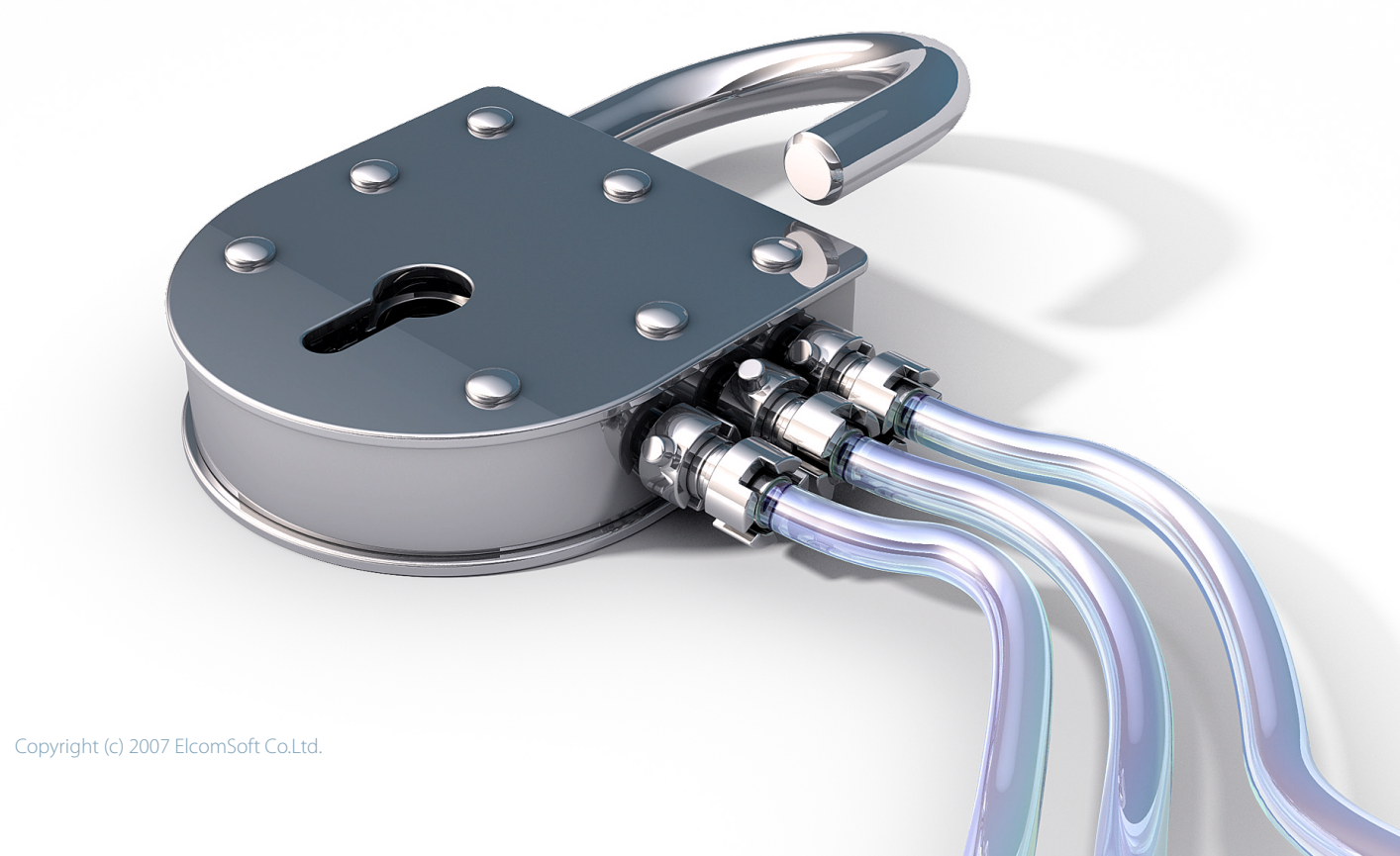
ELCOMSOFT
PROACTIVE SOFTWARE

EINE EFFEKTIVE METHODE ZUR WIEDERHERSTELLUNG DES SYSTEMZUGRIFFS UNTER WINDOWS

WHITEPAPER



ELCOMSOFT
PROACTIVE SOFTWARE

INHALTE

EINFÜHRUNG

Um wichtige Daten zu schützen, benutzen wir viele verschiedenen Methoden und Technologien, vor allem, wenn die besagten Daten vertraulich sind und für tägliche Geschäftstätigkeiten und wichtigen Verwaltungsentscheidungen gebraucht werden.

