1. Security

1.1 Windows-Server

1.1.1 SID2Username

Oft plagen sich Administratoren mit dem Problem, dass sie unter "HKEY_USER" den Registry-Eintrag eines bestimmten Benutzers suchen, ihn aber nicht sofort finden. Ähnlich sieht es bei Fehlermeldungen aus, die lediglich eine SID (Security-ID) enthält, aber keinen Hinweis auf den Benutzer, den das Problem betrifft. Besonders im Terminalserver-Umfeld, in dem sich viele Benutzer ein System teilen, sind dies zwei häufig anzutreffende Problemstellungen. Denn bei einem Terminalserver können unter "HKEY_USER" viele Hives existieren, die als Schlüsselnamen nur die SID besitzen. Das Werkzeug SID2Username [Link-Code nt001] erzeugt auf Knopfdruck den zur SID gehörigen Benutzernamen und umgekehrt. Wenn der Administrator das Programm startet, liest es die Zwischenablage aus und zeigt sofort die gewünschte Information an. Beispielsweise ermöglicht das Werkzeug über einen Rechtsklick in der Registry auf den entsprechenden Schlüssel über den Menüpunkt "Schlüsselnamen kopieren", den zugehörigen Benutzernamen sofort anzuzeigen.Voraussetzung für das Tool ist das .NET Framework – administrative Privilegien sind nicht nötig.

1.1.2 SetACL

Gerade bei der Installation von Clients und Servern mit allen nötigen Schritten ist die Schaffung eines vollautomatisierten Prozesses sehr hilfreich. Dabei kommen die unterschiedlichsten Methoden und Mittel zum Einsatz. Eine der wichtigsten Maßnahmen ist die Härtung des Servers durch Setzen von Rechten auf Dateien, Order, Registry-Schlüssel, Drucker, Diensten und Netzwerk-Freigaben – kurz: die Konfiguration der Access Control Lists (ACL). Mit Bordmitteln lässt sich das nur sehr aufwändig und mit einer Menge an unterschiedlichen Tools bewerkstelligen. Ein kleines Werkzeug jedoch bringt die vielen Arbeitsschritte unter einen Hut. Das Open-Source-Tool SetACL [Link-Code nt002] für die Befehlszeile ist ein vollwertiger Ersatz für das Windows-eigene CACLS.EXE und geht noch weit darüber hinaus. Nicht nur, dass es die Rechte für Dateien, Order, Registry-Schlüssel, Drucker, Dienste und Netzwerk-Freigaben setzen kann: Sie können auch ein komplettes Listing von ACLs für Ordner und deren Unterordner erstellen. SetACL ist durch die Verwendung in der Kommandozeile für Skripte und Batchfiles prädestiniert und existiert zudem als ActiveX-Control.

1.1.3 Userbooster Light und Userbooster Professional

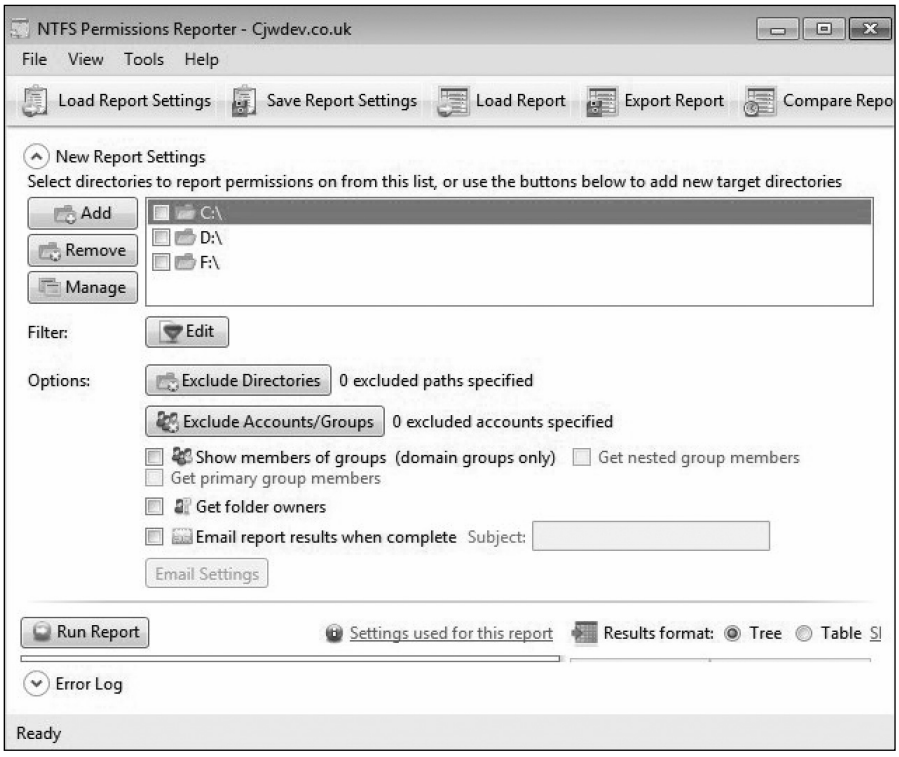
Die Verwaltung eines Verzeichnisdienstes wie etwa Microsofts Active Directory oder anderer LDAP-basierter Dienste ist aufgrund der oftmals vier- oder gar fünfstelligen

