kma
Klinik Management aktuell

www.kma-online.de • 19 Euro
24. Jahrgang • Oktober 2019

HOSPITALS FOR FUTURE

Die Jugend setzt sich für den Klimaschutz ein.
Krankenhäuser können das auch.

IT-SICHERHEIT IM KRANKENHAUS

Ohne Cybersicherheit gelingt keine nachhaltige Digitalisierung

IMPRESSUM

Redaktion Berlin

Georg Thieme Verlag KG
redaktion-kma@thieme.de
www.kma-online.de

Gestaltung und Umsetzung Berlin

Georg Thieme Verlag KG

Foto: kma Montage (AdobeStock / beeboys)

Thieme

IT-SICHERHEIT IM KRANKENHAUS

Ohne Cybersicherheit gelingt keine nachhaltige Digitalisierung

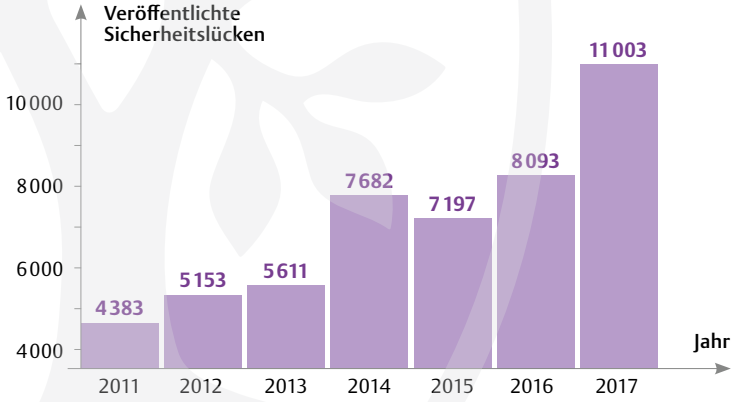
Krankenhäuser werden auch in der Zukunft eine wichtige Rolle im Gesundheitswesen spielen. Durch die zunehmende Digitalisierung verändern sich die Prozesse und Möglichkeiten für alle Beteiligten in den Krankenhäusern. Dadurch werden immer mehr IT-Sicherheits- und Vertrauensmaßnahmen notwendig, um einen stabilen Betrieb garantieren zu können.

Informationstechnik und das Internet sind Motor und Basis für das Wohlergehen der modernen und globalen Informations- und Wissensgesellschaft. Dies gilt auch für das Gesundheitswesen insgesamt und für Krankenhäuser insbesondere. Immer mehr IT-Innovationen werden dazu beitragen, eine flächendeckende und hochwertige Gesundheitsvorsorge umzusetzen.

Klar ist aber auch, dass seit Beginn des IT- und Internetzeitalters die Probleme im Bereich der Cybersicherheit jedes Jahr größer und nicht kleiner werden. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen der genutzten Systeme wie etwa Endgeräte, Server oder Netzkomponenten nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern standzuhalten. Täglich berichten Medien, wie sich kriminelle Hacker die unzureichende Qualität der Software für erfolgreiche Angriffe zu Nutze machen, Malware installieren, Passwörter sowie Identitäten stehlen, mit Fake News die Menschen beeinflussen und IT-Systeme ausspionieren. Eine angemessene, sichere und vertrauenswürdige IT zu erreichen, ist für die erfolgreiche Zukunft der Informations- und Wissensgesellschaft entscheidend. Letztlich muss die voranschreitende Digitalisierung auch die Nachhaltigkeit als strategisches Ziel haben.

Starker Anstieg der Sicherheitslücken

Mit zunehmender Komplexität nehmen die Fehler im Programmcode zu.



Quelle: Hasso Platner Institut (HPI) / Stand 01/2018

Das gelingt nur, wenn die IT-Technologien- und -Services sicher und vertrauenswürdig aufgebaut sind und sicher betrieben werden.

Die Gesundheitsbranche ist im Wandel. Neue Schwerpunkte entstehen wie zum Beispiel:

- Die Politik fordert virtuelle Krankenhäuser.
- Patienten wollen zunehmend selbstbestimmter sein. Digitale Technologien wie SmartWatches helfen ihnen dabei.
- Immer mehr sensible Daten werden erhoben, auch im Kontext privatwirtschaftlich handelnder Unternehmen.
- Die elektronische Patientenakte soll für alle und überall verfügbar sein.
- Die Patienten-Selbstbehandlung soll erweitert werden.
- Die Online-Interaktion wird zunehmend wichtiger.
- Ergebnistransparenz und Entscheidungsunterstützung werden immer wichtiger.

