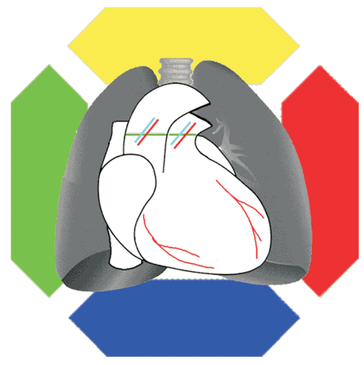
Datensicherheit beim Notebook Einsatz

B. Schütze[1], M. Thielmann[2], U. Herold[2], M. Kamler[2],
P. Massoudy[2], H. Jakob[2]

1) Verband der Hersteller von IT-Losungen fur das Gesundheitswesen e. V. (VHitG)
2) Klinik für Thorax- und Kardiovaskuläre Chirurgie, Universitätsklinikum Essen



Fragestellung

Notebooks sind das am häufigsten eingesetzte mobile Gerät (Abbildung 1), sie bieten vielfältige Vorteile:

- unmittelbare Erfassung der anfallenden Daten, d.h. Keine zeitliche Verzögerung
- Zugriff auf die benötigten Daten an nahezu jedem beliebigen Ort
- mobile Präsentation, z.B. Am Krankenbett, in der Lehre oder zur Vorstellung von Forschungsdaten auf Kongressen.

Gleichzeitig sind mobile Geräte die häufigste Ursache für Datenverlust (Abbildung2):

Wie sicher sind die Daten bei Verlust des Notebooks?

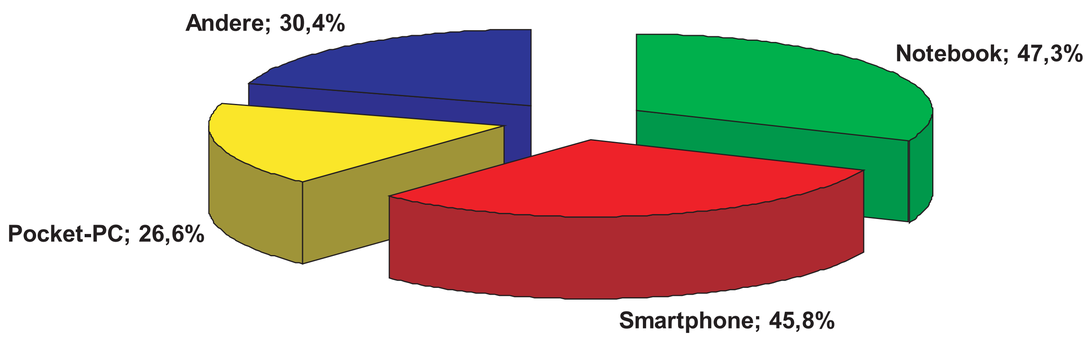


Abbildung 1: Häufigkeit des Einsatzes mobiler Geräte
Quelle: Infowatch, Studie "Sicherheit mobiler Geräte 2007"

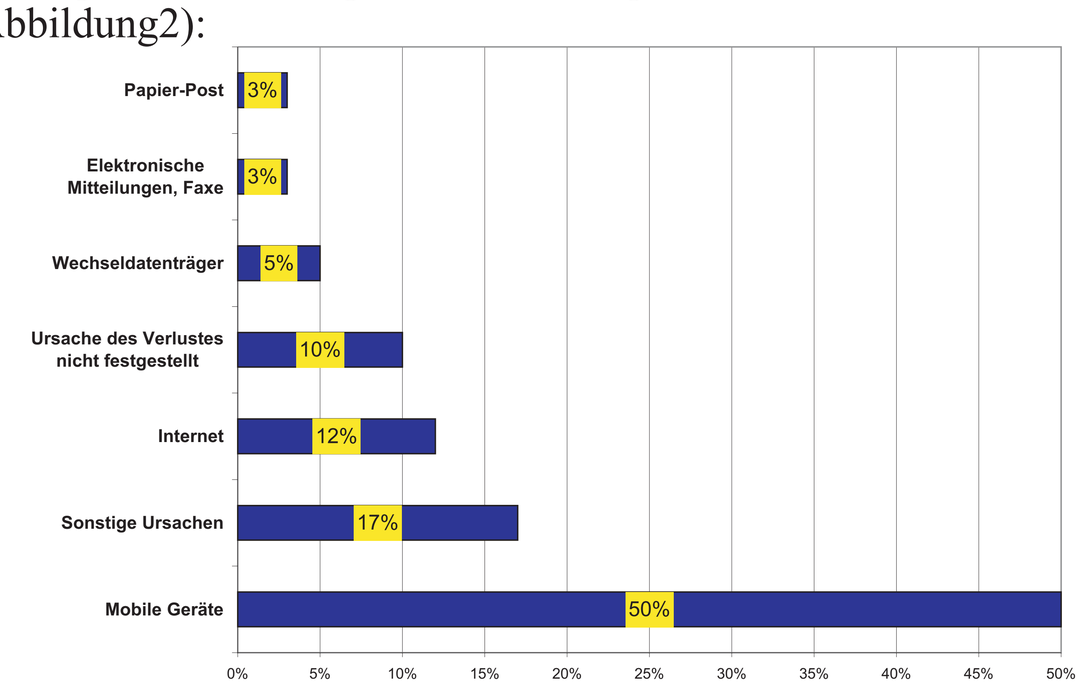


Abbildung 2: Ursache für den Verlust vertraulicher Daten
Quelle: Infowatch, Studie "Globale Studie zu Datenlecks 2006"

