SPENGERGASSE
ausbildung mit zukunft

Cyber - Sicherheit

Präsentiert von

Aynur Özmen, Tamara Nikolic, Harmanvir Singh,
Eldar Hajdarbegovic, Hannes Brainovic

AGENDA

- Relevante regulatorische Vorgaben zur IT – Sicherheit im Gesundheitssektor
- Relevante Standards und Best-Practices für IT-Sicherheitstechnik im Gesundheitssektor
- Verbreitung und Stand der IT-Sicherheitstechnik je Branche

Relevante regulatorische Vorgaben zur IT – Sicherheit im Gesundheitssektor

Allgemein

- Keine Vorgaben zur IT-Sicherheit
- Keine Bezugnahme auf IT-Sicherheit in den meisten Verordnungen
- MPBetriebV regelt regelmäßige „sicherheitstechnische Kontrollen“
  - → keine konkreten Vorgaben für IT-Sicherheitskontrollen
- Gesetzgebung → Datenschutz

Datenschutzgesetze

- Bundesschutzgesetz (BDSG)
- Landeschutzgesetze (LDSG)
- Kirchlichen Datenschutzbestimmungen
- Landeskrankenhausgesetz
- Sozialgesetzbuch V

BDSG

- Krankenhäuser in privater Trägerschaft
- Kliniken in öffentlich-rechtlicher Trägerschaft auf Bundesebene
- Niedergelassene Ärzte
- Labore

LDSG

- Krankenhäuser in öffentlich-rechtlicher Trägerschaft
- Krankenhäuser der Gemeinden und Kreise
- Universitätskliniken

Richtlinie für Netz- und Informationssicherheit

SPENGERGASSE
ausbildung mit zukunft

- Ziel: Die Netzwerk- und Informationssystemsicherheit in der EU zu stärken.
- EU-weite Mindestanforderungen → öffentliche als auch private Betreiber von Netzwerk- und Informationssystemen
  - Zentrale Meldestellen für Vorfälle einrichten
  - Meldestellen sollen untereinander vernetzt sein

Sozialgesetzbuch V

- Alle Bestimmungen zur gesetzlichen Krankenversicherung zusammengefasst.
- Kapitel 10 → gesammelten Daten und deren notwendigen Schutz
  - Personenbezogene Daten
  - Leistungs- und Abrechnungsdaten aus den jeweiligen Behandlungen
- Aufbewahrungsfristen und Auskunftspflichten für Daten
- Strafvorschriften

Medizinproduktebetreiberverordnung

- Vorschriften zu Errichtung, Betrieb und Anwendung von Medizinprodukten.
- Spezielle Vorschriften für aktive Medizinprodukte
  - Regelmäßige sicherheitstechnische Kontrollen durch den Betreiber

Medizinprodukte-Sicherheitsplanverordnung

- Regelt die Erfassung, Bewertung und Abwehr von Risiken im Verkehr oder in Betrieb befindlicher Medizinprodukte.
- Vorkommnisse und Rückrufe → melden bei dem Bundesinstitut für Arzneimittel und Medizinprodukte
- Zuständigkeiten für Risikobewertung und für die korrektiven Maßnahmen

DIMDIV

- Datenbankgestützte Informationssystem für Medizinprodukte des Deutschen Instituts für Medizinische Dokumentation und Information (DIMDIV)
- Enthält Vorgaben
  - Zentrales Erfassungssystem für Anzeigen und Anträge im Rahmen von klinischen Prüfungen und Leistungsbewertung.

Richtlinie 90/385/EWG

- Vorgaben für die Bewertung und Zulassung von aktiven implantierbaren Geräten.

Richtlinie 98/79/EG

- enthält wesentliche Vorgaben zu In-Vitro-Diagnostika, um die Sicherheit und Leistungsfähigkeit dieser Produkte sicherzustellen

Richtlinie 93/42/EWG über Medizinprodukte

- Verkehr der Medizinprodukte nur wenn die Anforderungen dieser Richtlinie eingehalten werden
- Konformitätsbewertung