Dazu werden neue Technologien, wie künstliche Intelligenz (KI), Mobilfunk der fünften Generation (5G), Blockchain und weitere verwendet.

Die Folge: Cybersicherheitsvorfälle häufen sich. Hier einige Beispiele:

- Patienten erhalten schädliche Strahlendosen durch defekte Strahlenbeschleuniger.
- Insulinpumpen können über das Netz manipuliert werden.
- Hunderttausende Herzschrittmacher weisen Sicherheitslücken auf.
- Angriffe mit Ransomware führen dazu, dass die gesamte IT eines Krankenhauses nicht mehr genutzt werden kann.

Die Auswirkungen von Cybersicherheitsvorfällen haben sich verändert und eine größere Bedeutung bekommen:

- Hacker haben Daten von 4,5 Millionen Patienten in den USA gestohlen.
- Ein Krankenhaus in den USA musste wegen eines Datenverlusts 5,5 Millionen US-Dollar Strafe bezahlen.
- Der frühere US-Vize Cheney fürchtete sich vor einem Anschlag auf seinen Herzschrittmacher.
- Eine Ransomware-Attacke im Lukaskrankenhaus in Neuss verursachte eine Million Euro Schaden.

Cybersicherheitsbedürfnisse

1. **Gewährleistung der Vertraulichkeit**
   Damit keine unautorisierten Personen oder Organisationen in der Lage sind, übertragene oder gespeicherte Informationen zu lesen.
2. **Gewährleistung der Authentifikation**
   Mit Hilfe des Cybersicherheitsmechanismus' „Authentifikation" wird verifiziert, wer der Partner bei der Kommunikation oder Transaktion ist beziehungsweise welcher Nutzer auf Betriebsmittel und Informationen zugreift.
3. **Gewährleistung der Authentizität**
   Mit Hilfe des Cybersicherheitsmechanismus Authentizität wird verifiziert, dass Informationen oder Identitäten echt sind.
4. **Gewährleistung der Integrität**
   Beim Cybersicherheitsbedürfnis „Gewährleistung der Integrität" wird überprüft, ob Informationen, die übertragen werden oder gespeichert sind, unverändert, das heißt original, sind.
5. **Gewährleistung der Verbindlichkeit**
   Das Cybersicherheitsbedürfnis „Gewährleistung der Verbindlichkeit" sorgt für die Gewissheit, dass die Prozesse und die damit verbundenen Aktionen auch verbindlich sind.
6. **Gewährleistung der Verfügbarkeit**
   Dieses Cybersicherheitsbedürfnis sorgt für die Gewissheit, dass die Informationen und Dienste auch zur Verfügung stehen.
7. **Gewährleistung der Anonymisierung / Pseudomisierung**
   Damit wird gewährleistet, dass eine Person nicht oder nicht unmittelbar identifiziert werden kann.

Cybersicherheitsprobleme

Die Angriffsflächen der IT- und Internet-Technologie werden durch komplexere Software-Systeme und kompliziertere Zusammenhänge zwischen Protokollen, Diensten und globalen Infrastrukturen vielfältiger und deutlich größer. Dadurch werden auch die Angriffe verteilter, raffinierter und professioneller ausgeführt. Bei der kritischen Beurteilung der aktuellen Cybersicherheitssituation fallen einige, sehr unterschiedliche Sicherheitsprobleme besonders deutlich auf. Diese müssen gelöst werden, um mehr notwendige IT-Sicherheit und Vertrauenswürdigkeit aufzubauen.

