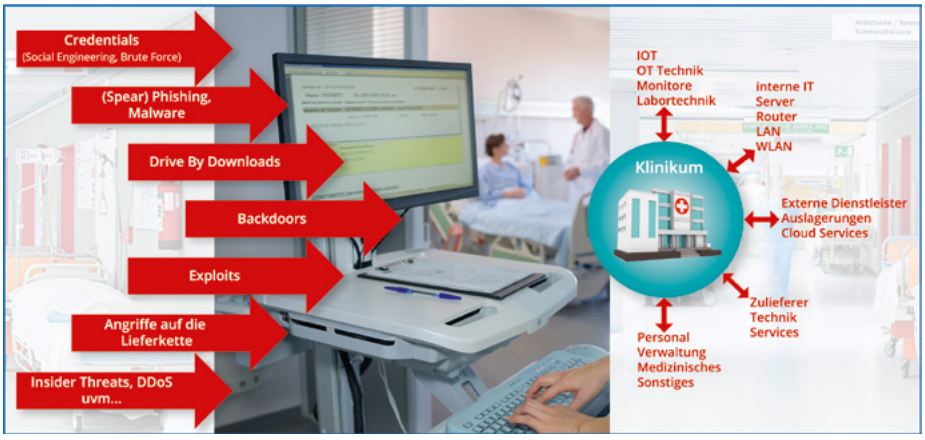
IT-Sicherheitsgesetz, E-Health-Gesetz, Patientendaten-Schutz-Gesetz (PDSG) und Krankenhauszukunftsgesetz (KHZG): Auf die Kliniken prasseln derzeit eine Menge damit verbundener Auflagen ein.

Durch das PDSG werden nun alle Krankenhäuser verpflichtet, entsprechende sicherheitstechnische Vorkehrungen zu treffen. Das im Oktober 2020 in Kraft getretene KHZG macht sogar die grundsätzliche Förderbarkeit aus dem Krankenhauszukunftsfonds von Investitionen in die IT-Sicherheit abhängig.

Für rund 90 Großkliniken in Deutschland dürften darüber hinaus die verschärften Security-Vorgaben aus der 2. Auflage des IT-Sicherheitsgesetzes relevant werden. Beispielsweise sollten Intrusion-Detection-Systeme (IDS) in KRITIS-Kliniken bis zum 1.1.2022 nachgerüstet werden, sofern diese noch nicht existieren. Allen Krankenhäusern ist gemeinsam, dass sie vor dem Problem stehen, sämtliche Auflagen in der gebotenen Zeit finanziell stemmen zu müssen. Angesichts der rasant steigenden Komplexität von Angriffen keine leichte Aufgabe, zumal technische Implementierungen für die speziellen Anforderungen des Krankenhaus-Alltags oftmals nicht ausreichen, weil sie meist ausschließlich auf die fachlich-funktionale Seite ausgerichtet sind und nicht auf die Sicherheit.

ANGRIFFSVEKTOREN ...

Dabei sind die Bedrohungen immens, wie folgende Grafik veranschaulicht:



Headerbild: ©LuckyStep - stock.adobe.com

... UND DIE GEEIGNETEN ANTWORTEN HIERAUF

Durch den Angriff auf Passwörter und Log-in-Daten können Hacker leichten Zugang zum Netzwerk der Klinik erhalten – insbesondere, wenn die Netzwerkstrukturen nicht zur Abwehr derartiger Angriffe gerüstet sind. IDS – Intrusion-Detection- und auch UBA – User-Behaviour-Analysis-Systeme sind in der Lage, derartige Angriffe aufzudecken und zu vereiteln. Microsegmentierung und Zero Trust Networking können solche Attacken eingrenzen.

Endpoint-Detection & Response-Systeme, wie zum Beispiel Tanium, erkennen zusätzlich zu den eingesetzten Antivirensystemen bereits frühzeitig mögliche Angriffe. Dies gilt auch für Bedrohungen, die Mitarbeiterinnen und Mitarbeiter neben der absichtlichen Schädigung durch Insider Threats unbewusst und unwissentlich mittels erfolgreicher Phishing-Kampagnen (aka Emotet) oder Drive-by-Downloads maliziöser Software im Browser auslösen.

Eine andere Herangehensweise muss für Backdoors und Exploits in den Kliniksystemen gewählt werden. Hier wird die zugrunde liegende Systemarchitektur direkt angegriffen – entweder über Fehler in der Software (Exploits) oder über mutwillig eingebrachte Hintertüren (Backdoors). Sind die Systeme selbst angegriffen, so kann dies anhand des Verhaltens der Angreifer, zum Beispiel mithilfe von Host-Intrusion-Prevention-Systemen (HIPS) oder Network-Intrusion-Prevention-Systemen (NIPS), erkannt werden. Zusätzlich sollte ein vorausschauendes Patch-Management stattfinden.

Im Vorweg lassen sich solche Fehler in Kliniksystemen durch Sicherheitsanalysen, wie Code Reviews, Sicherheitsscans und Pentests, ermitteln. Unterstützt wird eine solche Live-Analyse durch ein übergreifendes Logging, zum Beispiel mit Splunk, welches idealerweise in einem SIEM zusammengeführt wird und frühzeitig zu entsprechenden Alarmen führt.

Wir unterstützen Sie darin, das für Ihr Klinikum geeignete Sicherheitssystem zu implementieren und dieses mit bereits vorhandenen Dienstleisterverträgen, komplexen Systemarchitekturen entlang verschiedenster Verantwortlichkeiten sowie Schnittstellen in Einklang zu bringen. ■

Mehr dazu hier

CONSIST
Business Information Technology

Wenn Sie mehr zum Sicherheitsmanagement wissen möchten, kontaktieren Sie Florian Baitz/Consist unter:

Florian Baitz
PORTFOLIO MANAGER IT SECURITY
Telefon: +49 (0)431 3993-567
Mobil: +49 (0)173 2836-768
E-Mail: baitz@consist.de

Laden Sie sich das **Whitepaper** zum Thema SIEM herunter:
consist.de/siem-info