HEALIX – PROAKTIVE SICHERHEIT FÜR DEN ELEKTRONISCHEN AUSTAUSCH VON GESUNDHEITSDATEN

Mense A[1], Hoheiser-Pörtner F[2], Wahl H[1]

Kurzfassung

*In Zeiten der Umsetzung der elektronischen Gesundheitsakte (ELGA) und internationaler Großveranstaltungen in Österreich kommt einer sicheren Kommunikationsinfrastruktur für die medizinische Versorgung eine zentrale Bedeutung zu. Das Projekt HEALIX (e-**HEAL**th **I**ntere**X**change) beschäftigt sich mit dem Aufbau einer e-Health Kommunikationsarchitektur, welche sich von dem Ansatz einer impliziten Sicherheit in geschlossenen Netzen löst und neben einer dezentralen sicheren physikalischen Basis auch proaktive Sicherheitskomponenten - z.B. für die Erkennung und Weiterreichung von Informationen bei Auftreten potentieller Bedrohungen – definiert. Damit wird es möglich Sicherheitszwischenfälle in dieser kritischen Infrastruktur rasch zu erkennen, über effiziente Strukturen zu kommunizieren und die Auswirkungen zu verhindern, zu minimieren oder zumindest lokal zu begrenzen. HEALIX implementiert somit ein Kommunikationssystem für Bedrohungen im E-Health und eine virtuelle operative Krisenmanagementarchitektur.*

1. Einleitung

Die Bedeutung des Schutzes von Gesundheitsdaten vor missbräuchlicher Verwendung sowohl bei der Speicherung als auch bei der Übertragung steht außer Frage. Dem wird auch im rechtlichen Sinn durch zahlreiche Gesetze und Vorgaben Rechnung getragen. Speziell dem Schutz des elektronischen Austauschs solcher, gem. Definition im Datenschutzgesetz [1] und Gesundheitstelematikgesetz [2], spezieller sensibler Daten über weit reichende Netzwerke kommt bei Überlegungen zur Informationssicherheit aufgrund der Kritikalität dieser Basisfunktionalität eine wesentliche Bedeutung zu. Bisherige Ansätze zum Schutz der Datenkommunikation gehen dabei häufig von geschlossenen Infrastrukturen und einer damit implizit gegebenen hohen Sicherheit gegen Störeinflüsse aus. Das Projekt HEALIX (e-**HEAL**th **I**ntere**X**change der Krankenanstalten) hat sich zum Ziel gesetzt eine Kommunikationsarchitektur für Teilnehmer in e-Health Prozessen zu entwickeln, die nicht nur auf eine ausfallsichere physische Basis aufsetzt sondern auch eine explizite proaktive logische Sicherheitsarchitektur beinhaltet, welche auf eine breite technische und organisatorische Vernetzung der beteiligten Akteure aufbaut. Vorliegendes Dokument gibt einen Überblick über inhaltliche Strukturen und geplante Aktivitäten des Projekts das gerade erst begonnen wurde.

[1] Fachhochschule Technikum Wien, Institute of Information Engineering & Security
[2] Wiener Krankenanstaltenverbund

2. Kritische (Informations-) Infrastrukturen

Das Bundesamt für Informationssicherheit in Deutschland definiert kritische Infrastrukturen wie folgt:

> „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." ([3])

Kommt es zu Ausfällen oder Störungen in entsprechenden Infrastrukturen so können unter Umständen Kettenreaktionen ausgelöst werden, die zu wesentlichen Beeinträchtigungen des öffentlichen Lebens führen können. Informationstechnik und Telekommunikation ist dabei in praktisch fast allen Bereichen ein wesentlicher Faktor für das Funktionieren der Infrastruktur. Diese bilden dabei einen eigenen Infrastruktursektor, beschreiben aber auch eine Querschnittsinfrastruktur von der viele Sektoren abhängig sind (siehe [3]). Der Schutz kritischer Infrastrukturen (Critical Infrastructure Protection – CIP) und kritischen Informations-Infrastrukturen (Critical Information Infrastructure Protection – CIIP) sind daher ein wesentliches nationales aber auch EU weites Ziel [4].

