Informationsschutz

Jeder, der mit Computern arbeitet, hat früher oder später mit Informationen zu tun, welche nicht unbedingt in einer Bildzeitung veröffentlicht oder Unberechtigten zur Kenntnis gelangen sollten. Im Folgenden soll eine Möglichkeit aufgezeigt werden, wie solche sensitive Informationen mit relativ geringem Aufwand geschützt werden können.

OMNIA MEA MECUM PORTO
Ich trage alles - was mir wichtig ist - bei mir.

Dieser Spruch aus der Zeit der alten Römer hat auch in der heutigen Zeit seinen Sinn. Glücklich kann sich schätzen, wer das, was ihm wichtig ist, mit sich tragen kann.

Im Besonderen trifft dies auch für persönliche Informationen zu.

Bei den „Dingern“ in der nebenstehenden Aufnahme handelt es sich um sogenannte MemorySticks, auf welchen 128 MB gespeichert werden können.

Das Tüpfelchen auf dem „I“ ist, dass die Information beim oberen Stick durch ein Passwort und beim unteren durch einen Fingerabdruck geschützt ist. Mittlerweile gibt es MemorySticks mit 4 GByte Speicherumfang.

Kann damit sensitive Information geschützt werden?

Ohne weitere Schutzmassnahmen muss diese Frage klar verneint werden.

Der Grund liegt in der Arbeitsweise der Computer, Betriebssysteme und Verarbeitungsprogramme. Bei der Bearbeitung von Informationen werden Sicherheitsdateien angelegt, um im Falle eines Unterbruches möglichst wenig Informationen zu verlieren. Werden Informationen neu gesichert, wird die neue Datei in einem Bereich gespeichert, der schon lange nicht mehr benutzt wurde. Der von der ursprünglichen Datei belegte Speicherplatz wird anschliessend freigegeben, jedoch nicht überschrieben. Bei immer grösseren Festplatten, kann es einige Zeit dauern, bis ein Bereich ein zweites Mal benutzt wird. Das gleiche passiert beim „Löschen“ einer Datei. Dabei wird lediglich der von der Datei belegte Speicherplatz freigegeben, die Information jedoch nicht überschrieben.

Sensitive Informationen werden zudem nicht nur lokal bearbeitet und gespeichert, sondern vielfach auch elektronisch übermittelt. Ohne weitere Schutzmassnahmen sind Mails und deren Anhänge auf dem Netz völlig schutzlos, verbreiten sich auf unvorstellbaren Wegen und hinterlassen auf zig Servern ihre Spuren.

Erschwerend kommt dazu, dass heutige Rechner bei Betrieb sofort ans Netz gehen (z. B. mit ADSL). Leider ist die Situation so, dass nicht nur der Benutzer Zugriff auf das Netz, sondern auch das Netz Zugriff auf den Computer und damit auf die gespeicherten Informationen hat.

Was ist zu tun?

Im Laufe der Zeit werden auf einem PC viele Dateien gespeichert. In den meisten Fällen liegen diese Dateien irgendwo auf der Festplatte herum.

Beim Kauf eines neuen Rechners respektive beim Ausfall einer Festplatte können diese Informationen nur mit ausserordentlichem Aufwand auf eine neue Festplatte gerettet werden. Ganz zu schweigen vom Risiko, dass diese Dateien bei der Weitergabe des Rechners in unbefugte Hände geraten können.

Leider lässt sich das Problem nicht mit Chiffrieren der ganzen Festplatte lösen. Diese Massnahme bietet optimalen Schutz gegen das unbefugte Aufstarten. Einmal in Betrieb erben alle Prozesse die Berechtigungen und können damit auch auf chiffrierte Informationen zugreifen. Dies gilt auch für das Netz!

Idealerweise sollte Information nur dann offen auf dem System zur Verfügung stehen, wenn die Information berechtigt benötigt wird. Nach der Bearbeitung sollte die Information wieder geschützt, die Zwischendateien gelöscht und der unbenutzte Speicherplatz überschrieben werden.

Es drängt sich daher auf, die Dateien zu strukturieren, indem zusammengehörende Dateien in Verzeichnissen gespeichert und diese Verzeichnisse periodisch auf externe Datenträger abgesichert werden. Als Analogie dazu mögen Ordner mit gedruckten Dokumenten gelten.

Im folgenden wird ***SafeToolSoftware*** beschrieben, welches auf obigen MemorySticks installiert und benützt werden kann, ohne dabei die Anlage, auf welcher diese verwendet werden, in irgend einer Form zu beeinflussen.

SafeToolSoftware wurde auf der Basis von WINSEC weiterentwickelt. WINSEC wurde vom Generalstabs der Schweizer Armee entwickelt und wurde Kommandanten militärischer Formationen zum Schutz militäri-

Karli SafeTools, Hauptstrasse 75 b, CH-4528 Zuchwil
+41 (32) 685 13 60 / karli@safetools.ch
SafeTool+KeyPrint: 03 85 ec 49 9c 8f 1e 17 ae af 20 db a9 ed c7 d1 19 db 98 53

scher und personeller Informationen bei der Verwendung von privaten Informatikmitteln unentgeltlich zur Verfügung gestellt. ***SafeToolSoftware*** bietet gegenüber WINSEC neben der Anpassung auf neuere Betriebssysteme zusätzliche Funktionen und eine bessere Benutzerunterstützung.