IT-Sicherheitsgesetz

- Erhöhung der Sicherheit
- Sicherstellung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit IT-Systeme
- Drei wichtige Paragraphen
  - §7a: Befugnis des Bundesamtes für Sicherheit in der Informationstechnik IT-Produkte und -Systeme zu Beratungs- und Warnungszwecken zu untersuchen; ggf. mit Unterstützung Dritter
  - •§8a: Verpflichtung von Betreibern kritischer Infrastrukturen, technische und organisatorische Vorkehrungen nach dem Stand der Technik zur Vermeidung von Störungen / Ausfällen zu treffen und in regelmäßigen Zeitabständen nachzuweisen
  - •§8b: Meldepflicht für Betreiber kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik

eHealth-Gesetz

- Soll den Aufbau einer flächendeckenden elektronischen Infrastruktur für medizinische Mehrwertdienste (u.a. elektronische Arztbriefe, Notfalldaten, Medikationspläne, …) und eine verbesserte Patientenversorgung fördern

Relevante Standards und Best-Practices für IT-Sicherheitstechnik im Gesundheitssektor

Allgemein

- Vielzahl von Standards und Best-Practices
- Normen internationaler Herkunft, die von DIN übernommen wurden
  → deutsche Norm

Internationale/nationale Standards

- internationale Standards
  - ISO - International Organization for Standardization
  - IEC - International Electrotechnical Comission
- EN - Europäische Normen
  - CEN - European Committee for Standardization
- DIN - Deutsches Institut für Normung

SPENGERGASSE
ausbildung mit zukunft

National

BSI-Standards 100-1 bis 100-4
Empfehlungen für IT-Sicherheit (organisatorisch)

BSI-Standards IT-Grundschutzkataloge
Empfehlungen für IT-Sicherheit (organisatorisch und technisch)

DIN EN 80001-1
Risikomanagement für IT-Netzwerke von Medizinprodukten

DIN ISO/IEC 27001 & 27002
Managementsystem für IT-Sicherheit

DIN EN ISO 27799
IT-Sicherheit im Gesundheitswesen

Orientierungshilfe KIS (OH KIS)
Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus & Technischen Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

International

Common Criteria (ISO/IEC 15408)
Kriterien zur Bewertung der Sicherheit von IT-Systemen

ISO/IEC 20000
Anforderungen an IT Service Management

ISO/IEC 22301
Business Continuity Management

IHE (Integrating Health Care Enterprises)
Standardisierung des Datenaustauschs zwischen IT-Systemen im Gesundheitswesen

DICOM (Digital Imaging and Communications in Medicine)
Standard zur Speicherung und zum Austausch von Informationen im medizinischen Bilddatenmanagement

HL7 (Health Level 7)
Internationaler Standards für den elektronischen Datenaustausch zwischen Organisationen im Gesundheitswesen

BSI-Standards 100-1 bis 100-4

- Empfehlungen zu Methoden, Prozessen und Verfahren
- Vorgehensweisen und Maßnahmen zur Informationssicherheit
- Angaben
  - zum Aufbau eines Informationssicherheits-Managementsystems (ISMS) (100-1)
  - zu der Vorgehensweise nach IT-Grundschutz (100-2)
  - zu der Erstellung einer Risikoanalyse für hohen bzw. sehr hohen Schutzbedarf (100-3)
- BSI-Standard 100-4 „Notfallmanagement“

BSI-Standards IT-Grundschutzkataloge

- baustein-orientiertes Handbuch zur Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen
- verschiedene Ebenen der gesamten Organisation
- Schutzmaßnahmen, Handlungsempfehlungen, Konfigurationsvorschläge

DIN EN 80001-1

- Management von Risikoprozessen in medizinischen IT-Netzwerken
- alle Phasen des Lebenszyklus von Medizinprodukten.
- klare Verantwortlichkeiten, Aufgaben und Zuständigkeiten
- Wendung an Betreiber von Kliniken, Medizinprodukthersteller und Anwender

DIN ISO/IEC 27001 & 27002

- Maßnahmen für die Implementierung von IT-Sicherheit in unterschiedlichen Bereichen eines Unternehmens
  - z.B. Sicherheit von Rechenzentren
- mit BSI-Standard 100-1 → Best-Practice für die Implementierung eines Managementsystems

DIN EN ISO 27799

- Sicherheit von Gesundheitsinformationen, Umsetzungsplänen und Folgerungen für die Gesundheitsversorgung
- Sicherstellung von Schutz, Vertraulichkeit und Integrität → Vorhaltung von notwendigen Informationen
- Scopespezialisierung: geht auf die Besonderheiten im Gesundheitswesen ein

