Der Gesundheitsbrowser – sicher browsen im Internet

Lars Hilker
Zentrum für Telematik im Gesundheitswesen GmbH

Der Gesundheitsbrowser ermöglicht den Anwendern im Gesundheitswesen die Nutzung des Internetdienstes WWW und schützt gleichzeitig die sensiblen Daten auf den Systemen mit gleichzeitiger Patientendatenverarbeitung.
Der auf der Mozilla-Architektur basierende Internetbrowser wird nach Common Criteria Entwicklung begleitend evaluiert und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert. Die Sicherheitsvorgabe lehnt sich dabei dem BISS-Schutzprofil („Benutzerbestimmbare Informationsflusssicherheit") des BSI an.
Das im August 2003 gestartete Projekt ist ein Baustein der Landesinitiative eHealth.nrw und wird durch die Landesregierung Nordrhein-Westfalen im Rahmen der Initiative secure-it.nrw 2005 gefördert.

Ausgangssituation

Um die Attraktivität des Internets noch weiter zu steigern, wird bei der Entwicklung von Internetseiten mehr und mehr auf Dynamik und Flexibilität gesetzt. U. a. mit den weit verbreiteten Technologien Java, Java Script und ActiveX, aber auch durch Plugins, die der Erweiterung der Browserfunktionalität dienen.

Der Einsatz dieser Technologien hat aber auch zur Folge, dass durch das unbemerkte Ausführen der in den Internetdokumenten vorkommenden Programme, ein Zugriff auf die lokalen Dateien des Nutzers erfolgen kann. Das kann schwer wiegende Auswirkungen für die gesamte Systemumgebung der betroffenen Einrichtung im Gesundheitswesen haben, da Personen bezogene Daten ausgelesen, modifiziert oder gar gelöscht werden können. Ebenso kann auch der Zugriff auf lokale Ressourcen wie den Arbeitspeicher, die Betriebssicherheit eines Systems beeinträchtigen. Ist der betroffene Rechner einem Netzwerk angebunden, ist der Schaden meist weitaus höher.

Die Rede ist hier von aktiven Inhalten, deren ausgelöste Aktionen in der Regel nicht verhindert werden können. Insbesondere mit dem häufig in Webseiten eingebundenen Java-Script verbindet man diese Gefahr. Bei aktiviertem Scripting bieten handelsübliche Browser keinen ausreichenden Schutz. Ebenso kann der alleinige Einsatz von Firewalls diese Bedrohungen nicht abwehren.

Da die hochsensiblen Patientendaten beispielsweise auf Klinik- oder Arztpraxiscomputern höchsten Sicherheitsanforderungen unterliegen, sind diese vor unberechtigtem Zugriff zu schützen. Um ein Höchstmaß an Sicherheit zu gewährleisten, fordert der Bundes- und Landesdatenschutz daher die strikte Trennung von Patientendaten und Internet.

Diese Forderung steht allerdings der stetig wachsenden Bedeutung des Internets gegenüber, dessen Nutzung künftig in Einrichtungen des Gesundheitswesens nicht mehr wegzudenken ist. Medizinische Online-Datenbanken stellen da nur eine der wertvollen Informationsquellen dar.

Eine physische Trennung von Internet und Patientendaten kann daher keine zeitgerechte und für den Arbeitsalltag praktikable Lösung sein. Diese Erkenntnis war gleichzeitig auch die Motivation zur Realisierung eines sicheren Browsers für das Gesundheitswesen.

