Dr. Veronika Kraus (in Vertretung DDr. Thomas Schabetsberger)

Sicherheit in vernetzten Gesundheitsinformationssystemen – Versuch einer ganzheitlichen Betrachtung

Inhaltsverzeichnis

Informationssicherheit

Informationen sind schützenswerte Güter

- Gesundheitsinformationen sind sensible Daten nach dem DSG
- **Schutzziele:**
  - Vertraulichkeit (Confidentiality)
  - Integrität (Integrity)
  - Verfügbarkeit (Availability)

Hintergrund: Gesundheitsinformationssysteme

- Gesundheitseinrichtungen arbeiten IT-unterstützt
- Personalisierte Gesundheitsdaten sind besonders schutzwürdige Daten (sensible Daten)
- Sicherheitsvorgaben in den Einrichtungen zum Schutz der Daten

- Zunehmende Zusammenarbeit im Gesundheitswesen erfordert Vernetzung der Daten
- Integrierte / kooperative Versorgung; eHealth
- IHE zur Verbesserung der Interoperabilität zwischen Gesundheits-IT Systemen
- Bereitstellung von Daten in Netzwerken zum Zugriff durch Berechtigte
- In Österreich: ELGA (weitere Portale und Netzwerke schon seit vielen Jahren)
- Hunderte Beispiele und Aktivitäten auf der ganzen Welt

„Security by Design“

- Sicherheit eines eHealth Netzwerkes beginnt bei der Planung
- Software wird von Grund auf für höchste Sicherheitsanforderungen ausgelegt
- Konkret durch Berücksichtigung von „Security Pattern“
  - bereits ab der Requirements Engineering Phase;
    User stories und use-cases auch administrativer Natur mit einbeziehen!
- Schadwillige Praktiken werden von Beginn an in die Überlegungen mit einbezogen
  - Z.B. Identifikation von Abuse Cases und Angriffsvektoren
- Der Aufbau solcher Systeme ist nicht geheim. Auch andere sollen sich damit befassen und zur weiteren Sicherheitssteigerung beitragen können („Linus's Law“)
- Berücksichtigung von internationalen Best Practice Ansätzen
- Durchführung von Sicherheitsanalysen und kontinuierliches Sicherheits-Monitoring
- Sicherheitsvorgaben für den laufenden Betrieb (technisch / organisatorisch / persönlich)

Trans-institutionale IT Architekturen

- Client/Server ebenso wenig geeignet wie Peer2Peer oder Grids
- Hybrider Ansatz mit dezentraler Datenhaltung und zentralen Registern erscheint vorteilhaft
- Verteilung kritischer Daten auf mehrere zentrale Register (PIX Manager, Document Registry, Document Repository, etc.)
  - jedes führt nur (für sich unkritische) Teilinformationen
  - Saubere, **durchgängigeTrennung** notwendig
  - Zusätzliches Verschleiern durch Einstreuung von Dummy Informationen möglich

- Gesetzliche Rahmenbedingungen und Patienten Consent wird an den **datenführenden** Registern und Datenspeichern „enforced“
- **Unidirektionaler** Zugriff auf datenführende Komponenten nur über **mehrere** Sicherheitszonen

Sicherstellung der Vertraulichkeit

- Mehrstufiges Berechtigungssystem:
  - Abgesicherte Netzwerkverbindung (**Verschlüsselung** auf Transportebene mit zertifikatsbasierter Authentifizierung zwischen allen Diensten - IHE ATNA)
  - Sichere **Authentifizierung** der Anwender mit Hilfe von Sicherheitstoken (IHE XUA++)
  - **Authorisierung** über den Sicherheitstoken und durch Soll/Ist Vergleich verfügbarer sensibler Informationen mit den hinterlegten Sicherheitsregeln (XACML; IHE Access Control)

- Lückenlose Protokollierung und Offenlegung der Transaktionen (IHE ATNA)
- Konstante Überprüfung, Reporting
- Sicherheitsrichtlinie, die in der Organisation den Umgang mit Zugangsdaten regelt
- Periodische Schulungen der Anwender und Sensibilisierung

Sicherstellung von Integrität und Verfügbarkeit

Integrität

- Verteilung der Programme und Zertifikate durch organisatorische Maßnahmen geregelt
- Signatur über verfügbar gemachte Dokumente als Teil der Metadaten verspeichert
- Signatur über relevante Metadaten als weiteres Metadatum verspeichert
- Qualifizierte Signatur von Dokumenten wäre empfehlenswert (IHE DSG)

➔Sicherstellung, dass weder Programme, noch Inhalte (Dokumente oder Metadaten) verändert wurden