Das Prinzip „Wenn Sie Informationen besitzen, besitzen Sie die Welt" wurde zum Grundsatz unserer Zeit, da die Datenkontrolle von enormer Wichtigkeit ist. Der Verlust des Zugriffs auf die wichtigen Daten kann sehr negative Auswirkungen auf die Firmenangelegenheiten haben.

Unter diesen Umständen werden die Systemadministratoren zeitweise mit dem Problem der Wiederherstellung des Zuganges zu Kunden-PCs konfrontiert, da die betrieblichen Passwörter verloren gehen.

Leider wird solch ein Problem von den Systemadministratoren oft mithilfe der 'Brute-Force' – Methode gelöst, ohne daß eine spezielle Software zum Zurücksetzen und Wiederherstellung der Passwörter benutzt wird. Der Gegenstand dieses Dokumentes ist, wie man solche Probleme richtig und effektiv löst.

JEDER VERLIERT PASSWÖRTER

Das Festlegen eines Systempasswortes ist – wie wir annehmen – eine der populärsten, sowohl die sicherste Methode zum Schützen der Daten von unbefugten Nutzern. Wie es oft ist, hat es auch seine Kehrseite.

Unser Ziel ist das Festlegen eines "schwierigen" Passwortes, damit man dieses schwerer errät und keinen unberechtigten Systemzugang bekommt. Doch dann vergessen wir dieses und bringen uns selbst in eine heikle Situation. Danach verlieren wir komplett den Systemzugriff.

Das Leben ist voll von unvorhersehbaren Wendungen: der Systemnutzer könnte, zum Beispiel:

- das Passwort vergessen, da dieses zu kompliziert war und nach einer Dienstreise oder Urlaub schlicht vergessen wurde;
- ein Fehler beim Ändern des Passwortes machen, da er, zum Beispiel, ein falsches Zeichen eingegeben hat oder eine sehr komplexe Variante von Anfang an auswählte;
- Jemanden behindern und sagen, man habe das Passwort vergessen (zum Beispiel, vor der Kündigung, falls es ein Konflikt mit der Firmenverwaltung oder Mitarbeiter bestand);
- die Firma verlassen oder einfach verschwinden, ohne Informationen über den Systemzugriff zu hinterlassen (aus Nachlässigkeit oder absichtlich, als Gegenschlag).

Falls es keine anderen Systemkonten gibt – und dies ist wegen den Sicherheitsmaßnahmen sehr oft der Fall – ist das System somit vollständig unzugänglich.

Der Verlust des Systempasswortes ist vor allem dann ungelegen, wenn es nicht nur den Zugriff auf Dateien, Anwendungen und Services unterbindet, sondern auch den gesamten Arbeitsplatz außer Betrieb setzt, mit allen damit verbundenen Konsequenzen.

WAS SIND DIE FOLGEN, WENN MAN EIN SYSTEM-PASSWORT VERLIERT

POTENTIELLE KOSTEN

Die Untersuchung von Datamonitor[1] zeigte, dass die internen Ausgaben für die Problembeseitigung bei Passwort-Fragen zwischen $10 und $40 (je nach Firmengröße) betragen (für einen Antrag für jeden PC). Im Durchschnitt sind es 25$ oder 57 Minuten der täglichen Arbeitszeit eines qualifizierten IT-Spezialisten. Im Verlaufe des Jahres belaufen sich die Durchschnittskosten für große Firmen mit über 2 000 Mitarbeitern auf 150 000 USD.