Ziele und Funktion des Gesundheitsbrowsers

Das Ziel des Gesundheitsbrowsers ist es, allen Akteuren im Gesundheitswesen eine sichere, komfortable und kostengünstige Lösung anzubieten, die den Internetdienst WWW von ihren Patientendaten verarbeitenden Systemen aus nutzen möchten. Zu diesen Akteuren zählen u. a. das Personal in Arztpraxen, Krankenhäusern, Apotheken und Krankenkassen. Er soll die hohen Datensicherheitsanforderungen im Gesundheitswesen mit der Nutzung des unsicheren Internetdienstes WWW vereinbaren und hat die Aufgabe, die von aktiven Inhalten ausgehenden Risiken abzuwehren, ohne dass die Deaktivierung bestimmter aktiver Komponenten, wie Java und Java-Script, notwendig wird. Mit dem sicheren Gesundheitsbrowser werden sicherheitsrelevante Technologien, wie Firewall und Virenscanner, zwar nicht überflüssig, aber sinnvoll zu schon bestehenden Sicherheitsanforderungen ergänzt.

Um diese Ziele umzusetzen, wird der Gesundheitsbrowser dem Nutzer anzeigen, wenn von seinem System aus unbemerkt Daten während der Internetsitzung verschickt werden sollen, womit ein ungewollter Datenversand unterbunden werden kann. Er verweigert zudem den Zugriff auf sensible Bereiche des Systems, während der Nutzer online ist und verhindert, dass unerwünscht Daten gelesen, modifiziert oder gelöscht werden. Ein privilegierter Nutzer kann dazu Informationsflussregeln für verschiedene Nutzer an-

Autor: Lars Hilker
Titel: Der Gesundheitsbrowser – sicher browsen im Internet
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2005
Seite: 242-245

legen und festlegen, welche Dateiformate, Operationen und Informationskategorien für welchen Nutzer zugelassen werden. Die Informationsflüsse zwischen WWW und dem Gesundheitsbrowser werden somit kontrollierbar.

Damit der Nutzer dem Gesundheitsbrowser Vertrauen entgegenbringt, werden die zum Mozilla Firefox entwickelten Komponenten (s. Abb. 2) Entwicklung begleitend evaluiert und zertifiziert. Für die Entwicklung des sicheren Browsers wird dazu auf den ISO-Standard 15408 (Common Criteria - CC) sowie auf die BISS-Schutzprofile zurückgegriffen.

Zertifizierung nach Common Criteria

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Schutzprofile (Protection Profiles – PP) BSI-PP-0007-2002 und BSI-PP-0008-2002 beschreiben auf Basis des international anerkannten CC-Kriterienwerkes Sicherheitsanforderungen für Produktklassen, für die eine benutzerbestimmbare Informationsflusskontrolle realisiert werden soll. Die durch die Schutzprofile ausgedrückten Sicherheitsanforderungen werden für den Anwendungsfall „Browsen im Internet“ angepasst und in einer konkreten Sicherheitsvorgabe (Security Target – ST) umgesetzt. Die Sicherheitsvorgabe ist dabei das Basisdokument für die Evaluierung des Gesundheitsbrowsers, welche dem Evaluator die Evaluation, aber auch dem Entwickler die Arbeit im Sinne einer durchgängig strukturierten und transparenten Dokumentation erleichtert. Die hohe Transparenz trägt wesentlich dazu bei, dass Fehler und somit potentielle Sicherheitslücken bei der Evaluation aufgedeckt und frühzeitig vermieden werden können.

Neben der technischen Evaluation durch eine vom BSI akkreditierte Prüfstelle werden die vollständige Dokumentation und somit auch die Sicherheitsvorgabe zum Gesundheitsbrowser geprüft und bewertet. Sie beschreibt u. a. das Produkt bzw. den so genannten Evaluationsgegenstand (EVG) nach der in der Abb. 1 gegliederten Struktur. Hierzu beinhaltet das Kapitel 2 des CC-Kriterienkataloges nach Klassen, Familien und Komponenten gegliederte, funktionale Sicherheitsanforderungen, aus denen für den Gesundheitsbrowser relevante Komponenten, ausgehend von den Annahmen und der existenten Bedrohungslage im Gesundheitswesen, gewählt wurden. Die einwandfreie Sicherheitsfunktionalität wird durch die in den CC beschriebenen und zu erfüllenden Abhängigkeiten gewährleistet. Hingegen wird die Vertrauenswürdigkeit im Wesentlichen durch Prüfung und Bewertung geschaffen. Hier stellt das Kapitel 3 der CC die für die Erstellung der Sicherheitsvorgabe notwendigen Vertrauenswürdigkeitskomponenten zur Verfügung, auf deren Grundlage die Evaluation durchgeführt wird.

