

AK Sicherheit, 06.05.2009, Protokoll

Thema der Sitzung: Sicherheit in der Gesundheitstelematik

13:00 Registrierung
13:30 Beginn der Sitzung

Herr Schaffrin (Fachbereichsleiter eco) und Herr Dr. Brand (AK-Leiter und Geschäftsführer Pallas) begrüßten die Teilnehmer. Herr Dr. Brand zeigte an drei neuen Meldungen aus dem Krankenhausbereich (digitale Würmer und Lösegeld-Erpressung für Patientendatenbank) die Bedeutung der IT-Sicherheit im Gesundheitsbereich auf. Anschließend wurden verschiedene Aspekte des heutigen Themas in Referaten vorgestellt und in Diskussionen vertieft. Es folgt eine kurze Zusammenfassung, die Beiträge befinden sich im Dokumentenweb des Arbeitskreises (siehe <http://www.eco.de/arbeitskreise/1675.htm>).

Begrüßung und Vorstellung NetCologne

Ivan Andric, Leiter Systemberatung, NetCologne GmbH

Herr Andric (Hausherr der heutigen Sitzung) stellt NetCologne kurz vor. NetCologne sei in den Produktbereichen Privatkunden, MultiKabel und Businesskunden aufgestellt und habe derzeit 778 Mitarbeiter und einen Umsatz von über 300 Mio €.

Datenschutz und IT-Sicherheit: Empfehlungen von BÄK und KBV für Ärzte

Dr. med. Dipl.-Inform. Georgios Raptis, Referent Telematik / IT-Sicherheit, Bundesärztekammer

Die genannten Empfehlungen enthalten einen juristischen Teil sowie eine technische Anlage. Letztere stelle einen Leitfaden für die IT-Sicherheit in der Arztpraxis dar. Der Arzt sei gehalten, für die Umsetzung der organisatorischen Maßnahmen selbst zu sorgen, für den technischen Bereich wird die Hinzuziehung eines IT-Dienstleisters empfohlen, der möglichst eine Konformitätsbestätigung abgeben solle. Rechner mit Patientendaten dürften keine direkte Verbindung ins Internet haben, eine sichere VPN-Verbindung in ein Intranet sei aber erlaubt. Herr Dr. Raptis ging dann auf den elektronischen Arztausweis ein, der der Heilberufsausweis (HBA) der Ärzte sei und den Schlüssel des Arztes zur künftigen Telematikinfrastruktur darstelle. Der eArztausweis werde von der Ärztekammer herausgegeben, die nach KammerIdent-Verfahren die Produktion freigebe. In einer besonders gesicherten Umgebung (zertifizierter Konnektor) sei ein höherer Komfort z.B. durch Stapelsignaturen möglich. Das Zugriffsproblem bei einer späteren Erneuerung eines eArztausweises sei durch die Vergabe einer eindeutigen Telematik-ID für jeden Arzt gelöst. Herr Dr. Raptis bestätigte, dass im derzeitigen Test die vorläufigen Arztkarten mit der elektronischen Gesundheitskarte auf Patientenseite zusammenarbeiten. Er erhoffte sich ein klares Migrationskonzept zu den endgültigen und künftigen Karten.

Sichere Telematikanwendungen der elektronischen Gesundheitskarte (eGK)

Sven Marx, Leiter Datenschutz und Informationssicherheit, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Herr Marx stellte klar, dass die Bedeutung des eGK-Projektes im Aufbau einer Telematikinfrastruktur liege, die eine besondere Herausforderung darstelle durch besonders hohen Schutzbedarf, sehr große Anzahl wenig affiner Nutzer, durch öffentliche und politische Bedeutung. Die gematik habe dabei insbesondere die Aufgabe zu spezifizieren und die Zulassung von Anbietern, Komponenten und Diensten zu überwachen, die Interoperabilität sicherzustellen und die Patientenrechte zu wahren. Neben den Pflichtenwendungen mit der eGK (Stammdaten, eRezept, europäische Krankenversichertenkarte) sei eine Reihe von freiwilligen Anwendungen möglich (z.B. Notfalldaten, eArztbrief, ePatientenakte). Er beschrieb dann die mehrschichti-

gen Sicherheitsmechanismen in der Telematikinfrastruktur (zertifizierte Komponenten, Transportverschlüsselung, Zugriffskontrollen, individuelle Verschlüsselung) und erläuterte insbesondere die Rolle des Konnektors für die sichere Anbindung an das Gesundheitsnetz sowie für Verschlüsselung und Signatur. Für weitere Erläuterungen der Sicherheitsmechanismen verwies er auf das Dokument unter http://gematik.de/upload/gematik_whitepaper_sicherheit_3571.pdf.