Mit ***SafeToolSoftware*** können Verzeichnisse oder ***SafeToolOrdner*** mit zusammengehörenden Dateien archiviert, ausgelagert oder chiffriert und anschliessend die offenen Informationen überschrieben werden. Bei Bedarf können die ***SafeToolOrdner*** neu geladen oder dechiffriert und anschliessend bearbeitet werden.

Mit ***SafeToolSoftware*** können ***SafeToolOrdner*** so chiffriert werden, dass die darin enthaltene Informationen völlig gefahrlos über das Netz ausgetauscht werden können.

SafeToolSoftware verwendet zum Chiffrieren den IDEA ™ Algorithmus mit 128 Bit Schlüssellänge. Dieser Schlüssel wird zum Übermitteln mit einem asymmetrischen Schlüssel von 2048 Bit geschützt. In diesem Zusammenhang sei darauf hingewiesen, dass für militärische Forderungen ein asymmetrischer Schlüssel von 1024 Bit als genügend eingestuft wird.

Asymmetrische Schlüssel dürfen nur verwendet werden, wenn die Schlüssel eindeutig identifiziert werden. Normalerweise übernimmt diese Aufgabe eine Zertifierungsstelle. ***SafeToolSoftware*** geht hier einen anderen Weg, indem pro Schlüssel ein sogenannter KeyPrint berechnet und veröffentlicht werden kann. Beispielsweise ist der KeyPrint des Schlüssel KarlF in der Fussnote dieses Textes aufgeführt. So kann die Authentizität dieses Schlüssels jederzeit überprüft werden. Dies gilt natürlich auch für andere, selbsterzeugte Schlüssel, wenn der entsprechende KeyPrint analog ausgetauscht wird.

Um einer Person auf diese Weise geschützte Information zu übermitteln, muss der Absender über den öffentlichen Schlüssel des Empfängers verfügen. Selbstverständlich muss die Echtheit dieses Schlüssels mit KeyPrint überprüft werden.

Beim chiffrierten Datenaustausch wird der öffentlichen Schlüssel des Absenders mitgeliefert. Zudem wird die Information von ***SafeToolSoftware*** digital signiert. Völlig neu ist, dass ***SafeToolSoftware*** beim Dechiffrieren einer solchermassen geschützten Information die digitale Signatur gegenzeichnet. Dieses ***SafeToolAttest*** dient dem Absender als Hinweis, dass seine Information angekommen und dechiffriert wurde. Dieses ***SafeToolAttest*** erhält jedoch nur dann Rechtskraft, wenn die Beteiligten dies gegenseitig schriftlich festhalten.

Schlüssel werden mit einem persönlichen UserKey chiffriert. Mit dem persönlichen Schlüssel können ***SafeToolOrdner*** chiffriert werden. Normalerweise bieten Internet-Provider auch die Möglichkeit, Information auf dem Server zu speichern. Damit kann der Server des Internet-Providers als ***Virtueller Safe*** benutzt werden, indem so geschützte Informationen auf dem Server des Providers gespeichert werden.

SafeToolSoftware steht Interessenten auf www.safetools.ch gratis zur Verfügung.

Virtueller Safe

Neu entwickelt ***Karli SafeTools*** eine Version mit integriertem virtuellem Safe.

Normalerweise werden heutzutage wichtige Informationen auf CDs gebrannt und bei nächster Gelegenheit aus Sicherheitsgründen in den Safe einer Bank eingeschlossen. Leider ist man dabei auf die Öffnungszeiten dieser Bank angewiesen. Ein weiterer Nachteil ist, dass diese Datensicherung ortsgebunden ist.

Mit ***SafeToolSoftware*** ist es jedoch möglich, Informationen rund um die Uhr und rund um den Globus so zu sichern, dass diese bei Bedarf überall und jederzeit zur Verfügung stehen.

Wie ist das möglich?

Informationen können mit ***SafeToolSoftware*** im UserMode chiffriert werden. Diese Daten können nur dann wieder eingesehen und bearbeitet werden, wenn sie mit dem persönlichen UserKey wieder entschlüsselt werden. Solche UserMode-Chiffrate gelten als absolut sicher und können daher auch auf dem Server eines Providers gespeichert werden oder von dort wieder geholt werden.

Diese Aufgabe übernimmt jedes File-Transfer-Programm oder ***SafeToolSoftware***.

Fragen beantwortet karli@safetools.ch

Karli SafeTools, Hauptstrasse 75 b, CH-4528 Zuchwil
+41 (32) 685 13 60 / karli@safetools.ch
SafeTool+KeyPrint: 03 85 ec 49 9c 8f 1e 17 ae af 20 db a9 ed c7 d1 19 db 98 53