Bernd
Schütze

Ein Beitrag zur Entwicklung von kostenneutralen Internet-Lösungen für die Teleradiologie

Insbesondere im Bereich der Kommunikation über das Medium Internet haben sich die meist kostenlos zu beschaffenden Open-Source-Lösungen sehr bewährt. Im Gesundheitswesen müssen Lösungen für die Übertragung dem Schutz von Patientendaten (Patientenstammdaten, diagnostische und therapeutische Daten, ...) ein besonderes Augenmerk widmen, da die Daten des Gesundheitswesens nach dem deutschen Datenschutzrecht als höchst schützenswürdig gelten. Ein sicherer Linux-Server als Basis für eine Firewall zum Schutz vor unbefugtem Zugriff ist geeignet, um eine sichere, d.h. verschlüsselte Kommunikationslösung als Möglichkeit zur Abfrage von Patientendaten aus medizinischen Datenbanken durch einen Abfrageserver zu realisieren.

1. Einfühung

Angesichts des Kostendruckes im Gesundheitswesen wird es immer wichtiger, das Preis-Leistungsverhältnis bei Beschaffung, Einführung und Unterhalt von EDV-Lösungen in der Radiologie zu analysieren und die Alternativen abzuwägen. Neben den marktbeherrschenden meist proprietären kommerziellen Lösungen werden die Open-Source Lösungen wegen der praktisch kostenlosen Beschaffung zunehmend interessant. Da für die Folgekosten allgemein ein Unentschieden angenommen wird, rücken Softfacts in den Vordergrund der Diskussion. Dazu gehören Lösungen für die Sicherheit der Daten. In der Radiologie ist der Einsatz von Open-Source-Software als Picture Archiving and Communication System (PACS) oder als Betrachtungsstation für DICOM-Bilddaten schon länger bekannt. Hinsichtlich der erforderlichen Datensicherungssysteme würden ebenfalls Anschaffungskosten durch Open-Source wegfallen. Publikationen über

rechtsrelevante Schutzmechanismen der Patientendaten für diese Lösungen fehlen allerdings.

Im vernetzten Gesundheitssystem haben Partner bei der Patientenbehandlung, z.B. Krankenhaus und niedergelassene Ärzte, die Möglichkeit, eine gemeinsame Datenbasis bzgl. der angefallenen Patientendaten (Patientenstammdaten, diagnostische und therapeutische Daten, ...) zu nutzen. Die kostengünstigste Möglichkeit der Datenübertragung bietet hier das Medium Internet, da heutzutage fast jede Klinik eine Standleitung besitzt und die meisten Arztpraxen über DSL an das World Wide Web angeschlossen sind.

Daten des Gesundheitswesens gelten jedoch nach dem deutschen Datenschutzrecht als höchst schützenswürdig, d.h. bei der Datenübertragung muss darauf geachtet werden, dass

- die Daten von Unbefugten nicht gesehen werden
- das eine Manipulation der Daten immer sicher erkannt wird
- das Sender und Empfänger der Daten eindeutig identifiziert werden.

Hierzu ist bei der Datenversendung über das Internet der Einsatz einer Firewall unumgänglich. Die Anschaffungskosten kommerzieller Produkte liegen zwischen 15.000 und 60.000 . Diese Arbeit überprüft, ob mit dem Einsatz von Open-Source diese kostengünstigere Möglichkeiten eine Alternative schaffen kann, die alle erforderlichen Ansprüchen genügt.

2. Material und Methode

Um die Sicherheitsanforderungen bei der Datenübertragung zu erfüllen, können folgende Maßnahmen benutzt werden:

- Integritätssicherung: Um sicherzustellen, dass die übertragenen Daten nicht zufällig oder absichtlich verfälscht worden sind, können die Daten mit einer kryptographischen Prüfsumme versehen werden.
- Verschlüsselung: Um die Vertraulichkeit der übertragenen Daten sicherzustellen, können symmetrische (z.B. AES, Twofish) oder asymmetrische (z.B. RSA, Elliptische Kurven) Verschlüsselungsverfahren benutzt werden.
- Quittierung: Zur Quittierung kann der Empfänger aus den empfangenen Daten einen Hashwert bilden und diesen anschließend digital signiert als Empfangsquittung zurücksenden. Hierdurch kann der Sender nachweisen, dass
  - die Quittung vom Empfänger stammt (digitale Signatur) und

- dieser die Quittung nur durch Kenntnis der übermittelten Daten erstellen konnte (Hashwert).