Für den Gesundheitsbrowser wurde vorab die Vertrauenswürdigkeitsstufe EAL 1 (Evaluation Assurance Level), zunächst als ausbaufähiger Entry-Level festgelegt, der die Verwendung bestimmter, zu erfüllender Vertrauenswürdigkeitskomponenten vorschreibt.

Die Struktur der Sicherheitsvorgabe (s. Abb. 1) zum Gesundheitsbrowser ist analog der in den Schutzprofilen vorgegeben Struktur gegliedert.

Umsetzung der benutzerbestimmbaren Informationsflusskontrolle

Gerade der Phase der Spezifikation kommt innerhalb von IT-Projekten immer eine hohe Bedeutung zu, der vorab eine Analyse der Anforderungen an den Gesundheitsbrowser aus Sicht der Zielgruppen vorausging, um letztendlich eine hohe Akzeptanz zu erreichen. In der Spezifikation wurden dazu sicherheitsrelevante Eigenschaften neben den Aspekten der Funktionalität bzw. Nutzerfreundlichkeit berücksichtigt und umgesetzt. Dabei galt der Grundsatz, die Sicherheitsleistung des Browsers möglichst hoch zu halten, ohne die Funktionalität wesentlich zu beeinträchtigen.

Der Gesundheitsbrowser setzt das Prinzip der benutzerbestimmbaren Informationsflusskontrolle für das Browsen im Internet um. D. h., dass die Sicherheitspolitik des Gesundheitsbrowsers Informationsflüsse kontrolliert, die zwischen dem lokalen System und dem WWW erfolgen. Ein Informationsfluss bezeichnet dabei das Auslesen von Informationen aus Dateien oder das Schreiben von Informationen in Dateien.

