Please quote as: Sunyaev, A.; Dünnebeil, S.; Mauro, C.; Leimeister, J. M.; Krcmar, H. (2009): Sicherheitsbetrachtung der Primärsysteme in der Deutschen Gesundheitstelematik. In: Proceedings of 54. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS). Essen, 07.-10.09.2009.

Sicherheitsbetrachtung der Primärsysteme in der Deutschen Gesundheitstelematik

Sunyaev A.[1], Dünnebeil S.[1], Mauro C.[1], Leimeister J.M.[2], Krcmar H.[1]

[1] Technische Universität München, Lehrstuhl für Wirtschaftsinformatik
[2] Universität Kassel, Lehrstuhl für Wirtschaftsinformatik

Einleitung

Die geplante Einführung der elektronischen Gesundheitskarte (eGK) in Deutschland setzt den Aufbau einer nationalen Gesundheitstelematikplattform voraus. Die technischen Komponenten dieser Telematik Infrastruktur (TI) lassen sich in zwei Klassen gliedern:

- Zentrale Komponenten: Zugangsnetz, Broker, Backbonenetz, Zeitstempel, Public-Key-Infrastruktur, Auditierung, Directory Services sowie die Fachdienste.
- Dezentrale Komponenten: Smartcards, Kartenterminals sowie Konnektoren.

Eine sichere Internetverbindung soll die Kommunikation zwischen den beiden Bestandteilen der TI gewährleisten.

Methoden und Ergebnisse

Die dezentralen Komponenten der TI werden von den Leistungserbringern – z. B. Arztpraxen, Krankenhäusern oder Apotheken – verwaltet [1]. Über sogenannte Primärsysteme, wie Praxisverwaltungs- und Krankenhausinformationssysteme, können die Leistungserbringer die Funktionalitäten der Telematikdienste nutzen. Da Primärsysteme auf handelsüblichen Rechnern installiert werden, wird dabei auch auf standardisierte Dienste und Programme zurückgegriffen (Internet, Email etc.). Diese Anwendungen erhöhen das Angriffsrisiko auf Primärsysteme, die medizinische Informationen der behandelten Patienten elektronisch verarbeiten. In dieser Arbeit wurden die in Abbildung 1 dargestellten Angriffsszenarien auf medizinische Primärsysteme identifiziert und in Laborexperimenten getestet:

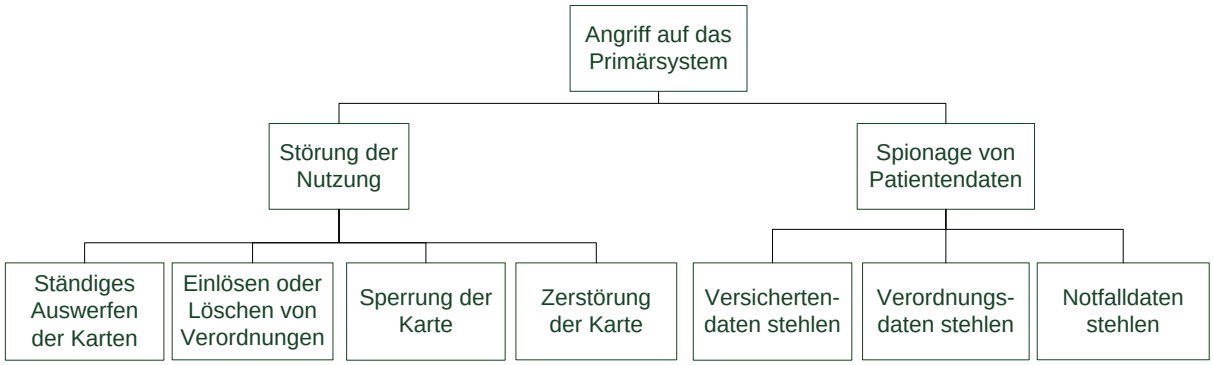

Abbildung 1: Untersuchte Angriffsszenarien auf die dezentralen Komponenten der TI

Die Verbindung zwischen Primärsystem und Konnektor ist nicht verschlüsselt. Die unverschlüsselte Datenübertragung wird von der gematik als „Restrisiko“ bewusst in Kauf genommen [2,3]. Weiterhin wird bei der Kommunikation zwischen Primärsystem und Konnektor auf eine Authentifizierung verzichtet. Dies kann zu einer unautorisierten Nutzung der Konnektorfunktionen führen.

Ausblick

Es lässt sich schlussfolgern, dass die Verbindung zwischen Primärsystem und Konnektor verschlüsselt werden und eine Authentifizierung gegeben sein sollte. Diese Lösung ist kostengünstig und unkompliziert umsetzbar. Weiterhin sollte ein Sicherheitskonzept für Primärsysteme spezifiziert werden, momentan werden die Primärsysteme von der gematik nicht als Teil der TI angesehen [4] und somit außen vor gelassen.

Als nächstes gilt es, die dezentralen Komponenten weiteren Penetrationstests auszusetzen, um (z. B. durch Man-in-the-middle-Angriffe zwischen verschlüsselten Netzwerkkomponenten der TI sowie durch Hardware-Manipulationstests) rechtzeitig vor der flächendeckenden Einführung der eGK technische Sicherheitsrisiken auf der Primärsystemseite minimieren zu können.

Literatur

[1] gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008. Konnektorspezifikation. Version 2.8.0. Seite 8.

[2] gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008. Spezifisches Sicherheitskonzept der dezentralen Komponenten - Einboxkonnektor-Szenario. Version 0.9.0 Kandidat. Seiten 16-17.

[3] gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008. Übergreifendes Sicherheitskonzept der Gesundheitstelematik. Version 2.3.0. Seite 297.

[4] gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008. Gesamtarchitektur. Version 1.4.0. Seite 71.