Anzahl von Objekten im Verzeichnis an sich schon eine komplexe Aufgabe. Erschwert wird die Administration beispielsweise noch durch die Vielzahl an Verwaltungsoberflächen, die zu durchlaufen sind, wenn an einem Objekt mehrere, unterschiedliche Aktivitäten wie etwa das Erstellen von Postfachkonten, die Modifikation von Dateisystemrechten oder das Verwalten von Gruppenmitgliedschaften notwendig sind. Das Tool Userbooster [Link-Code nt003] tritt daher an, die Administration zu homogenisieren und so Zeit zu sparen und Fehler zu minimieren. Das Programm ist, anders als früher, mittlerweile für den kommmerziellen und privaten Einsatz kostenlos verfügbar. Neben der Verwaltung des Verzeichnisdienstes über eine einheitliche GUI erlaubt das Tool, zusätzliche Aufgaben im Zusammenhang mit der Anlage eines Benutzerobjektes in einem Arbeitsschritt zu realisieren. Dazu gehören die Erstellung einer Mailbox, die Erzeugung von Profilbeziehungsweise Heimlaufwerken mit den jeweiligen Rechten im Dateisystem oder die Unterstützung von DFS (Distributed File System). Die Software arbeitet darüber hinaus mit Platzhalter-Variablen, die die Verwaltung der speziellen Anforderungen in einer generischen Vorlage ermöglichen. Zusätzlich ist die Integration in MS Office ein weiteres Hilfsmittel bei der Erstellung von Template-Vorlagen. Das direkte Importieren und Exportieren in MS Excel reduziert die notwendigen Anpassungen auf das absolute Mindestmaß.

1.1.4 NTFS Permissions Reporter

Administratoren, die viel mit Systemdateien arbeiten beziehungsweise diese modifizieren und ändern, müssen dazu oftmals die Besitzrechte, Sicherheitseinstellungen und Zugriffsrechte für eine solche Datei ändern. Der übliche Weg dazu führt über einen Rechtklick auf eine Datei oder einen Ordner, die Auswahl der Eigenschaften und ein Klick auf den Reiter "Sicherheit". Hier erhält der IT-Verantwortliche für jede Datei und jeden Ordner angezeigt, wem die Besitzrechte zugesprochen sind und welche Zugriffsrechte bestimmte User und Gruppen haben. Doch schon diese Beschreibung lässt erahnen, dass dieser Prozess bei vielen Dateien und vielen Rechten darauf leicht unüberschaubar wird. Das freie Werkzeug NTFS Permissions Reporter [Link-Code c5pe3] schafft hier Abhilfe. Es erlaubt Administratoren, sich schnell einen Überblick über die Zugriffsrechte und die Sicherheitseinstellungen zu verschaffen. Ebenfalls reportet das Werkzeug die Besitzrechte von Dateien und Ordnern. Das Programm listet die gewünschten Daten nach Auswahl der Partitionen, Ordner und Dateien detailliert auf. Ändern lassen sich diese Einstellungen aus dem NTFS Permissions Reporter jedoch nicht. Nach der Installation und dem Start des Programms legt der Administrator zunächst den zu scannenden Bereich fest. Dies erfolgt auf Basis der durch das Programm angezeigten vorhandenen Partitionen. Der Scanbereich lässt sich individuell anpassen, etwa indem ein einzelner Ordner außerhalb der festgelegten Partition zusätzlich ausgewählt wird. Als Ergebnis der Rechteuntersuchung erhält der Administrator eine

Übersicht der einzelnen Ordner und der darin enthaltenen Dateien mit ihren Sicherheitseigenschaften. Der NTFS Permissions Reporter liegt neben der freien auch als Kaufversion vor, doch erfreulicherweise bietet die freie Version dem IT-Verantwortlichen einen Funktionsumfang, der in vielen Fällen ausreicht.



