KANTON LUZERN

Datenschutzbeauftragter
des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Merkblatt “Festplattenverschlüsselung und Steganographie“

1. Zweck des Merkblattes

Dem unbestrittenen Nutzen eines mobilen Computers steht die erhöhte Gefahr des Diebstahls gegenüber. Allein im Jahr 2004 wurden in den USA 673’000 Notebooks als Verlust gemeldet – das ist ein Notebook von vierzehn.

Neben dem materiellen Schaden im Falle eines Diebstahls geraten dabei die auf der Notebook-Festplatte gespeicherten Daten in falsche Hände. Um zu verhindern, dass diese Daten von nicht berechtigten Personen eingesehen werden können, bestehen die Möglichkeiten der Festplattenverschlüsselung und der Steganographie.

Dieses Merkblatt soll aufzeigen, wie auf einer Festplatte abgelegte Daten vor dem Zugriff Unberechtigter geschützt werden können, auch wenn die Festplatte abhanden kommt.

2. Unterschied zwischen Zugriffsschutz und Verschlüsselung

Wird der Zugriff auf Daten durch einen Zugriffsschutz wie z.B. dem Windows-Login-Passwort verhindert, so werden die Daten dennoch unverschlüsselt auf der Festplatte abgelegt und können deshalb von einem anderen, beispielsweise von CD gebooteten Betriebssystem gelesen werden.

In diesem Zusammenhang muss erwähnt werden, dass auch ATA-Security zur Kategorie der Zugriffsschutzmechanismen gehört. Es handelt sich dabei um eine in der Firmware von Festplatten implementierte Passwortsperre (ATA Security Feature Set). Dies beinhaltet keine Verschlüsselung der Daten, sondern stellt nur einen Zugriffsschutz dar. Zumindest professionellen Datenrettern bereitet das Umgehen dieses Schutzes keine Schwierigkeiten[1]. ATA-Security ist für sensible Daten zu unsicher.

Im Gegensatz dazu sorgt eine Verschlüsselung dafür, dass die Daten so auf der Festplatte abgespeichert werden, dass sie zwar gelesen, aber ohne Entschlüsselung nicht verstanden werden können. Auch ein zweites, von CD gebootetes Betriebssystem sieht nur die verschlüsselten Daten und benötigt den richtigen Schlüssel, um die Daten verarbeiten zu können.

[1] http://www.heise.de/ct/05/08/172/#kasten1

3. Arten der Datenverschlüsselung

Die Arten der Verschlüsselung werden je nach Zeitpunkt im Verlauf des Computerstarts, in dem die Verschlüsselung einsetzt, unterschieden.

a) Verschlüsselung durch das Betriebssystem oder ein Hilfsprogramm

Eine Möglichkeit ist es, dass zuerst der Computer aufstartet, das Betriebssystem in unverschlüsselter Form von der Festplatte geladen wird und erst danach auf verschlüsselte Daten zugegriffen wird. Dazu führt das Betriebssystem ein Programm aus, das beim Benutzer das Passwort nachfragt und anschliessend Ver- und Entschlüsselung erledigt. Die entsprechenden Daten sind in einem sog. Container auf der ansonsten unverschlüsselten Festplatte untergebracht. Der Container ist dabei nichts anderes als ein vom System für verschlüsselte Daten reservierter Bereich.

Diese Technologie bietet sich an, wenn nur bestimmte Dateien verschlüsselt abgelegt werden sollen. Beispielsweise könnte der gemeinsame Einsatz eines Computers in einer Familie ein geeignetes Szenario sein, in dem jedes Familienmitglied einen eigenen, mit jeweils unterschiedlichem Passwort geschützten Bereich auf der Festplatte erhält.

Nachteil dieser Art der Verschlüsselung ist, dass der Benutzer dafür sorgen muss, dass er die zu sichernden Daten auch tatsächlich im verschlüsselten Bereich ablegt. Hier kommt es schnell zum versehentlichen Speichern in einem unverschlüsselten Bereich. Auch legen einige Programme Sicherungskopien der bearbeiteten Dateien an und speichern diese an unverschlüsselten Orten. Diese Daten können folglich auch Kenntnis des Passwortes gelesen werden.