  → akzentuierte Muss - Kriterien, insbesondere im Bereich des Datenschutzes der Patienten

Orientierungshilfe KIS (OH KIS)

- erstellt von den Arbeitskreisen "Gesundheit und Soziales" und "Technische und organisatorische Datenschutzfragen"
- Orientierungsrahmen bei der Umsetzung der Regelungen im Krankenhausbetrieb
- konkretisiert Anforderungen für eine datenschutzgerechte Gestaltung und Nutzung von KIS

  → Beschreibung von Berechtigungskonzepte für Zugriffe auf die Patientendaten

Common Criteria (ISO/IEC 15408)

- „Common Criteria for Information Technology Security Evaluation“ → internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten
- Anforderungen decken eine hohe Anzahl von Sicherheitszielen
- bei der Zertifizierung der Komponenten der Telematikinfrastruktur relevant

ISO/IEC 20000

- weltweit gültige Standard für das IT Service Management (ITSM)
- Bereitstellung und Erbringung effizienter Services zur Erfüllung
  - von Kundenanforderungen
  - der Wirtschaftlichkeit
  - der Geschäftsprozesse

ISO/IEC 22301

- Grundlagen für die Fortführung des Geschäftsbetriebs im Fall von Störungen
- Anforderungen für ein Krisenmanagementsystem
- Wahrscheinlichkeit solcher Ereignisse verringern

IHE (Integrating the Health Care Enterprise)

- Verbesserung des Datenaustausches zwischen IT-Systemen und Medizingeräten
- Reihe von Testtools
- Kompatibilitätstest → fehlerfreie Kommunikation
- Vereinheitlichung von Schnittstellen soll den Datenaustausch zwischen verschiedenen Leistungserbringern vereinfachen → IHE 2015

DICOM (Digital Imaging and Communications in Medicine)

SPENGERGASSE
ausbildung mit zukunft

- Verarbeitung, Speicherung und Übertragung von medizinischen Bilddaten und zugehörigen Informationen
- DICOM-Bild enthält eine Reihe von Datenelementen
  - z. B. Informationen zum Patienten, die Aufnahme
- Beschreibung von
  - Austauschformaten
  - Anforderungen an konforme Geräte
  - netzwerkorientierten Dienste

HL7 (Health Level 7)

- Austausch medizinischer, administrativer und finanzieller Daten im Gesundheitswesen
- HL7-Nachricht teilt sich in mehrere Segmente auf
  → jedes Segment definiert die Art der Information,
- Sicherstellung der branchenübergreifenden Interoperabilität KIS, AIS, LIMS

Verbreitung und Stand der IT-Sicherheitstechnik je Branche

Verbreitung und Stand der IT-Sicherheitstechnik je Branche

SPENGERGASSE
ausbildung mit zukunft

- Nutzungsgrad in Kategorien
  - Netzwerksicherheit
  - Endgerätesicherheit
  - Nachrichtensicherheit
  - Websicherheit
  - Datensicherheit
  - Identitäts- und Zugriffsverwaltung
  - Mobile Sicherheit

Verbreitung und Stand der IT-Sicherheitstechnik je Branche

SPENGERGASSE
ausbildung mit zukunft

- Experten werden gefragt für die jeweilige Kategorie/Branche
- Angaben sind subjektiv und von der Größe der Institution abhängig
  - Schwer Verallgemeinerungen zu treffen

Kategorien der IT-Sicherheitstechnik

- Die Netzwerksicherheit befasst sich mit der Sicherheit von internen und externen Netzwerken, insbesondere dem Schutz vor Bedrohungen von außerhalb des betreffenden Netzwerkes.
- Unter Endgerätesicherheit wird der Schutz vor ungewollten Eingriffen am Endgerät selbst verstanden
- Nachrichtensicherheit beschreibt den Schutz des Austauschs elektronischer Nachrichten (insb. E-Mail).
- Der Begriff Websicherheit fasst alle Produkte zusammen, die der sicheren Nutzung des World Wide Web dienen.