- Durch Verwendung von dynamischen Schlüsseln, Transaktionsnummern oder Zeitstempeln kann sichergestellt werden, dass wiedereingespielte manipulierte Nachrichten als solche erkannt und abgelehnt werden.

3. Firewall

Die vorgenannten Maßnahmen sichern nicht die eingesetzten Rechner bzw. die Datenbank mit den medizinischen Nutzdaten vor unbefugten Manipulationen. Hier ist die einzige Möglichkeit zur Verhinderung von Manipulationen der Einsatz einer Firewall. Dabei werden im wesentlichen zwei Mechanismen unterschieden: Paketfilter und Application Level Gateway (Proxy Gateways).

Paketfilter-Systeme routen Pakete zwischen internen und externen Rechnern. Sie gehen dabei allerdings selektiv vor: sie lassen bestimmte Pakettypen passieren oder blockieren sie auf eine Art, welche die Sicherheitspolitik eines Standortes widerspiegelt. Der in einem Paketfilter-Firewall verwendete Routertyp wird Überwachungsrouter genannt.

Proxy-Dienste sind spezielle Anwendungs- oder Serverprogramme, die auf einem Firewall-Host ablaufen: entweder auf einem Dual-Homed-Host mit einer Schnittstelle zum internen und einer zum externen Netz oder auf einem anderen Bastion-Host, der Zugang zum Internet hat und von den internen Rechnern aus angesprochen werden kann. Diese Programme greifen die Benutzeranfragen nach Internet-Diensten wie FTP oder Telnet auf und leiten sie an die eigentlichen Dienste weiter, sofern sie mit der Sicherheitspolitik des Standorts vereinbar sind. Die Proxies stellen Ersatzverbindungen her und fungieren als Gateways zu den Diensten. Deshalb werden Proxies auch manchmal als Application-Level-Gateways bezeichnet. Ein wesentlicher Vorteil von Proxies besteht darin, dass sie dem Benutzer gegenüber verborgen bleiben - sie sind völlig getarnt. Ein Proxy-Server vermittelt dem Benutzer den Eindruck, dass dieser direkt mit dem eigentlichen Server kommuniziert. Und gegenüber dem wirklichen Server tut der Proxy-Server so, als befände sich der Benutzer direkt auf dem Proxy-Host.

Der optimale Weg für den Aufbau einer Firewall besteht selten aus einer einzigen Technik; es ist meist eine geschickt gewählte Kombination zur Lösung unterschiedlicher Probleme. Für welche Probleme Lösungen gefunden werden müssen, hängt davon ab, welche Dienste den Benutzern angeboten werden sollen und in welchem Maße dabei Risiken in Kauf genommen werden können. Einige Protokolle wie z.B. Telnet und SMTP eignen sich gut für die Paketfilterung. Andere wie z.B. Archie, Gopher und WWW lassen sich effektiver mit Proxies bearbeiten.

Die meisten Firewalls verwenden eine Kombination aus Proxy-Diensten und Paketfilterung.

4. Sichere Kommunikation mittels Electronic Mail

Die Übermittlung medizinischer Daten, z.B. Befunde und Bilddaten muss den rechtlichen Rahmenbedingungen genügen. Hieraus resultiert die Forderung, dass die Daten mit sicheren kryptographischen Methoden verschlüsselt werden, sobald öffentliche Übertragungsmedien (Internet, Telefonleitungen, usw.) benutzt werden.

Die Verschlüsselung der medizinischen Nutzdaten erfolgt durch eine schnelle symmetrische Verschlüsselung mit einem als sicher anerkannten Verfahren, z.B. AES, Twofish. Die Nutzung von Public-Key-Verfahren wie z.B. PGP verbieten sich, da der private Schlüssel beschlagnahmt werden und damit das Schweigerecht / die Schweigepflicht des Arztes nicht länger aufrecht gehalten werden kann. Ein Programm, welches zum einen eine sichere Verschlüsselung mittels AES anbietet und zum anderen die zu sichernden Daten komprimiert und zusammen mit dem Entschlüsselungsprogramm zu einer ausführbaren Datei (exe-Datei) zusammenfasst, bietet die Firma DataRescue kostenlos im Internet an. Das Programm heißt aCrypt+.