Im Folgenden werden exemplarisch einige wichtige Cybersicherheitsprobleme aufgezeigt, die sehr unterschiedlich sind:

Zu viele Schwachstellen in Software

Ein großes Cybersicherheitsproblem besteht darin, dass in der aktuell genutzten Software aller IT-Systeme wie etwa Smartphone, Notebook, PC, Server oder IoT-Geräte (IoT, Internet of Things) zu viele Schwachstellen vorhanden sind. Die Software-Qualität der Betriebssysteme und Anwendungen ist für die heutige Bedrohungslage nicht mehr ausreichend. Die Fehlerdichte – die Anzahl der Softwarefehler pro 1 000 Zeilen Code – liegt bei qualitativ hochwertiger Software heute im Schnitt bei 0,3. Da gängige Betriebssysteme und größere Anwendungen mehr als zehn Millionen Zeilen Code haben, sind hier im Schnitt 3 000 Software-Fehler zu finden. Aus diesem Grund ist qualitativ schlechte Software eine besondere Herausforderung und sorgt dafür, dass zu viele IT-Systeme mit Malware (Schadsoftware) infiziert sind oder direkt angegriffen werden können.

Ungenügender Schutz vor Malware

Malware ist der Oberbegriff für Schadsoftware wie Viren, Würmer oder trojanische Pferde. Angreifer nutzen

Software-Schwachstellen und menschliche Unzulänglichkeiten aus, um Malware auf IT-Systemen zu installieren. Malware wird hauptsächlich über E-Mail-Anhänge oder unsichere Webseiten mit Hilfe von sogenannten Drive-by-Downloads unbemerkt in IT-Systeme eingeschleust.

Ein Botnetz ist eine Gruppe von IT-Systemen, die unter zentraler Kontrolle eines Angreifers stehen und von ihm für Angriffe genutzt werden. Dadurch können Angreifer Informationen von IT-Systemen mit Hilfe so genannter Keylogger, die alle Eingaben auf der Tastatur protokollieren, und Trojanern, auslesen, um IT-Systeme für die Massenversendung von Spam und verteilte (DDoS-) Angriffe nutzen, sowie mit Ransomware Daten verschlüsseln und Lösegeld für die Entschlüsselung verlangen. Mit Ransomware verschlüsselte IT-Systeme können nicht mehr genutzt werden. Nur wenn es aktuelle Backups gibt, kann mit einem hohen Aufwand der Betrieb wieder hergestellt werden.

Das Lukas-Krankenhaus in Neuss hat am 10. Februar 2016 einen Ransomware-Angriff erlebt und musste mit den Folgen pragmatisch umgehen. Ursache war eine Erpressersoftware, die über einen infizierten E-Mail-Anhang eingeschleust und durch einen unachtsamen Mitarbeiter aktiviert wurde. Nach der Entdeckung musste das Krankenhaus alle IT-Systeme herunterfahren und improvisieren: Boten überbrachten Befunde persönlich, Operationen und andere Maßnahmen wurden verschoben. Das ganze Krankenhaus war im Ausnahmezustand und musste spontan wie früher die Arbeitsprozesse und Untersuchungen ohne IT-Unterstützung umsetzen. Das Krankenhaus hatte sich entschieden, den Erpressern kein Geld zu zahlen. Es hat mehr als eine Million Euro gekostet, um alle IT-System insgesamt wieder voll funktionsfähig zu bekommen.

Wichtig ist in diesem Zusammenhang die schwache Erkennungsleistung der Anti-Malware-Lösungen: Bei Massenangriffen erkennt die Software nur 75 bis 95 Prozent der eingesetzten Malware. Bei gezielten und direkten Angriffen auf ein IT-System liegt die Erkennungsrate im Schnitt sogar bei nur 27 Prozent. Diese Entwicklung verdeutlicht, dass Signatur-basierte Erkennungen bei gezielten Angriffen ihre Wirkung verlieren. Jeder Angriff erfolgt mit individuellen Signaturen, weshalb die Anti-Malware-Hersteller zuvor keine Signaturen erstellen und verteilen können. Die Konsequenz diese Vorgehens: Symantec, der weltgrößte Hersteller von Anti-Malware-Lösungen, erkennt nach eigenen Angaben nur noch 45 Prozent der Malware. Diese Zahl spiegelt sicherlich das neue Verhältnis zwischen gezielten und Massenangriffen wider.

Keine internationalen Lösungen für Identifikation und Authentifikation

Im Jahr 2019 werden immer noch Passwörter für die Authentifikation im Internet genutzt, da dieses Verfahren einfach umzusetzen ist. Die Probleme sind bekannt: Entweder werden schlechte, weil leicht zu knackende Passwörter verwendet oder gute, die aber so kompliziert sind, dass man sie sich nicht merken kann und sie deshalb für viele Anwendungen verwendet werden. Ein weiteres Risiko entsteht, wenn Passwörter im Klartext in E-Mails durch das Internet übertragen werden. Viele Internetnutzer fallen zudem auf Phishing-E-Mails herein, die Passwörter abgreifen. Auch das Abgreifen von Passwörtern mit Hilfe von Keyloggern ist eine Möglichkeit, die Sicherheit des Authentifikationsverfahrens „Passwort“ auszuhebeln. Obwohl es deutliche sichere Identifikations- und Authentifikationsverfahren gibt, werden diese leider und unverantwortlicher Weise nicht genutzt.

