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 16:05:43 +01'00'

Braucht der Anatom Datenschutz?

B. Schütze, E.T. Peuker, 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

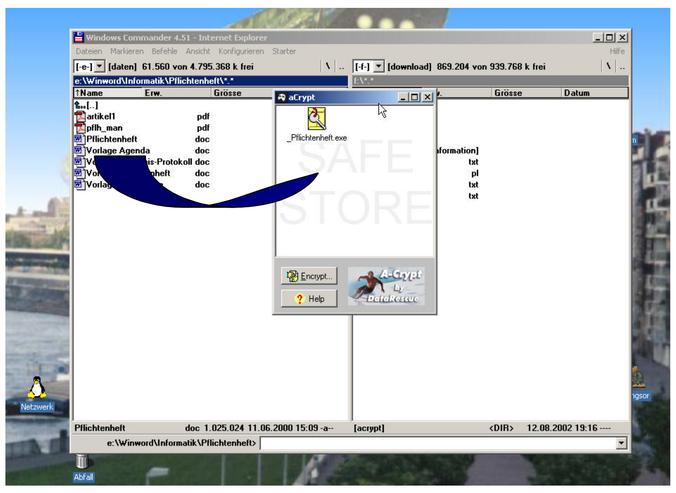

Abbildung 4: Einsatz von Acrypt+ zur sicheren Verschlüsselung sensitiver Daten

Einleitung: Die Möglichkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten wird durch die Datenschutzgesetze des Bundes, der Kirchen und der Länder stark reglementiert es existiert ein generelles Verbot, ausgenommen ein anderes Gesetz erzwingt die Datenerhebung. Der Anatom kommt mit diesen Beschränkungen immer häufiger in Konflikt oftmals, ohne dass es ihm bewusst wird.

Gesetzeslage: Für die Verwaltung von Kursplätzen sowie der Prüfungen/Prüfergebnissen der Studenten werden die personenbezogenen Daten der Studenten wie Name, Matrikelnummer usw. erhoben. Für Behörden und Einrichtungen und sonstigen öffentlichen Stellen des entsprechenden Landes gelten die länderspezifischen Datenschutzgesetze, für Einrichtungen des Bundes das Bundesdatenschutzgesetz. Aus diesen Gesetzen geht zwingend hervor, dass die personenbezogenen Daten in dem anatomischen Institut nur gespeichert werden dürfen, wenn die Studenten schriftlich ihr Einverständnis erklärt haben.

Gleiches gilt für die digitale Speicherung und Verarbeitung der Daten der Körperspender. Auch hier muss die Rechtsperson ihr Einverständnis zur Datenspeicherung gegeben haben.

In Studien kommen medizinische Aspekte hinzu. Die jeweiligen Länder haben für den medizinischen Bereich eigene Gesetze. Eine Übersicht gibt die folgende Tabelle:

Gefahrenpotential: Zugriffsmöglichkeiten, die auf den ersten Blick nicht offenbar sind, können eine Gefährdung der Sicherheit der erhobenen Daten bedeuten. In der Regel sind die Daten keine „Stand-Alone-PCs“ sonder befinden sich in einem Rechnernetz innerhalb derAbteilung. Im Umkehrschluss bedeutet dies aber auch, dass auf diesen Rechner von jedem anderen Rechner der Abteilung aus potentielle Zugriffsmöglichkeiten bestehen. (Abbildung 1, Pfeil 1)

Die Abteilung befindet sich in der Regel in einem Kliniknetz, so dass die eigene Abteilung mit den anderen Abteilungen Daten austauschen kann. Wiederum besteht die Gefahr, dass damit von einem Rechner aus einer anderen Abteilung ein Angreifer die Möglichkeit auf den Zugriff der zu schützenden Daten bekommt. (Abbildung 1, Pfeil 2)

Gehört die Abteilung zu einem universitären Betrieb ist der Klinikbetrieb häufig mit dem Lehrbetrieb vernetzt. Dies bedeutet im Umkehrschluss, dass ein Angreifer prinzipiell die Möglichkeit hat, aus dem Lehrbetrieb heraus auf die zu schützenden Daten zuzugreifen. (Abbildung 1, Pfeil 3)

Nicht zuletzt existiert häufig 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, Pfeil 4)

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.

Schutzmöglichkeiten: Abgesehen von Schutzmöglichkeiten, welche die Organisationsleitung (Abteilung, Klinik, usw.) ergreifen muss wie z.B. Firewall, Intrusion-Detection-Systeme, Virenscanner etc., sollten zu schützende Daten nicht leicht zugänglich (als Word-, Excel-Datei oder ähnliches) aufbewahrt werden, ohne dass die Daten mittels gut dokumentierter und ausgetesteter kryptographischer Algorithmen verschlüsselt werden. Abbildung 4 zeigt das Tool 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.

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. 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 auf Antrag verfolgt.