Diesen Definitionen folgend sind Einrichtungen der medizinischen Versorgung und assoziierte Gesundheitsdiensteanbieter (GDA) als kritische Infrastrukturen einzustufen. Dabei sind mehr und mehr Prozesse von einer funktionierenden Informationsinfrastruktur abhängig. Eine weitgehende Vernetzung verschiedenster medizinischer Institutionen, welche bereits heute für den medizinischen Datenaustausch benötigt wird und mittelfristig für das Funktionieren einer verteilten flächendeckenden Versorgung und die Implementierung einer verteilten Gesundheitsakte unabdingbar ist, bringt jedoch zunehmend Gefahren für den Datenverkehr aber auch für lokale Infrastrukturen.

Aus diesem Grund ist der Aufbau eines Österreich-weiten Sicherheitsmanagements für eine sichere Vernetzung im e-Health Umfeld als Aufgabe hoher Priorität zu sehen.

3. HEALIX - Sicherheitsphilosophie

Das Datenschutzgesetz schreibt beim Umgang mit personenbezogenen sensiblen Daten zwangsläufig den Einsatz entsprechender Datensicherheitsmaßnahmen vor. Diese werden in der Regel im Rahmen einer umfassenden Informationssicherheit abgebildet in deren Zusammenhang die Analyse von Bedrohungen und damit verbundener Risiken essentiell ist. Im Rahmen einer Risikoanalyse werden alle Bedrohungen erfasst und im Bezug auf die Sicherheitsgefährdung kategorisiert, wobei diese Erfassung lückenlos und ohne versteckte Annahmen durchzuführen ist und das Verfahren transparent zu machen ist (vgl. [5])! Dieses trifft umso mehr noch für entsprechende kritische Informationsinfrastrukturen zu. Deshalb wird im Rahmen von HEALIX ein holistischer und standardbasierter Ansatz für den Umgang mit Sicherheit gewählt. Es werden Analysen und Maßnahmen auf technischer, organisatorischer und menschlicher Ebene berücksichtigt.

4. Sicherheitsarchitektur

Die Sicherheitsarchitektur von HEALIX baut auf folgende wesentlichen Ebenen auf:

1) Ausfallsichere physikalische Ebene, welche eine Sicherheitssektorenbildung innerhalb des Netzwerkes ermöglicht
2) Kombinierte technische und organisatorische Informationssicherheitsebene, welche eine frühzeitige Erkennung von kritischen Ereignissen ermöglicht und definierte Maßnahmen auslöst.
3) Melde- und Warn- Kommunikationsebene, welche auf einem engen Netzwerk von Verantwortungsträgern im IT-Bereich beruht und eine effiziente Meldekette ermöglicht

Die größten Herausforderungen stellen die Punkte 2 und 3 obiger Liste dar, da es in diesen Bereichen bisher kaum Erfahrungswerte gibt.

5. Technische Infrastruktur

Das Rückgrad des Netzwerkes bildet eine ausfallsichere Netzwerkstruktur welche von einem österreichischen Telekomanbieter über ein Netz der österreichischen Energieversorger aufgebaut wird. Der geplante Aufbau der Strukturumfasst wie in *Abbildung 1* dargestellt mehrere Ebenen.

