cebis
Landkreis Neu-Ulm

Digitale Verschlüsselung: Für Datenschutz unerlässlich

Die Verschlüsselung von Daten ist seit Herbst vergangenen Jahres **in einem Gesetz fixiert**, und zwar in § 9 des Bundesdatenschutzgesetzes (BDSG): Öffentliche und nicht-öffentliche Stellen, die **personenbezogene Daten** erheben, verarbeiten oder nutzen, haben die **technischen und organisatorischen Maßnahmen** zu treffen, die erforderlich sind, um den Datenschutz zu gewährleisten. Einen Katalog derartiger Maßnahmen enthält die Anlage zu § 9 Satz 1 BDSG; sie nennt **Maßnahmen**, die u. a. in der Lage sind,

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer **Zugriffsberechtigung** unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung **nicht unbefugt gelesen, kopiert, verändert oder entfernt** werden können (**Zugriffskontrolle**),
4. zu gewährleisten, dass personenbezogene Daten **bei der elektronischen Übertragung** oder **während ihres Transports** oder **ihrer Speicherung auf Datenträger** nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können … (**Weitergabekontrolle**).

Bei diesen Kontrollen steht die Verschlüsselung der Daten im Mittelpunkt; Satz 3 der Anlage bestimmt: "Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von **dem Stand der Technik entsprechenden Verschlüsselungsverfahren**".

Verschlüsselung im Gesetz: Kann oder Muss?

Schon in der Begründung des Gesetzentwurfes zur BDSG-Novelle 2009 wurde auf das Thema Verschlüsselung eingegangen. Verschlüsselungsverfahren gehören dort zu den technischen und organisatorischen Maßnahmen zur Zugangs-, Zugriffs- und Weitergabekontrolle von Daten. Im Gesetz werden sie ausdrücklich deswegen als geeignete Maßnahme erwähnt, da sie in der Praxis noch nicht im wünschenswerten Umfang eingesetzt werden. Die Formulierung „dem Stand der Technik entsprechende“ bringt für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, zum Ausdruck, dass **fortschrittliche Verfahren gemeint sind, die sich in der Praxis bewährt haben** und einen hohen Sicherheitsstandard gewährleisten. Allerdings, so Schaar: „Aus dem Wortlaut ‚insbesondere’ im Gesetzestext ergibt sich für mich aber nicht, dass eine Verschlüsselung in jedem Fall zwingend durchzuführen ist. Für mich liegt tatsächlich nahe, dass der Gesetzgeber **lediglich eine Empfehlung** zur Verschlüsselung nach dem Stand der Technik aussprechen wollte“.

Im Zusammenhang mit der Speicherung von **„sensiblen Daten"** (besondere Arten personenbezogener Daten, etwa nach § 3 Absatz 9 BDSG) liegt es für Schaar jedoch nahe, auf Verschlüsselungstechniken zurück zu greifen; den jeweils für den Datenschutz Verantwortlichen empfiehlt Schaar, dass sie **ausdrücklich begründen, wenn sie dort keine Verschlüsselung anwenden**. Das bedeutet, dass überall dort, wo der Zugang, der Zugriff und die Weitergabe von sensiblen Daten nicht mit Verschlüsselungstechnik kontrolliert wird, es einer hieb- und stichfesten datenschutzrechtlichen Begründung bedarf.

Verschlüsselungs-Werkzeuge

Ein Blick auf die aufgeklappten Laptops in Büros, Wohnungen und Veranstaltungen genügt und man kann den Mangel an Einsatzfreude bei Verschlüsselungstechnik sehen - und auch die datenschutzrechtlichen Folgen davon leicht voraussagen. Dabei stehen eine Reihe von meist sogar **kostenlosen Verschlüsselungs-Tools** zur Verfügung: Per Mausklick legt man ein virtuelles verschlüsseltes Laufwerk für sensible Daten an, versieht Ordner per Kontextmenü mit einem Passwort oder verschlüsselt gleich die ganze Systempartition. Das clevere Verstecken von verschlüsselten Laufwerken und das Anlegen von Alibi-Dateien befriedigen meist sogar professionelle Anforderungen; so sieht bei Alibi-Dateien ein Angreifer nur unwichtige Daten während die vertraulichen Daten verschlüsselt im Speicher eines des verschlüsselten Laufwerks verborgen sind. Beispiele für solche Tools sind:

- **TrueCrypt** sichert vertrauliche Daten in einem verschlüsselten virtuellen Laufwerk. Das TrueCrypt-Laufwerk ist zunächst versteckt, nach der Auswahl eines freien Laufwerksbuchstabens und Eingabe des entsprechenden Passworts taucht es im Windows-Explorer auf. Die Informationen sind so unter Windows, Linux und Mac OS sicher vor Ausspähung. Seit Jahren erhält Truecrypt immer beste Kritiken und selbst das FBI hat zugegeben, eine mit Truecrypt verschlüsselte Festplatte auch nach langwierigen und wiederholten Versuchen nicht entschlüsseln zu können.
- **aborange Crypter** verschlüsselt Dateien, Texte und E-Mails sicher; es verwendet AES-Verfahren (http://de.wikipedia.org/wiki/Advanced_Encryption_Standard). Zusätzlich enthalten ist ein Passwortgenerator und eine Funktion zum Datenlöschen durch mehrmaliges Überschreiben.
- **ArchiCrypt Live** verschlüsselt Daten in Echtzeit; zur Ver- und Entschlüsselung nutzt das Programm 256 Bit AES sowie Blowfish (http://de.wikipedia.org/wiki/Blowfish).
- **AxCrypt** ist geeignet zum Verschlüsseln sensibler Daten (128 Bit AES), z. B. auf einem Netzlaufwerk. Praktisch: Das Tool integriert sich in das Kontextmenü des Windows-Explorers. Möchte man geschützte Daten per E-Mail an einen Empfänger senden, so wird die E-Mail einfach mit "Encrypt Copy to .EXE" verschlüsselt und die Datei in die Endung „.TXT“ umbenannt und damit bei vielen Mail-Servern nicht mehr ausgefiltert. Die Funktion "Shred and Delete" ermöglicht das sichere Löschen von Daten.
- **Challenger** verschlüsselt Dateien, Ordner oder ganze Laufwerke. Das Tool klinkt sich ins Kontextmenü ein. Per Popup-Menü wählt man die Verschlüsselungs-Methode und vergibt ein Passwort.
- **Crosscrypt** bindet Image-Dateien als verschlüsselte, virtuelle Laufwerke ein. Ein Image kann beispielsweise auf der lokalen Festplatte, auf einem USB-Stick, einem Wechselmedium oder auf einem Netzserver liegen.
- **Cryptool** arbeitet mit unterschiedlichen Verschlüsselungsverfahren wie RSA (http://de.wikipedia.org/wiki/RSA-Kryptosystem) oder DES (http://de.wikipedia.org/wiki/Data_Encryption_Standard).
- **Drag'n'Crypt ULTRA** verschlüsselt sensible Daten ganz einfach per Drag and Drop. Drag'n'Crypt ULTRA muss nicht installiert werden und kann auch von einem USB-Stick aus verwendet werden.
- **Easy Crypto Deluxe** verwendet die Blow-Fish-Methode zum Verschlüsseln von Dateien und Verzeichnissen. Die Freeware bindet sich als Shell-Erweiterung ins Kontextmenü ein und stellt Funktionen wie „Verschlüsseln“ und „Zu Easy Crypto Zip“ bereit. Die Ursprungsdateien werden sicher gelöscht. Auch komplette Ordner lassen sich mit einem Klick verschlüsseln. Zur Weitergabe der verschlüsselten Archive als selbstentpackende EXE-Datei dient die Option „Archiv erzeugen“.
- **Folder Lock** schützt ausgewählte Verzeichnisse auf Festplatten und Wechselmedien. Dem Anbieter zufolge soll der Schutz auch nach einem Rechner-Neustart im abgesicherten Modus und unter DOS weiter bestehen bleiben.
- **Free CompuSec** sichert Rechner schon vor dem Bootvorgang per Passwort ab und erlaubt auch, einzelne Festplatten und Ordner zu verschlüsseln. Zusätzlich soll „ClosedTalk“ eine VoIP-Verbindung schützen. Mit „DriveCrypt“ verschlüsselt das Tool auch Datencontainer.
- **Gpg4win** ist eine komplexe Open-Source-Software zum Verschlüsseln von Dateien und E-Mails. Das Programm ist eine Weiterentwicklung von „GnuPG“.
- **Grafik Key** verschlüsselt wichtige Texte und versteckt diese dann in einer Bilddatei.
- **Guardian of Data** verschlüsselt einzelne Dateien und komplette Ordner mit 256 Bit AES. Eine übersichtliche Bedienerführung und ein Programm-Assistent macht die Handhabung dieser Freeware sehr einfach.
- **Opheus Quantum** erstellt vor der Verschlüsselung der Daten eine eigene Benutzermatrix mit Passwort. Daraus errechnet das Programm jeweils eine 1024-Bit-Matrix zur Verschlüsselung; ein Angreifer muss den vollständigen Schlüsselsatz haben, um Dateien entschlüsseln zu können.
- **Sophos Free Encryption** hat eine einfache und komfortable Oberfläche, um jeden beliebigen Dateityp zu verschlüsseln. Die kostenlose Software nutzt 256-Bit-AES-Verschlüsselung und verfügt außerdem über zahlreiche Zusatzfunktionen. Während der Passworteingabe bestimmt der Anwender die Passwortstärke in drei Stufen. Nach dem Verschlüsselungsprozess entfernt das Tool auf Wunsch die Originaldatei durch sicheres Löschen. "Brute-Force-Attacken" beim Entschlüsseln

