
KHZG – FÖRDERTATBESTAND 10: IT-SICHERHEIT DIGITALISIERUNG IM HEALTHCARE-BEREICH SICHER GESTALTEN MIT WALLIX IDENTITY & ACCESS SECURITY LÖSUNGEN

Zielsetzung

Ziel dieses Fördertatbestandes ist es, die IT- bzw. Cybersicherheit in Krankenhäusern, die nicht zu den kritischen Infrastrukturen gehören, sowie in Hochschulkliniken zu verbessern. Entsprechende Maßnahmen sind bisher von der Förderung durch den Krankenhausstrukturfonds ausgeschlossen. Durch die zunehmende Digitalisierung und die damit verbundenen Prozesse sollen deshalb auch Krankenhäuser, die nicht zur kritischen Infrastruktur nach dem BSI-Gesetz (BSI-KritisV-Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) gehören, berücksichtigt werden.

Um Patientinnen und Patienten optimal zu versorgen und den Krankenhausbetrieb gleichzeitig effizient zu gestalten, sind teilweise hochkomplexe IT-Systeme nötig und nicht mehr wegzudenken. Mit immer mehr unterschiedlichen, miteinander vernetzten Systemen und Komponenten steigen auch die Risiken, die durch Systemausfälle oder -beeinträchtigungen entstehen können. Zeitgleich werden die Angriffsflächen der IT- und Internettechnologien zunehmend vielfältiger und deutlich größer. Geeignete Maßnahmen zur Steigerung der Cybersicherheit müssen dem entgegenwirken. Die von Herstellern bzw. Systemanbietern bereitgestellten Information für eine sichere Konfiguration bzw. notwendige ergänzende Maßnahmen im Netzwerk sollten beachtet werden.

Dabei sind sichere IT-Systeme und die damit verarbeiteten Informationen in der Gesundheitsversorgung von höchster Bedeutung. Die störungsfreie **Verfügbarkeit, Integrität und Vertraulichkeit der IT-Systeme**, Komponenten und Prozesse muss sichergestellt sein. Gleiches gilt auch für die **Authentizität der Informationen**. Nur so können die Patientensicherheit und eine effektive Behandlung sowie die Funktionsfähigkeit des Krankenhauses aufrechterhalten und geschützt werden.

Für die fortschreitende Digitalisierung in den Kliniken ist Cybersicherheit dringend nötig. Ein geeignetes Managementsystem zur Informationssicherheit nach ISO 27001 nativ oder BSI IT-Grundschutz kann dies steuern und überwachen. Insbesondere die Umsetzung des Branchenspezifischen Sicherheitsstandards (B3S) für die Gesundheitsversorgung im Krankenhaus kann dies vollständig gewährleisten.

Die im Folgenden skizzierten Anforderungen des KHZG und die darin beispielhaft genannten Sicherheitssysteme sind nicht ausschließlich einem der Bereiche Prävention, Detektion, Mitigation, Response oder Awareness zuzuordnen. So kann eine einzelne Anwendung mehrere Bereiche abdecken.

ANFORDERUNGEN (MUSS)

IHR VORHABEN ZUR VERBESSERUNG DER IT- BZW. CYBERSICHERHEIT WIDMET SICH EINEM DER FOLGENDEN ZIELE ODER EINER KOMBINATION DAVON:

Prävention

vor Informationssicherheits-Vorfällen (u. a. Systeme zur Zonierung von Netzwerken, Next Generation Firewalls, sichere Authentisierungssysteme, MicroVirtualisierung /Sandbox-Systeme, Schnittstellen-Kontrolle, Intrusion Prevention Systeme; Network Access Control, Schwachstellenscanner, Software-versionsmanagement, Datenschleusen, Datendiode, VPN-Systeme, verschlüsselte Datenübertragung, verschlüsselte mobile Datenträger, ISMS).

oder Detektion

von Informationssicherheits-Vorfällen (u. a. Security Operation Center, Log Management Systeme, Security Information Event Management Systeme, Intrusion Detection Systeme, lokaler Schadsoftwareschutz mit zentraler Steuerung, Schadsoftwareschutz in Mailsystemen bzw. bei Mailtransport).

oder Mitigation

von Informationssicherheits-Vorfällen (u. a. automatisierte BackupSysteme, lokaler Schadsoftwareschutz mit zentraler Steuerung).

oder Awareness

Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen bzw. der Bedeutung von IT-/Cybersicherheit (u. a. regelmäßige Risikoanalysen, Schulungsmaßnahmen, Informationskampagnen, Awareness-Messungen).

WALLIX Identity & Access Security Lösungen

WALLIX Identity & Access Security Lösungen sind für den Einsatz im Bereich der elektronischen Datenverarbeitung in Krankenhäusern prädestiniert, um die Anforderungen an eine moderne IT-Sicherheitsinfrastruktur zu erfüllen.