Diese Angaben beinhalten allerdings nur die Kosten für die angeheuerten IT-Spezialisten. Die Kosten, die durch die Unterbrechung anderer geschäftlichen Vorgänge resultieren, potentielle Vertrags- und Reputationsverluste sind noch separat zu behandeln.

Das Problem ist vielleicht nicht so kritisch, falls das Passwort für den "leeren" Arbeitsplatz oder für den durchschnittlichen Firmenmanager gedacht ist. Hier sind die Verluste niedrig gehalten: die Zeit, die von den Systemadministratoren verbraucht wird, um das System wiederherzustellen, und teilweise Einkommensverluste, die mit der Inaktivität des Mitarbeiters während dieser Zeit zusammenhängen.

Was ist aber, falls der Zugang zum Server, mit allen Kunden-Datenbänken, Firmen- Abrechnungsakten, oder zum Laptop des Geschäftsführers verloren wurde? Diese Situation kann viele interne Probleme verursachen, Firmen-Arbeitsablauf zum Stillstand bringen, sowohl zu beträchtlichen materiellen und betrieblichen Ausgaben führen. Hier ist es unmöglich, die Totalverluste im Geschäft zu kalkulieren, und somit gibt es nur eine Lösung – diese Risikotypen müssen minimiert werden.

WARUM EINFACH NICHT DAS PASSWORT ZURÜCKSETZEN?

Falls der PC ein Teil des Domains ist, kann dessen Passwort durch den Netzwerk-Administrator zurückgesetzt werden. In diesem Fall ist das Problem schnell gelöst, und das Passwort muss nicht wiederhergestellt werden. Diese simple Methode ist die erste Lösung, die in den Sinn kommt, jedoch bringt sie ernste Konsequenzen mit sich.

Was ist, zum Beispiel, die beste Methode, falls der PC EFS (Encrypting File System) oder andere Services benutzt hat, die direkt in das Konto angebunden sind, für welches das Passwort verloren wurde?

Das Problem ist, daß die EFS-geschützten Dateien auf dem Laufwerk mit FEK (File Encryption Key) verschlüsselt sind, der unter den Datei-Eigenschaften gespeichert ist. FEK ist mit dem Hauptschlüssel verschlüsselt, der seinerseits mit den Schlüsseln dieser Nutzer verschlüsselt ist, die Zugang zu den Daten haben. Nutzerschlüssel selbst sind mit den Passwort-Hashes dieser gleichen Nutzer verschlüsselt. Aus diesem Grund verlieren Sie den Zugriff auf EFS-verschlüsselte Daten, falls Sie das Passwort im Domain zurücksetzen werden.

Falls der PC nicht ein Teil des Domains ist, kann das lokale Administrator-Passwort nicht zurückgesetzt werden.

[1] „The ROI case for smart cards in the enterprise," Datamonitor, November 2004 (http://mediaforms.siemensenterprisemedia.com/forms/_docs/Smart%20cards%20ROI%20white%20paper.pdf)

Betriebssystem neu zu installieren, um das Problem der verlorenen Passwörter zu lösen, ist es eine Brute-Force-Methode, die nicht ausprobiert werden sollte. Es kann zum Verlust der wichtigen Daten, sowohl zu den internen Kosten führen.

Wenn das Systempasswort verloren ist, ist es viel sinnvoller, das verlorene Passwort mithilfe der speziellen Software (unten ausdiskutiert) wiederherzustellen.

WIE MAN DEN SYSTEMZUGRIFF WIEDERHERSTELLT?

VORHANDENE LÖSUNGEN

Um die Anwendung zur Wiederherstellung des Systempasswortes zu starten, werden Sie den vollständigen Zugang zur Festplatte des "Problem"-PCs brauchen.

