Fileverschlüsselungstool secureEFS

A-SIT bietet unter: **http://www.a-sit.at/de/technologiebeobachtung/tools_und_prototypen/secure_efs.php** das kostenlose Tool **"secureEFS"** für die Dateiverschlüsselung mit der Bürgerkarte an.

Ziel

Das Werkzeug zur Unterstützung der Datei- und Bereichsverschlüsselung baut auf den unter Windows und NTFS verfügbaren Verschlüsselungsmechanismen auf und unterstützt deren kontrollierte Verwendung durch:

- Anwendung auf Geräten in ungesicherter Umgebung sowie auf Laptops
- Schutz vor Verlust der Vertraulichkeit im Falle von Geräteausfällen oder Teilausfällen
- Kontrollierte Zugänglichkeit mit Hilfe der Verschlüsselung von geheimen Schlüsseln mit der Bürgerkarte
- Verwendung von ein oder mehreren unabhängigen Karten zum Zugang durch unterschiedliche Personen oder nach Verlust einer Karte
- Verwendung von extern erzeugten und damit bereits gesicherten Schlüsseln (EFS-Zertifikaten), die einen Datenverlust vermeiden lassen

Das System geht davon aus, dass nur einzelne Bereiche zu verschlüsseln sind und dass nicht mehrere unterschiedliche Schlüssel oder EFS-Zertifikate vorhanden sind.

Organisation der Vertraulichkeit setzt ein Grundwissen darüber voraus, wo sensible Daten bei deren Verwendung und Verarbeitung abgelegt werden.

Voraussetzungen

- Das Gerät muss Windows2000® oder WindowsXP® verwenden.
- Es muss NTFS als Filesystem verwendet werden.
- Vor der Installation muss ein EFS-fähiges Zertifikat beigestellt werden. Dazu wird unter

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

  ein geeignetes Werkzeug angeboten.
- EFS-Verschlüsselung darf zuvor nicht aktiv sein.
- Es wird eine Bürgerkartenumgebung verlangt, die Ver- und Entschlüsselung nach dem Konzept Bürgerkarte zur Verfügung stellt.

Wirkung

secureEFS verwendet die in Windows vorhandenen Werkzeuge zum Verschlüsseln von Dateien.

Es wird zu Beginn einer Session (nach dem GINA Login) ein Task gestartet, der den geheimen Schlüssel wirksam löscht. Da dieser im Prozessor für Diskzugriffe gecached wird, ist der **Schlüssel noch bis zum Ende der Sitzung vorhanden**.

- Bricht die Sitzung ab oder wird diese beendet, so kann keine verschlüsselte Datei mehr gelesen werden.
- Beim Neustart wird der geheime Schlüssel aus einer verschlüsselten Datei mittels der Bürgerkarte zurückgewonnen und nach dem Cachen vom System gelöscht.
- Das System kann damit auch im Wartungsfall problemlos verwendet werden. Wartungstechniker oder Systemadministratoren gewinnen keinen Zugriff auf verschlüsselte Materialien.
- Beim Löschen wird ein DOD-anerkannter Mechanismus eingesetzt um tatsächliches Löschen sicherzustellen.

Verschlüsseln und Löschen

- Der normale Löschvorgang unter Windows löscht die Datei nicht physikalisch. Dies ist auch beim Löschen aus dem Papierkorb nicht gegeben.
- Der Verschlüsselungsvorgang unter Windows hinterlässt die ursprüngliche Datei als einen gelöschten Windows-Bereich zurück.

Verschlüsseln Sie nie einzelne Dateien. Legen Sie verschlüsselte Verzeichnisse an und erzeugen Sie in diesen verschlüsselte Dateien.

Sollten Sie dennoch eine bestehende Datei verschlüsseln wollen, dann kopieren Sie diese in einen verschlüsselten Bereich und löschen die ursprüngliche Datei mit einem geeigneten Werkzeug.

Beachten Sie, dass Programme zwischendurch Dateien bzw. Dateiteile in temporären Verzeichnissen hinterlassen, die trotz Verschlüsselung der eigentlichen Datei analysiert werden könnten.

Was sollte verschlüsselt werden

1. In der Praxis wird es sinnvoll sein, die Applikationsbereiche des Benutzers zu verschlüsseln.

2. Für Webapplikationen wird es notwendig sein, die Cachebereiche des Browsers zu verschlüsseln.

3. In verschiedenen sicherheitsrelevanten Anwendungen wie etwa Mailprogrammen wird es auch notwendig sein, die Konfigurationsverzeichnisse des entsprechenden Programms zu verschlüsseln.

4. Die Zertifikate und Zugangspasswörte zu Services und Verbindungen müssen verschlüsselt werden, um einen Zugriff bei Verlust oder Missbrauch des Gerätes zu vermeiden.

Beachten Sie, dass beim Backup gesicherte Dateien nicht verschlüsselt sind und gehen Sie entsprechend vorsichtig mit den Sicherungsmedien um.

Bedenken Sie weiters, dass vor Abschluss der Initialisierung verschlüsselte Dateien nicht erfolgreich geöffnet werden können. Sie dürfen daher die Dateien des Windows Betriebssystems bzw. Dateien von Drivern nicht verschlüsseln, da sonst ein Neustart nicht mehr möglich ist.

Verlust von Schlüssel oder Token

Ohne weitere Vorkehrungen gibt es nach Verlust des Schlüssels (etwa durch Zerstörung der entsprechenden Datei) oder des Tokens keine Möglichkeit, die Entschlüsselung durchzuführen oder die Daten zurückzugewinnen.

- Gehen Sie entsprechend vorsichtig mit Schlüssel und Token um.
- Sichern Sie in regelmäßigen Abständen und verwahren Sie das gesicherte Material gut.

- Verwenden Sie nur geeignet erzeugtes und abgesichertes Schlüsselmaterial, damit auch nach Fehlern weiterhin die Möglichkeit des Recovery besteht.
- Sie können zusätzlich in anderen Verzeichnissen oder für andere Benutzer weitere sEFS Instanzen installieren und dafür das gleiche EFS Zertifikat verwenden. Das sEFS Tool kann entsprechend erweitert werden, damit in Notfällen auch mit diesen Alternativzugängen gearbeitet werden kann.

Fragen

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

www.a-sit.at 2006-10

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

Fileverschlüsselung secure EFS

E-Government Flyer Nr.207

Werkzeuge zum Verschlüsseln von Dateibereichen und Absicherung mit der Bürgerkarte

DIGITAL AUSTRIA