Kategorien der IT-Sicherheitstechnik

- Die Datensicherheit umfasst alle Maßnahmen zur Wahrung der Vertraulichkeit, Verfügbarkeit, Integrität und Echtheit von Daten
- Unter Identitäts- und Zugriffsverwaltung wird die zentrale Verwaltung digitaler Identitäten und deren Rechte inklusive aller unterstützenden Soft- und Hardware verstanden.
- Unter mobiler Sicherheit versteht man alle Methoden und Verfahren, um die Sicherheit der Daten und Informationen auch bei Zugriff von mobilen Endgeräten sicherzustellen.

Stationäre Versorgung

- Stark durch IT unterstützt und abhängig dieser IT-Unterstützung
- Grad der IT-Sicherheit variiert
  - Zwischen den einzelnen Leistungserbringern

Verbreitung & Stand der IT-Sicherheitstechnik

- **Netzwerksicherheit** ist gut gesorgt
- Firewalls im Einsatz, Netzwerke über WPA2 und externe Kommunikation verschlüsselt
- Hard- und Software beschränkt
  - Gegenüber unerwünschter Ankopplung
- **Endgerätesicherheit** gemischtes Bild
  - Programme → Viren- und Schadprogrammerkennung → Standard
  - Identifikation zugelassener Wechseldatenträger oder Verschlüsselung der Festplatten → nicht flächendeckend im Einsatz

Verbreitung & Stand der IT-Sicherheitstechnik

- **Nachrichtensicherheit** nicht weit Fortgeschritten
  - E-Mails nur bei der externen Kommunikation verschlüsselt
- Maßnahmen der **Websicherheit** gut umgesetzt
  - Browser aktuell
  - Internetnutzung im privaten Bereich dediziert
  - Zugriffsmöglichkeiten beschränk
- **Datensicherheit** ist gewährleistet
  - Datenbanken verschlüsselt
  - Regelmäßige lokale und dezentrale Sicherungen

Verbreitung & Stand der IT-Sicherheitstechnik

- **Identitäts- und Zugriffsverwaltung** für die Absicherung der Daten und Krankenhaussysteme ist nicht üblich
  - Smartcards und 2-Faktor-Authentifizierung nicht flächendeckend

- **Mobile Endgeräte** werden von Mobility Management Softwarte verwaltet und abgesichert
  - Anwendungen im Container vom Rest des Geräts softwareseitig abkapselt
  - Verbindung zum Unternehmensnetzwerk über VPN

Umsetzungsgrad Standards und Best-Practices

SPENGERGASSE
ausbildung mit zukunft

- Die **DIN EN ISO 27799** sowie Standards wie DICOM, HL7 sowie IHE sind von besonderer Bedeutung für die Gesundheitsversorgung und werden daher häufig umgesetzt.
- Das Wissen um die **Orientierungshilfe KIS** ist in der Branche insgesamt weit verbreitet, wenn auch zumeist nur punktuelle Übernahmen einzelner Empfehlungen erfolgen.
- **DIN EN 80001-1** besagt unter anderem, dass eine Person benannt werden sollte, die sich über (neue) Risiken in Netzwerken informiert und, wenn möglich, mithilfe der internen Abteilungen und den externen Partnern, z. B. Herstellern, Risiken begrenzt.

Umsetzungsgrad Standards und Best-Practices

SPENGERGASSE
ausbildung mit zukunft

- **BSI Grundschutzkatalog** dient zur Orientierung wird aber nicht häufig verwendet, wegen mangelnder Ressourcen
- Best-Practices → Bezug auf **Datenschutz** → strenge Vorgaben, die einzuhalten sind
- **ISO/IEC 20000** ist ein Qualitätsstandard für das IT Service Management und wird insbesondere bei großen Kliniken und Klinikketten mit einer ausreichend großen und professionellen IT-Abteilung berücksichtigt

Schlussfolgerung und weiterführende Gedanken

SPENGERGASSE
ausbildung mit zukunft

- Netzwerksicherheit und Datensicherheit weit verbreitet, doch mangelt es häufig an Endgerätesicherheit
  - Bezug auf Mobile Device Control
- IT-Sicherheits-Standards und Best-Practices
  - Hoher Schutzstandard gewährleistet
- Trennung von medizinischen und nicht-medizinischen Netzwerken
  - Komplexität der Krankenhausinfrastruktur reduziert
  - Gebotenen Manipulations- und Datensicherheit Rechnung getragen werden