werden verhindert: Immer wenn ein falsches Passwort eingetippt wird, verlängert die Software die Zeit bis zur nächsten Passworteingabe. Das Tool komprimiert auch jede verschlüsselte Datei platzsparend. Für die Privatnutzung ist Sophos Free Encrypt kostenlos, beim Einsatz von gekaufter Sophos-Technologie lassen sich die Sophos Free Encryption-Dateien einbinden.

- **Steganos LockNote** verwendet einen AES-256-Bit-Schlüssel. Man kann damit einfach einen Text in das Programmfenster eingeben oder zieht per Drag und Drop fertige Dokumente auf Locknote. Die verschlüsselten Daten werden als ausführbare Dateien gespeichert und können nur mit dem Passwort geöffnet werden. Das Programm muss nicht installiert werden.
- **Steganos Safe One** legt zwei Archive mit jeweils bis zu 1 GB Größe an. Dabei ist es egal, um welche Art Daten es sich handelt. Zusätzlich lassen sich mit dem kostenlosen Tool Passwörter generieren und auf einem USB-Stick speichern. Dabei prüft das Steganos-Utility, ob das gewählte Passwort ausreichend kompliziert ist. Die AES-Verschlüsselung mit 256 Bit Verschlüsselungstiefe ist hinreichend sicher.

Diese Liste, die weder beansprucht vollständig zu sein, noch alle Varianten aufbietet, zeigt die Vielfalt angebotener kostenloser Tools. Unerwähnt geblieben sind die Tools, die als Passwortsafes dienen, alle Tools zum verschlüsselten Datenbackup und die vielen Passwortgeneratoren. Für jeden, der schützenswerte Daten besitzt, **stehen also genügend Werkzeuge zur Verfügung**.

Disziplin wahren!

