Die Suva setzt auf Festplattenverschlüsselung

Das Datenschutzgesetz schreibt vor, dass Personendaten durch einen angemessenen Datenschutz zu sichern sind. Die Suva setzt im Aussendienst 900 Notebooks mit Daten ein, die einen sehr hohen Schutzbedarf aufweisen. Damit die Daten im Falle eines Verlusts vor Missbrauch geschützt werden können, wurden alle Notebooks bei der Suva mit einer Festplatten-Verschlüsselung der kanadischen Firma WinMagic ausgestattet. Die komplette Festplatte bleibt dabei jederzeit vollständig verschlüsselt und nur berechtigte Personen können sich mittels Pre-Boot Authentifikation anmelden. Dank dieser Massnahme wird ein sehr wirksamer Datenschutz bei Diebstahl, Verlust und unberechtigtem Zugriff auf die Notebooks erreicht.

Die Suva (Schweizerische Unfallversicherungsanstalt) setzt 900 Notebooks ein, auf denen sich schützenswerte Personen- und Gesundheitsdaten befinden. Gemäss den Vorgaben des Datenschutzgesetztes müssen solche Informationen einen angemessenen Datenschutz erfahren, der die Informationen insbesondere gegen Diebstahl, zufälligen Verlust oder widerrechtliche Verwendung schützt. Im Falle einer ungewollten Veröffentlichung der Daten müsste im schlimmsten Fall mit einer Strafverfolgung gerechnet werden.

Warum hat sich die Suva nach einer eingehenden Produktevaluation für ***SecureDoc*** von der kanadischen Entwicklungsfirma **WinMagic** entschieden? Die einzige sichere Methode, um Informationen auf Notebooks wirksam gegen die erwähnten Risiken zu schützen, besteht darin, dass die gesamte Festplatte jederzeit vollständig verschlüsselt bleibt und sich die Benutzer nach dem Einschalten des Notebooks mittels Pre-Boot Logon authentifizieren müssen. Erst danach wird das Betriebssystem gestartet. Informationen befinden sich nicht nur dort, wo sie bewusst hinkopiert werden, sondern auch im Page-File, in temporären Verzeichnissen, in Offline-Dateien des Mail-Programms, im Papierkorb oder in nicht vollständig beschriebenen Sektoren der Festplatte (Slack-Space). Der durchschnittliche Anwender wäre überfordert, alle diese Kopien der Informationen jeweils zu löschen. Die Abbildung 1 zeigt, wo sich Informationen überall auf der Festplatte befinden können.

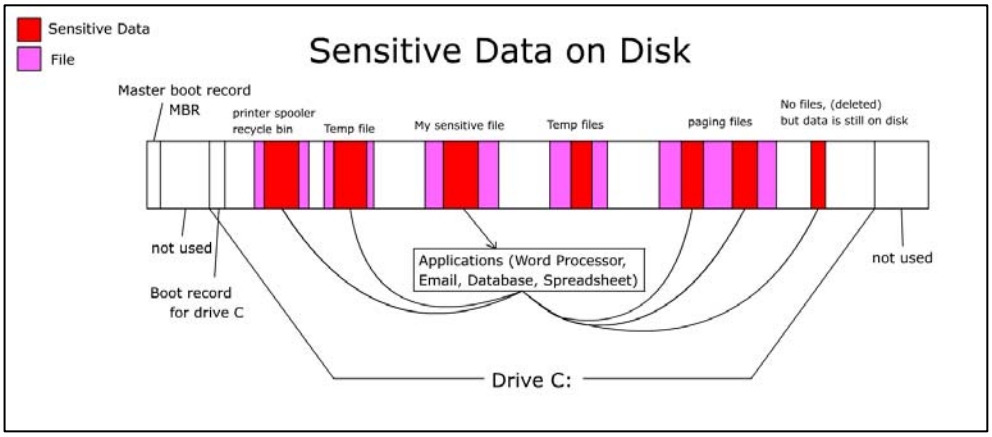

Abbildung 1: Wo sich die Informationen befinden

Bei der Bewertung der verschiedenen Verschlüsselungsmethoden wurde ersichtlich, dass viele Produkte und Methoden nicht sämtliche Informationen auf der Festplatte verschlüsseln. Mit der Datei- oder Container-Verschlüsselung können zwar die durch die Benutzer spezifizierten Dateien sicher verschlüsselt werden, die Schatten-Kopien dieser Dateien liegen jedoch unverschlüsselt auf der Festplatte. Es stellt auch kein grosses Problem dar, Informationen aus momentan unbenutzten Bereichen der Festplatte mittels Analyse-Tools zu lesen. Nur die komplette Festplatten-Verschlüsselung gewährt den erforderlichen Schutz.