Schlussfolgerung und weiterführende Gedanken

SPENGERGASSE
ausbildung mit zukunft

- Die **Standardisierung** von verwendeten Bibliotheken, Formaten und Programmiersprachen könnte zu einer geringeren Anzahl problematischer Schnittstellen und somit auch zur Reduktion von kritischen Softwarefehlern führen
- Durch die steigende Nutzung von mobilen Endgeräten (Tablets, Smartphones) auch in Krankenhäusern sind der Aufbau von **sicheren WLAN-Verbindungen** und ein professionelles **Device Management** nötig

Schlussfolgerung und weiterführende Gedanken

SPENGERGASSE
ausbildung mit zukunft

- Die Telematikinfrastruktur führt künftig zu immer weitreichender integrierten Anwendungen durch die bereitgestellten Schnittstellen zwischen verschiedenen Versorgungsdienstleistungen, wie etwa die Übertragung von Patientendaten zwischen niedergelassenen Ärzten und Krankenhäusern
- Qualifizierte elektronische Signatur und Authentifizierung weitflächig sollen weit nutzbar gemacht werden

Ambulante Versorgung

- geringe IT-Anhängigkeiten
- jedoch personenbezogene Daten → IT-Sicherheit!!!
  - keine gesetzlichen Vorgaben
  - Regelungen und Empfehlungen

Verbreitung & Stand der IT-Sicherheitstechnik

- viele Leistungserbringer → Verallgemeinerung schwierig
- Sicherheitsniveau: niedrig + heterogen

Netzwerksicherheit

- Firewalls
- Trennung personenbezogener Daten vom Internet
- Zugriffsrechte für Fernzugriffe beschränken
  z.B. durch regelmäßige Passwort-Änderung
- Protokollierung der Zugriffe

Endgerätesicherheit

- Software zur Erkennung unsicherer Wechseldatenträger (z.B. USB-Stick)
- Sicherheitsupdates

Nachrichtensicherheit

- Digitalisierung der Übertragung von elektronischen Arztbriefen
  → noch nicht umgesetzt
- Wenn Telematikinfrastruktur im Einsatz
  - Anwengung KOM-LE (Kommunikation zwischen Leistungserbringern)
  - elektronische Signatur von Arzt
  - Verschlüsselung der Nachricht

Websicherheit

- Aktualität der Webbrowser
- Datenübertragung über webbasierte „Order-Entry-Systeme“

  → Verschlüsselung SSL (Secure Socket Layer)

Datensicherheit

- Daten in APIS meist unverschlüsselt
- wird häufig nicht unterstützt

- Datensicherung → Informationen verschlüsselt exportiert

Identitäts- & Zugriffsverwaltung

- 1-Faktor-Authentifizierung
  - Benutzername
  - Passwort
- Jedoch: regelmäßige Passwortänderung oft nicht eingehalten
- Zugriff auf Daten oft nicht geregelt
  → Personal hat volle Zugriffsrechte

mobile Endgeräte

- einige APIS bieten Applikationen für mobiles Endgert
- Applikation
  - sicher
  - abgekapselt vom restlichen System

    → wenig Angriffsfläche

Umsetzungsgrad Standards und Best-Practice

- verpflichtende Vorgaben können oft nicht eingehalten werden

  → Branchenstruktur nicht festlegbar
- meist wegen Datenschutz
- Entwicklung nach Standards: moderne Sicherheitsanforderungen
- DICOM: fast immer genutzt für Radiologie

Schlussfolgerung

- kaum professionalisierte IT-Sicherheit
- Freiberufler – „Kleinsteinheiten“

  → Mangel an IT-Sicherheitsbeauftragten
- kaum zusätzliche Absicherung gegen IT-Sicherheitslücken
- getrennte Rechnernutzung
  - Internetzugeng
  - Administration der Patientendaten
- Telematikinfrastruktur → Steigerung des Vernetzungsgrads

im Bereich der ambulanten Versorgung

- im extramuralen Bereich: Trennung medizinischer / nicht medizinischer Netzwerke
- Standardisierung von
  - Bibliotheken
  - Formaten
  - Programmiersprachen
- sichere WLAN-Verbindungen + Device- & Benutzer-Management für mobile Endgeräte
- Telematikinfrastruktur

