universität Witten/Herdecke

Bernd Schütze

Digital unterschrieben von Bernd Schütze
CN: CN = Bernd Schütze, C = DE
Ursache: Ich bestätige die Richtigkeit und Integrität dieses Dokuments
Datum: 2003.11.05 16:03:02 +01'00'

GRÖNEMEYER INSTITUT FÜR MIKROTHERAPIE

Sicherer elektronischer Datenaustausch durch Electronic Mail

B. Schütze, T. Geisbe, D.H.W. Grönemeyer, T.J. Filler

Bundesland	Private Krankenhäuser	Krankenhäuser des Bundes	Krankenhäuser des Landes
Baden Württemberg	LKHG	LKHG	LKHG
Bayern	LKHG	LKHG	LKHG
Berlin	LKHG	LKHG	LKHG
Brandenburg	LKHG	LKHG	LKHG
Bremen	KHDSG	BDSG	KHDSG
Hamburg	LKHG	LKHG	LKHG
Hessen	LKHG	LKHG	LKHG
Mecklenburg-Vorpommern	LKHG	LKHG	LKHG
Niedersachen	BDSG	BDSG	LDSG
Nordrhein-Westfalen	GDSG	BDSG	GDSG
Rheinland-Pfalz	LKHG	LKHG	LKHG
Saarland	LKHG	LKHG	LKHG
Sachsen	LKHG	LKHG	LKHG
Sachsen-Anhalt	BDSG	BDSG	LDSG
Schleswig-Holstein	BDSG	BDSG	LDSG
Thüringen	LKHG	LKHG	LKHG

Tabelle 1: Gesetzgebung und Datenschutz in der Medizin

BDSG Bundesdatenschutzgesetz,
GDSG Gesundheitsdatenschutzgesetz,
LDSG Landesdatenschutzgesetz,
LKHG Landeskrankenhausgesetz
KHDSG Krankenhausdatenschutzgesetz
KHDsV Krankenhausdatenschutzverordnung

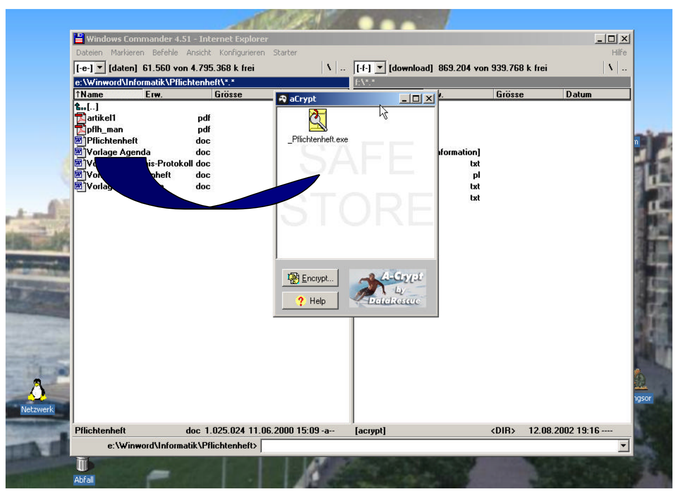

Abbildung 5: Einsatz von Acrypt+

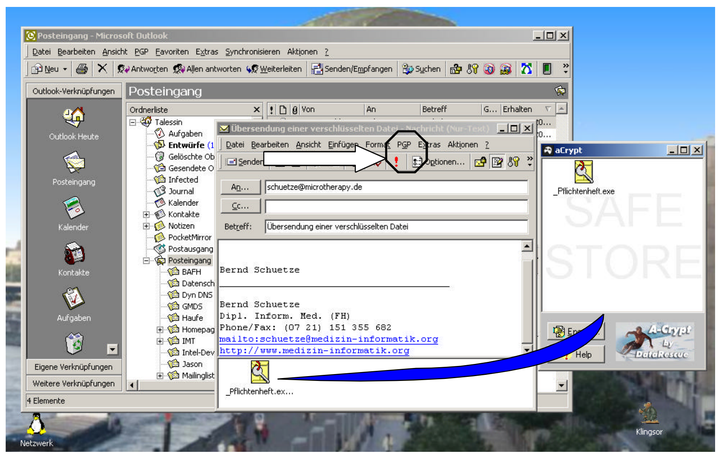

Abbildung 6: Übergabe der verschlüsselten Datei an MS Outlook mit anschließender Verschlüsselung durch PGP

Einleitung: „Electronic Mail“, kurz eMail, wird häufig genutzt, um schnell Patientendaten austauschen zu. Vielen Anwendern von EMail-Programmen ist jedoch nicht bekannt, dass die Daten im Klartext übertragen werden, d.h. jeder Netzwerkadministrator kann in seinem Bereich alle EMails lesen. Auch wenn bis heute kein entsprechender Vorfall bekannt geworden ist, besteht auf Grund der aktuellen Gesetzeslage die Pflicht, Patientendaten vor ungerechtfertigter Kenntnisnahme zu schützen.