Ein Beispiel für ein freies open-source Tool, mit dem verschlüsselte Festplattenbereiche erstellt und verwaltet werden können, ist TrueCrypt[2]. Ähnliches leistet das Encryption File System[3] von Microsoft. Es funktioniert allerdings nur auf NTFS-formatierten Datenträgern und ist nur in der Professional-Version von Windows XP enthalten.

b) Verschlüsselung des gesamten Festplatteninhalts

Um den genannten Nachteilen der Verschlüsselung durch das Betriebssystem zu begegnen, lässt sich die Verschlüsselungskomponente in einen anderen Bereich des Computersystems verlegen, nämlich in eine Komponente, die schon vor dem eigentlich Aufstarten („pre-boot“) des Computers aktiv ist. Diese Komponente erfragt beim Einschalten des Computers das Passwort des Benutzers noch bevor das Betriebssystem geladen wurde. Ist das eingegebene Passwort korrekt, kann der Computer auf die Festplatte und die darauf verschlüsselt abgelegten Daten zugreifen.

Bei diesem Verfahren werden immer alle (!) Daten auf der Festplatte verschlüsselt. Insbesondere ist es nicht mehr möglich, Daten oder temporäre Dateien versehentlich auf einen unverschlüsselten Bereich der Festplatte zu speichern.

Nachteil dieser Methode ist, dass eine Komponente zur Passwortabfrage vor dem Computerstart („pre-boot-authentication“) in den Computer eingebaut sein muss.

Bekannte Produkte sind etwa Ultimaco SafeGuard Easy, WinMagic SecureDoc Disk Encryption oder NEC SafeBoot. Es existieren auch Festplatten mit eingebauter

[2] http://www.truecrypt.org/
[3] Eine Beschreibung, wie EFS benutzt wird, findet sich unter http://support.microsoft.com/default.aspx?scid=kb;de;308989&sd=tech.

Verschlüsselung. Wenn diese proprietäre Verschlüsselungsalgorithmen verwenden, ist allerdings Vorsicht geboten[4].

4. Steganographie

Bei der Steganographie werden Daten nicht verschlüsselt, sondern versteckt. Die Daten sind also jederzeit lesbar, werden aber in der Regel nicht entdeckt – ausser man weiss, dass sie da sind. Ein einfaches Beispiel sind Wasserzeichen, die auf einem Dokument die Nachricht übermitteln, welches der tatsächliche Ursprung des Dokumentes ist.

Im Fall von Computerdaten wird Steganographie so eingesetzt, dass Daten in anderen Daten versteckt werden. Grundlage dafür ist das sog. Datenrauschen. Damit wird die Ungenauigkeit bezeichnet, mit der analoge Signale wie beispielsweise Bilder oder Töne in eine digitale, computerlesbare Form übersetzt werden. So gibt es für jedes Bild eine Unmenge von unterschiedlichen digitalen Repräsentationen mit minimalen Unterschieden zueinander, die aber alle für das menschliche Auge das gleiche Bild ergeben. In diesem Toleranzbereich lassen sich Informationen unterbringen, ohne dass der Mensch die hinzugefügte Information erkennen könnte.

Das bekannteste Programm für die Verwendung von Steganographie zum Verstecken von Informationen in Computerdateien ist Steganos Security Suite[5].

5. Schlussfolgerung

Weil der Zugriffsschutz über das Windows-Login-Passwort ungenügend ist, empfiehlt sich der Einsatz von Verschlüsselung, Steganographie oder sogar einer Kombination beider Verfahren. Kommt der PC oder das Notebook in falsche Hände, so sind zumindest die abgelegten Daten nicht einsehbar.

6. Fragen und Informationen

Für Fragen und weitere Informationen stehen Ihnen die Datenschutzbeauftragten gerne zur Verfügung.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Telefon:	+ 41 41 228 66 06
Fax:	+ 41 41 228 69 13
E-Mail:	dsb@lu.ch **WARNUNG**: Der E-Mail-Verkehr ist unsicher. Vertrauliches gehört deshalb nicht in E-Mails!
Internet:	http://www.datenschutz.lu.ch

Luzern, März 2006

[4] http://www.heise.de/security/artikel/60711
[5] http://www.steganos.de/