



Gehen Sie mit Verschlüsselung und mit Schlüsseln sorgsam um!

- Mit dem preisgegebenen Schlüssel ist der Schutz weg!
- Bei Schlüsselverlust, hat NIEMAND mehr Zugang!

Welche Schlüssel werden verwendet?

Datenverschlüsselung sollte bewusst verwendet werden. Setzen Sie diese nur dort ein, wo sie auch benötigt wird.

a) Verschlüsselung von E-Mail.

E-Mail wird auf für den Benutzer nicht sichtbaren Kommunikationswegen übertragen und gespeichert. Vertrauliche Kommunikation erfordert Verschlüsselung.

b) Verschlüsselung auf Ihrem Gerät.

Vertrauliche Daten (z.B. sensible Informationen Ihrer Firma) sollten jedenfalls verschlüsselt werden, wenn

- Sie hin und wieder mit dem Gerät unterwegs sind,
- auch Dritte zum Gerät Zugang haben könnten,
- Wartungs- und Reparaturpersonal zu Ihren Daten keinen Zugang haben sollte.

Wird Verschlüsselung verwendet, so sollte dies dem Anwender bekannt sein.

Das Bewusstsein des notwendigen Schutzes vor Betriebsespionage ist in vielen Fällen schwach ausgeprägt. Schützen Sie Ihr KNOW-HOW!



Signatur und Verschlüsselung

Elektronische Signatur sichert die Datenintegrität und ordnet einzelne Dokumente sowie deren Inhalte einer Person zu. Jedermann kann signierte Dokumente prüfen und auch ohne Schlüssel öffnen. **Zur Prüfung wird nur ein öffentlich bekannter Schlüssel benötigt.**

Verschlüsselung grenzt die Benutzung von Dokumenten und Datenbereichen auf den Benutzerkreis ein, der über einen **privaten und geheim zu haltenden Schlüssel** verfügt.

Der Zugang zu den Daten ist nur solange gegeben, als der ENTSCHLÜSSELUNGSSCHLÜSSEL verfügbar ist!

Gehen Sie besonders sorgfältig mit diesem Schlüssel um!

Die Schlüssel der Signatur und der Verschlüsselung sollten aufgrund der unterschiedlichen Verwendung jedenfalls unterschiedlich sein!

Zwei Beispiele der Verschlüsselung

1. E-Mail-Verschlüsselung

Der Absender benötigt die geeignete **Verschlüsselungssoftware** und den **Schlüssel des Empfängers**.

Die Verschlüsselung gilt primär nur für die Kommunikation. Es wird sichergestellt, dass nur die im E-Mail genannten Adressaten Zugang zum Inhalt dieses E-Mails bekommen.

Der Zugang zum verschlüsselten E-Mail ist nur solange gegeben, wie der private Schlüssel verfügbar ist. Bei manchen Systemen ist dies auch für ausgehende Mails der Fall (z.B. OUTLOOK)!

2. Filesystemverschlüsselung

Mit speziellen Produkten (PGP, UTIMACO, ...) werden Teile des Filesystems gegen fremden Zugriff gesichert.

Die Verschlüsselung bietet aufgrund der Systemstruktur oft nur auf der Ebene der Verzeichnisse hinreichenden Schutz.

Beim Kopieren in andere Bereiche kann der Schutz eingeschränkt sein. Dies trifft temporär auch für Systemfunktionen zu (z.B. backup oder cut and paste). Ein sorgfältiger Umgang mit diesen Systemelementen (etwa Backup Medien) ist daher essentiell.



Wer sollte Schlüssel erzeugen?

- Als Privatperson sollten Sie Ihre Schlüssel zur Verschlüsselung selbst erzeugen, damit sichergestellt ist, dass Dritte keinen Zugang zu Ihren Daten haben können.
- Werden Daten einer Organisation verschlüsselt, so werden die Schlüssel sinnvollerweise durch die Organisation zur Verfügung gestellt, um auch in Notfällen die betroffenen Daten nicht zu verlieren.
- In jedem Fall wird die Person, die die Schlüssel erzeugt, auch die Verantwortung für die Verfügbarkeit selbst bei Systemstörungen haben und gegebenenfalls Sicherungen anlegen.

- Für reine Kommunikationsschlüssel sind Sicherungen nicht relevant und können die Sicherheit eher verringern als erhöhen.
- A-SIT stellt für Verschlüsselungsschlüssel von E-Mails und für Fileverschlüsselung unter Windows (EFS) zur Erhöhung der allgemeinen Sicherheit gratis ein Werkzeug zur Verfügung, das auch die Sicherung der betroffenen Schlüssel ermöglicht.

http://demo.a-sit.at/it_sicherheit/ca_toolkit



Verwahren von Schlüsseln

- Verschlüsselungsschlüssel werden im Betriebssystem und gegebenenfalls auf einem Sicherungsmedium gespeichert und verwahrt.
- 😊 **Die Absicherung der Schlüssel im System ist nur so gut wie der Zugangsschutz zum System.**
- 😊 **Lassen Sie keinesfalls den Export von Schlüsseln zu.**
- 😊 Zur angemessenen Sicherheit sollte der Zugang zu Verschlüsselungsschlüsseln bzw. deren Verwendung zusätzlich durch einen Token (Karte, USB-Stick, ...) abgesichert werden.
- 😊 Wägen Sie das Risiko des Sicherheitsverlustes und des Datenverlustes ab.
In den meisten Fällen wird sich daraus die Notwendigkeit eines Backups der Verschlüsselungsschlüssel zur Vermeidung von Datenverlust ergeben.

BACKUP VON SCHLÜSSELN IST BESONDERS SENSIBEL!

ACHTEN SIE AUF TECHNISCH UND ORGANISATORISCH ANGEMESSENE METHODEN!



Umgang mit Daten

- Beachten Sie, dass mit jedem Kopiervorgang, bei jeder Zwischensicherung, Anzeige, Kompression, Archivierung (etwa eines Textdokumentes), etc. Informationen abgelegt und gegebenenfalls kommuniziert werden können.
- Beachten Sie, dass gelöschte Informationen in Ihrem Dateisystem noch immer vorhanden sein können - auch dann, wenn Sie den Papierkorb leeren.
- Als Organisation sollten Sie daher in Ihrer Sicherheitspolicy klar auf den Umgang mit unverschlüsselten und verschlüsselten Daten sowie auf verwendbare Formate und Werkzeuge eingehen.



Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

www.a-sit.at

2006-10



Erzeugung und Wartung von Verschlüsselungsschlüsseln

E-Government Flyer Nr.203

Methoden und Werkzeuge für das Erzeugen und Warten von Schlüsseln zur Verschlüsselung

- Welche Schlüssel werden verwendet
- Unterschied Signatur - Verschlüsselung
- Zwei Beispiele der Verschlüsselung
- Wer sollte Schlüssel erzeugen
- Wie sollte ich Schlüssel verwahren
- Wie gehe ich mit den Daten um

DIGITAL ■ AUSTRIA