Dies kann auf folgenden Wegen geschehen:

1. Booten unter anderem Konto mit Administratoren-Rechten (falls vorhanden).
2. Festplatte physikalisch abschalten und diese auf dem anderen Arbeitsplatz installieren; dabei Entschlüsselungs-Software nutzen.
3. Booten mit anderem Betriebssystem, das (falls vorhanden) auf gleichem PC installiert ist.
4. Booten mit dem Betriebssystem vom speziellen bootsfähigen CD-Rom oder anderen Wechselmedien, wie USB-Flashlaufwerk.

Die Methode der Nutzung von Wechselmedien ist die bequemste, da es die Unterstützung vom Personal zum schnellen und sicheren Booten mit Administratorenrechten, sowohl den kompletten Zugang zur Festplatte ermöglicht.

WINPE-BOOTSFÄHIGE CD BENUTZEN

Der bevorzugte bootsfähige Disk, der in diesem Fall benutzt werden sollte, ist der Microsoft Windows Preinstallation Environment (WinPE) - Disk. Dieses Tool bietet minimale Funktionalität des standardmäßigen Windows XP – Betriebssystems, das sich selbst für DOS ersetzt und System-Setup im automatischen Modus ermöglicht.

WinPE wird benutzt, um einen Boot-Disk – für Problemfälle konfiguriert – zu erstellen; dieser wird vom Administrator benutzt, um Software-Setup oder Systemwiederherstellung nach Systemzusammenbruch zu automatisieren, wenn das normale Booten unmöglich wird. Dies ist nun genau unser Problem!

Mit dem Boot-Disk kann ein Techniker schnell eine Wiederherstellungs-CD erstellen, dann den Problem-PC problemlos booten, Zugang zu Inhalten der Festplatte verschaffen und spezielles Programm ausführen, um das Passwort zurückzusetzen.

Es ist besser, einen bereits erstellten Rücksetz-Disk mit WinPE zu nutzen, da der Administrator diesen dann nicht erstellen und in die WinPE-Komplexitäten eintauchen muss.

Falls der PC kein CD-Laufwerk hat (zum Beispiel, ein Laptop), können Sie den extra vorbereiteten USB-Rücksetzlaufwerk benutzen.

KOSTENLOSE LÖSUNGEN, DIE AUF LINUX/UNIX BASIEREN

Kostenlose „Open Source"-Lösungen, die auf Linux/UNIX basieren, können als eine Alternative zum WinPE dienen, auch wenn sie kaum als bequeme oder sichere Tools betrachtet werden können. Das Format der kostenlos vertriebenen Software garantiert keine akzeptable Qualität, Update-Veröffentlichungen oder technischen Support. Dabei fehlen oft die übersichtlichen Dokumentationen.

Mehr noch bieten existierende, Linux-basierende Lösungen, wie Offline NT Password & Registry Editor, Bootdisk / CD (http://home.eunet.no/pnordahl/ntpasswd/bootdisk.html) (im Unterschied zu Lösungen, die auf WinPE basieren) keine bequeme und nutzerfreundliche Benutzeroberfläche. Der Nutzer muss bestimmte Kenntnisse besitzen, diese Alternativen zu nutzen. Zum Beispiel, muss der Nutzer wissen, wo die Passwort-Hashes platziert sind, und viele Befehlszeile-Vorgänge ausführen.

Die Kompatibilität der Linux-basierten Lösungen lässt auch zu wünschen übrig. So müssen, zum Beispiel, die Nutzer die Treiber für SATA/RAID/SCSI – Geräte für Linux online finden und diese dann manuell laden.

Ein erfahrener Nutzer würde wahrscheinlich Erfolg haben, doch die anderen nicht. Zusätzlich kann der Nutzer nicht nur Probleme mit der Festplatte, sondern auch mit USB-Tastatur erleben.

Aus diesem Grund sind kommerzielle Lösungen, die auf WinPE basieren, angemessener, um das Problem der Wiederherstellung des Windows-Systemzugriffs zu lösen, da sie höhere Qualität, bekannte Windows-Nutzeroberfläche bieten und keine zeitintensiven Aktionen vor der Nutzung brauchen. Zusätzlich wird Ihnen mit WinPE technischer Produktsupport vom Hersteller garantiert.