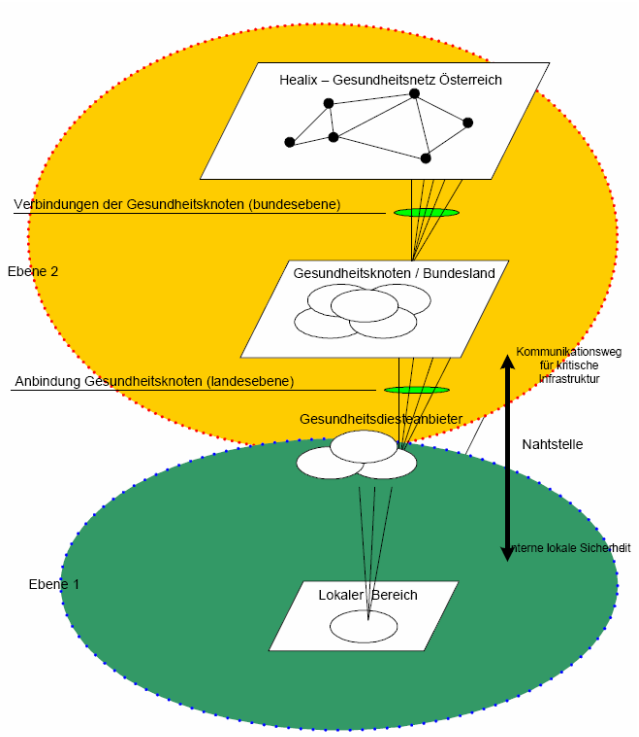

Abbildung 1. Ebenenstruktur Healix

Die unterste Ebene stellen die lokalen Netzwerke der Krankenhäuser oder Gesundheitseinrichtungen dar wobei diese in der Regel auch regional vernetzt sind. Diese Netze werden jeweils an einen Gesundheitsknoten je Bundesland angebunden. Diese stellen die Verbindung zwischen den GDAs der einzelnen Bundeländer und dem nationalen HEALIX Backbone dar. Dieser Backbone umfasst ganz Österreich und ist als Ringschaltung mit teilweiser Vermaschung ausgeführt. Durch die Implementierung der Gesundheitsknoten ist im Notfall eine stufenweise Isolation von sicherheitskritischen Abschnitten möglich (d.h. durch Trennung einzelner Knoten vom Backbone kann die Ausbreitung von Sicherheitszwischenfällen verhindert und eine lokale Kommunikation aufrecht erhalten werden).

6. Informationssicherheit – Herausforderungen und Ziele

Leider gibt es noch sehr wenig Erfahrungen im Bereich der Erkennung von Krisenfällen in großen Netzwerken und damit verbunden auch weder praktische noch akademische befriedigende Lösungen. Wie bereits im Bericht über die „C(I)IP Aktivitäten in Österreich“ festgehalten wird ist beim Schutz von Informations-Infrastrukturen eine besondere Situation gegeben:

> „Ein CIIP Verhaltensmuster in einer Katastrophe, das uns ein hinreichend nachahmbares Vorbild gegeben hätte, können wir allerdings nicht beisteuern. Insgesamt wird dies an der Komplexität und an der Vernetzung dieser Systeme liegen, da Krisenfälle in ihrer Vernetzung auch keine Test- bzw. Trainingsmöglichkeit bieten. Umso wichtiger ist das Erstellen von Systematiken und Krisenablaufplänen“ ([6], Seite 3)

Hier setzt die analytische Arbeit des HEALIX Projektes an. Es werden die Komponenten von kritischen Informationsinfrastrukturen im e-Health Bereich erhoben, katalogisiert und kategorisiert und Anforderungen an diese ermittelt. Darauf aufbauend wird eine gemeinsame Terminologie für die weiteren Schritte definiert.

Durch Analysen von Angriffstrukturen auf Informations-Infrastrukturen der letzten Jahre und deren Ausbreitung und Auswirkungen werden Strukturen zur Vorbeugung, Anomalien- und Angriffserkennung, für Schutzmaßnahmen und für die Kommunikation erarbeitet.

Auf Basis der ermittelten Klassen von Bedrohungen und deren Charakteristika werden Systematiken erstellt, Ablauf-/Notfallpläne und Meldewege erarbeitet und gemeinsam abgestimmt. Hierbei folgt eine Vernetzung mit entsprechenden nationalen Sicherheitsorganisationen. Als mögliches Resultat soll eine angepasste, erweiterte Form des österreichischen Sicherheitshandbuches für den Gesundheitsinformatikbereich entstehen.

Darauf aufbauend werden technische Maßnahmen zur automatisierten Erkennung von Anomalien und Bedrohungen bzw. zur Alarmierung aufgesetzt. Die Alarmmeldungen laufen in eine gemeinsame Warnzentrale wo Sie zentral ausgewertet und mit Maßnahmen verknüpft werden. Eine wesentliche Aufgabe stellt dabei die Untersuchung der gegenseitigen Abhängigkeiten und der Zusammenhänge von Alarmmeldungen dar.