insinova ag
Sumpfstrasse 32
6300 Zug

Telefon +41(0)41 748 72 00
Telefax +41(0)41 748 72 01
www.insinova.ch

Das Produkt ***SecureDoc*** überzeugt durch die einfache Verbreitung der Software auf den Notebooks, die Unterstützung von mehreren Tastatur-Sprachen für den Pre-Boot-Logon und das perfekte Zusammenarbeiten mit Viren-Scannern und Systemtools. Ebenfalls überzeugt das durchdachte Schlüssel-Konzept von ***SecureDoc***. Jedem Benutzer wird eine Schlüssel-Datei zugeordnet, in der sich beliebig viele Schlüssel befinden können. So befinden sich jeweils der einzigartige Festplatten-Schlüssel sowie mehrere individuelle und gemeinsame Schlüssel zum Verschlüsseln von Wechseldatenträgern (z.B. USB-Token, Micro-Drives) in jeder Schlüsseldatei. Dies ermöglicht den sicheren Austausch von Wechseldatenträgern innerhalb der Suva, weil jeder Benutzer über den gemeinsamen Schlüssel verfügt. Sollte ein Wechseldatenträger verloren gehen, kann dieser ausserhalb der Suva nicht gelesen werden.

Zentrales Element der Lösung ist der ***SecureDoc Enterprise Server***, auf welchem alle Benutzer, Notebooks und Einstellungen verwaltet werden. Sämtliche Definitionen (z.B. Bildschirmanzeige für den Pre-Boot-Logon, Tastatur-Layout, Passwort-Richtlinien) werden darin verwaltet. Die Ausbreitung auf die Notebooks ist denkbar einfach. Mit wenigen Klicks lassen sich für die Benutzer Konfigurationsdateien erzeugen, welche mittels Software-Verteilmechanismen auf die Notebooks kopiert werden. Danach wird das für alle Notebooks gleiche Setup-Programm gestartet, welches anhand der Konfigurations-Dateien die Festplatte des Notebooks verschlüsselt. Der Benutzer spürt keinen Performanceverlust durch die Verschlüsselung. Die benötigte Systemleistung zum Ver- und Entschlüsseln liegt bei weniger als 2%, was nicht wahrnehmbar ist. Nach dem Einschalten des Gerätes wird der Benutzer mittels Pre-Boot-Logon aufgefordert, ein Passwort einzugeben. Erst danach wird das Betriebssystem gestartet. ***SecureDoc*** funktioniert somit mit allen Virenscannern, Backup- und Komprimier-Programmen und unterstützt den Hibernation-Mode von Windows.

SecureDoc unterstützt zudem eine sehr grosse Anzahl von PIN-geschützten USB-Token und Smart Cards, um sich am Pre-Boot-Logon anmelden zu können. Eine Integration in bestehende PKI-Lösungen kann somit mit der gleichen Smart Card bzw. mit den Zertifikaten erfolgen (siehe Abbildung 2). Diese Kombination wird unter anderem beim **Bundesamt für Informatik und Telekommunikation BIT** und beim **Kanton Aargau** eingesetzt.

Abbildung 2: Token- und PKI-Integration

Um die mobile Sicherheit abzurunden, hat WinMagic auch eine Verschlüsselung für PDAs entwickelt, welche unter dem Betriebssystem Microsoft PocketPC läuft.

Wichtigste Features
- komplette Festplattenverschlüsselung
- transparent für die Benutzer
- Anmeldung mittels Challenge-Response-Verfahren für den Notfall
- volle Interoperabilität mit Windows, Viren-Scannern, Komprimierprogrammen
- unterstützt grosse Anzahl Token und X.509 Zertifikate
- sehr einfacher Roll-Out mit SecureDoc Enterprise Server
- unterstützt den Hibernation-Mode und verschiedene Tastatur-Layouts am Boot-Logon

Weitere Informationen:

insinova ag
Sumpfstrasse 32
6300 Zug
Tel. 041 748 72 00
www.insinova.ch