Controlware Cyber Defense Services

IDEALER SCHUTZ FÜR KRANKENHÄUSER UND MEDIZINISCHE EINRICHTUNGEN

Cyberangriffe stellen eine der größten Bedrohungen für Krankenhäuser und damit für die medizinische Versorgung dar. Lag bisher der Fokus auf präventiven Schutzmaßnahmen, liegt dieser heute auf der Detektion und Bewertung von Angriffen. Bereits das Erkennen von Cyberangriffen ist für IT-Abteilungen intern kaum noch zu leisten. Hinzu kommt, dass es – neben dem Einsatz geeigneter Detektionslösungen – essenziell ist, den Kontext eines Angriffs zu verstehen, um angemessen reagieren zu können.

Controlware bietet umfangreiche, modulare Cyber Defense Services und unterstützt Krankenhäuser aktiv bei der Bewältigung von Cyberangriffen. Auf Basis dieser Services lassen sich die Herausforderungen des IT-Betriebs von medizinischen Versorgungseinrichtungen erfolgreich adressieren:

- Wie lässt sich Risikotransparenz erreichen?
- Wie können moderne, gezielte Angriffsszenarien erkannt werden?
- Wie können Korrelationen über Ereignisse oder Ereignisketten hergestellt werden?
- Wer unterstützt mit verständlichen und umsetzbaren Anleitungen zur Risikobehandlung?
- Wie lässt sich überprüfen, ob durchgeführte Maßnahmen erfolgreich waren?

DIE MODULAREN CONTROLWARE CYBER DEFENSE SERVICES

Mit den Controlware Cyber Defense Services lassen sich Cybergefahren, Schwachstellen und Anomalien erkennen – ergänzt durch Dienstleistungen zur Analyse, Bewertung und Priorisierung von Security Incidents. Ein besonderer Schwerpunkt liegt unter anderem auf der ständigen Beobachtung der weltweiten aktuellen Bedrohungslage, um Angriffsmuster zu verstehen und die Detektionsmechanismen kontinuierlich darauf anzupassen.

VULNERABILITY MANAGEMENT SERVICE (VMS)

Im Rahmen des VMS-Moduls wird eine Plattform zur Identifizierung und Inventarisierung von Assets sowie zur Erkennung und Nachverfolgung von Schwachstellen innerhalb der IT-Infrastruktur bereitgestellt und betrieben. Alle erkannten Schwachstellen werden priorisiert dargestellt und mit Handlungsempfehlungen versehen.

ADVANCED LOG ANALYSIS (ALA)

Die vom ALA-Modul zur Sammlung und Auswertung von Log-Daten bereitgestellte Plattform dient der Erkennung Security-relevanter Ereignisse. Über spezielle, von Controlware entwickelte Use Cases ist es möglich, Angreifer-Verhalten und eingesetzte Techniken in den unterschiedlichen Phasen eines Angriffs sicher zu erkennen. Darüber hinaus erfolgt eine Bewertung von Security Incidents im kundenspezifischen Kontext. Gleichzeitig werden regulatorische Anforderungen nach Sammlung und strukturierter Auswertung von Log-Daten – sogenannte SIEM-Lösungen – erfüllt. Wichtig – alle Daten verbleiben grundsätzlich beim Kunden. Die Verarbeitung erfolgt im Rahmen der EU-Datenschutz-Bestimmungen.

ADVANCED THREAT DETECTION (ATD)

Im Rahmen des ATD-Moduls wird eine Plattform zur Erkennung von Anomalien im Netzwerk-Datenverkehr, im Benutzerverhalten oder in E-Mails bereitgestellt und betrieben.

ENDPOINT DETECTION & RESPONSE (EDR)

Mit der EDR-Lösung zur Anomalie-Erkennung am Endpoint lassen sich neben dem unmittelbaren Schutz vor Cyberangriffen auch Hinweise auf Cyber-Security-relevante Vorgänge und Ereignisse feststellen und analysieren.

ANALYSE UND REAKTION – „SOC AS A SERVICE"

Die Cyber Security-Analysten im ISO 27001-zertifizierten Cyber Defense Center von Controlware – am Standort Deutschland – analysieren, bewerten und priorisieren die Risiken. Anschließend werden konkrete Handlungsempfehlungen gegeben und die Kunden bei der Beseitigung der Cybergefahren und -risiken aktiv unterstützt. Controlware ist als Systemintegrator und IT-Dienstleister damit der ideale Partner – mit langjähriger Praxiserfahrung und tief greifendem Know-how. ■

Mehr dazu hier

Controlware GmbH
Waldstraße 92 | 63128 Dietzenbach
Tel. +49 6074 858-00
managedservices@controlware.de
www.controlware.de
blog.controlware.de

controlware