Gefahrenpotential: Häufig existiert ein direkter Zugriff auf das Internet, kurz das WWW (World Wide Web). Aus Sicht der Forschung ist dies durchaus wünschenswert, da hiermit ein Zugriff auf die vielfältigen Datenbanken (Medline, Aidsline, Cancerlit, ...) existiert. Eine Netzwerkverbindung ist jedoch niemals eine Einbahnstrasse. daher bietet der WWW-Zugang einem Angreifer potentielle Möglichkeiten der Datenübernahme. (Abbildung 1)
Häufig werden gerade die Gefahren aus dem Internet als irreal angesehen. Dabei ist die Anzahl der Internetbenutzer innerhalb der deutschen Bevölkerung wie auch die der das Internet nutzenden Ärzte gerade in den letzten Jahren sprunghaft angestiegen. (Abbildung 2) Die Anzahl der Missbräuche, die beim amerikanischen CERT (Computer Emergency and Rescue Team) gemeldet werden, haben sich seit 1998 mehr als vervierfacht. (Abbildung 3) Die Gefahr aus dem Internet ist daher durchaus real.

Gesetzeslage: Laut Bundesdatenschutzgesetz sind Daten im Gesundheitswesen als besonders schützenswert anzusehen. Für die Übermittlung der Patientendaten mittels eMail ist daher ein entsprechender Schutz vorzusehen. Für die Einhaltung der betreffenden Datenschutzgesetze ist die Stelle und die Person verantwortlich, bei der die personenbezogenen Daten erhoben und digital gespeichert bzw. verarbeitet werden, d.h. der behandelnde Arzt.
Die einzige Möglichkeit die Patientendaten bei der Übersendung via eMail zu schützen, ist die Verwendung kryptographischer Methoden. Dennoch werden EMails, die Patientendaten übermitteln, selten verschlüsselt. Warum wird die Möglichkeit der Verschlüsselung so selten eingesetzt? Die Gründe sind mannigfaltig, eines der Hauptargumente ist jedoch die Inkompatibilität der Verschlüsselungsprogramme untereinander. Weiterhin existiert keine Infrastruktur, welche die Kommunikation im Gesundheitswesen ermöglicht. Dies hat mehrere Gründe: zum einen wirken proprietäre und wirtschaftliche Bestrebungen hier teilweise hemmend, andererseits ist die Gesetzeslage in Deutschland selbst für Juristen verwirrend.
Ein weiteres Problem stellt die asymmetrische Verschlüsselung da. Um die zu übermittelnde Datei verschlüsseln zu können, wird der öffentliche Schlüssel des Empfängers benötigt. Hierzu muss bundesweit eine „Public Key Infrastructure“ (PKI) aufgebaut werden, damit alle Partner im Gesundheitswesen erreicht werden können. Der digitale Arztausweis ist ein erster Schritt in diese Richtung, jedoch sind damit noch viele Partner von der Kommunikation ausgeschlossen: der Patient, alle Heil- und Hilfsberufe, die Kostenträger.
Um dennoch als Arzt von der elektronischen Kommunikation profitieren zu können, bieten sich kleine Programme als Zwischenlösung an. Der Sender verwendet zur sicheren Kommunikation ein spezielles EMail-Programm, welches die zu schützenden Daten vor dem Versand mittels sicherer kryptographischer Methoden verschlüsselt. Als ausführbare Datei („exe-Datei“) werden die verschlüsselten Daten versendet. Der Empfänger erhält die zum entschlüsseln benötigte Passphrase je nach Dringlichkeit bzw. Vertraulichkeit der Daten per Einschreiben, Telefon oder Fax. So kann zwar nicht verhindert werden, dass die EMail von einer nicht autorisierten Person abgefangen wird, aber diese Person kann die zu schützende Information nicht verwerten. Die Patientendaten sind sicher. Der Vorgang wird in Abbildung 4 aus Sicht des Senders wie auch des Empfängers dargestellt.
Abbildung 5 zeigt die Anwendung des Tools Acrypt+, welches die Firma „DataRescue“ kostenlos im Internet anbietet. (http://www.acrypt.com/) Acrypt+ nutzt den kryptographischen Algorythmus AES, welcher als einer der z. Zt. sichersten und am besten getesteten gilt. Acrypt+ erzeugt eine ausführbare Datei („exe-File“), welche an den Empfänger mittels eines beliebigen eMail-Programms versendet wird. Das eMail-Programm signiert die Nachricht, wie in Abbildung 6 zu sehen ist, mittels des Tools PGP. Hierdurch kann der Empfänger sicher sein, dass die Nachricht auch vom Sender stammt.

