



## Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35  
Tel.: (+43 1) 503 19 63-0  
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a  
Tel.: (+43 316) 873-5514  
Fax: (+43 316) 873-5520

<http://www.a-sit.at>  
E-Mail: [office@a-sit.at](mailto:office@a-sit.at)

### HINWEISE ZUM EFS RECOVERY-TOOL AEFSDR

Das Tool [AEFSDR](#) der Firma ElcomSoft Co. Ltd. ermöglicht die Wiederherstellung bzw. Entschlüsselung von Dateien, die basierend auf dem Dateiverschlüsselungssystem EFS von Microsoft auf einer NTFS Partition verschlüsselt wurden. Heise Online widmet dem Erscheinen der Version 3.0 von AEFSDR sogar eine [Meldung](#) mit dem Titel „Russisches Tool knackt EFS-Schutz“. Diese reisserische Überschrift jedoch verleitet zu der falschen Annahme, EFS selbst wäre geknackt worden. [SecureEFS](#) – eine bürgerkartenbasierte EFS Erweiterung – macht eine Wiederherstellung mittels eines Tools wie AEFSDR praktisch unmöglich.

Am 2. März 2005 ist die Version 3.0 des EFS Recovery Tools AEFSDR der Firma ElcomSoft Co. Ltd. erschienen. Das Programm ermöglicht laut Beschreibung eine Wiederherstellung bzw. Entschlüsselung von Dateien, die auf NTFS Partitionen mittels des Dateiverschlüsselungssystems EFS von Microsoft verschlüsselt wurden.

Dies ist jedoch ohne Weiters nur unter bestimmten Voraussetzungen möglich. Dazu gehören z.B. ein aktivierter [SYSKEY](#) Schutzmechanismus unter Windows 2000 mit lokal gespeichertem Kennwort in der Registry. Unter Windows XP basieren die Verschlüsselungsschlüssel nicht mehr auf SYSKEY. Eine andere Voraussetzung wäre, dass das lokale Administratorkonto gleichzeitig der standardmäßige „Recovery Agent“ ist. Dies trifft z.B. für einen deaktivierten Recovery Agent oder einen domain-basierten Recovery Agent nicht zu.

Sind diese Voraussetzungen nicht erfüllt, so kann AEFSDR einzig und allein durch die Eingabe des Benutzerpassworts die Dateien entschlüsseln, sofern der private Schlüssel auf dem System gefunden wurde.

Heise Online widmet dem Erscheinen der Version 3.0 von AEFSDR eine Meldung mit der reißerischen Überschrift „Russisches Tool knackt EFS-Schutz“. Von „Knacken“ kann hier nicht die Rede sein, denn Tools wie AEFSDR suchen lediglich Partitionen nach privaten EFS Schlüsseln sowie lokal gespeicherten SYSKEYS ab und entschlüsseln Dateien nur unter bestimmten Voraussetzungen (oben aufgelistet) bzw. nach Eingabe des korrekten Benutzerpassworts.

SecureEFS – eine bürgerkartenbasierte EFS Erweiterung – verschlüsselt den privaten Schlüssel zusätzlich durch die österreichische Bürgerkarte. Damit ist der private EFS Schlüssel für Tools wie AEFSDR nicht zugänglich. Dateien, die mit SecureEFS verschlüsselt wurden, können mit diesen Tools daher nicht wiederhergestellt werden. Voraussetzung dafür ist, dass kein lokaler Recovery Agent verwendet wird.