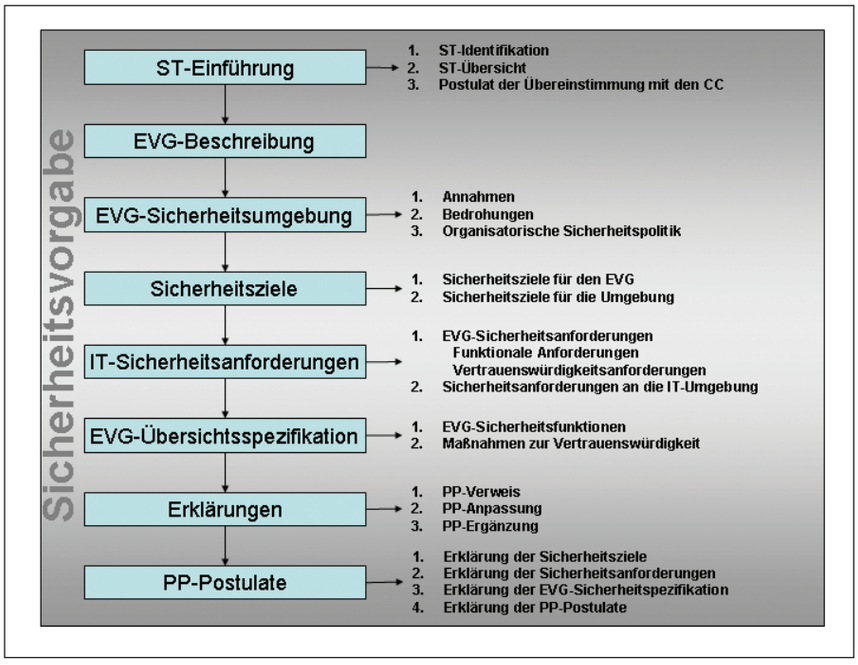

Abbildung 1: *Struktur der Sicherheitsvorgabe (Security Target - ST)*

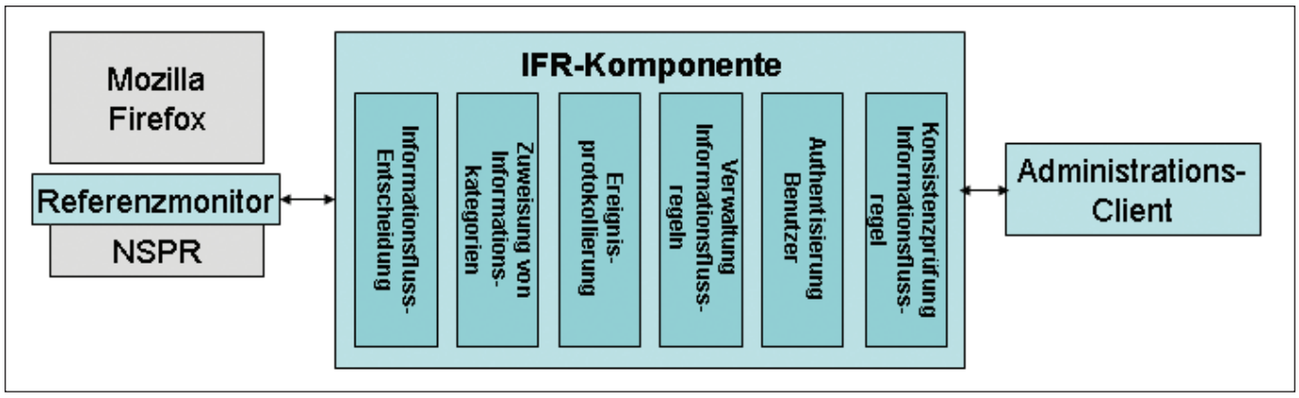

Abbildung 2: *Architektur des Gesundheitsbrowsers*

Der Gesundheitsbrowser gewährleistet, dass keine Daten aus lokalen, schutzwürdigen Dateien in das Internet gelangen und keine Daten aus dem Internet in lokale Dateien geschrieben werden. Die Entscheidung, ob ein Informationsfluss zulässig ist oder nicht, wird dabei ausschließlich auf Basis von Informationsflussregeln (IFR) getroffen, mit denen alle zulässigen Informationsflüsse beschrieben werden. Grundsätzlich werden somit alle Informationsflüsse verboten, die nicht ausdrücklich durch eine Informationsflussregel erlaubt sind. Patientendaten sowie andere zu schützende Daten lassen sich dadurch wirkungsvoll schützten.

IFR werden anhand der Nutzer, der Operationen und anhand von Verzeichnissen festgemacht. So kann über die IFR festgelegt werden, welche Nutzer welche Informationsflüsse anfordern dürfen. Die Angabe der Operation ist dazu notwendig, um unterscheiden zu können, ob Informationen an das Internet übertragen oder in das lokale Dateisystem geschrieben werden.

Die Besonderheit bei der Realisierung einer Benutzer bestimmbaren Informationsflusskontrolle für den Gesundheitsbrowser liegt in der Unterscheidung zwischen vertraulichen und nicht vertraulichen Informationen. Dazu werden Verzeichnisse in den IFR festgelegt aus denen Informationsflüsse in das Internet zugelassen werden können, sofern der Nutzer diesen ausdrücklich zustimmt. Dies trifft auch auf alle Unterverzeichnisse dieser Verzeichnisse zu. Alle anderen Informationsflüsse werden durch den Gesundheitsbrowser abgewehrt und dürfen nicht über Regeln gestattet werden.

Gegebenenfalls weisen IFR Einschränkungen auf, denen, bevor ein Informationsfluss gestattet wird, entsprochen werden muss. So kann bspw. verhindert werden, dass ein Informationsfluss mit bestimmten Dateitypen (z. B. *.txt) stattfindet. Auch die Zulässigkeit von Informationsflüssen kann an die explizite Erlaubnis durch den Nutzer gebunden sein.