Arzneimittel und Impfstoffe

Akteursgruppen: unterschiedliche Anforderungen

1. Wertschöpfungskette d. Pharmahersteller: Informationssystem für
   - Forschung und Entwicklung
   - Simulationen
   - klinischen Studien
   - Zulassungsprozess
   - Lieferprozess
2. Pharmagroßhändler: v.a. Ein- & Ausgangslogistik
3. Apotheke: z.B. Bestellung, Abrechnung, …

Verbreitung und Stand der IT-Sicherheit

Verbreitung d. IT-Sicherheitstechnik:

1. große Pharmahersteller und Großhändler
2. hoch fragmentierter Apothekenmarkt

Netzwerksicherheit

- sehr wichtig
- Verlust / Manipulation von Informationen zu Rezepten und Wirkstoffen

  → wirtschaftlicher Schaden
- Firewalls

Endgerätesicherheit

- Antivirus- und Erkennungs-Programme: bereits im Einsatz
- auf neuestem Stand
- guter Grundschutz

Nachrichtensicherheit

- z.B. E-Mails unverschlüsselt

  → sollte besonders geschützt sein
  zum Verhindern von Datenlecks

Websicherheit

- SSL Verschlüsselung
- automatisierte Updates auf Browser

  → aktuellster Sicherheitsstand
- private Internetnutzung untersagt
- Zugriffsmöglichkeiten beschränkt

Datensicherheit

- regelmäßige Sicherungen von
  - Daten
  - Systemständen

Identifikation

- üblicherweise: 1-Faktor-Authentifizierung
  - Benutzername
  - Passwort
- sensible Daten: 2-Faktor-Authentifizierung
  - Einmalpin
  - Sicherheitstoken
- recht gut abgesichert!

mobile Sicherheit

- kein konsistentes Bild
- mögliche Einsatzgebiete mobiler Endgeräte in Entwicklung
- Verbesserungspotential: Device Management

Apotheken

- „Kleinsteinheiten“
- Niveau der IT-Sicherheitstechnik: niedrig
- Kritikalität durch Redundanz & fragmentierte Struktur

  → gering eingeschätzt

Umsetzungsgrad Standards und Best-Practice

Branche v. Arzneimittel + Impfstoffe

→ stark reguliert, trotzdem meine Vorgaben zu IT-Sicherheit

- Empfehlungen, Standards und Regelungen
  - sicherer Datenaustausch
  - physische & elektronische Sicherung
- professionelle IT-Abteilung

Umsetzungsgrad Standards und Best-Practice

Pharmagroßhändler und Apotheken

- grundsätzliche Aussage treffen: schwierig
  - fragmentierte Struktur
  - unabhängige Einheiten
  - viele verwendete Systeme
- etwas professionellere IT-Abteilung

Schlussfolgerung

- Arzneimittel + Impfstoffbranche
  - IT-Standards modern
  - professionelles IT-Management (Selbstschutz)
- Apotheken
  - weniger professionalisiert
  - Absicherung vorantreiben
  - Telematikinfrastruktur erweitert für sichere Kommunikation

im Bereich Versorgung mit Arzneimitteln

- Trennung von Systemen
  - Administration Personalplanung
  - Administration von Medikamenten, …
- Manipulations- und Datensicherheit
- Standardisierung von
  - Bibliotheken
  - Formaten
  - Programmiersprachen
- sichere WLAN-Verbindungen + Device- & Benutzer-Management für mobile Endgeräte

Laboranalytik

- IT-Abhängigkeit in der Branche → sehr hoch
- Schutz vor unbefugte Zugriffe → um Missbrauch oder Manipulationen zu vermeiden
- Die Daten für über eingesetzte IT-Sicherheitstechniken oder angewandte Standard → gering

Verbreitung & Stand der IT-Sicherheitstechnik

- Netzwerksicherheit ist ausreichend umgesetzt → Firewalls und Netzwerkzugangskontrollen sind im Einsatz
- Endgerätesicherheit → Antivirusprogramme installieren und Festplatten verschlüsseln
- Nachrichtensicherheit
  - E-Mail Verschlüsselung → nicht flächendeckend genutzt
  - Medizinische Prozesse, beispielsweise Datenaustausch zwischen Arztinformationssystemen → höhere Sicherheit → standardisierten und abgesicherten Protokollen