7. Meldewesen und Warnzentrale

Die Überwachung des Netzwerkes erfolgt durch eine gemeinsame Warnzentrale. Dort laufen sowohl automatisierte Alarmierungen als auch manuelle Meldungen verantwortlicher IT-Stellen zusammen und werden ausgewertet. Computer Emergency Response Teams (CERTs) bewerten die Daten und leiten technische bzw. organisatorische Schritte ein welche über definierte kurze Meldewege kommuniziert werden. Die Definition der effizienten und effektiven Meldewege und Ablaufpläne erfolgt im Rahmen der Analysephase (vgl. Abschnitt 6.).

8. Zusammenfassung

Eine funktionierende Informationskommunikationsinfrastruktur im Bereich des Gesundheitswesens ist für die Gesundheitsversorgung bereits heute unerlässlich und deren Bedeutung wird in den kommenden Jahren noch rapide steigen. In diesem Zusammenhang stellt die Vernetzung bereits

existierender lokaler Infrastrukturen auf gesamtösterreichischer (und weiters auf europäischer) Ebene eine zentrale Aufgabe dar. Mit dem Wachsen der Netze steigt jedoch auch insgesamt die Bedrohung der Informations- und Kommunikationssysteme und die Gefahr von Angriffen auf diese kritischen Komponenten steigt zunehmend. Deshalb sind umfassende Konzepte zum Schutz dieser kritischen Infrastruktur dringend erforderlich!

Das HEALIX Projekt beschäftigt sich mit

- der Möglichkeit einer hochverfügbaren und sicheren österreichweiten Vernetzung von Informationssystemen im Gesundheitsbereich
- der umfangreichen Erkennung, Analyse und Qualifizierung von Bedrohungen
- der Definition von erforderlichen Maßnahmen sowie Organisations- und Kommunikationsstrukturen auf technischer und organisatorischer Ebene
- sowie der Schaffung einer logischen Sicherheitsebene zwischen physikalischer Infrastruktur und den Gesundheitsinformationssystemen.

Dabei müssen die Ergebnisse von HEALIX dem hochkomplexen, über die Grenzen einzelner Bedarfträgerprozesse, hinausgehende Zusammenspiel auf technischer, organisatorischer und verfahrensorientierter Ebene unter Berücksichtigung der Datenschutzbestimmungen Rechnung tragen. Das bedeutet die Notwendigkeit einer starken technischen aber auch sozialen Vernetzung der Organisationen und die Schaffung kurzer „Meldewege“ für die Kommunikation mit allen Bedarfsträgern.

Durch den proaktiven Ansatz können Bedrohungen und Angriffe rascher erkannt und über die Kommunikationsstrukturen effektiv abgefangen werden.

Ziel ist letztendlich die Schaffung eines Sicherheitsschildes für die Republik Österreich im Bereich der umfassenden Vernetzung der Informations- und Kommunikationssysteme des Gesundheitswesens.

9. Literatur

[1] Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999

[2] Gesundheitstelematikgesetz (GTelG), BGBl. 1 Nr. 179/2004

[3] Bundesamt für Informationssicherheit, http://www.bsi.bund.de/fachthem/kritis/index.htm, Zugriff 01.02.2008

[4] Kommission der Europäischen Gemeinschaften, Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen, Brüssel 2005

[5] Österreichisches Bundeskanzleramt, Österreichisches IT-Sicherheitshandbuch, Version 2.3, April 2007

[6] POSCH, R., LEITOLD H., C(I)IP Aktivitäten in Österreich, Wien 2005

[7] Bundesamt für Informationssicherheit, Die Lage der IT-Sicherheit in Deutschland 2007, Köln 2007

[8] DUNN M., WIGERT I., International CIIP Handbook 2006 (Vol.I), ETH Zurich 2006, ISBN 3-905696-07-X

[9] DUNN M., WIGERT I., International CIIP Handbook 2006 (Vol.II), ETH Zurich 2006, ISBN 3-905696-08-8