

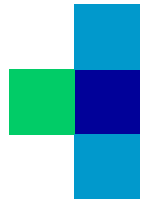
IT-Sicherheit im Krankenhaus - Arbeitsgebiete eines IT- Sicherheitsbeauftragten, Notwendigkeit und erste Erfahrungen

21.6.2007

Jochen Kaiser

IT-Sicherheitsbeauftragter des Universitätsklinikums Erlangen
jochen.kaiser@uk-erlangen.de

Universitätsklinikum
Erlangen



Seite 2

Viele Anwendungen - heterogene Anforderungen

- Vernetzung von Komponenten und Verfahren, untereinander (klinische Anwendungen) aber auch mit dem Internet (Fernwartung, Telemedizin)
 - eingesetzte (klassische) Schutzmaßnahmen (Firewall, Virenschutz) genügen nicht, da zu viele individuelle Anforderungen existieren
 - etablierte Abteilung oft technisch aber immer organisatorisch überfordert (fehlendes Mandat der Geschäftsführung; fehlende Unabhängigkeit)
 - Beurteilung der Risiken um adequate Maßnahmen zu finden, die den Betrieb nicht einschränken und nicht stilllegen. (Verhältnismäßigkeit!)
- Expertenwissen ist gefragt
- Das Universitätsklinikum Erlangen hat diesen Experten im Jahr 2005 in Form eines IT-Sicherheitsbeauftragten eingesetzt.



Einführung und auch Abgrenzung zum Datenschutz

- Unterscheidung zwischen dem Datenschutzbeauftragten (DSB) und dem IT-Sicherheitsbeauftragten (ITSB) notwendig
- §9 BDSG sieht zwar organisatorische und technische Schutzziele vor, diese sind aber oft nicht Bestandteil des Aufgabengebiets des behördlichen Datenschutzbeauftragten
- Datenschutzbeauftragter orientiert sich an gesetzlichen Regelungen, formalen Vorgehensweisen und relevanten Urteilen.
- IT-Sicherheitsbeauftragter zieht bekannte Standards und Vorgehensweisen aus der IT-Sicherheit heran für eine Risikobewertung
- Orientierung an den fünf klassischen Zielen der IT-Sicherheit

Technischer Exkurs: Ziele der IT-Sicherheit

- Datenintegrität
„Daten werden nicht korrumpiert durch technische Fehler oder Manipulationsversuche“
- kontrollierter Zugang
„Authentifizierung (Logins) und Autorisierung (Rollenmodelle)“
- Vertraulichkeit
„Verschlüsselung von Daten“
- Protokollierung
„(Post-Mortem) Revisionsfähigkeit, Zurechenbarkeit“
- Verfügbarkeit
„Garantie, dass die Institution jederzeit auf die IT-Systeme und die gespeicherten Daten zugreifen kann“

Unterschiede im Verhalten des DSB und ITSB nach der Registrierung von Verstößen

- Nach erkanntem Verstoß wird abhängig vom Grad des Vergehens zunächst der Anwender und der Verantwortliche informiert, allerdings mit unterschiedlicher Konsequenz:
- DTSB: Gesetzesverstoß (Datenschutz, ärztliche Schweigepflicht)
→ Gefängnisstrafe für die Beteiligten und Verantwortlichen
- ITSB: evtl. Gesetzesverstoß (BDSG, StGB), wahrscheinlicher aber, dass das Sicherheitsziel Verfügbarkeit gefährdet ist
→ Gefährdung des ordnungsgemäßen Betriebs der Institution
→ sofortiges Handeln notwendig

Entstehung der Stabsstelle IT-Sicherheit

- Ausgangslage: „unabhängige“ Netzabteilung; Kooperation mit der Universität in der Netzbetreuung. Netzabteilung der Universität sah sich als „Netzpolsizei“ (– ehrlich gesagt: war auch notwendig)
- Schreiben des StMWFK aus dem Jahre 2004, dass Institutionen mit Zugang zum Behördennetz einen IT-Sicherheitsbeauftragten benennen sollen
- Protagonisten (Vorstand, CIO, DSB, IT-Lenkungsausschuss) waren für die Einführung und unterstützten diese aktiv

Kenntnisse und Fertigkeiten (1)

- Oft sind Vorschläge (hier z.B. des bayerischen Landesbeauftragter für den Datenschutz) zu Kenntnissen eines IT-Sicherheitsbeauftragten (ITSB) zu lesen:
 - Studium der Informatik o. ä.
 - alternativ dazu, langjährige Erfahrung in der EDV
- nicht generell empfehlenswert, da z.B. im Informatikstudium Vorlesungen über System- oder Netzwerksicherheit weder überall angeboten werden, noch dann dort Pflichtveranstaltungen sind.
- Beratung der Leitungsebene bei der Einstellung notwendig: Bereiten Sie ein fiktives Szenario vor: Bewerber muss Verständnis für einen medizinischen Betrieb haben, muss die Probleme analysieren können und adäquate Lösungsvorschläge anbieten.