Die Ergebnisse des NTFS Permissions Reporter in der Baumansicht.

1.1.5 Attack Surface Analyzer

Eine der kniffeligsten Fragen für den IT-Sicherheitsbeauftragten dreht sich um die Änderung des Sicherheitsstatus eines Windows-Server, wenn darauf eine neue Applikation installiert wird. Denn ein bis dahin als nachweislich sicher kategorisierter Server kann nach dem Aufspielen durchaus neue Sicherheitslöcher aufweisen. Doch zu ermitteln, welche dies sind und wie schwer diese wiegen, kann in der Praxis enorm schwierig sein. Für besonders kritische Server stellt dies in Sachen Auditierbarkeit und Compliance unter Umständen ein ernstes Problem dar. Microsoftbietet dafür den freien Attack Surface Analyzer [Link-Code d4pe3]. Dieses Werkzeug soll sowohl Systemadministratoren als auch Softwareentwickler dabei unterstützen, die möglicherweise durch eine neue Applikation erzeugten Sicherheitsmängel aufzuspüren. Dazu erstellt das Tool zunächst einen Snapshot des Rechners, um den aktuellen Systemzustand festzuhalten. Danach kann der IT-Verantwortliche die Windows-Installation

beliebig verändern, zum Beispiel indem er ein neues Programm einrichtet. Anschließend läuft der Attack Surface Analyzer ein zweites Mal und vergleicht den neuen Systemzustand mit dem zuvor angefertigten Snapshot. Dieser Analyse entgeht keine Abweichung: Registrierungseinträge, Dateien, geöffnete Netzwerk-Ports und mehr. Ein großer Vorteil für den IT-Verantwortlichen im Unternehmen ist dabei natürlich, das diese Analyse funktioniert, ohne dass Zugriff auf den Quellcode besteht. Ein Zustand, der eher Normalität denn Ausnahme ist. So kann unabhängig vom Hersteller eine Aussage hinsichtlich der Sicherheit der neuen Anwendung getroffen werden. Die Analyse selbst erfolgt dabei über eine GUI. Die Kommandozeile wird benötigt, wenn ältere Windows-Versionen untersucht werden sollen oder der Wunsch nach Automatisierung der Prüfung besteht.

1.1.6 AD ACL Scanner

Hat der Administrator den Auftrag, einem neuen Kollegen im Unternehmen seine Rechte im Active Directory einzurichten, fällt sein Blick vielleicht auch auf Rechte, die so eigentlich gar nicht mehr benötigt werden – beispielweise solche von Gruppen oder Anwendern, die gar nicht mehr existieren oder auch zu privilegierte Rechte einzelner User. Hier gibt es zahlreiche denkbare Szenarien und Möglichkeiten, doch leider sind die Möglichkeiten für den Administrator, solche problematischen Rechte effektiv zu ermitteln, nicht sonderlich groß. Das dachte sich wohl auch der schwedische Microsoft-Mitarbeiter Robin Granberg und stellt Windows-Admins seinen AD ACL Scanner [Link-Code d8pe4] kostenlos zur Verfügung. Im Kern dokumentiert das Tool die Berechtigungen in einer Active-Directory-Struktur. Es untersucht die AD-internen Berechtigungen auf OUs, Benutzerobjekte et cetera, nicht jedoch Berechtigungen auf Dateiservern und vergleichbares. Im Kern ist das kleine Werkzeug ein PowerShell-Skript mit grafischer Oberfläche. Es erzeugt tabellarische Übersichten der Berechtigungen von Active-Directory-Containern und -Objekten. Die Berichte lassen sich als HTML- oder CSV-Dateien exportieren. Auf diesem Wege ist es auch möglich, verschiedene Stände der Berechtigungen miteinander zu vergleichen. Ebenfalls sehr nützlich auf dem Weg zu sauberen Berechtigungen ist die Fähigkeit des Scanners, die Ergebnisse zu filtern.