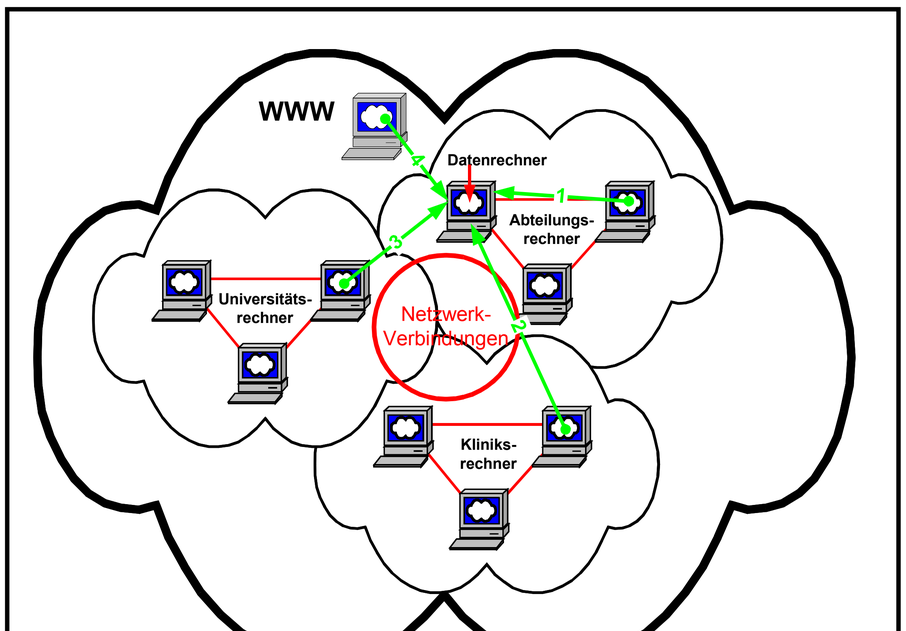

Abbildung 1: Denkbare Angriffsszenarien aus gespeicherte Daten

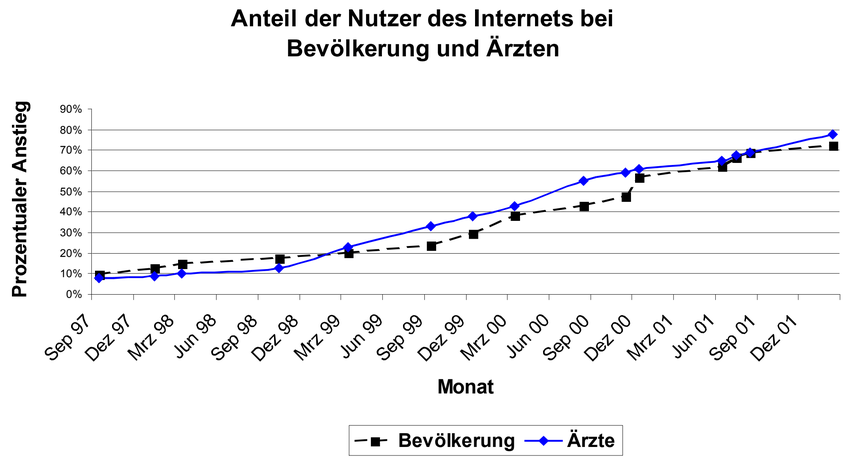

Abbildung 2: Prozentualer Anstieg der Nutzer des Internets in der Bevölkerung und bei Ärzten
Quelle Nutzer in der Bevölkerung: NUA Internet Surveys; 2002; http://www.nua.ie/surveys/how_many_online/europe.html;
Quelle Nutzer unter Ärzten: medicine online; Vortrag; Stand 01.01.2001

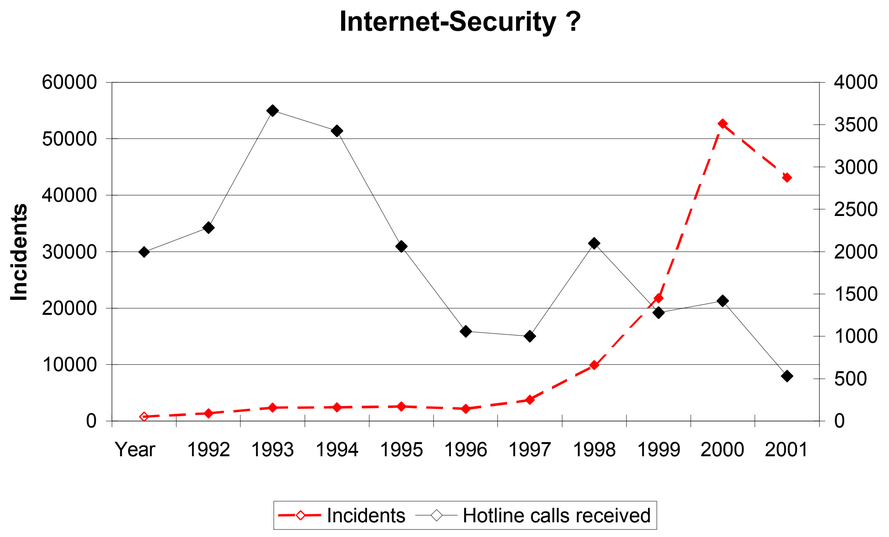

Abbildung 3: Zunahme der Anzahl der von Sicherheitsbeeinträchtigungen bei gleichzeitiger Abnahme der Hot-Line-Calls beim CERT;
Quelle: CERT® and CERT Coordination Center®;
http://www.cert.org/stats/cert_stats.html; August 2002