Für die Durchsetzung der funktionalen Sicherheitspolitik des Gesundheitsbrowsers ist es erforderlich, dass sich die IFR nicht widersprechen. Diese Anforderung wird vor allem dann wichtig, wenn die zulässigen Informationsflüsse durch mehrere unterschiedliche IFR spezifiziert werden. Damit eine Liste von IFR als konsistent gilt, müssen gewisse Eigenschaften erfüllt sein, die sicher stellen, dass es zu einer eindeutigen Selektion der Regeln kommt.

Es muss also vor der Entscheidung, ob ein Informationsfluss genehmigt wird, die heranzuziehende IFR selektiert werden.

Informationsflussregeln, also zulässige Informationsflüsse, werden von einem als vertrauenswürdig eingestuften EVG-Administrator definiert. Ihm wird damit das Recht eingeräumt, die Benutzer des Gesundheitsbrowsers zu bestimmen und in den IFR festzulegen. Zudem obliegt dem EVG-Administrator, neben der Zuständigkeit für die sicherheitsspezifische Konfiguration des Gesundheitsbrowsers, die Auswertung von Ereignisprotokollen.

Es werden weitere Rollen unterschieden, zu denen der für die Installation des Gesundheitsbrowsers verantwortliche IT-Administrator und der als Web-Angreifer bezeichnete Urheber von verfügbaren Informationen im Internet gehört. Letzterer gehört nicht zu den Nutzern des lokalen Systems und gilt als potentieller Angreifer. Zusätzlich werden die IT-Benutzer unterschieden, die nicht in den IFR aufgeführt sind. Sie sind jedoch autorisiert das lokale System einschließlich des Gesundheitsbrowsers zu nutzen.

Die Aktivität des Gesundheitsbrowsers bleibt für den Nutzer weitest gehend transparent. Er wird bei unzulässigen Informationsflüssen und bei Informationsflüssen, für welche der Benutzer die Erlaubnis erteilen muss, sichtbar. Ein Nutzer muss sich explizit beim Gesundheitsbrowser authentifizieren. Dadurch ist eine Unterscheidung mehrerer Personen möglich, ohne dass bei einem Nutzerwechsel eine Ab- und Neuanmeldung am Betriebssystem erforderlich ist. Der Gesundheitsbrowser verfügt somit über eine eigene Nutzerverwaltung. Bis auf den Gesundheitsbrowser-Administrator, der sich am Betriebssystem authentifiziert, melden sich alle über den Browser an [2].

Architektur des Gesundheitsbrowsers

Die Abbildung 2 stellt die Komponenten des Gesundheitsbrowsers (türkis hinterlegt) dar, so dass die Architektur des Gesundheitsbrowsers ersichtlich wird.

Der Gesundheitsbrowser basiert auf der Mozilla-Firefox-Architektur. Diese Architektur weist eine dedizierte Schicht zum

Zugriff auf Betriebssystemfunktionen auf, über die alle Informationsflüsse zwischen lokalem Dateisystem und angebundenem Netz verlaufen. Der Gesundheitsbrowser setzt dabei auf dieser Zwischenschicht, der so genannten Netscape Portable Runtime (NSPR) auf und kann alle Informationsflüsse registrieren und kontrollieren.

In der Applikation Gesundheitsbrowser ist dazu ein Referenzmonitor eingebunden, der die NSPR kapselt. Seine Funktion umfasst das Erkennen von angeforderten Informationsflüssen sowie die Umsetzung der Entscheidung, ob ein Informationsfluss zugelassen wird oder nicht. Auch das Einholen der Erlaubnis des Benutzers zählt hierzu, welche gefordert werden kann, bevor ein Informationsfluss zugelassen wird.

Die Entscheidung, ob ein Informationsfluss zugelassen wird und welche Maßnahmen für einen zugelassenen Informationsfluss zu ergreifen sind, trifft allerdings nicht der Referenzmonitor. Diese Funktion übernimmt die IFR-Komponente. Auch der Zugriff zur Verwaltung der Informationsflussregeln, die Nutzerverwaltung und die Authentisierung der Benutzer des Gesundheitsbrowsers werden über diese Komponente möglich. Daneben überprüft sie die Informationsflussregeln auf Konsistenz und übernimmt die Aufgabe der Ereignisprotokollierung.