5. Sichere Abfrage aus einem Informationssystem

Der Internet-Client äußert über Port 80 (= HTTP) eine Anfrage an den sich in der DMZ befindlichen Internet-Server. Der Internet-Server ist durch eine externe Firewall, die eine Kommunikation nur über den Port 80 gestattet, für WWW-Anfragen erreichbar. Die Kommunikation erfolgt mittels SSL.

Die SSL-Verbindung wird von einem Zertifikats-Server überwacht. Auf dem Webserver wird durch die Anfrage ein CGI-Skript gestartet, welches eine Kommunikation auf einem nicht-privilegierten Port (> 1024) mit einem durch die interne Firewall geschützten Kommunikations-Server aufbaut. Der Kommunikations-Server fungiert als Abfrage-Client, d.h. hier wird die eigentliche SQL-Abfrage an das medizinische Informationssystem durchgeführt.

Entscheidend hierbei ist, dass der Arzt, bei dem die medizinischen Patientendaten angefallen sind, vor der Abfrage festlegen muss, welche Daten von wem eingesehen werden dürfen. Generell gilt das Prinzip der Datenvermeidung und des

Datenschutzes auch bei der Zurverfügungstellung von Daten. Es müssen so wenige Daten wie notwendig anderen zur Einsicht gegeben werden. Außer dem Patienten darf nur ein mitbehandelnder Mediziner bzw. eine vom Patienten legitimierte Person in die für die Mitbehandlung notwendigen bzw. die bereitgestellten Daten Einblick erhalten. Verantwortlich für die Zuteilung ist außer dem Patienten der Besitzer der Patientendaten: der behandelnde Arzt, der das Informationssystem verwendet. Aus Gründen des Datenschutzes muss er die Daten aktiv an seinen Kollegen versenden. Der umgekehrte Weg der Kollege holt sich die Daten aus der Datenbank ist nicht gestattet. Die Alternative ist die aktive Freischaltung einzelner Daten im Informationssystem durch den behandelnden Arzt nach Rücksprache mit dem behandelten Patienten, so dass der mitbehandelnde Arzt nur die speziell für ihn aufbereiteten Daten sehen kann. Eine Ausnahme bildet hier der Patient selbst, der selbstverständlich alle ihn betreffenden Daten sehen darf.

Abbildung 1 beschreibt den Datenfluss einer Abfrage mittels eines Webclients aus dem WWW und die Rückübermittlung der Antwort:

1. der Client aus dem Internet richtet seine Anfrage SSL-verschlüsselt an den Webserver in der DMZ, hierbei wird auch der Name und das Kennwort zur Identifizierung des Abfragenden übermittelt (gestrichelte schwarze Linie)
2. der Webserver aus der DMZ gibt die Anfrage an den Abfrageserver im privaten Netz weiter (gestrichelte schwarze Linie)
3. der Abfrageserver richtet die Anfrage an die Datenbank (gestrichelte schwarze Linie)
4. die Datenbank übermittelt das Ergebnis an den Abfrageserver (gestrichelte blaue Linie)
5. der Abfrageserver verschlüsselt das Ergebnis mit Hilfe des Schlüsselservers unabhängig von der im Internet gebräuchlichen SSL-Verschlüsselung (gestrichelte blaue bzw. grüne Linie)
6. der Abfrageserver übermittelt das verschlüsselte Ergebnis an den Webserver in die DMZ (gestrichelte grüne Linie)
7. der Webserver übergibt das Ergebnis an den Client im Internet (gestrichelte grüne Linie).

Für Daten, die in unmittelbaren Zusammenhang der Patientenbehandlung angefallen sind, gilt ein Beschlagnahmeverbot. Um also die Patientendaten telemedizinisch nutzen zu können, muss für den jeweiligen Behandlungsfall ein einmalig zu verwendender Schlüssel generiert werden. Da dieser Schlüssel direkt mit der Behandlung des Patienten in Zusammenhang steht, ist dieser Schlüssel durch das Beschlagnahmeverbot geschützt. Es bietet sich für die Verschlüsselung der medizinischen Daten ein symmetrischer Schlüssel an, der große Vorteil der asymmetrischen Verfahren die Mehrfachverwendung mit der nur einmalig auftretenden Problematik der Schlüsselübermittlung entfällt, da stets neue Schlüssel generiert werden müssen.

