Erkennung von Cyberangriffen beim Betrieb Kritischer Infrastrukturen in der stationären Gesundheitsversorgung: Aufbau einer Testumgebung

Simon Weber, Stefan Stein, Prof. Dr. Michael Pilgermann, Prof. Dr. Thomas Schrader
Technische Hochschule Brandenburg

Motivation

Die zunehmende Vernetzung von (smarten) medizinischen Geräten führt zu neuen sicherheitstechnischen Herausforderungen für den stationären Gesundheitsbereich. Die Gesundheitsbranche war 2018 weltweit am zweithäufigsten von Cyberangriffen betroffen[1,2]. Um dieser verschärften Bedrohungslage zu begegnen, hat der Gesetzgeber mit dem IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) die Anforderungen an die IT-Sicherheit von Kritischen Infrastrukturen in Deutschland verschärft. Zukünftig werden u.a. Systeme zur Angriffsdetektion gefordert, die dem Stand der Technik entsprechen. Für weit verbreitete IT-Systeme (z.B. sog. Office-IT) sind Intrusion Detection Systeme (IDS) und Security Information and Event Management (SIEM) Systeme seit Jahren im Einsatz, so dass eine Übertragbarkeit auf die Anforderungen solcher Systeme auch in Kliniken möglich und sinnvoll erscheint. Die Überwachung von netzwerkfähiger Medizintechnik hingegen stellt gerade auf Grund ihrer Heterogenität, der langen Lebensdauer der Mehrheit der Geräte und problematischem Patchmanagement ein wenig beachtetes und gleichzeitig potentiell anfälliges Feld dar[3].

virtuelles Krankenhaus

An der TH Brandenburg wird derzeit ein digitaler Zwilling eines Krankenhauses aufgebaut. Ziel ist es, mit diesem Zwilling realitätsnahe Angriffs- und Detektionsszenarien zu entwickeln, die in einem echten Krankenhaus im laufenden Betrieb nicht umsetzbar wären. Die Testumgebung besteht aus drei Bereichen: Der erste Bereich umfasst das virtuelle Krankenhaus, an das netzwerkfähige Medizintechnik angebunden ist. Die Kernkomponente dieses Bereichs bildet das Open Source Krankenhausinformationssystem (KIS) myCare2.x. Daran werden ein Digital Imaging and Communications in Medicine (DICOM) Server und ein MIRTH Kommunikationsserver für das Health Level 7 (HL7) Protokoll angeschlossen. Zusätzliche Informationssysteme für die Labor- und Radiologieumgebung (LIS/RIS) bieten die Möglichkeit, medizinische Geräte dieser Fachbereiche in die Testumgebung einzubinden.

KH- und TI-Anbindung

Im zweiten Bereich befindet sich die Anbindung an die Partnerkrankenhäuser sowie die Telematikinfrastruktur (TI). Hier sind zusätzlich digitale Gesundheitsanwendungen eingebunden, die sich teilweise noch vor der Marktreife und noch in der Entwicklung befinden. Diese Anbindung wird über einen TI-Konnektor hergestellt, damit die Nutzung digitaler Anwendungen wie beispielsweise die elektronische Patientenakte oder das e-Rezept simuliert werden können. Es ist somit eine Simulation der Informationskette vom Patienten über die Verarbeitung beim Arzt bis hin zum persönlichen Speicherort möglich.