Eine weitere Komponente des Gesundheitsbrowsers ist der Administrations-Client, über dessen grafische Nutzeroberfläche die Verwaltung des Gesundheitsbrowsers und somit die Erstellung und Pflege aller IFR, aber auch die Durchsicht der generierten Protokolldaten erfolgen kann [2].

Der Gesundheitsbrowser stützt sich zum Erreichen der Sicherheitsziele zusätzlich auf die IT-Umgebung. So wird bspw. die Beschränkung der Administration auf den Gesundheitsbrowser-Administrator nicht durch den Gesundheitsbrowser sichergestellt, sondern auf die Funktionalität des Betriebssystems zurückgegriffen.

Die Common Criteria (CC) sind gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit in der Informationstechnik (IT).
Sie schaffen Vergleichbarkeit der Ergebnisse unabhängiger Prüfungen und Bewertungen der IT-Sicherheit und dienen als Leitfaden für die Entwicklung von Produkten mit Sicherheitsfunktionen, aber auch als Orientierungshilfe bei der Beschaffung dieser. Der ISO/IEC-Standard 15408 (CC) befasst sich u. a. mit den Schutzkategorien Vertraulichkeit, Integrität und Verfügbarkeit. Das umfangreiche Kriterienwerk umfasst drei Teile [1].

ZTG Zentrum für Telematik im Gesundheitswesen GmbH

Die ZTG Zentrum für Telematik im Gesundheitswesen GmbH wurde im November 1999 auf Initiative und mit Unterstützung der Landesregierung NRW von führenden Informations- und Kommunikationstechnologie-Anbietern sowie von Institutionen und Organisationen des Gesundheitswesens in NRW gegründet. Schwerpunktmäßig setzt die ZTG GmbH interoperable Lösungen für eine integrierte Versorgung um. Ihre Kunden berät sie neutral und analog zu den neuesten technologischen Entwicklungen, um die Entwicklung, Einführung und Verbreitung von neuen modernen Informations- und Kommunikationstechnologien im Gesundheitswesen zu fördern.

Ausblick

Der Gesundheitsbrowser entfaltet seine volle Funktionalität für den Internetdienst WWW auf Workstations mit Multiuser fähigen Microsoft Betriebssystemen (z. B. Windows NT, Windows 2000).

Aufbauend auf der im Rahmen der Anforderungsanalyse durchgeführten Analyse der Bedrohungen, wird derzeit ein Gesamtkonzept entwickelt, das notwendige sicherheitsrelevante Komponenten und Maßnahmen für die Einsatzumgebung aufzeigt, in die der Gesundheitsbrowsers zu integrieren ist. Mit dem Konzept soll den Nutzern ein geeigneter Leitfaden an die Hand gegeben werden, um ein größtmögliches Maß an Sicherheit in ihrer Einrichtung umsetzen zu können. Sicherheitslücken werden identifiziert, so dass nur ein vertretbares Restrisiko mit der zu schaffenden Gesamtlösung existieren kann.

Das Gesamtkonzept wird zusammen mit der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen abgestimmt und noch in diesem Jahr vorliegen. Eine Neubeurteilung der schon im 15. Landesdatenschutzbericht geforderten Trennung Patientendaten/Internet, könnte so für den Internetdienst WWW mit dem Gesundheitsbrowser möglich werden.

Der zusammen mit dem Fraunhofer-Institut für Software- und Systemtechnik (ISST), Dortmund entwickelte Browser wird Anfang 2005 kostenfrei zum Download auf der Internetseite der ZTG GmbH erhältlich sein. Der Prototyp wird noch in diesem Jahr auf der Medica vorgestellt.

Literatur

[1] Common Criteria, Version 2.1, August 1999
[2] Security Target Gesundheitsbrowser