Unsichere IoT-Geräte

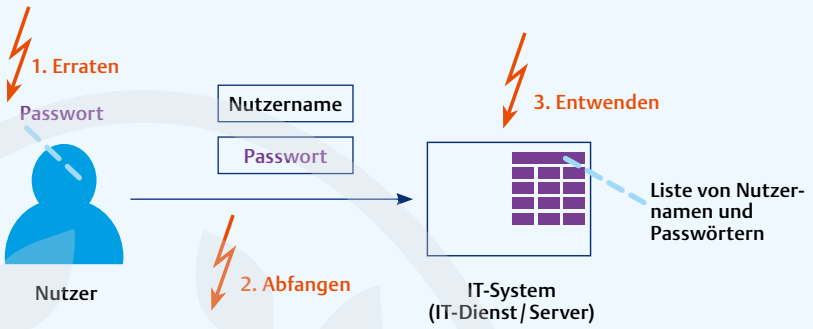
Die Hersteller von IoT-Geräten wie zum Beispiel Internet-Videokameras haben IT-Technologie zur Verfügung gestellt, die bei weitem nicht die Cybersicherheitsanforderungen erfüllen. Wenn einfache Internet-Videokameras gehackt werden können, ist das zuerst einmal ein Problem des Nutzers. Ein Angreifer kann dann zum Beispiel ein Wohnzimmer oder ein

Cybersicherheitsmechanismen

1. Personelle Maßnahmen:
   - Auswahl von Mitarbeitern, die für die Cybersicherheit verantwortlich sind
   - Sensibilisierung und Schulung der Mitarbeiter im Bereich der Cybersicherheit
2. Organisatorische Maßnahmen:
   - Verantwortlichkeiten und Befugnisse definieren
   - Schutzbedarfsanalyse erstellen
   - Erstellung von Cybersicherheitsrichtlinien und -Dienstanweisungen
   - Durchführung von Audits und Penetrationstest
3. Technische Maßnahmen:
   - Verschlüsselung für übertragene und gespeicherte Daten
   - Moderne risikobasierte und adaptive Multifaktor-Authentifizierung
   - Vertrauenswürdige IT-Systeme
   - Firewalls zur Reglementierung der grundsätzlichen Möglichkeiten
   - Update- und Patch-Management
   - Organisation und Umsetzung von Backups

Das Passwort als „Schlüssel zum Erfolg“

Wie Hacker ein Passwort erbeuten und das IT-System manipulieren.



Quelle: Dr. Norbert Pohlmann

Behandlungszimmer beobachten. Ein weit größeres Problem ist es, wenn Angreifer sehr viele Internet-Videokameras und weitere elektrische Geräte, die mit dem Internet verbunden sind, wie Drucker, Haarföne oder Kaffeemaschinen, unter ihre Kontrolle bringen, um die Infrastruktur des Internets erfolgreich durch eine Überlastung mittels DDoS-Attacken anzugreifen. Dies ist ein sehr großes Problem und macht das Internet sehr verletzlich und damit nicht verlässlich.

An dieser Stelle sind die IT-Hersteller gefordert. Sie müssen eine besondere Verantwortung übernehmen und nur noch sichere und vertrauenswürdige IT-Geräte im Internet zu Verfügung stellen, die den Stand der Technik im Bereich der Cybersicherheit berücksichtigen.

Mit Cybersicherheitsmechanismen den Krankenhausbetrieb schützen

Krankenhäuser haben unterschiedliche Cybersicherheitsbedürfnisse (siehe Kasten auf Seite 56). Diese beschreiben, mit welchen prinzipiellen Cybersicherheitsmechanismen welche Grundwerte der Cybersicherheit befriedigt werden können. Das heißt, die Krankenhäuser brauchen passende Cybersicherheitsmechanismen (siehe Kasten), um sich angemessen zu schützen und damit ihren eigentlichen Auftrag sicher und vertrauenswürdig umsetzen zu können. Durch die immer schneller werdende Digitalisierung werden auch immer mehr Cybersicherheitsmechanismen benötigt.