Diskussion: Für die Einhaltung der betreffenden Datenschutzgesetze ist die Stelle und die Person verantwortlich, bei der die personenbezogenen Daten erhoben und digital gespeichert bzw. verarbeitet werden. In der Regel ist dies der behandelnde Arzt. Je nach Organisationsstruktur trifft natürlich dem beaufsichtigenden Facharzt ein Mitverantwortung. Ebenso trägt natürlich die Geschäftsleitung, welche die Infrastruktur zur Verfügung stellt, eine Mitverantwortung.
Verstöße gegen dieses Gesetz stellen eine Ordnungswidrigkeit dar, die mit einer Geldbuße bis zu 250.000 € geahndet werden kann. Bei vorsätzlichem Verstoß gegen Entgelt oder in der Absicht, eine Person zu schädigen, droht zusätzlich eine Freiheitsstrafe bis zu 2 Jahren bzw. eine entsprechende Geldstrafe. Allerdings werden derartige Verstöße nur aufAntrag verfolgt.
Wünschenswert ist, dass die Hersteller von Informationssystemen im medizinischen Umfeld in Zukunft die kryptographischen Möglichkeiten direkt in ihre Systeme einbauen, so dass ein Arzt die Systeme als sichere Lösung im klinischenAlltag zur Kommunikation nutzen kann.

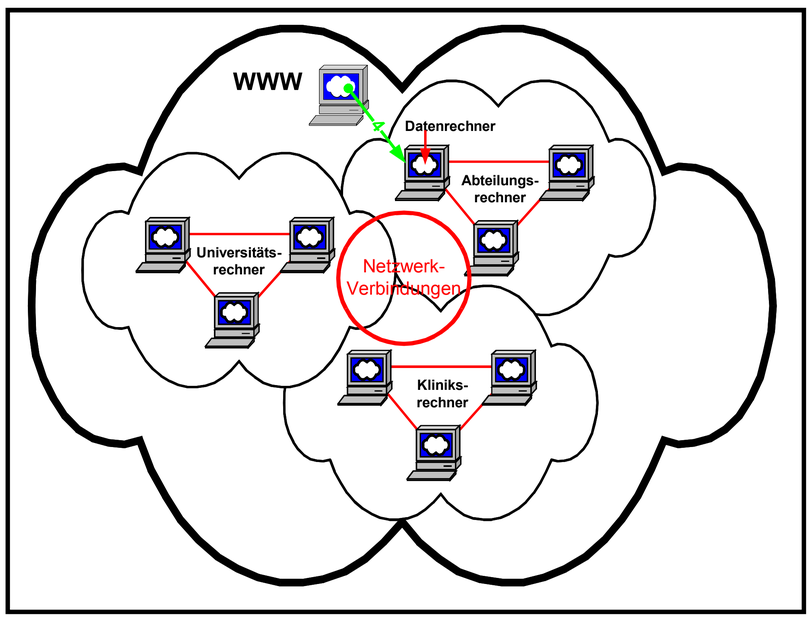

Abbildung 1: Gefahrenpotentiale bedingt durch die Verbindung von Daten-Rechnern mit dem WWW