Verbreitung & Stand der IT-Sicherheitstechnik

- Websicherheit → Verbesserungspotential
- Datensicherheit → in Bezug auf die Ausfallsicherheit sehr positives Fazit → online/offline Sicherungen und Backups
- Mobile Sicherheit → Verbesserungspotential → mangelt an Verschlüsselung der Daten
- Identitäts- und Zugriffverwaltung → keine Informationen

Umsetzungsgrad Standards und Best-Practices

- Standards und Best-Practices → in Bezug auf die Sicherheit der Mitarbeiter umgesetzt → Gefährdungspotential durch chem. Und biologische Stoffe
- IT-spezifische Best-Practices → keine Informationen → man geht von gültigen Standards wie dem IT-Grundschutzkatalog oder ISO/IEC 22301 aus

Schlussfolgerung und weiterführende Gedanken

- IT-Infrastruktur → mäßig robust
- Datensicherheit → gut
- Nachrichtensicherheit → durch die standardisierten Protokolle zum Austausch von Informationen abgesichert
- Netzwerksicherheit → Fernwartungszugänge → problematisch
- Mobile Endgeräte → Sicherheitslücke

Schlussfolgerung und weiterführende Gedanken

- Sicherheit erhöhen
  - Trennung zwischen Netzwerken (die kritische Informationen enthalten) → um die Manipulations- und Datensicherheit zu gewährleisten
  - Standardisierung
  - Sichere WLAN-Verbindung
  - Telematikinfrastrukur

Versorgung mit Medizintechnik

- Beispielsweise:
  - Diagnosetechnik: CT
  - Therapietechnik: medizinische Pumpen

  EU → gesetzliche Regelungen auf die IT-Sicherheit von Medizingeräten fehlen

  Europäische Richtlinie über Medizinprodukte 93/42/EWG → CE-Kennzeichnung bei Medizinprodukten notwendig → aber keine spezielle Prüfung der IT-Sicherheit

Verbreitung & Stand der IT-Sicherheitstechnik

- Betrachtung der Geräte und nicht der Betreiber
- Netzwerksicherheit → eher gering → unkontrollierte Fernzugänge
  - Network Access Controller → Netzwerke sicher zu gestalten
- Endgerätesicherheit → gering → veraltete Betriebssysteme
  - Herzschrittmacher oder Insulinpumpen → Fernsteuerung → Zugang zu den Daten → Gefahr für den Patienten
- Nachrichtensicherheit → sehr relevant →Austausch von Daten zwischen den Informationssystemen

Verbreitung & Stand der IT-Sicherheitstechnik

- Websicherheit → nicht relevant
  - keine originäre Funktionalität für die Internetanbindung
- Datensicherheit → deutliche Lücken → keine einheitlichen Standards/ gesetzliche Vorgaben
- Identitäts- und Zugriffsverwaltung → erfüllt großteils nicht die Anforderungen
  - Kennwort und Benutzername
  - 2-Faktor-Identifikation → selten
- Mobile Sicherheit → nicht wichtig → Medizintechnik selbst nicht mobil

Umsetzungsgrad Standards und Best-Practices

- Fokus auf die Geräte und nicht auf den Hersteller
- BSI-Standards 100-1 bis 100-4 → nicht für Einzelgeräte → sondern für die Hersteller
- Direkt auf die Produkte → z.B Commen Criteria

Schlussfolgerung und weiterführende Gedanken

- Sicherheitsmängel bei den Geräten
  - Betriebssysteme veraltet
  - Fernwartungszugänge nicht kontrolliert
  - Softwareaktualisierungen werden nicht vorgenommen
- Künftig → IT-Sicherheit als Teil der Zertifizierung der Produkte

Schlussfolgerung und weiterführende Gedanken

- Sicherheitsmaßnahmen:
  - aktueller Stand regelmäßig dokumentieren
  - Trennung von medizinischen und nicht-medizinischen Netzwerken
  - Netzwerkschnittstellen und Software unabhängig voneinander entwickeln → Schutz vor Angriffen
  - Verwendung von Standards
  - Striktes Benutzermanagement mit Verschlüsselung

SPENGERGASSE
ausbildung mit zukunft

Vielen Dank für Ihre Aufmerksamkeit!