ELCOMSOFT SYSTEM RECOVERY - EIN EINFACHER WEG, DEN SYSTEMZUGRIFF WIEDERHERZUSTELLEN

SCHLÜSSELFEATURES

Elcomsoft System Recovery (ESR) ist solch ein spezialisiertes Softwaretool, um Windows-Systempasswörter wiederherzustellen. Dieses kann benutzt werden, um den Zugang zum Windows-PC innerhalb der kürzesten Zeit, komplett mit gebrauchten Nutzerberechtigungen, wieder zu bekommen.

Der Systemadministrator muss auch nicht viel Zeit verbrauchen, um die Systemfunktionalität und Datenzugriff wiederherzustellen. Es ist genauso leicht, wie das Booten des PCs von der WinPE - bootsfähigen CD. Führen Sie Elcomsoft System Recovery aus und gehen Sie zurück zu Ihren alten Aufgaben.

Ein separates Hilfsmittel auf der Boot-CD kann dazu benutzt werden, ein bootsfähiges USB-Flashlaufwerk zu erstellen (falls gebraucht). Dies ist vor allem dann nutzvoll, wenn der "Problem"-PC kein CD-Laufwerk hat (wenn es, zum Beispiel, ein Laptop ist).

Ein bootsfähiges USB-Flashlaufwerk ist geeignet, wenn nicht das Passwort zurückgesetzt werden muss, sondern ESR für die Backup-Systemdateien zu benutzen ist, die Passwort-Hashes enthalten, um die Plaintext-Passwörter später auf anderen PCs wiederherzustellen.

ESR probiert erst die Wiederherstellung der Passwörter mithilfe des vordefinierten Angriffs (Wörterbuch- und Direktsuche) aus. Zusätzlich können einige Passwörter aus dem Cache, Systemservices, Autoanmeldung (falls konfiguriert) und so weiter extrahiert werden. Verschiedene Kombinationen werden ausprobiert (Wörterbuch-Attacke), wenn, zum Beispiel, das Passwort mit dem Nutzernamen übereinstimmt, nur mit einer oder zwei beigefügten Zahlen am Ende.

All das ist effektiv genug, das verlorene Passwort wiederherzustellen. Dieser Vorgang dauert nicht länger, als paar Minuten. As Ergebnis besteht es in vielen Fällen keine Notwendigkeit, das Passwort zurückzusetzen, was somit die Datensicherheit auf dem PC garantiert.

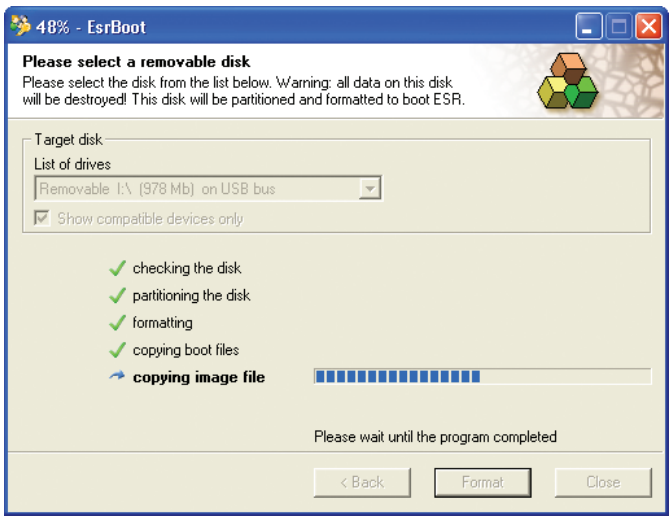


Bild. 1. Bootsfähiges USB-Flashlaufwerk erstellen.