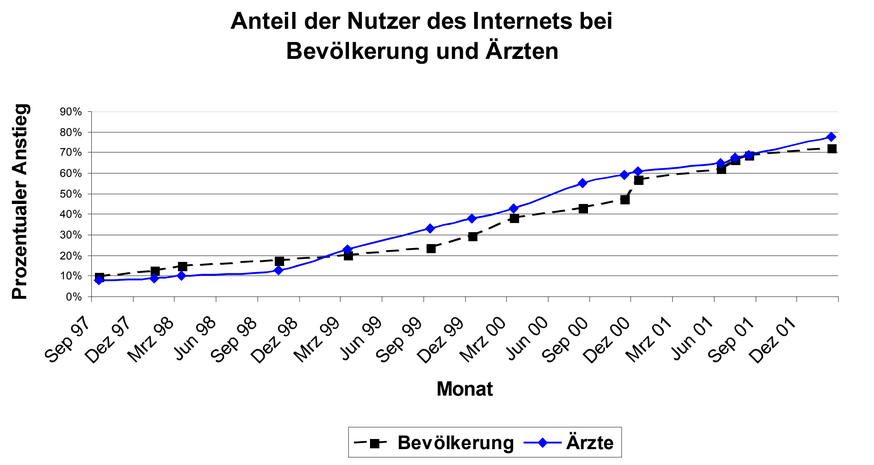

Abbildung 2: Prozentualer Anstieg der Nutzer des Internets in der Bevölkerung und bei Ärzten
Quelle Nutzer in der Bevölkerung: NUA Internet Surveys; 2002; http://www.nua.ie/surveys/how_many_online/europe.html;
Quelle Nutzer unter Ärzten: medicine online; Vortrag;
Stand 01.01.2001

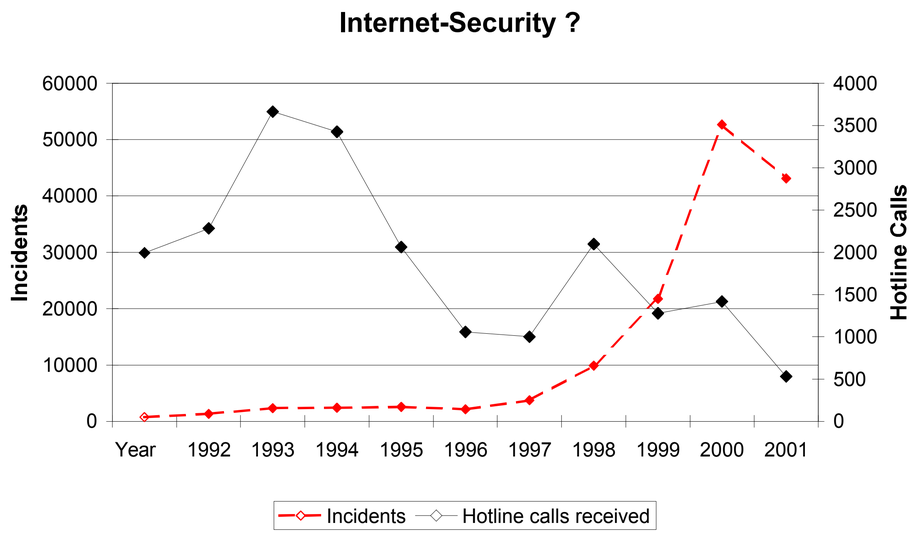

Abbildung 3: Zunahme der Anzahl der von Sicherheitsbeeinträchtigungen bei gleichzeitiger Abnahme der Hot-Line-Calls beim CERT;
Quelle: CERT® and CERT Coordination Center®;
http://www.cert.org/stats/cert_stats.html; August 2002

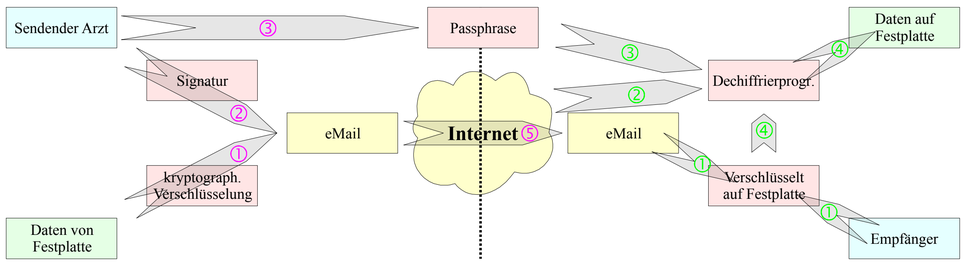

Abbildung 4: Übersicht über die Schritte zur Ver- und Entschlüsselung der zu versendenden Daten,

Ziffern der linken Seite zur Tätigkeit des Senders:

1. Verschlüsselung der Daten
2. Signierung der eMail mit dem privaten Schlüssel
3. Übermittlung der Passphrase unter Umgehung des Internet
4. Versenden der eMail

Ziffern der rechten Seite zur Tätigkeit des Empfängers:

1. Empfangen der eMail und prüfen der Signatur
2. Öffnen des Dechiffrierprogramms (ggf. mitübermittelt oder einmalig)
3. Empfang der Passphrase unter Umgehung des Internet
4. Entschlüsseln der eMail mit der Passphrase