WALLIX Identity & Access Security Lösungen sind bereits im KRITIS Umfeld etabliert, weil unterschiedlichste Anforderungen (Controls) der ISO 27001 bzw. des entsprechenden B3S-Dokuments an die IT-Sicherheit durch den Einsatz dieser Lösungen effektiv erfüllt werden. An erster Stelle sind hier die Compliance-Anforderungen für einen dedizierten Genehmigungsworkflow, die Nachvollziehbarkeit aller Aktivitäten von Dienstleistern und internen Administratoren auf kritischen Systemen, sowie die revisions-sichere Speicherung dieser Daten in verschlüsselter Form zu erwähnen.

Des Weiteren muss gemäß B3S klar unterscheidbar sein, welche Arbeiten auf diesen kritischen Systemen von internen Mitarbeitern und welche von externen Mitarbeitern oder Dienstleistern ausgeführt wurden. Die bei diesen Arbeiten anfallenden Log-Informationen dürfen dabei unabhängig von den Zugriffsrechten des Benutzers z.B. im Verzeichnisdienst nicht manipulierbar sein.

WALLIX IDENTITY & ACCESS SECURITY LÖSUNGEN UNTERSTÜTZEN DABEI DIE ETABLIERUNG EINES GEREGETEN ROLLENKONZEPTE, INDEM ZU JEDER ZEIT NACHVOLLZIEHBAR UND KONTROLLIERBAR IST, WELCHE ANWENDERROLLE DER LÖSUNG WELCHE AKTIONEN VORGENOMMEN HAT.

Dabei unterscheidet WALLIX zwischen vier Anwenderrollen:

- 1. Benutzer (User)**, der auf den für ihn berechtigten Zielsystemen (z.B. Server, Anwendungen, Datenbanken, Netzwerkkomponenten, etc.) administrative Tätigkeiten ausübt.
- 2. Genehmiger (Approver)**, der die Zugänge, für die ein Genehmigungsprozess definiert wurde, genehmigen oder ablehnen kann.
- 3. Auditor**, der laufende und aufgezeichnete Sitzungsdaten einsehen kann. Diese Rolle hat ebenfalls die Möglichkeit, sich über ein Vier-Augen/Vier-Hände-Prinzip aktiv mit auf eine bestehende Sitzung aufzuschalten
- 4. PAM-Administrator**, der die PAM-Software administriert, d.h. Benutzer, Zielsysteme und Regelwerke verwaltet.

In Bezug auf das KHZG – Fördertatbestand 10 – IT-Sicherheit, bieten WALLIX Identity & Access Security Lösungen in den Bereichen Prävention, Detektion, Mitigation und Awareness folgende dedizierte Leistungen:

Prävention:

Im Bereich Prävention sind WALLIX Identity & Access Security Lösungen exemplarisch für die Absicherung folgender Funktionalitäten einsetzbar:

Sichere Authentisierungssysteme: WALLIX Identity & Access Security Lösungen bieten im Bereich sichere Authentisierungssysteme folgende Vorteile: Zum eine ist es nicht notwendig, einen externen Mitarbeiter mit einem privilegierten Konto an der Systemlandschaft anzumelden. Hier ist entweder ein lokales Konto auf der Access Security Lösung oder ein nicht-privilegiertes Konto im Verzeichnisdienst - ausreichend. In diesem Zusammenhang kann einem derartigen Konto eine Autorisierung für einen privilegierten Zugang zu einem Zielsystem (z.B. Server, Anwendungen, Datenbanken, Netzwerkkomponenten, etc.) gewährt werden.

Dabei kann zusätzlich ein Genehmigungsworkflow etabliert werden, der gewährleistet, dass externe Zugänge nicht zu jedem beliebigen Zeitpunkt genutzt werden können. Hier wird explizit revisionssicher protokolliert, wer diesen Zugriff genehmigt hat. Der Zugriff auf das Zielsystem kann dabei so gestaltet werden, dass der User die verwendeten Zugangsdaten (z.B. Passwörter, SSH-Keys, Zertifikate) nicht kennt oder einsehen kann, da diese in einem sicheren digitalen Tresor abgelegt sind. Zugangsdaten können regelmäßig - je nach Compliance-Vorgabe - automatisiert geändert oder rotiert werden.

Netzwerkperimeter können dadurch erheblich sicherer konfiguriert werden (angreifbare Fernzugriffsschnittstellen können durch die WALLIX Identity & Access Security Lösung vollständig ersetzt werden).

Zusammenfassung: Präventiv wird also ein dedizierter Zugang über jeweils nur einen Weg in das Unternehmen festgelegt. Es ist sichergestellt, dass jeder Zugriff genehmigt, nachvollziehbar dokumentiert und lückenlos aufgezeichnet wird. Zugangsdaten werden effektiv geschützt und bleiben den Benutzern verborgen. Herkömmliche Zugriffsverfahren können somit teilweise oder vollständig abgeschafft werden.