Kenntnisse und Fertigkeiten (2)

- Folgende Fähigkeiten und Fertigkeiten wünschenswert:
 - Vorhandensein von technischem Know How im Bereich der IT und die Fähigkeit, in diesem Arbeitsgebiet konzeptionell zu arbeiten
 - Kenntnisse über technische Standards, Vorgehensweisen und Produkte aus dem Bereich der IT-Sicherheit
 - Verständnis für Anforderungen von Institutionen aus dem Medizinsektor, damit Forderungen und Maßnahmen adäquat sind und nicht mehr Schaden anrichten als die Verletzung der IT-Sicherheitsziele
 - Vorhandensein analytischer Kenntnisse und Methoden
 - Ausreichende juristische und organisatorische Kenntnisse um mit d. DSB und den Funktions- und Leitungsstellen zusammenarbeiten zu können
 - Durchhalte- und Durchsetzungsvermögen, da IT-Sicherheit eine sehr langwierige Angelegenheit ist und sich Erfolge oft erst später einstellen

Organisatorische Einbettung

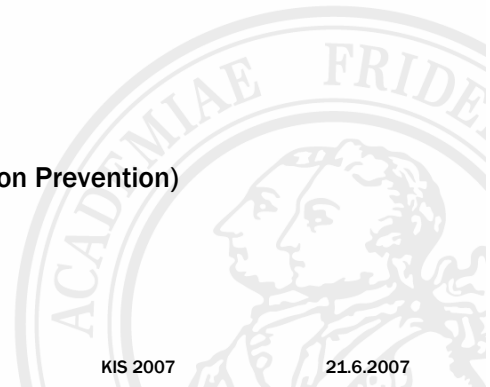
- der IT-Sicherheitsbeauftragte sollte kein Bestandteil des medizinischen Rechenzentrums sein:
 - Freiheit vor Weisungen des RZ-Leiters
 - Neutralität ist gewährleistet
 - Keine operative Verpflichtung eigene Systeme zu betreiben (wirkt sich störend auf die Tätigkeit des ITSB aus)
 - dennoch Nähe zum Medizinischen RZ notwendig
Realisierung am UK Erlangen: Dauergast bei AL-Sitzung des Medizinischen IK-Zentrums
- Unabhängigkeit wichtig:
 - Realisierung am UK Erlangen: Stabsstelle des Vorstands, Berichtspflicht (gegenüber Vorstand, CIO)
- Etablierung einer Arbeitsgruppe:
 - Realisierung am UK Erlangen: ITSB, DSB, Projektleiter für klinischen Arbeitsplatz und medizinische Bildverarbeitung: *Der Sicherheitsrat*

Arbeitsgebiete eines IT-Sicherheitsbeauftragten

- konzeptionelle Tätigkeiten
 - Erstellung von IT-Sicherheitsrichtlinien
 - speziell: Entwicklung eines Fernwartungskonzepts
 - Verbesserung der Schutzmaßnahmen
- Kontrollen
 - Begehung von Kliniken
 - Kontrolle von Systemen und Verfahren
- Tagesgeschäft
 - mehrere Anfragen pro Woche mit kurzfristigem Reaktionswunsch
- *Neu im Angebot: Zusammenarbeit mit Medizinproduktherstellern um deren Installation im Universitätsklinikum zu verbessern*

Werkzeuge und Hilfsmittel

- technische Kompetenz in Kerngebieten:
(Unix, Server, Client, Vernetzung, Anwendungen)
- Kenntnisse über die einschlägigen Sicherheitsstandards
- Zusammenarbeit mit anderen Funktionsstellen im Krankenhaus
 - Datenschutzbeauftragter
 - Einkauf/Controlling
 - Kollegen der Netzabteilung
- SIMS – Security Information Management
- technische Werkzeuge
 - ... zur lokalen Evaluierung eines Systems (Patchlevel)
 - ... zur Evaluierung des Angriffsprofils (Scanner)
 - ... zur Kontrolle des malignen Internetverkehrs (Intrusion Prevention)
 - ...



Erfahrungen und Fazit

- Zusammenarbeit des IT-Sicherheitsbeauftragten mit dem Datenschutzbeauftragten bewirkt eine starke Beschleunigung der Beantwortungszeit auf Anfragen (technische Anfragen)
- Die IT-Sicherheits-Arbeitsgruppe hat sich als weiteres Zugpferd erwiesen
- Großer Umfang des technischen Gebiets:
→ Vor- und Nachbereitung von Besprechungen notwendig.
- Zusammenarbeit/Engagement in der medizinischen Informatik wichtig
- Umfang des Tagesgeschäfts:
 - Anfragen belasten – öffnen aber auch Zugänge
 - Zeitmanagement
 - Abkürzung von Anfragen (d.h. Urteil beendet Anfrage und nicht immer die Bereitstkurzfristige ellung einer Lösung)



- *... es wird immer genug Arbeit geben.*
- Novelle der EU-Richtlinie 93/42/EWG wird Software, die zur Diagnose und Therapie einsetzt als Medizinprodukt plazieren:
→ intensivere Zusammenarbeit mit den Verantwortlichen aus der Medizintechnik
- IEC/ISO 80001 wird vermehrten Einsatz eines IT-Sicherheitsbeauftragten/Network Integrators fordern. In diesem Zusammenhang werden Hersteller das sog. Restrisiko (Vernetzung) an den Betreiber übergeben. „Jemand“ muss das bewerten und beurteilen.
- integrierte Versorgung/Telemedizin
- Ermöglichung des sicheren und schnellen Datenaustauschs von vernetzten Diagnose- und Befundungskomponenten