Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

Technische Anlage und Elektronischer Arztausweis

eco, Arbeitskreis Sicherheit, Köln

6. Mai 2009

Dr. med. Dipl.-Inform. Georgios Raptis
Telematik, Bundesärztekammer

Empfehlungen

Die Empfehlungen der Bundesärztekammer (BÄK) und der Kassenärztlichen Bundesvereinigung (KBV) enthalten:

- Einen juristischen Text (Print-Ausgabe und online, vom Mai 2008) zu
  - Ärztliche Schweigepflicht
  - Datenschutz
  - Einsatz von IT in der Arztpraxis
- Eine Technische Anlage (nur online, neu) zu
  - IT-Sicherheit

Zielsetzung Technische Anlage

Technische Anlage zu den Empfehlungen:

- Leitfaden IT-Sicherheit für Arztpraxen
- Dokument soll kompakt und verständlich sein
- Enthält organisatorische und technische Maßnahmen
- Organisatorische Maßnahmen: Umsetzung durch den Arzt
- Technische Maßnahmen: Umsetzung durch Arzt oder (empfohlen) durch IT-Dienstleister
- Abschnitte „Für Experten“ zu technischen Maßnahmen

Grundlagen

Grundlagen der Technischen Anlage:

- IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI), ISO27001
  - Gratwanderung: kompaktes und allgemein verständliches Dokument vs. ISO27001 Konformität
- Technische Richtlinie BSI-TR03116
- Aktueller Stand der Wissenschaft und Technik zur IT-Sicherheit und Kryptographie
- Abstimmung mit dem BSI

Dokument wird bei Bedarf aktualisiert, um neuere Bedrohungen und Entwicklungen im Bereich IT-Sicherheit zu berücksichtigen

Bedrohungspotential, Einordnung der Technischen Anlage

Medizinische Daten sind sensible Daten

Angriffe sind immer möglich gewesen, mit IT-Einsatz können sie besser skalieren

- Kein IT: Einbruch in Praxis erforderlich, Entwendung von Papierakten (schwer, unhandlich) notwendig, Risiko für den Angreifer durch Nachbarn, Polizei.
  - Maßnahmen: Stabile Tür mit Schloss, Stahlschrank, ggf. Alarmanlage usw.
- IT wird eingesetzt, offline: Einbruch in Praxis erforderlich, Einbrecher kann Rechner mit *allen* Patientendaten der Praxis entwenden, Entdeckungsrisiko durch Nachbarn, Polizei.
  - Empfohlene zusätzliche Maßnahmen: Lokale Verschlüsselung der Daten
- „Online-Praxis“: zusätzlich elektronischer Einbruch möglich (Angriff aus der Ferne, Risiko für Angreifer geringer), Einbrecher kann alle Daten der Praxis entwenden,
  - Empfohlene zusätzliche Maßnahmen: s. Technische Anlage ☺
- Patientendaten zentral in einer Infrastruktur (online ePatientenakten, bereits auf den Markt): Angriff hat alle Daten aller Patienten als Ziel, darf nie erfolgreich sein.
  - Empfohlene zusätzliche Maßnahmen (kein „Mission Impossible“…) : (Dezentrale) Verschlüsselung, Geflecht von Sicherheitsmechanismen gemäß eines Sicherheits-konzeptes, kryptographisch abgesicherte Berechtigungskonzepte, sichere kryptographische Schlüssel auf Chipkarten, Sicherheitszertifizierungen usw.

Nutzung vorhandener Schutzmechanismen

Gängige Betriebssysteme (Windows, Linux, Mac OS X usw.) bieten bereits eine Fülle von Schutzmechanismen:

- Nutzen Sie sichere Passwörter!
- Handbuch lesen, sichere Einstellungen verwenden (z.B. keine automatische Anmeldung ohne Passwort)
- Aktueller Virenschutz
- Nicht mit Administrator-Rechten arbeiten
- Zugriffsrechte beschränken (müssen alle Rechner oder Mitarbeiter vollen Zugriff auf alle Daten haben?)
- Daten auf Notebooks: unbedingt verschlüsseln! (empfohlen auch für stationäre Rechner)

Intranet und Internet

- Rechner mit Patientendaten dürfen keine direkte Verbindung ins Internet haben.
  - Medline-Recherchen, öffentliche E-Mail usw. im Internet nur mit einem isolierten dedizierten („Stand-alone“) Rechner möglich
  - Sichere Trennung (physische oder logische) zwischen IT-System oder Netzwerk mit Patientendaten und Internet erforderlich
- Sichere Verbindung mit einem Intranet ist OK (VPN)
  - Authentifizierte und verschlüsselte Verbindung über ein sicheres dediziertes Hardware-Gerät (VPN-Device mit Firewall), Provider übernimmt Verantwortung für die Sicherheit
  - Oder direkter „Einwahl“ (auf OSI-Schicht 2) ins Intranet durch Provider (z.B. einige KV-Safenet-zertifizierte Intranets)
  - Einsatz von hochwertigem Firewall und Virenschutz erforderlich
  - Intranet-Provider ist für die Sicherheit des Intranets verantwortlich