Verfügbarkeit

- Redundanzen in Hardware und Netzwerk
- Ausreichende, intensive Testphasen
- Gut geschulte Anwender und Betriebsmitarbeiter
- Konstantes Monitoring und Alerting

Erfüllung der Sicherheitsziele

- Höchstmaß an technischer Absicherung wird gewährleistet, **technische Risiken** gut kalkulierbar. Sicherheitsziele scheinen gut abgedeckt.
- Behebung allfälliger organisatorischer Schwachstellen
- Laufende Schulungen und Sensibilisierung von Mitarbeitern (Administratoren, Endbenutzer)
- Periodisch wiederkehrende, systematische Sicherheitsanalysen, um am Stand der Zeit und der Technik zu bleiben
- Vorbeugen von Angriffen durch **Überwachung des Netzwerkverkehrs** (Intrusion detection & prevention) und **Verfolgen von Sicherheitsnachrichten** (z.B. cert.at, heise.de,)
- Enge Zusammenarbeit zwischen Systemherstellern und Systembetreibern ist Voraussetzung!
- Worst-Case trainieren!
  - Einspielen von Hotfixes bis zum kontrollierten Abschalten des Systems
- Einführung und Leben eines ISMS samt Zertifizierung wie ISO 27001 für Betreiber sinnvoll!

Besten Dank für Ihre Aufmerksamkeit!

Dr. Veronika Kraus
Product Manager

IITH icoserve GmbH – a Siemens company

Innrain 98
6020 Innsbruck

Tel.: +43 (512) 89059-435
Mobil: +43 (664) 8011717700

E-Mail:
veronika.kraus@ith-icoserve.com

DDr. Thomas Schabetsberger
Head of Technical Sales & Product Management

ITH icoserve GmbH – a Siemens company

Innrain 98
6020 Innsbruck

Tel.: +43 (512) 89059-436
Mobil: +43 (664) 8011716238

E-Mail:
thomas.schabetsberger@ith-icoserve.com

Answers for life.

Disclaimer

Aufgrund lokaler Einschränkungen von Vertriebsrechten und Serviceverfügbarkeiten können wir leider nicht gewährleisten, dass alle hierin aufgeführten Produkte weltweit gleichermaßen durch Siemens vertrieben werden können.

Die Informationen in diesem Dokument beinhalten allgemeine technische Beschreibungen von Leistungen und Ausstattungsmöglichkeiten, die nicht in jedem Einzelfall vorliegen müssen. Verfügbarkeit und Ausstattungspakete können sich von Land zu Land unterscheiden. Aus diesem Grund sind die gewünschten Leistungen und Ausstattungen im Einzelfall bei Vertragsschluss festzulegen.

Siemens behält sich das Recht vor, Konstruktion, Ausstattungspakete, Leistungsmerkmale und Ausstattungsmöglichkeiten ohne vorherige Bekanntgabe zu ändern. Die aktuellsten Informationen erhalten Sie bei Ihrer zuständigen Siemens-Vertretung.

Hinweis: Innerhalb definierter Toleranzen kann es Abweichungen von den technischen Beschreibungen in diesem Dokument geben. Bei der Reproduktion verlieren Ergebnisbilder immer ein gewisses Maß an Detailtreue.

Alle in Software-Screenshots oder in anderer Art und Weise in diesem Dokument dargestellten Patientendaten sind rein fiktiv. Screenshots werden auf Siemens eigenen Systemen zum Zweck der Demonstration kreiert.

Die hierin enthaltenen Aussagen basieren auf Ergebnissen, die von Siemens-Kunden in deren jeweiligen spezifischen Nutzungsumfeld erzielt wurden. Es ist zu beachten, dass es kein „typisches" Krankenhaus gibt und die Resultate von verschiedenen Variablen abhängen (wie z. B. der Größe des Krankenhauses, des Behandlungsspektrums, des Grads der IT-Integration). Aus diesem Grunde besteht keine Garantie dafür, dass andere Kunden dieselben Ergebnisse erzielen werden.

sense® und syngo®.share sind Softwarelösungen der ITH icoserve technology for healthcare GmbH, einer Tochterfirma der Siemens AG. Bitte beachten Sie, dass die hier genannten Produkte derzeit nur in ausgewählten Ländern erhältlich sind.

Legal Manufacturer sense® and syngo®.share
ITH icoserve technology for healthcare GmbH
Innrain 98
A-6020 Innsbruck
Österreich

Global Siemens Healthcare Headquarters
Siemens AG
Healthcare Sector
Henkestrasse 127
91052 Erlangen
Telephone: +49 9131 84-0
Germany

Siemens Healthcare Österreich
Siemens AG Österreich
Healthcare Sector
Siemensstraße 90
1210 Wien
Telephone: +43 51707-0
Österreich