Die Qualität jeder Verschlüsselung steht und fällt mit der **Komplexität des gewählten Passwortes**: Sonderzeichen und Zahlen, Groß- und Kleinschreibung und keine Silben aus bekannten Sprachen sind ein Muss; je länger und komplexer, desto sicherer. Ja, der Mensch kann sich komplexe Passworte mit nahezu unendlicher Länge merken, auch wenn man es sich im Moment nicht vorstellen kann. Aber Achtung: Nicht jedes der oben aufgelisteten Software-Tools weist den Nutzer bei der Einrichtung auf ein zu schwaches Passwort hin! Wer die „Stärke“ seines Passwortes prüfen will, kann das auch unter https://passwortcheck.datenschutz.ch/check.php auf der Seite des schweizerischen Datenschutzbeauftragten tun.

Am meisten Disziplin fordern die Tools, die nur eine manuelle Verschlüsselung von **einzelnen Dateien** oder Verzeichnissen ermöglichen. Diese sind zwar für gelegentlichen Verschlüsselungsbedarf geeignet und für Daten, die sicher final archiviert werden sollen. Wer jedoch viele Daten oder immer wieder erneut aktuelle Daten vor unbefugtem Zugriff schützen will, wird bei der Verwendung von manuellen Tools schnell müde werden oder die eine oder andere Datei mit zu verschlüsselndem Inhalt aus Versehen sogar vergessen.

Komfortabler ist es, **ganze Partitionen oder (System-)Festplatten** zu verschlüsseln; dann ist eben alles ein Geheimnis und das System fährt nur verschlüsselt hoch. Nachteil für Reisen in die USA, Singapur und China: Der freundlichen Aufforderung, seinen Rechner funktionsfähig dem Grenzbeamten vorzuführen oder auf die Einreise zu verzichten, ist die direkte Einladung zum staatlich gewünschten Abräumen der nunmehr ungeschützten Daten.

Wenn man möglicherweise auf verschiedenen Rechnern mit seinen Nutzdaten arbeiten will, z. B. am Arbeitsplatzrechner im Büro und auf dem Laptop unterwegs, dann kann eine **verschlüsselte mobile Festplatte** eine gute Lösung sein. Einige Tools lassen sogar als Basisformatierung ein betriebssystemübergreifendes Dateisystem zu, so dass man mit Windows, Linux und MacOS transparent seine Daten verarbeiten kann.

Risiken und Nebenwirkungen

Vor der Auswahl eines geeigneten Tools sollte man sich über einige Aspekte zur Verschlüsselungstechnologie ein paar Gedanken machen:

- „Ab Werk“ **mitgelieferte Verschlüsselungssoftware** (Windows Vista, Windows 7, MacOS X) genügt häufig nicht einmal elementaren Sicherheitsanforderungen - was nicht unbedingt am eingesetzten Algorithmus liegt, sondern an der Tatsache, dass wesentliche Teile der verwendeten Verschlüsselungstechnologie auf unverschlüsselten Partitionen bzw. Swap-Laufwerken liegen können.
- Wer (sichere) Verschlüsselung einsetzt, muss sich darüber im Klaren sein, dass sich die verschlüsselten Daten jedem Versuch zur Datenrettung entziehen. Das Verschlüsseln von Daten verlangt also nach einem zuverlässigen **Backupverfahren**.

- Kümmern Sie sich rechtzeitig um **Vorsorge** (z. B. durch Passworthinterlegung bei einer eingeweihten Vertrauensperson) **für die Entschlüsselung Ihrer Daten im Notfall**, also bei Unfall, Koma, Tod oder Gedächtnisverlust.
- Die Schwachstelle jeden Verschlüsselungsverfahrens ist der **Arbeitsspeicher** des eingesetzten Rechnersystems, der je nach Modell durchaus die Entschlüsselungssequenz bis zu 20 Minuten nach dem Ausschalten noch (ungewollt) auslesbar bevorratet.
- In Deutschland ist die Verweigerung zur Preisgabe des Entschlüsselungspasswortes **straffrei**, in anderen Ländern hingegen nicht (z. B. England per Gesetz, USA per Gerichtsurteil).
- **Ältere Softwarepakete** (MS Office 2000, 2003; Adobe Photoshop 3.0 bis 5.X; QuarkXPress 4.0 bis 6.5), die unter Umständen auf dem jeweiligen Arbeitslaufwerk zwischenspeichern wollen, kommen dabei nicht immer mit verschlüsselten Partitionen zurecht.