6. Aufbau der Demilitarisierten Zone (DMZ)

Als Basis für einen Firewall-Server bzw. einen Abfrage-Server ist beispielsweise ein sicherer Linux-Server geeignet. Eine Härtung des Linux-Systems mittels dem von der National Security Agency (NSA) entwickelten Security Enhanced Linux (SE Linux) bietet eine bewährte Grundlage für die Implementierung einer Firewall. Die Hardware-Anforderungen, die eine Linux-Firewall stellt, sind im Vergleich zu kommerziellen Produkten sehr gering:

- ab Pentium I und kompatibel (z. B. AMD, Cyrix, IBM),
- 256 MB RAM,
- Festplatte min. 1 GB, 10 GB empfohlen (für Logdateien),
- CD-ROM zwecks Installation wünschenswert,
- zwei oder mehr Netzwerkadapter.

Zum Lieferumfang einer modernen Linux-Distribution gehört der Netfilter-Firewallmechanismus, welches i.d.R. nach dem zugehörigen Administrationsprogramm iptables, dem Nachfolger von ipchains, benannt wird. iptables bietet gegenüber ipchains eine Reihe von Vorteilen:

- umfangreicherere, erweiterbare Logmeldungen,
  - Logging ist nicht paketentscheidend, d.h. LOG-Target wird transparent durchlaufen, Paket bleibt erhalten, Festlegen des Loglevels, Festlegen eines Prefixes für Logmeldungen,
  - Loggen spezieller Paketeigenschaften:
    - TCP-Sequenznummern,

    - TCP-Optionen,
    - IP-Optionen

- Protokollhandler (ICMP, TCP, UDP) als Erweiterungen,
- geänderte Paketverarbeitung (Stateful Filtering),
- Limiting möglich
    - limit matcht nur für vorgegebenes Rate (x-mal),
    - verwendet token bucket filter,
    - konstantes Limit und Burstlimit, aktueller Burst erhöht sich um eins bis Burstlimit für jedes Mal Nichterreichen des konstanten Limits,
    - beliebig mit anderen Möglichkeiten kombinierbar,

- Packet State Matching
- Matching auf den Zustand der Verbindung, mögliche Zustände:
    - NEW: Paket erzeugt neue Verbindung,
    - ESTABLISHED: Paket ist Teil einer existierenden Verbindung,
    - RELATED: Paket hat mit existierender Verbindung zu tun, ist aber nicht Teil davon,
    - INVALID: Paket kann nicht zugeordnet werden,

- NAT überarbeitet
    - D-NAT (Destination NAT) erfolgt in:
        - PREROUTING (hereinkommende Pakete),
        - OUTPUT (lokal erzeugte Pakete),
        - REDIRECT: Teilmenge von D-NAT,

    - S-NAT (Source NAT): in POSTROUTING,
        - MASQUERADING ist jetzt eine Teilmenge von S-NAT,

    - minimales Loadbalancing,
    - minimales Umschreiben der Pakete.

iptables legt Regeln für den Paketfiltermechanismus der Firewall fest. Diese Regeln werden in Tabellen im Kernel gespeichert, separat für jede Regel-Kette (= Chain) (INPUT, OUTPUT, FORWARD) in der Reihenfolge, in der sie festgelegt wurden. Die Reihenfolge, in der Regeln definiert werden, ist die Reihenfolge, in der die Pakete verglichen werden.