1.1.7 File Permissions Check

Auch im gepflegtesten Windows-Dateiserver kann es vorkommen, dass die Rechte in Dateien und Ordnern nicht konsistent sind. Hat sich in den für "Normaluser" unzugänglichen Ordner der Geschäftsführung ein File eingeschlichen, das sich nicht um diese restriktive Zugriffspolitik schert, kann dies durchaus unangenehm für das Unternehmen und den IT-Verantwortlichen werden. Im Regelfall kann der Administrator erwarten, dass ein in einem bestimmten Ordner abgelegtes File die Rechte dessen Zugriffsrechte annimmt. Hat der Admin jedoch den Verdacht, dass sich dies

in dem einen oder anderen Fall nicht so verhält, unterstützt ihn das freie File Permissions Check [Link-Code f4pe2] bei der Suche nach Abweichlern. Dazu liefert das Tool eine intuitive GUI, über die sich Datei-Shares hinsichtlich abweichender Rechte scannen lassen. So gefundene Dateien lassen sich mit File Permissions Check auf das geforderte Rechte-Niveau setzen. Damit ist die Funktionalität des Werkzeugs auch schon allumfänglich erläutert und es bleibt nur zu erwähnen, dass sich die Ergebnisse des Scans als CSV- oder HTML-Bericht exportieren lassen.

1.1.8 LauschAngriff

Eine ganze Reihe von Szenarien sind vorstellbar, bei denen der IT-Verantwortliche Ordner oder Laufwerke auf Löschungen, Umbenennungen, Kopieren oder Zugriffe überwachen möchte. Denkbare wäre der Bedarf nach einer sehr genauen Überwachung, ob Malware sensible Daten verändert. In einem anderen Umfeld soll vielleicht sichergestellt werden, dass gewisse Dateien nicht unbeobachtet gelöscht werden. Sofern die fraglichen Daten nicht absolut hochsensibel sind und daher professionellen Schutz unterliegen sollten, ist vielleicht das kostenlose Tool LauschAngriff [Link-Code fape2] ein Weg um sicherzustellen, dass niemand Unbefugtes Daten manipuliert. Mit der Software lassen sich Ordner oder ganze Laufwerke überwachen und die dortigen Vorgänge dokumentieren. Das Tool dokumentiert beispielsweise Schreibzugriffe sowie das Löschen. Kopieren und Umbenennen von Dateien. Ebenso werden Erstellzeitänderungen, Zugriffszeitänderungen, Dateiattribute und Sicherheitseinstellungen überwacht. Die ermittelten Daten lassen sich als XLS, CSV, TXT oder HTML exportieren. Gezielte Prüfungen ermöglicht LauschAngriff etwa durch Filter zur Auswahl bestimmter Dateitypen zur Überwachung. Nach der Installation lässt sich das zu überwachende Laufwerk oder Verzeichnis über eine Baumstruktur auswählen. Die zu überwachenden Änderungen lassen sich granular einstellen, beispielsweise ist es möglich, eine Datei nur hinsichtlich einer möglichen Größenänderung zu monitoren.

1.1.9 Local Administrator Password Solution

In Windows-Umgebungen, in denen sich Anwender ohne Domänen-Credentials in das Netz einloggen, ist das Passwortmanagement unter Umständen eine komplexe Angelegenheit. Umso mehr, als dass Microsoft seit einiger Zeit die Verteilung lokaler Adminpasswörter über Gruppenrichtlinien unterbunden hat. Zu groß sind die Sicherheitsbedenken bei diesem Vorgehen, dass ein Ausspähen von Username und Passwort per Pass-the-Hash ermöglicht. Für die Verwaltung solcher Passwörter stellt Microsoft das Tool Local Administrator Password Solution (LAPS) [Link-Code g3pe2] bereit. LAPS generiert pro Client ein dynamisches Passwort und hinterlegt es im Active Directory. Dazu wird es in vier Komponenten ausgeliefert: Die "GPO Client Side Extension" werden auf jedem Client benötigt, der mittels LAPS verwaltet werden soll; als Managementtools sind ein "Fat Client UI" zum Auslesen der Passwörter aus