Sicherheit von mobilen Geräten

Im Gegensatz zu PCs, Laptops und Netbooks haben die Hersteller bei **mobilen Geräten** (Mobile Devices) – man kann schon sagen „traditionell" – in Sachen Sicherheit gepatzt: Sicherheit und Verschlüsselung fordern (Rechen-)Leistung und Energie, die dann für die eigentlichen Anwendungen fehlt. Schon heute hangeln sich manche Handynutzer von einer Auflademöglichkeit zur anderen. In Japan sind bei Partys Ladestationen genauso selbstverständlich im Angebot wie Getränke und Snacks; „Charging-Kioske" sind ein profitables Geschäftsmodell.

Der Schutz von privaten bzw. geschäftlichen Daten auf mobilen Geräten ist bestimmt auch lukrativ, aber die Sensibilität für den Schutz von Daten und die Bereitschaft, dafür Zeit und Geld aufzuwenden, ist beim typischen Benutzer meist nicht vorhanden. Aber auch die App-Programmierer leisten keinen Beitrag zur Sicherheit, weil sie in den Apps Konnektivität einbauen, die die Anwendung selbst gar nicht braucht: Warum muss eine Übersetzungs-App GPS-Daten senden? Warum braucht ein Navigationsprogramm Zugriff auf die persönlichen Mail-Adressbücher?

Die Sicherheit des mobilen Gerätes wird bedauerlicherweise nicht von der Gerätesoftware bestimmt, sondern die Verantwortung wird bei der Installation der Apps in die Hände des Besitzers gelegt. Und der klickt in der Regel auf „weiter", „weiter" und „weiter" und dann ist die Sicherheit perdu… Verschlüsselung wird auf mobilen Geräten nur von einigen Apps ausgeführt, ist als Vorgabe meist ausgeschaltet oder gelegentlich wird ein Algorithmus verwendet, der inzwischen nicht mehr sicher ist. Wer sich dennoch um die Sicherheit seiner Daten auf dem Smartphone, Handheld, Palm oder Tablet sorgt, hat zwar nur beschränkte, aber dennoch wirkungsvolle Möglichkeiten:

- Verlieren Sie ihr Gerät nicht.
- Sperren Sie das Gerät bei Nichtbenutzung.
- Aktivieren Sie „entferntes Löschen" (Remote Wipe").
- Verbieten Sie bei der Einrichtung von Apps unnötige Verbindungswünsche.
- Updaten Sie das Betriebssystem immer auf die aktuelle Version.
- Kaufen Sie erst ab Mitte 2012 spezielle Virenschutzprogramme für mobile Geräte oder sofort wenn ihr Hersteller es empfiehlt.

CEBIS hilft weiter

Unternehmen, die Informations- und Beratungsbedarf zu Chancen, aber auch Risiken von IT und Internet haben, können sich an CEBIS wenden. In Veranstaltungen und Einzelberatungen wie beispielsweise am **09. Februar 2012** können Unternehmen Hilfestellung durch kompetente Experten erhalten. An diesem Tag findet eine Veranstaltung zum Thema **„Vorbereitung auf die CEBIT"** statt, wo ebenfalls Verschlüsselungstechnologien ein Thema sein werden.

Bitte beachten Sie dazu das **CEBIS-Jahresprogramm 2012 auf der CEBIS-Website http://www.cebis-neu-ulm.de**. Die Veranstaltungen sind kostenlos; eine vorherige Anmeldung unter **Fax: 0731 7040-665** oder **E-Mail info@cebis-neu-ulm.de** ist erforderlich.

Tipp des Monats Dezember 2011