SPEZIELLE FEATURES VON ELCOMSOFT SYSTEM RECOVERY

Hier sind einige der speziellen Elcomsoft System Recovery - Features:

- Das ESR – Set enthält einen betriebsfertigen Bootsdisk (CD oder USB-Flashlaufwerk), der mit jedem PC mit Windows-Betriebssystem kompatibel ist.
- ESR basiert auf Windows PE (Preinstallation Environment), vom Microsoft lizenziert.
- ESR ist mit Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 und Windows Vista kompatibel.
- ESR unterstützt alle US- und ortsgebundene Windows-Versionen, sowohl die Nutzernamen und Passwörter in verschiedenen Sprachen.
- ESR unterstützt alle RAID-Datenfelder und SCSI-Laufwerke (nutzt die Windows-Treiber).
- ESR identifiziert automatisch alle Betriebssysteme, die auf dem PC installiert sind, was die Wahl des Betriebssystems aus der Liste relativ unkompliziert macht.
- ESR gibt die Option des Vergebens von Administratoren-Rechten für den anderen PC-Nutzer, mit bekanntem Passwort. Somit ist es nicht nötig, das verlorene Passwort zurückzusetzen oder wiederherzustellen.
- ESR extrahiert Password-Hashes von SAM/SYSTEM – Dateien oder Active Directory – Datenbank, sowohl für den Domain-Administrator, als auch für Domain-Nutzer. Diese Option ist nicht bei den anderen Firmen auf dem Markt vorhanden. Die gesammelten Hashes werden in eine Textdatei für spätere Analyse und Wiederherstellung mit erweiterten Möglichkeiten und Methoden, wie Rainbow-Angriff (der mit anderem Produkt, zum Beispiel, Proactive Password Auditor von ElcomSoft, länger dauert) geschrieben.

Wenn Sie ESR benutzen, können Sie leicht:

- Eine Liste mit allen lokalen Nutzerkonten und deren Beschreibungen bekommen; hier finden Sie die, die Administratorenrechte haben.
- Berechtigungen der Nutzerkonten durchsehen (mit Ausnahme derer, die lokale und Gruppen-Sicherheitspolitik nutzen).
- Konten mit leeren Passwörtern aufdecken.
- Administratorenrechte für jedes Nutzerkonto aufgeben.
- Deaktivierte/blockierte Nutzerkonten aktivieren/entblocken.
- Passwörter für spezielle Systemkonten sofort wiederherstellen (solche, wie IUSR_, HelpAssistant und andere).
- Passwörter für lokale oder Active Directory – Nutzerkonten zurücksetzen und ändern.

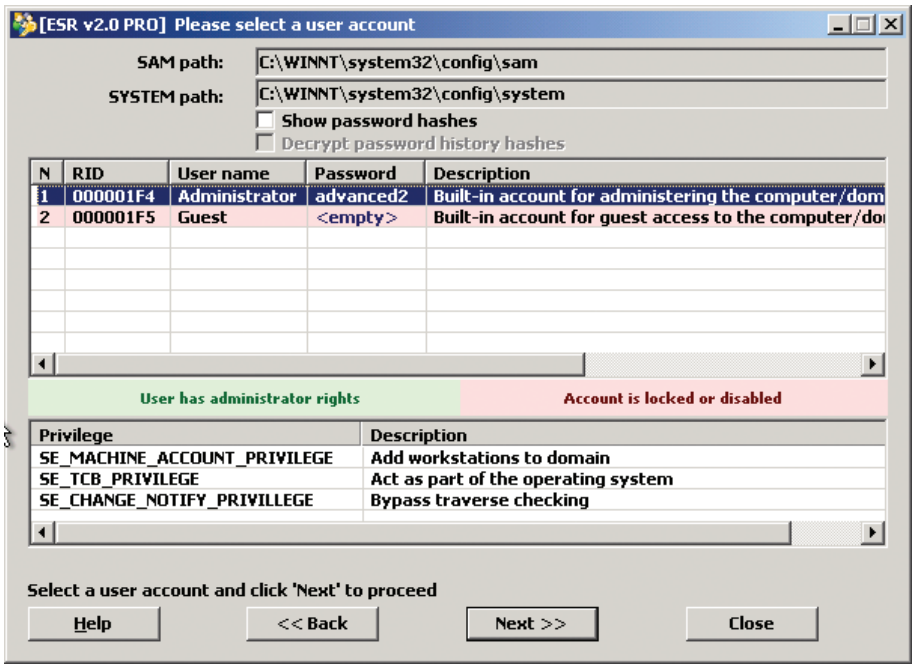


Bild 2. Konto aus der Liste auswählen, um das Passwort zurückzusetzen oder andere Aufgaben durchzuführen.