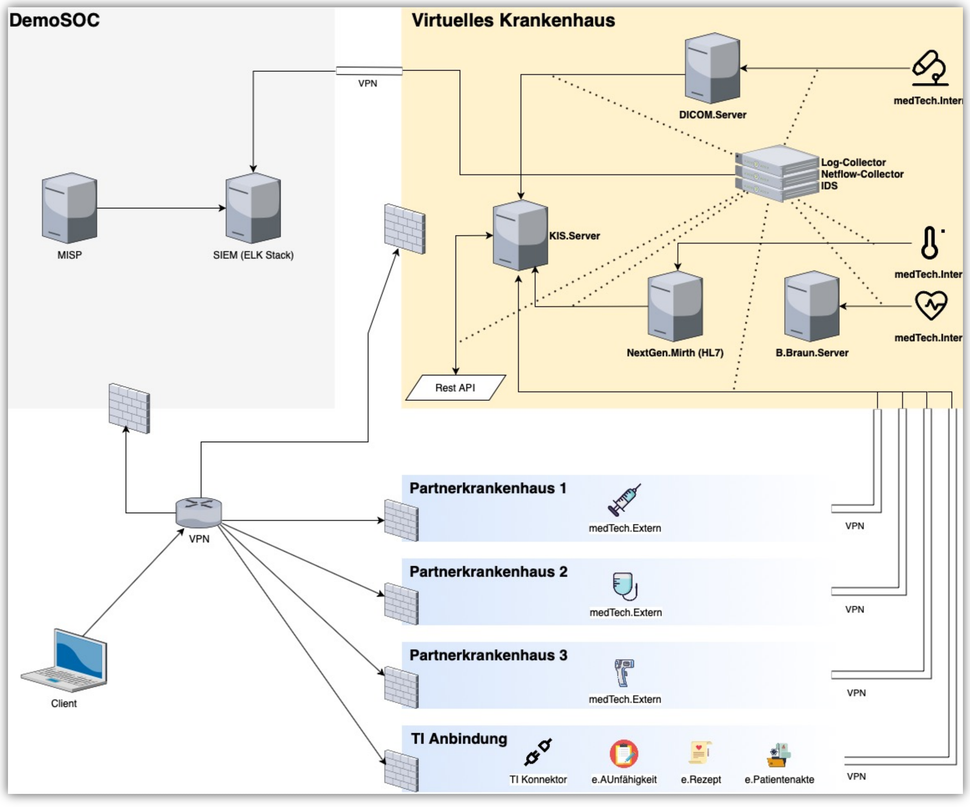

Abbildung: Die Netzstruktur des SOC4Hosp Testumgebung

DemoSOC

Das Security Operations Center (SOC), in dem Logs und Alerts zentral zusammengeführt und ausgewertet werden können, bildet den dritten Bereich. Das SOC besteht zentral aus einem SIEM System und wird dezentral durch Client- und Netzwerküberwachungssysteme (IDS-Protokolle, Systemprotokolle u.ä.) erweitert. Als SIEM System wird die Open Source Software Elastic Search in Verbindung mit Kibana (ELK-Stack) genutzt[4]. Als IDS kommt die Open Source Software Snort zum Einsatz[5]. Für die strukturierte Entwicklung der Angriffs-Szenarien wird das MITRE ATT&CK Framework eingesetzt[6]. Teil der Vision ist ebenfalls eine Threat Intelligence Plattform (TIP), die auf die Bedürfnisse des Gesundheitssektors zugeschnitten ist. Dafür wurde die Open Source Plattform MISP (Malware Information Sharing Platform[7]) in die Testumgebung integriert. Alle Bereiche werden derzeit modular geplant, so dass einzelne Komponenten durch alternative Systeme mit einem äquivalenten Funktionsumfang ausgetauscht werden können, um die heterogene Toollandschaft des Gesundheitssektors in Deutschland und weltweit besser abbilden zu können.

Diskussion

Angriffssimulationen im Forschungskontext auf bestehende Krankenhausnetzwerke sind aufgrund der möglichen realen Auswirkungen auf Patienten nicht durchführbar. Durch diesen realitätsgetreuen Nachbau eines Krankenhauses soll zukünftig ein möglichst realistischer Krankenhaus-Netzwerkverkehr simuliert werden können, an dem die IT-Sicherheit von Krankenhäusern näher erforscht werden kann. Dieses Vorgehen soll Aufschluss über potentielle Risiken und zu erwartende Auswirkungen auf den täglichen Betrieb geben. Zur Sicherstellung der Realitätsnähe kooperiert die Forschungsgruppe mit mehreren großen deutschen Krankenhäusern, von denen sich drei zur aktiven Einbringung und Mitgestaltung verpflichtet haben.

Referenzen

1. Die Lage der IT-Sicherheit in Deutschland 2020. BSI. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.html?nn=132646
2. Cyberangriffe im Gesundheitswesen weit verbreitet . www.service-medical.de. 2021. Verfügbar unter: https://www.service-medical.de/cyberangriffe-im-gesundheitswesen/
3. Thamilarasu G, Odesile A, Hoang A. An Intrusion Detection System for Internet of Medical Things
4. Die Kernprodukte des Elastic Stack. Verfügbar unter: https://www.elastic.co/de/elastic-stack/
5. Network Intrusion Detection & Prevention System – Snort. Verfügbar unter: https://www.snort.org
6. Matrix - Enterprise | MITRE ATT&CK®. Verfügbar unter: https://attack.mitre.org/matrices/enterprise/
7. The MISP Threat Sharing project. Verfügbar unter: https://www.misp-project.org