Möglichkeit 1: Verschlüsselung (einzelner) Partitionen

Die Verschlüsselung von Partitionen bietet verschiedene Vorteile:

- Zugriff auf Daten erfolgt nach Authentifizierung transparent
- Auch bei Stromausfall ist Datensicherheit gegeben (abhängig vom Betriebssystem)
- Cross-Crypt (Tabelle 1) ist anfällig(er) für Rainbow-Table-Attacken, daher nur bedingt empfehlenswert
- PGP bietet "Master-Password", durch welches Administratoren Zugriff auf Daten bei vergessenen Passwörtern haben

Aber:

- Werden die zu schützenden Daten auch wirklich nur in der dafür vorgesehenen Partition gespeichert?
- Was ist z. B. mit Auslagerungsdateien?

	CrossCrypt	TrueCrypt	PGP Disk
Betriebssystem	SuSE Linux, Windows 2000, Windows XP	Linux (Debian, RedHat SuSE), Windows 2000, Windows XP, Windows Vista	Windows 2000, Windows XP, Windows Vista, Mac OS X
kryptograph. Algorithmen	AES, Twofish	AES, Blowfish, Twofish, CAST5, Serpent, Triple DES	AES
Bitlänge	128, 192, 256 (AES), 160 (Twofish)	256	256
Authentifikation	Passwort	Passwort, Einzelne Dateien, Ordner im Dateisystem	Passwort, Aladdin eToken
Quelltext verfügbar	Ja	Ja	Ja
Preis	0 €	0 €	~ 200 €

Tabelle 1: Software zur Verschlüsselung (einzelner) Partitionen

Möglichkeit 2: Pre-Boot Authentification (PBA)

- Gesamte Festplatte inkl. Bottsektor verschlüsselt
- Filtersoftware zwischen Festplatte und Betriebssystem sorgt für notwendige Kommunikation
- Zugriff auf Daten erfolgt nach Authentifizierung transparent
- Die Daten werden während der Arbeit direkt ver- und entschlüsselt, d.h. auch bei Stromausfall ist Datensicherheit gegeben (abhängig vom Betriebssystem)
- ☺ ALLE Daten liegen nur verschlüsselt vor

	CompuSec	DriveCrypt Plus Pack	SafeGuard Easy
Betriebssystem	Windows 2000, Windows XP, Windows 2003 Linux Red Hat Linux SuSE	Windows 95,98, ME, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista	Windows 2000, Windows XP Windows 2003
Dateisystem	AT-12, FAT-16, FAT-32, HPFS, NTFS, NTFS5, EXT 2, EXT3	FAT-16, FAT-32, NTFS, NTFS5	FAT-12, FAT-16, FAT-32, HPFS, NTFS, NTFS5
Speichermedien	– Festplatten (IDE, SCSI, serial ATA)	– Festplatten (IDE, SCSI, serial ATA)	– Festplatten (IDE, SCSI, serial ATA, PCMCIA, Firewire, USB)
Hibernation Modus	Ja	Ja	Ja
Single-Sign-On zum Betriebssystem	Ja	Ja	Ja
Unterstützte Anzahl von Festplatten	8 Festplatten pro PC, maximal 8 Partitionen pro Festplatte	∞	4 Festplatten pro PC, maximal 8 Partitionen pro Festplatte
kryptographische Algorithmen	AES	AES	AES
Schlüssellänge	128	256	256
Authentifikation	Benutzername / Passwort, Aladdin eToken	Benutzername / Passwort, Aladdin eToken, Rainbow USB-Token	Benutzername / Passwort, Aladdin eToken, Verisign USB Token, RSA SecurID 800-Token, Fingerabdruckscanner, TPM Chip
Zertifizierung	keine	keine	Common Criteria EAL3, FIPS 140-2, VS-NfD
Kosten	keine	~ 60 €	~ 180 €

Tabelle 2: Software zur Pre-Boot Authentification (PBA)

Schlussfolgerung

- ☞ Schutz von Patientendaten durch gesetzliche Bestimmungen geregelt
- ☞ Schutz von Forschungsdaten i.d.R. immer gewünscht
- ☞ Auch aus Imagegründen liegt Datenschutz im Interesse des Anwenders

Vorgestellte Lösungen

- 👍 erfüllen gesetzliche Bestimmungen
- 👍 sind kostengünstig einsetzbar
- 👍 Pre-Boot Authentifizierung immer bevorzugen!
- 👎 CompuSec speicher Benutzername und Passwort im Klartext!

corresponding author:
Dr. Bernd Schütze
E-Mail: schuetze@medizin-informatik.org
http://www.medizin-informatik.org