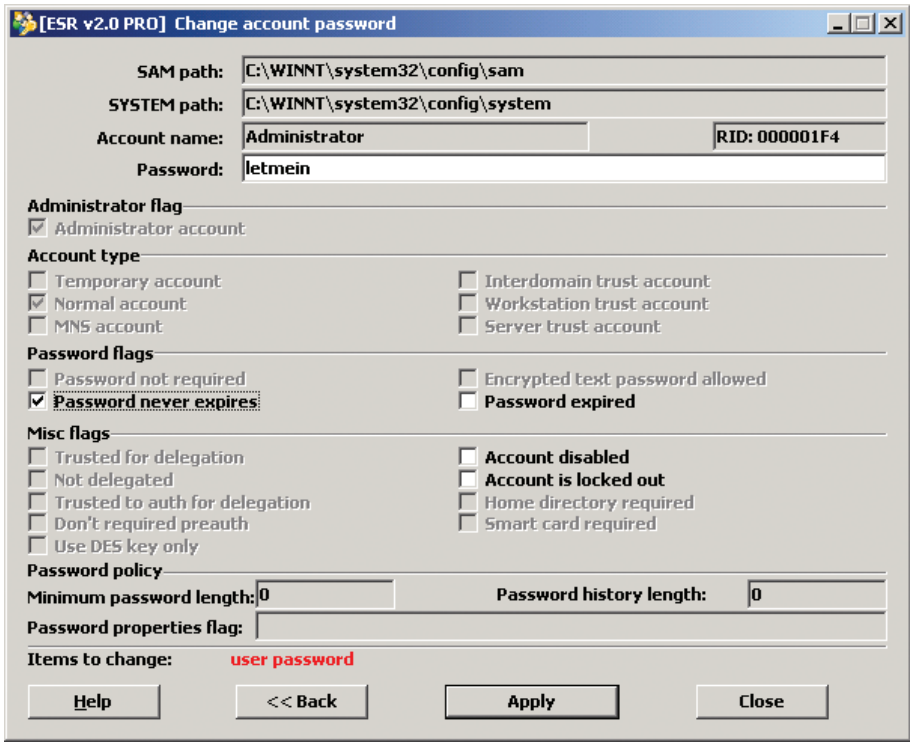


Bild 3. Änderung des Nutzer-Passworts.

ESR steht in drei verschiedenen Versionen zur Verfügung bereit: Basic, Standard und Professional. Die Unterschiede zwischen den Versionen sind in der Tabelle unten aufgelistet:

	ESR Basic	ESR Std	ESR Pro
Unterstützung der Windows-Versionen			
Unterstützt Windows Vista	●	●	●
Unterstützt Windows NT/2000/XP – Arbeitsplatzsysteme	●	●	●
Unterstützt Windows NT/2000/XP - Server	●	●	●
Unterstützt Nicht-US-amerikanische Windows-Versionen	●	●	●
Allgemeine Features			
Mehrsprachiges Nutzer-Interface	●	●	●
Basiert auf Windows PE	●	●	●
Unterstützt alle RAID/SCSI/SATA - Geräte	●	●	●
Automatischer Modus (Liste aller installierten Systeme)	●	●	●
Manueller Modus (sucht nach Registry – Dateien)	●	●	●
CD zur Passwort-Wiederherstellung	●	●	●
Erstellung eines USB-Flash-Laufwerkes zur Passwort-Wiederherstellung	●	●	●
Zurücksetzen der lokalen Administrator-Passwörter	●	●	●
Aktiviert/entblockt Administrator-Konto	●	●	●
Erweiterte Features			
Zurücksetzen des Passwortes für andere Nutzerkonten	●	●	●
Markieren der Konten mit Administrator- Erlaubnis	●	●	●
Nachschlagen der Kontorechte	●	●	●
Aktiviert/entblockt deaktivierte/blockierte Konten	●	●	●
Gibt Administratorrechte für jedes Nutzerkonto	●	●	●
Wiederherstellung der Passwörter für einige System-konten	●	●	●
Setzt Domain-Administrator-Passwort zurück	●	●	●
Setzt die AD-Nutzerpasswörter zurück	●	●	●
Lädt Passwort- Hashes für lokale Konten ab	●	●	●
Lädt Passwort- Hashes für AD-Konten ab	●	●	●

