

IT-SECURITY-HELPDESK

Plus und Minus von EFS

Wir haben Windows XP und wollen künftig vertrauliche Informationen verschlüsseln. Bietet das Encrypted File System (EFS) von Microsoft ausreichenden Schutz?



Um diese Frage beantworten zu können, muss zunächst geklärt werden, wie der Verschlüsselungsmechanismus von EFS funktioniert, welche Algorithmen und Betriebsarten unterstützt werden und welche Mängel EFS aufweist.

Die EFS-Verschlüsselung basiert auf dem Hybrid-Modell aus asymmetrischer und symmetrischer Verschlüsselung. Jedes File erhält einen individuellen symmetrischen Encryption Key (FEK). Dieser wird mit dem Public Key des Benutzers verschlüsselt und zusammen mit dem File abgelegt. Gleichzeitig wird der FEK mit dem Public Key des Recovery Agents verschlüsselt. So wird es möglich, verschlüsselte Daten bei einem allfälligen Verlust des Schlüssels zurück zu gewinnen. Die Verschlüsselung des Files erfolgt jeweils auf der Harddisk des Zielsystems. Filesharing wird ab Windows XP und Windows 2003 auf File- nicht aber auf Folder-Ebene unterstützt.

Ab Windows XP SP1 werden neben 3DES (112 Bit) und DESX (56 Bit) auch AES (256 Bit) für die symmetrische und RSA (1024 Bit) für die asymmetrische Verschlüsselung unterstützt.

Die Funktion des Recovery Agents ist problematisch und ist bei Default dem Sys-Admin zugeordnet. Oft werden aber Informationen verschlüsselt, um den Zugang der Administratoren zu diesen vertraulichen Informationen zu verhindern. Der Recovery Agent ist daher einem besonderen Account zuzuordnen, der nur über eine klassische Notfall-Prozedur zugänglich gemacht wird.

Weil die Verschlüsselung auf der Harddisk des Zielsystems (Servers) erfolgt, ergeben sich zwei Probleme: Erstens sind die Informationen während der Übertragung ungeschützt. Um sie zu schützen, müsste zwischen Client und Server eine IPSec-Verbindung aufgebaut werden. Eine Alternative wäre der Aufbau von Web Folder anstelle des klassischen

New Technology File System (NTFS) für verschlüsselte Informationen. Zweitens benötigt der Server für die Entschlüsselung der Daten Zugang auf das lokale Profil des Benutzers. Daher unterstützt EFS den Einsatz von Smartcards nicht.

Die Sicherheitsadministration liegt bei den Benutzern und nicht bei einer zentralen Verwaltung. Jeder autorisierte Benutzer kann bestimmen, für welche Personen die Informationen zugänglich sein dürfen. Das heisst: Gibt der Eigentümer

trieb. Auch wenn dies heute keine besonders schwierige Aufgabe mehr ist, sollte doch eine PKI dazu verwendet werden, um mehrere Anwendungen unterstützen zu können. So ist es sicher sinnvoll, neben der File/Folder-Verschlüsselung auch starke Authentisierung für das Logon und den Applikationszugang zu implementieren. Empfehlenswert ist es daher, den Smartcard-basierten Windows Logon (Authentisierung) auch mit Secure E-Mail und File Encryption (Verschlüsselung) zu verbinden.

Aus dieser ganzheitlichen Betrachtung ergibt sich folgende Antwort: Zunächst müssen Sie eine Bedarfs- und

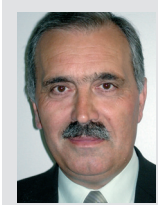
Risikoanalyse erstellen. Anhand dieser sollten Sie prüfen, ob sich ein kommerzielles Produkt bekannter Hersteller (Safenet, Utimaco, Winmagic) für Ihre Ansprüche nicht besser eignet. Achten Sie bei der Evaluierung der Lösungen darauf, wie der Hersteller sicherstellt, dass die Vertraulichkeit der Informationen auch bei gemeinsamer Bearbeitung in definierten Gruppen gewährleistet ist, ohne bestehende Prozesse einzuschränken. ■

Smartcards sind die benutzerfreundlichen Sicherheitselemente für alle kryptologischen Funktionen.

eines Files «X» den Personen «Markus» und «Nicole» den Zugang frei, können Markus und Nicole zu einem späteren Zeitpunkt weiteren Personen den Zugang zum File X freigeben. Das macht es sehr schwierig, die Vertraulichkeit der Informationen zu kontrollieren.

EFS von Microsoft weist also einige Unzulänglichkeiten auf, die je nach Einsatzbedarf die Sicherheit reduzieren und für die etablierten Betriebsprozesse hinderlich sind.

Überdies erfordert EFS den Aufbau einer PKI (Public Key Infrastructure) im eigenen Be-



Der Autor
Antonio Retica ist Leiter IT-Security bei ITRIS Trading in Spreitenbach.
www.itris.ch

Jede Woche beantworten Sicherheitsexperten Ihre Leserfragen:

Haben Sie Fragen rund ums Thema IT-Sicherheit?

Schreiben Sie uns:
it-security@computerworld.ch

 **Archiv aller Helpdeskartikel:**
www.computerworld.ch