Infrastruktur in der Arztpraxis, Kommunikationsnetze

- Dokumentation und Kontrolle über das Netzwerk in der Arztpraxis, kein Zugriff auf das LAN für Unbefugte
- Möglichst kein WLAN
  - Falls WLAN unabdingbar: nur mit Verschlüsselung (WPA2) und wirklich sicherem Passwort, regelmäßige Kontrolle der Einstellungen
- VoIP (Voice over IP, Internet-Telefonie): u.U. höheres Risiko, Abhören z.T. auch für nicht professionellen Angreifer leicht möglich
  - VoIP ist nicht unter allen Umständen unsicher, Bestätigung von gleichwertiger Sicherheit wie konventioneller Telefonie erforderlich
  - Im Übrigen: auch einige schnurlose Telefone (DECT) sind nicht sicher
- Reparatur von IT-Systemen: unter Aufsicht
- Entsorgung von Rechnern und Datenträgern: Daten vorher sicher löschen

Datensicherung, Fernwartung, elektronische Dokumentation

- Datensicherung: regelmäßig durchführen, Backup-Medien sicher aufbewahren
- Fernwartung: Explizite Autorisierung jeder einzelnen Fernwartung (danach Passwort für Fernwartung ändern), Verschlüsselte und authentifizierte Verbindung
- Fernwartung nach Möglichkeit mit Testdaten, ohne Zugriff auf Patientendaten
- Überwachung der Fernwartung am Bildschirm, Protokollierung
- Elektronische Dokumentation und Archivierung
  - Am sichersten mit Einsatz von qualifizierten elektronischen Signaturen und Zeitstempeln, s. Technische Anlage

Einsatz von Chipkarten

- Chipkarten sind sichere Träger von kryptographischen Schlüsseln. Damit verschlüsselte Daten sind sehr gut geschützt
- Für die Absicherung der Authentizität und Vertraulichkeit von sensiblen Daten sollten Chipkarten eingesetzt werden
  - Z.B. Anmeldung in einem medizinischen Portal viel sicherer mit Chipkarte als mit Username/Passwort
  - Verschlüsselung vor Übertragung von Dokumenten (z.B. Arztbriefen), Chipkarte ist für die Entschlüsselung notwendig
  - Elektronische Signatur: Verbindlichkeit und Authentizität von elektronischen Arztbriefen
- Elektronischer Arztausweis: kann Kommunikation im Gesundheitswesen effektiv absichern

Architektur des Heilberufsausweises

- Schlüssel des Arztes für die Telematik-Infrastruktur
- Weitgehende Kompatibilität zur eGK-Plattform
- Ziel: Interoperabilität
- Ziel: Schnelle Verfügbarkeit, Kostenreduktion

Grundlage: HPC-Spezifikation

Arten von Chipkarten für Heilberufler

- Heilberufsausweis (HBA)
  - Grundlage: HPC-Spezifikation Part 1 und 2
  - Persönliche Chipkarte
  - Für Ärzte: eArztausweis, herausgegeben von Ärztekammer
- Muss qualifizierte Signatur unterstützen

Arten von Chipkarten für Heilberufler (2)

- Secure Module Card (SMC)
  - Grundlage: HPC-Spezifikation Part 1 und 3
  - SMC-A: Arbeitsplatzkarte, steckt im Kartenterminal, Freischalten der eGK, entfernte PIN-Eingabe, ggf. Identität des Kartenterminals
  - SMC-B: Institutionskarte, Authentifizierung gegenüber der Telematik-Infrastruktur, einfache Signatur („Praxisstempel“)
- Weitere SMCs für Konnektor usw.
- SMCs werden in diesem Vortrag nicht betrachtet

Stand Spezifikationen und Ausgabestrukturen

- Spezifikationen für den eArztausweis sind final
  - PKI-Struktur, Verzeichnisdienste, Profile usw.
  - Ausgabeprozesse, mit ZDA erprobt
  - Rahmenbedingungen, Verträge in der finalen Abstimmung

Stand Spezifikationen und Ausgabestrukturen

- eArztausweise werden in einem marktoffenen Modell herausgegeben
  - Zulassung der ZDA durch die Ärztekammern
  - Unterschrift Rahmenvertrag
  - Für jede Chipkarte: die Ärztekammer bestätigt des Attribut „Ärztin/Arzt“ und gibt die Produktion frei
  - Bestätigung des „KammerIdent“-Verfahrens nach SigG für Identifizierung, Attributbestätigung und sicheres Handling durch die Ärztekammern

Sicherheitsanforderungen für den Heilberufsausweis

- Sicherheitszertifizierung nach Common Criteria, gemäß Protection Profiles
  - Als sichere Signaturerstellungseinheit
  - Als Heilberufsausweis
- Bestätigung nach Signaturgesetz

Trennung der zwei PPs ist seit HPC V2.3.0 nicht mehr so einfach (Stapel- und Komfortsignaturen!)