Für die Abfrage aus dem Informationssystem bietet sich ein Linux-Server mit installiertem Apache-Webserver an. Die Abfragen selber können mit php erfolgen, da diese Sprache zum einen Unterstützung für die gängigen Datenbanksysteme (Oracle, MySQL, Sybase, SQL-Server,...) bietet und zum anderen gut zu erlernen ist. Da es sich bei den zu übertragenden Daten um personenbezogene Daten aus dem Behandlungsprozess eines Patienten handelt, müssen diese Daten verschlüsselt übertragen werden. Hierzu bietet sich die Nutzung des SSL-Protokolls (Secure Sockets Layer) an. Bedingt durch die kryptographischen Exportbestimmungen der USA besitzt der Apache-Webserver keine (direkte) Integration von SSL. Daher empfiehlt sich die Einbindung von OpenSSL, dem Nachfolger von SSLeay. OpenSSL stellt Unterstützung für SSL in den Protokollversionen 2 und 3 sowie der TSL-Version 1 (Transport Layer Security, der Nachfolger von SSL) zur Verfügung. Gängige Distributionen wie die von SuSE oder Red Hat liefern OpenSSL mit aus und installieren es auf Wunsch. Eine Beschreibung für die Einbindung in den Webserver Apache findet man in den gängigen Büchern.

In einer auf dem Abfrageserver installierten MySQL-Datenbank werden die zu einer Abfrage an das Informationssystem berechtigten Benutzer gespeichert, so dass sich die Benutzer zuerst bei der MySQL-Datenbank anmelden müssen. Hierbei gibt es einen Super-User, der die anderen Benutzer verwalten kann. Dieser Super-User ist der Patient, der damit die Möglichkeit hat, anderen Zugriff auf seine Daten zu gewähren. Der Patient ist also Herr über seine Daten und gibt von sich aus anderen die Möglichkeit, auf diese Daten zuzugreifen. Damit werden die Anforderungen der entsprechenden Datenschutzgesetze erfüllt, die eine Einwilligung des Patienten in die Weitergabe seiner Daten fordern. Intern besteht die MySQL-Datenbank aus drei Tabellen:

Passwort	Pat_ID	1 1..n	Benutzer
Passwort zur Abfrage des Informations-Systems (wird verschlüsselt abgelegt)	eindeutige Patienten ID aus dem Informations-System		Benuzter
			Passwort
			Superuser ja/nein

Der Patient als Superuser hat die Möglichkeit, mittels einer speziell eingerichteten Webseite die ihm zugeordneten Benutzer zu verwalten, d.h. er kann

- neue Benutzer anlegen und ihnen ein Password geben
- Benutzer löschen
- das Password von Benutzern ändern.

Alle anderen Benutzer können sich lediglich die Patientendaten anzeigen lassen.

Die Abfrage der Patientendaten ist vordefiniert, d.h. es sind keine freien SQL-Abfragen möglich. Dies wird ausgeschlossen, um die Ausnutzung eventuell in der Zukunft auftretender potentieller Sicherheitslücken der Abfragesprache php zu erschweren. Der authentifizierte und berechtigte Benutzer, dies schließt selbstverständlich den Patienten mit ein, hat dann die Möglichkeit, sich die vordefinierten Abfragen anzusehen, z.B.:

- Patientenstammdaten
- Risikofaktoren
- Diagnosen
  - Dauerdiagnosen
  - Fallbezogene Diagnosen
- Therapien
  - Medikation
  - operative Therapien
  - ...
- Bilddaten
- ...

7. Ergebnisse / Diskussion

Open-Source-Software erfüllt alle Anforderungen, die an eine sichere Übermittlung von Gesundheitsdaten mit dem Medium Internet gestellt werden müssen. Sowohl eine Firewall wie auch die Möglichkeit Patientendaten aus medizinischen Datenbanken abzufragen können mittels des Betriebssystems Linux und anderer Open-Source-Software realisiert werden. Die eingesparten Kosten bei der Anschaffung der Software bedingen auf der anderen Seite eine Einarbeitung in die Benutzung der entsprechenden Software. D.h. es muss im Bereich der Informatik Personal mit Spezialkenntnissen eingestellt werden:

- einen IT-Bereichsleiter, mittleres Jahresgehalt von 72.003
  - ggfs. einen Datenbankadministrator, mittleres Jahresgehalt von 47.637
  - einen Administrator für die Firewall, mittleres Jahresgehalt von 40.817
  - einen Webprogrammierer, mittleres Jahresgehalt von 37.550

Diese Personalkosten sind jedoch zu relativieren: ohne einen IT-Leiter kann heute kein Krankenhaus existieren, d.h. die Kosten fallen nicht zusätzlich an. Gleiches gilt für den Administrator der Firewall: ist ein Anschluss an das Internet vorhanden, muss eine Firewall eingesetzt werden, d.h. auch diese Kosten sind schon abgedeckt. Die Datenbankanbindung an das Internet selbst kann i.d.R. auch das Systemhaus als (einmalige) Auftragsarbeit vornehmen, die auch das eingesetzte Informationssystem (Arztpraxissystem, KIS, RIS, ...) wartet.

Wenn die Vorteile für eine teleradiologische Betätigung für eine einzelne Arztpraxis oder für kleinere Krankenhäuser angenommen werden können oder erwiesen sind, so ist bei der Beurteilung der Gesamtkosten zu berücksichtigen, dass vielfach ein Mitarbeiter mit anderen Aufgaben die IT-Arbeit mit übernimmt und ggf. die Einarbeitung in die neue Umgebung nicht leisten kann. Hier empfiehlt sich der Zusammenschluss mehrerer Praxen bzw. Krankenhäuser zu einem telematischen Verbund mit einem externen Dienstleister, welcher die Wartung der Firewall sowie die Programmierung der Internet-Präsentation der Patientendaten übernimmt.

Fazit: Im Vergleich zu den anschaffungskostenträchtigen kommerziellen Lösungen für die rechtsbedingten Sicherungssysteme für die Patientendaten in der Teleradiologie sind die kostenlosen Open-Source-Lösungen wenigstens gleich leistungsfähig.

8. Literatur

Langer S.G. OpenRIMS: An Open Architecture Radiology Informatics

Management System J Digit Imaging 2002 Jun;15(2):91-7

Marzola P, Da Pra A, Sbarbati A, Osculati F. A PC-based workstation for processing and analysis of MRI data MAGMA 1998 Nov;7(1):16-20

Bergmann L., Möhrle R., Herb A. Datenschutzrecht, Teil III Kommentar zum Bundesdatenschutzgesetz Richard Boorberg Verlag, ISBN 3-415-00616-6, Februar 2002

Bundesamt für Sicherheit in der Informationstechnik (BSI) http://www.bsi.bund.de/esig/basics/techbas/krypto/index.htm

Schütze B., Geisbe Th., Grönemeyer D.H.W., Filler T.J. Sicherer elektronischer Datenaustausch durch Electronic Mail Telemed 2002;

DataRescue aCrypt+; Februar 2003 http://www.acrypt.com

Homepage des OpenSSL Project http://www.openssl.org

Eilebrecht L., Rath N., Rohde Th. Apache Webserver Installation, Konfiguration, Administration; mitp-Verlag, Berlin, ISBN 3-8266-0829-1, 2002

Meyer A. Wer verdient wie viel? Ergebnisse der c't-Gehaltsumfrage ct; 6, 110 117, 2002

Bundesamt für Sicherheit in der Informationstechnik Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN http://www.bsi.bund.de/gshb/deutsch/m/m5083.htm; Oktober 2000

Bundesamt für Sicherheit in der Informationstechnik Firewallsysteme: Konzeption - Implementation Audit http://www.bsi.bund.de/literat/tagung/cebit00/vt_071.htm; Cebit 2000

Stepken G. Firewall Handbuch für LINUX 2.0 und 2.2 http://www.xinux.de/docs/buecher/sicherheit/fw-handbuch/zusammen-5.html#ss5.2, Juni 1999

SuSE Linux AG SuSE Firewall on CD 2 - Systemvoraussetzungen http://www.suse.de/de/business/products/suse_business/firewall/system_requirements.html, Oktober 2002

9. Authoren

B. Schütze, Universität Witten/Herdecke Lehrstuhl für Radiologie und Mikrotherapie Universitätsstr. 142, 44799 Bochum

M. Kroll, Fachhochschule Dortmund Fachbereich Informatik Emil-Figge-Str. 42, 44227 Dortmund

Th. Geisbe, Universität Witten/Herdecke Lehrstuhl für Radiologie und Mikrotherapie Universitätsstr. 142, 44799 Bochum

D. H. W. Grönemeyer, Universität Witten/Herdecke Lehrstuhl für Radiologie und Mikrotherapie Universitätsstr. 142, 44799 Bochum

T. J. Filler, Universitätsklinikum Münster Institut für Anatomie / Klinische Anatomie Vesaliusweg 2 - 4, 48149 Münster