Geschäftsmodelle für IT-Sicherheit im Gesundheitswesen

Frank Bodenstein, Business Development Manager, DGN Deutsches Gesundheitsnetz Service GmbH

Wie Herr Bodenstein erläuterte, ist die dgnservice ein Tochterunternehmen der apoBank, welche an 51 % der Existenzgründungen im Gesundheitswesen beteiligt sei. Die dgnservice entwickle elektronische Geschäftsprozesse, betreibe sichere Zugangsnetze und Portale und produziere qualifizierte Signaturkarten, welche über die Schwestergesellschaft medisign im Gesundheitsbereich vertrieben würden. Er erläuterte dann, dass sowohl Vernetzungsprodukte als auch Signaturkarten besser durch konkrete Anwendungen in den Markt gebracht werden könnten. An mehreren konkreten Beispielen belegte er diese These (Online-Abrechnung, Patientenmanagement, Online-Banking).

Aufbau einer hoch sicheren eHealth-Infrastruktur in Baden-Württemberg

Jörg Stadler, Head of eHealth Infrastructure Product House und Dr. Jens Urmann, Product Management Security, InterComponentWare AG (ICW)

Das von den Herren Stadler und Dr. Urmann vorgestellte Projekt setzt auf der neuen hausarztzentrierten Versorgung auf, durch die künftig 30 % bis 40 % der Honorare über Ärzte-Vertragsgemeinschaften ausgeschüttet werden sollen. In einem Projekt mit der AOK Baden-Württemberg seien 951 Arztpraxen mittels ICW-eigenem Healthcare Connector angebunden worden. Die AOK bekomme damit künftig die Möglichkeit, die Auswirkungen einer ePatientenakte auf das Gesundheitsverhalten der Versicherten zu erforschen. Die Komponenten und Sicherheitsfunktionen des Healthcare Connectors wurden vorgestellt, wobei ICW zwei Modelle einsetzt, einen auf Basis der Cisco AXP und einen SINA-basierten. Wichtige Erfahrungen aus dem vorgestellten Projekt seien die günstige TCO durch Fernwartbarkeit der Komponenten und die Erkenntnis, dass die Stolpersteine eines Massen-Rollouts schon bei der Terminvereinbarung beginnen. Im Hinblick auf den schwierigen Konnektoren-Markt und eine absagende Verlautbarung von Siemens bekräftigt Herr Stadler, dass sich ICW nicht aus dem Konnektorenengagement zurückziehen wolle.

Die aktuelle Lage im Sicherheitsbereich

Dr. Kurt Brand, Arbeitskreisleiter und Geschäftsführer Pallas GmbH

Herr Dr. Brand zeigt mittels einer Pallas-Statistik, dass der Spam-Anstieg der letzten 6 Wochen so stark wie nie zuvor gewesen sei. Der Kredit-Spam habe sich passend zur Wirtschaftskrise im ersten Quartal 2009 verzehnfacht, für Phishing frisierte Webseiten seien am häufigsten im Gesundheitsbereich anzutreffen. Er glaubt, dass die in der Politik diskutierte Selbstbeteiligung von Managern bei eigenverursachten Schäden positive Impulse für den Security-Markt bringen könnte. Er ging sodann auf die Gefährdungstrends nach der neuen BSI-Studie "Die Lage der IT-Sicherheit in Deutschland 2009" ein.

Verschiedenes, Themen und Termine

Der Arbeitskreis tagt an drei festen Terminen pro Jahr, und zwar jeweils am ersten Mittwoch der Monate 02 / 05 / 10. Die nächste Sitzung findet also am 07.10.2009 statt, das Thema wird später festgelegt, Input ist willkommen.

17:45 Ende der Sitzung
gezeichnet: Dr. Kurt Brand (Arbeitskreisleiter), 12.05.2009