Architektur des Heilberufsausweises

- „Standard“-Chipkarte, die besondere Anforderungen des Gesundheitswesens berücksichtigt:
  - **Standard-Funktionen**: qualifizierte Signatur, Authentisierung, Entschlüsselung
  - **Card verifiable certificates**, Authentifizierungsmechanismus mit Rollenkonzept
  - Mindestens 4 Logische Kanäle (Sicherheitskontexte)
  - Entfernte PIN-Eingabe
  - Stapelsignaturen und Komfortsignaturen
  - Unterstützung für Identity-Management Konzepte

Architektur, Standard-Funktionen

- Qualifizierte Signatur:
  Standard **QES-Anwendung**
- Authentisierung, Entschlüsselung:
  Standard **ESIGN-Anwendung**
- Option für institutionsspezifische Authentifizierung
- Zertifikatsprofile und PKI-Spezifikationen:
  Common-PKI mit SigG-Profil für alle Zertifikate

Architektur, Identity Management

- Problemstellung: Arzt bekommt neuen eArztausweis. Berechtigungen (Zugriff auf Patientendaten) sind aber an das alte Zertifikat geknüpft. Keine Korrelation zwischen alten und neuen Zertifikaten, kein Zugriff auf die Patientendaten durch den neuen Arztausweis
- Lösung: **Telematik-ID**
  - Arzt bekommt eine eindeutige Telematik-ID mit dem HBA.
  - Die Telematik-ID wird von der herausgebenden Ärztekammer vergeben. Berechtigungen werden an die Telematik-ID geknüpft
  - Bei neuem eArztausweis: Der Arzt kann entscheiden, die Telematik-ID im neuen Zertifikat wieder aufzunehmen, oder eine neue Telematik-ID zu beantragen.
    - Dadurch datenschutzrechtlich OK, mit BfDI abgestimmt
  - Identity-Management Konzepte werden ermöglicht

Stand: heute, Test-HBAs

- Alte HPC-Spezifikation in der Version 2.1.1
- Karten in den Testregionen,
  Zusammenspiel mit eGK funktioniert
- Keine Bestätigung nach SigG

Stand: heute, HPCqSig

- HPCqSig: SigG-bestätigte HPC für Projekte außerhalb der gematik
- Basiert auf HPC-Spec 2.1.1
  - Ausnahmen: keine CV-Zertifikate, logische Kanäle, Secure Messaging (also Elemente, die für die Interaktion mit der eGK benötigt werden)
- Wird in Nordrhein und Sachsen ausgegeben
- Wir können damit bereits Projekte außerhalb der Telematik-Infrastruktur bedienen und unterstützen

Stand, nahe Zukunft

- HPC-Spezifikation in der Version 2.3.1 ist final, enge Abstimmung mit der gematik
  - Entspricht der veröffentlichten Version 2.3.0 mit den allen „Specification related questions“ (SRQs)
- Soll als Gegenpart zu den „echten“ eGKs der Generation 1 ausgegeben werden
- Voraussetzung: SigG-Bestätigung
- Erwartet: einige Wochen nach Bereitstellung der entsprechenden Generation-1 eGKs

Stand, künftige Generationen

- Entwicklung künftiger HPC-Spezifikationen in Abstimmung mit der gematik
  (Grund: Kompatibilität / Interoperabilität zur eGK)

- Zeitplan: hängt vom eGK-Zeitplan ab

Migrationskonzept

- eGK und HPC müssen kompatibel sein, damit sie interagieren können
- Karten der Generation 1 sind zu den derzeitigen Karten in den Testregionen nicht abwärtskompatibel, d.h. alle Testkarten werden mit Roll-Out der G1-eGK ausgetauscht
- Anforderungen aus Sicht der Bundesärztekammer für künftige Kartengenerationen:
  - **Klares Migrationskonzept** mit vernünftigem **Übergangszeitraum**, welches uns und den Kartenherstellern Planungs- und Investitionssicherheit gibt
  - **Faire Migration**, beide Karten (eGK/HPC) müssen jeweils abwärtskompatibel sein oder eine andere Lösung muss gefunden werden.
    - Austausch sämtlicher HBAs ist keine Option

Fragen ?

Dr. med. Dipl.-Inform. Georgios Raptis
Referent Telematik
Bundesärztekammer
georgios.raptis@baek.de
030 400456304

Vielen Dank!

Technische Anlage im Internet:

www.aerzteblatt.de/plus1908

Spezifikationen eArztausweis:

http://www.baek.de/page.asp?his=1.134.3421.4132