Erweiterte Features			
Zeigt LM/NTLM –Hashes	●	●	●
Zeigt Passwort-Verlaufs- Hashes	●	●	●
Testet kurze und einfache Passwörter	●	●	●
SAM – Datenbank-Editor	●	●	●
Lizenz, Erhaltung, Lieferung, Preis			
Für Firmennutzung lizensiert	●	●	●
Ein Jahr kostenloser Updates	●	●	●
Lieferung	Download (ISO)	Express-Zustellung	Express-Zustellung
Preis	49 Euro	199 Euro	599 Euro

Die 'Basic' – Version wird online vertrieben, ohne der betriebsfertigen CD, die aus dem Archiv, mithilfe der ISO-9660 – Disk-Image, erstellt werden kann. Die Versionen Standard und Professional werden mit der Boots-CD geliefert und können benutzt werden, um den bootsfähigen USD-Laufwerk zu erstellen.

Lesen Sie über die Produktdetails von Elcomsoft System Recovery hier (http://www.elcomsoft.com/esr.html).

ÜBER ELCOMSOFT

Der 1990 gegründete russische Software-Entwickler ElcomSoft Co. Ltd. zählt zu den führenden Experten im Bereich Software zur Sicherheitsprüfung und Wiederherstellung von Passwörtern und Kennungen, mit denen sie Windows-Netzwerke sichern bzw. auf wichtige Dokumente zugreifen können. Dank der einzigartigen Technologien genießen die Produkte des Unternehmens weltweite Anerkennung.

Zu den Kunden von ElcomSoft zählen weltbekannte Unternehmen aus folgenden Branchen:

High Tech: Microsoft, Adobe, IBM, Cisco
Regierungseinrichtungen: FBI, CIA, US Army, US Navy, Department of Defence
Consulting-Unternehmen: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finanzdienstleistungen: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telekommunikation: France Telecom, BT, AT&T
Versicherungen: Allianz, Mitsui Sumitomo
Handel: Wal-Mart, Best Buy, Woolworth
Medien & Unterhaltung: Sony Entertainment
Hersteller: Volkswagen, Siemens, Boeing
Energie: Lukoil, Statoil
Pharmazie: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

Das Unternehmen ist Microsoft Gold Certified Partner, Intel Software Partner, Mitglied der Russian Cryptologie Association (RCA), des Computer Security Institute (CSI) und der Association of Shareware Professionals (ASP).

Auf die technologischen Errungenschaften von Elcomsoft wird in vielen bekannten Büchern Bezug genommen, beispielsweise, in der Microsoft-Enzyklopädie „Microsoft Encyclopedia of Security", „The art of deception" (Kevin Mitnick), „IT Auditing: Using Controls to Protect Information Assets" (Chris Davis) und „Hacking exposed" (Stuart McClure).

Mehr über Elcomsoft können Sie auf der Webseite des Unternehmens erfahren.

ADRESSE:

ElcomSoft Co. Ltd.
Zvezdnyi blvd. 21, Office 541
129085 Moskau

FAX:

USA (toll-free): +1 (866) 448-2703
Großbritannien: +44 (870) 831-2983
Deutschland: +49 18054820050734

WEBSEITEN:

http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr