

Secure eHealth in der Schweiz – Die Technologie ist vorhanden

von Marco A. Demarmels, Bereichsleiter eHealth, AdNovum Informatik AG

Bei der Absicherung von elektronischen Daten und Anwendungen im Gesundheitswesen kann auf Security-Standards und -Lösungsansätze aufgebaut werden, die sich in anderen Branchen mit hochsensitiven Daten bewährt haben. Ihre Handhabung muss aber auf zusätzliche Anforderungen ausgelegt werden. Darüber hinaus gilt es, Ängste abzubauen und die Bevölkerung zu einem selbstverständlichen Umgang mit Datensicherheit zu befähigen. Das Tempo bei der Umsetzung von eHealth-Lösungen wird deshalb heute weitgehend von organisatorischen und kommunikativen Aspekten bestimmt.



Marco A. Demarmels
Bereichsleiter eHealth
AdNovum Informatik AG

Definition und übergeordnete Ziele

Eine treffende Erklärung des Begriffs eHealth findet sich in der bundesrätlichen «Strategie eHealth Schweiz», die am 27. Juni 2007 verabschiedet wurde: eHealth bezeichnet den «integrierten Einsatz von Informations- und Kommunikationstechnologien (IKT) zur Gestaltung, Unterstützung und Vernetzung aller Prozesse und Teilnehmer im Gesundheitswesen». Wozu dient diese Strategie? Wo will uns der Bundesrat mit eHealth hinführen? Das Ziel ist es, dafür zu sorgen, dass die Bevölkerung Zugang zu einem «bezüglich Qualität, Effizienz und Sicherheit hochstehenden und kostengünstigen Gesundheitswesen» hat. Einen solchen Nutzen wünschen wir uns alle. Zu Beginn sind In-

vestitionen erforderlich, die wohl eine gewisse Zeit benötigen, bis sie kostensenkend wirken.

Prozesse im Gesundheitswesen

Prozesse im Gesundheitswesen sollen über Kantons- und Landesgrenzen hinweg mit Informations- und Kommunikationstechnologien unterstützt, vernetzt und – nota bene – auch neu gestaltet werden. eHealth soll also nicht althergebrachte Arbeitsweisen zementieren, sondern Innovation ermöglichen. Es soll Prozesse befähigen, über Systemgrenzen hinweg zu funktionieren, also interoperabel zu werden. Dies ist in erster Linie eine organisatorische Aufgabe. Technische Standards sind dafür aber notwendige Hilfsmittel.

Es wird vermutlich eine prioritäre Aufgabe für das per 1. Januar 2008 operative Koordinationsorgan eHealth von Bund und Kantonen sein, die Prozesse des Gesundheitswesens zu identifizieren und zu beschreiben. Ein gutes Beispiel dafür, wie diese Aufgabe gelöst werden kann, liefert der eGovernment-Leistungskatalog der eCH, der zur Zeit als Standard eCH-0070 im Entwurfstatus vorliegt (www.ech.ch).

Entscheidend dabei ist, dass nicht Arbeitsweisen, sondern die organisatorischen Übergabestellen zwischen den Akteuren festgelegt und die erwarteten Lieferergebnisse vereinheitlicht werden. Eine Standardisierung würde über das Ziel hinausschiessen und nicht akzep-

tiert werden, wenn sie auch noch vorschreiben wollte, wie ein Prozess umzusetzen ist. Der Fachperson kommt eine Analogie in der Informatik in den Sinn: Verteilte Systeme funktionieren nur, wenn für die kooperierenden Komponenten Schnittstellen und zu übergebende Datenstrukturen definiert sind; die Implementierung der einzelnen Komponenten wird nicht vorgegeben.

Erhöhte Sicherheitsanforderungen

Die Anforderungen an die Sicherheit werden durch die Vernetzung der Prozesse erhöht. Bereits vor jeder Vernetzung mit Drittparteien muss die Identität und Zugriffsberechtigung aller Prozessteilnehmer elektronisch überprüfbar sein. Dies ist erst recht der Fall, wenn Akteure in die Prozesse einbezogen werden, die nicht «im Hause» tätig sind. Ein digitales Zertifikat auf einem Datenträger (Smartcard, USB-Token u.a.m.), wie es seit kurzem in der Schweiz bei akkreditierten Ausgabestellen erhältlich ist, bildet eine mögliche Grundlage für die elektronische Authentisierung, also die Feststellung der Identität. Wie aber verwaltet ein Spital digitale Identitäten? Und vor allem: Wie geht es mit Ausnahmefällen um, wenn zum Beispiel eine Smartcard unauffindbar ist? Solche Fragen des PKI-Managements werden akut.

Auch das Datenschutzgesetz treibt die Anforderungen hoch: Der Patient hat die Verfügungsgewalt über seine Daten. Er hat das Recht, darüber zu entscheiden, wer diese einsehen und verändern

darf. Ob dieses Recht wahrgenommen wird, steht auf einem anderen Blatt. Um dem Gesetz Genüge zu tun, muss jedoch ohnehin die Möglichkeit einer differenzierten Autorisierung geschaffen werden. Die Verwaltung von Autorisierungsinformation und vor allem die Anpassung aller Applikationen kann dabei umfangreich werden, je nachdem, wie viele verschiedene Rollen benötigt werden und wie feingranular die Zugriffsberechtigungen vergeben werden sollen.

In der eHealth-Strategie verlangt das Ziel A7 aus dem Handlungsfeld «Elektronisches Patientendossier», dass für

alle Menschen in der Schweiz bis ins Jahr 2015 ein dauernd verfügbarer elektronischer Zugriff auf die eigenen behandlungsrelevanten Daten bei jedem Leistungserbringer bereitgestellt wird. Papierene Krankengeschichten werden danach definitiv ausgedient haben. Dies führt zwangsläufig zu einem erhöhten Anpassungsbedarf bei IT-Sicherheitsinfrastrukturen und Anwendungen in den kommenden Jahren.

Offene Fragen und Ängste

eHealth soll gleichzeitig den 7x24-Stunden-Zugriff auf individuelle Gesundheitsdaten und einen gesetzeskonformen

Umgang mit den Daten bringen: Schnell und sicher zugleich. Ist das möglich? Kann da nichts schief laufen? Können Hacker nicht trotz aller Vorsichtsmaßnahmen an meine Daten gelangen? Darauf gibt es nur eine Antwort: Es gibt keine hundertprozentige Sicherheit. Die heutigen technischen Möglichkeiten wie starke Authentisierung und Datenverschlüsselung bilden zwar praktisch unüberwindbare Barrieren, doch der grösste Unsicherheitsfaktor bleibt: Der Mensch, der durch Unkenntnis oder Nachlässigkeit vertrauliche Informationen preisgibt und dadurch anderen unbeabsichtigt Zugang zu schützenswerten Daten ermöglicht.

Sichere Portale in der Praxis

Das Zürcher Softwarehaus AdNovum Informatik AG setzt seit Jahren Sicherheitsprojekte für Kunden mit besonders schützenswerten Daten um. Zu seinen Kunden zählen namhafte Finanzdienstleister, Banken, Die Schweizerische Post, Bundesbehörden und Bundesämter wie das EJPD, kantonale Behörden und Versicherungen. Die Software-Systeme werden auf der Basis der AdNovum-eigenen Sicherheitsarchitektur Nevis entwickelt.

Nevis bietet alle Funktionen und Mechanismen, welche für die Entwicklung eines sicheren Gesundheitsportales für alle Bürgerinnen und Bürger im Sinne der eHealth-Strategie des Bundes benötigt werden. Es ist modular aufgebaut und erlaubt eine sichere Integration bestehender Applikationen in ein SSO-Portal, das allen Benutzern über einen zentralen Login einen individualisierten 7x24-Stunden-Zugriff auf ihre Daten und Anwendungen ermöglicht.

Auf der Basis von Nevis wurden unter anderem die folgenden sicheren Portale realisiert:

EJPD SSO-Portal

Dieses Portal bietet über 15'000 Benutzern einen sicheren Zugriff auf rund 70 Applikationen. Die Authentisierung erfolgt wahlweise mittels UserID/Passwort, Zertifikaten oder Challenge-Response-Verfahren.

SSO-Portal für Swiss Post International

Über das SSO-Portal der Swiss Post International greifen Mitglieder aus aller Welt rund um die Uhr auf die SPI-Applikationen zu. Infolge der Internationalität von SPI bestehen hohe Anforderungen an die Verfügbarkeit der Applikationen.

SSO-Portal für My Post Business

PostLogisticcs, der Logistikzweig der Schweizerischen Post, bietet seinen Geschäftskunden ein SSO-Portal für den Zugriff auf die passwortgeschützten Online-Anwendungen.

Der gläserne Patient, ein gängiges und auch reales Schreckbild, ist kein schicksalhaftes Phänomen des Internetzeitalters, dem wir machtlos ausgeliefert sind. Es liegt in unserer Hand, wie transparent dieses Glas werden soll. Wir ziehen ja auch Vorteile daraus, wenn gewisse Daten anderen zugänglich sind. Im Gesundheitswesen ist diese Tatsache evident. Letztlich entscheiden wir, welches Risiko wir bezüglich unserer Daten eingehen wollen, indem wir Risiko und Nutzen gegeneinander abwägen.

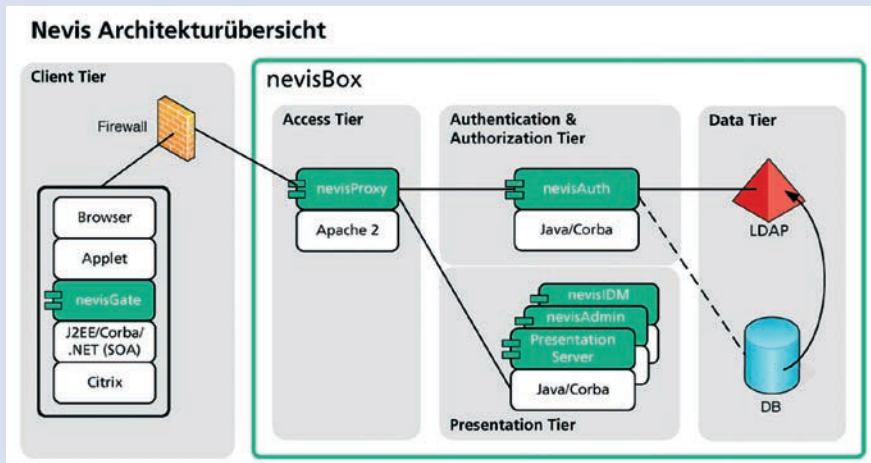
Gesundheitsportal für alle

Ziele B2 bis B4 der eHealth-Strategie fordern ein gemeinsames Gesundheitsportal für alle Bürgerinnen und Bürger sowie öffentlichen und privaten Anbieter. Die Technologien für die Erfüllung der hohen Sicherheitsanforderungen im Bereich eHealth sind vorhanden und in anderen Branchen praktisch erprobt. In der Finanzwelt zum Beispiel sind die Sicherheitsanforderungen und gesetzlichen Auflagen mit den Erfordernissen im Gesundheitswesen mindestens auf vergleichbarem Niveau. Hier gibt es zahlreiche Beispiele von erfolgreich eingeführten sicheren Portalen (siehe Kasten «Sichere Portale in der Praxis»).

Damit die eingesetzten technischen Hilfsmittel jedoch die nötige Akzeptanz in der breiten Bevölkerung finden, müssen sie den spezifischen Anforderungen der Endbenutzer genügen und in der Handhabung einfach sein. Wir können

Nevis - Die Technologie für sichere Portale

Die Sicherheitsarchitektur Nevis besteht aus frei zusammenstellbaren Modulen und ist optimal auf die Integration von Dritprodukten ausgelegt. Die zentralen Komponenten sind in der folgenden Illustration abgebildet:



- **nevisGate**

Mit der SSL-Tunnel-Lösung nevisGate lassen sich speziell auch Legacy-Systeme mit proprietären Protokollen in die Lösung integrieren. Sie lassen sich so auf einen aktuellen Sicherheitsstand bringen und lassen sich mit dem breiten Angebot von Authentisierungsmiteln und der Auditingfunktionalität von Nevis betreiben.

- **nevisProxy und nevisAuth**

Der Proxy Server übernimmt zusammen mit dem Authentisierungsservice nevisAuth die Rolle einer Web Application Firewall. nevisProxy bietet wirksame Mechanismen gegen verschiedene Attacks und Multiprotokoll-Support IIOP(S), HTTP(S), Citrix/ICA etc. nevisAuth ist für die Authentisierung, Autorisierung und das Session Manage-

ment zuständig und wird mit einer Vielzahl von bereits eingebauten Plugins ausgeliefert, z.B. für LDAP, User-ID/PW, Zertifikate, OracleDB, NIS+, Secure Token, ACE/SecurID, Challenge/Response, X509, Kerberos, Streichlisten und SAML.

- **nevisAdmin und nevisRum**

Hier handelt es sich um eine Web-Applikation für das Systemmanagement und die Administration von Nevis-Komponenten. nevisAdmin bietet eine Anbindung an System Monitoring Tools mittels JMX, Monitoring von Runtime-Statistiken von Nevis-Komponenten und/oder JMX-unterstützenden Komponenten von Dritt-Herstellern (z.B. Java VM, J2EE Containers). Die Verwaltung von Authentisierungs- und Autorisierungsdaten übernimmt nevisRum.

- **nevisIDM**

Für das zentralisierte und sichere Identitätsmanagement kommt nevisIDM zum Einsatz. Mit dieser Komponente können Benutzerkonten zentral administriert und Rechte verwaltet werden. Die Benutzer können einen Teil ihrer Daten selbst administrieren.

Dank der grossen Basis produktiver Installationen wird Nevis kontinuierlich ausgebaut und auf dem neusten technischen Stand gehalten. Mit seinen schnellen Implementations- und Deploymentzyklen verkürzt Nevis die Time-to-Market. Nevis gewährleistet darüber hinaus optimale Flexibilität, Skalier- und Erweiterbarkeit.

Bestehende Service-Instanzen können wiederverwendet und die Nevis-Komponenten und -Funktionen individuell nach Kundenbedürfnissen ausgewählt werden. Als schlanke Lösung ermöglicht Nevis so die schnelle, risikoarme und günstige Realisierung anspruchsvoller Projekte und senkt die Betriebskosten.

Neue top-rated Sicherheitsmechanismen und andere Technologien können kontinuierlich und ohne Risiken eingefügt werden.

beispielsweise älteren oder kranken Personen nicht in jedem Fall zumuten, dass sie sich Passwörter merken und diese eintippen oder Zahlen generieren, um diese in ein Challenge-Response-System einzugeben, wenn sie in der Apotheke per eRezept Medikamente beziehen wollen. Biometrische Geräte, die etwa statt

eines Passwortes Fingerabdrücke verwenden, könnten hier herkömmliche Geräte ergänzen. Bis jeder Teilnehmer im Schweizer Gesundheitswesen seine Daten elektronisch verwalten kann, bedarf es jedoch mit Sicherheit noch einiger Anstrengung und Überzeugungsarbeit.

AdNovum Informatik AG
Marco A. Demarmels
Bereichsleiter eHealth
Röntgenstrasse 22
CH-8005 Zürich
Tel. 044 272 61 11
marco.demarmels@adnovum.ch
www.adnovum.ch