Einsatz von künstlicher Intelligenz

Cybersicherheitssysteme werden in der Zukunft verstärkt durch künstliche Intelligenz (KI) unterstützt. KI eignet sich deutlich besser zur Entdeckung intelligenter Hacker und deren Angriffe, um letztendlich Schäden zu vermeiden und Risiken im Digitalisierungsprozess zu minimieren. Wie KI die Cybersicherheit erhöhen kann, zeigen die nachfolgenden Beispiele:

1. **Erhöhung der Erkennungsrate von Angriffen**

Mit Hilfe von künstlicher Intelligenz können Angriffe über Netzwerke und in IT-Endgeräten besser erkannt werden. Dazu sind adaptive Modelle notwendig, die unabhängig und kontinuierlich neu lernen, weil sich auch das Verhalten der IT-Systeme und des Nutzers, aber auch die Angriffsstrategien, ständig ändern.

2. **Unterstützung der Cybersicherheitsexperten (von denen wir nicht genug haben)**

Nicht alle Ereignisse können durch Cybersicherheitsexperten verarbeitet werden, da die Anzahl der Ereignisse die Verarbeitungsfähigkeit und -kapazitäten menschlicher Analysten an ihre Grenzen bringen. Eine große Herausforderung für die Verteidiger besteht darin zu erkennen, für welche der sehr vielen sicherheitsrelevanten Ereignisse noch menschliche Analysten notwendig sind.

In Zukunft wird künstliche Intelligenz die vorhandenen sicherheitsrelevanten Daten analysieren und Handlungsempfehlungen für die Cybersicherheitsexperten geben, damit diese im Sinne von mehr Sicherheit optimal arbeiten können. Dadurch werden weniger Schäden auftreten.

Ein weiteres Feld, beim dem die künstliche Intelligenz die Cybersicherheitsexperten unterstützen kann, ist die (Teil-) Autonomie bei erkannten Angriffen im Sinne einer höheren Resilienz. Ein Beispiel in diesem Bereich ist, dass bei einem erkannten Angriff die Firewall-Regeln reduziert werden, sodass das eigentliche Kerngeschäft weiter ausgeführt wird, die Angriffsfläche für den Angreifer jedoch kleiner ist. Dies ermöglicht es, eine höhere Ausfallsicherheit für das geschützte Netzwerk und die verwendeten IT-Systeme zu erreichen.

Damit werden die wenigen vorhandenen Ressourcen gezielter eingesetzt und das Cybersicherheitsniveau insgesamt erhöht.

3. Ein weiterer wichtiger Bereich: die Verbesserung der bestehenden Cybersicherheitslösungen

Die künstliche Intelligenz trägt zu größerer Wirkung und Robustheit von Cybersicherheitslösungen bei. Zum Beispiel bei einer risikobasierten und adaptiven Authentifizierung, indem die Bewegungen des Nutzers passiv gemessen werden, um einen weiteren Faktor für die Authentifizierung zu verwenden, ohne dass der Nutzer eine andere Aktion durchführen muss: mehr Sicherheit bei optimaler Bedienbarkeit.

Zusammenfassung

Die Digitalisierung erhöht die Möglichkeiten, Patienten zu heilen und die Prozesse in den Krankenhäusern zu optimieren. Dadurch erhöhen sich prinzipiell auch die Risiken für einen Angriff auf die Krankenhaus-IT. Diese potenziellen Risiken müssen durch geeignete Cybersicherheitsmechanismen reduziert werden. Da in Krankenhäusern neben dem finanziellen Schaden auch die Unversehrtheit von Menschen auf dem Spiel steht, sind die Einrichtungen gut beraten, den Aspekt Cybersicherheit ernst zu nehmen. Sie müssen in der Lage sein, bei einem temporären Problem die Patienten notfalls auch ohne IT-Unterstützung behandeln zu können. Am besten sollten solche Situationen mit allen Beteiligten trainiert werden. ▬

▸ **Literatur**

N. Pohlmann: „Cybersicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cybersicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019

Norbert Pohlmann, Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

Foto: Prof. Dr. Norbert Pohlmann.