Detektion:

Im Bereich Detektion sind WALLIX Identity & Access Security Lösungen exemplarisch für die Absicherung folgender Funktionalitäten einsetzbar:

Alle in WALLIX Identity & Access Security Lösungen konfigurierten Einstellungen bezüglich Sicherheit, Genehmigungsverfahren, Systemereignissen, Richtlinienverstößen sowie sämtliche durchgeführten Aktionen auf kritischen Zielsystemen (z.B. Server, Anwendungen, Datenbanken, Netzwerkkomponenten, etc.) werden protokolliert und können für die Generierung von Alarmen, Analysen und Auswertungen an ein beliebiges SIEM System (z.B. Splunk, LogPoint, QRadar, etc.) übermittelt werden.

So ist es möglich, Verstöße gegen Sicherheitsrichtlinien aktiv zu verfolgen, vorzusehen oder im Nachgang nachzuvollziehen. Des Weiteren bieten die internen Funktionen der WALLIX Identity & Access Security Lösungen auch eine umfassende Kontrolle und Nachvollziehbarkeit sämtlicher Tätigkeiten innerhalb von Sitzungen an. Diese können live überwacht oder per Videoaufzeichnung und Log-Analyse auditiert werden.

In Verbindung mit EPM (Endpoint Privilege Management) ist es zudem möglich, einzelne Prozesse auf Serversystemen exakt zu steuern und diese in unterschiedlichen Berechtigungsstufen auszuführen. Dabei können z.B. unternehmenseigene Applikationen (durch Auswertung der Hashwerte) in eine White List überführt werden. Die Ausführung nichtautorisierter Software und Systemprozesse - und damit auch die Ausführung von Schadcode - wird somit verhindert. Auf Serversystemen kann zudem der Zugriff durch nicht-autorisierte Software oder Schadcode auf die Verschlüsselungsbibliotheken des Betriebssystems vollständig unterbunden werden. Ransomware (Verschlüsselungstrojaner) wird somit effektiv daran gehindert, schadhafte Prozesse auszuführen.

Diese Funktionalität ist auch für Endgeräte (z.B. PCs, Notebooks, Tablets) verfügbar. Die Endgeräte werden proaktiv gehärtet und Zugriffe auf die Verschlüsselungsbibliothek zuverlässig detektiert und gestoppt.

Zusammenfassung: Im Zusammenspiel mit einem SIEM-System ist ein effektives Alarming bei Verstößen gegen Sicherheitsrichtlinien einfach zu konfigurieren. Verstöße können zudem während eines aktiven Session Monitorings (Beobachtung) gestoppt und über EPM die Ausführung von Schadcode verhindert werden. Zugriffe auf die Verschlüsselungsbibliotheken der Betriebssysteme werden detektiert und sicher unterbunden.

Mitigation:

Im Bereich Mitigation sind WALLIX Identity & Access Security Lösungen exemplarisch für die Absicherung folgender Funktionalitäten einsetzbar:

Wie im Bereich Detektion bereits festgestellt, kann durch Einsatz der WALLIX Identity & Access Security Lösungen (Privilege Access Management und Endpoint Privilege Management) die Ausführung unerwünschter Aktionen und Prozesse, wie z.B. die Ausführung von Schadcode proaktiv unterbunden werden.

Zusätzlich zu den Mechanismen von EPM bietet WALLIX mit der patentierten Technologie „Session Probe“ (temporärer Agent auf dem Zielsystem) die Möglichkeit, bei Fernzugriffen bestimmte Aktionen zu unterbinden (z.B. die nicht-autorisierte Nutzung als Jump host) oder den Zugriff auf weitere Netzwerksegmente zu unterbinden. Somit kann ein Zugriff auf personenbezogene Daten auf anderen kritischen Systemen des Unternehmens verhindert werden.

Die Möglichkeiten zur Unterbindung schadhafter Prozesse wurden bereits im Punkt Detektion erörtert. Die Funktionalitäten überschneiden sich hier in den aufgeführten Anforderungsbereichen.

Awareness:

Im Bereich Awareness sind WALLIX Identity & Access Security Lösungen exemplarisch für die Unterstützung folgender Szenarien einsetzbar:

Durch Einsatz der WALLIX Identity & Access Security Lösungen findet im Allgemeinen ein den Benutzer unterstützender Prozess statt. Security Awareness ist im Rahmen von Mitarbeiterschulungen ein tragender Pfeiler. Allerdings sind die Methoden von Angreifern mittlerweile sehr gut getarnt.

Gefälschte E-Mails mit Schadsoftware im Anhang (z.B. Makroviren) sind oftmals im Kontext von echten E-Mails nicht mehr zu unterscheiden. Ist der anhängende Virus noch sehr neu, so ist es möglich, dass herkömmliche Antimalware-Lösungen den Schadcode nicht erkennen (Zero Day Exploit). Durch diese Erfahrung bleibt bei vielen Nutzern die Angst vor falschem Verhalten und der unfreiwilligen Auslösung eines Sicherheitsvorfalls.

Durch den Einsatz einer EPM-Lösung kann dem Benutzer in diesem Zusammenhang eine gewisse Sicherheit zurückgegeben werden.