Das neue Sicherheitspaket für OS/400 und die Verbesserungen von V3R2. von Jelan Heidelberg, für den deutschen Markt überarbeitet von Mathias Spateneder

Niemand wird behaupten, Systemsicherheit w&aumlre einfach, geschweige denn ein System w&aumlre in dieser Hinsicht narrensicher. Einige, seit kurzem von IBM zur Verfügung gestellte Funktionen und Informationen, vereinfachen jedoch die Absicherung der AS/400 erheblich. Nachfolgende 19 Tips reichen von der Frage, wie die Verwaltung von Benutzerprofilen einfacher und effektiver gestaltet werden kann, bis hin zur erh&oumlhten Sicherheit des Netzwerkes. Einige dieser Techniken benutzen Tools, die dem neuen Sicherheits-Toolkit für OS/400 entstammen, andere basieren auf den Verbesserungen von OS/400, V3R2. Die wenigen Minuten, die es ben&oumltigt, diese Tips zu lesen, k&oumlnnen sp&aumlter Stunden sparen. Vielleicht zeigt sich auch eine Sicherheitslücke im System – und wie man diese beheben kann.

Das neue Sicherheitspaket für OS/400 und die Verbesserungen von V3R2

19 Tips

1. Standard-Kennwörter aufspüren

IBM liefert die AS/400 mit allgemein bekannten Kennwörtern für Benutzerprofile mit weitreichenden Berechtigungen aus (das Kennwort für das Benutzerprofil des Sicherheitsbeauftragten, QSECOFR, ist z.B. »QSECOFR«).
Ein Hacker mit AS/400-Kenntnissen wird als Erstes versuchen, mit einem Standard-Kennwort in das System einzudringen. Auch bei der Neuanlage eines Benutzerprofils wird als Standard-Kennwort der Name des Benutzerprofils verwendet. Sollte ein neuer Anwender sich für Tage (oder Wochen) nicht anmelden, öffnet sich ein Tor zum System. Wer das Schema kennt, nach dem die Namen für Benutzerprofile vergeben werden, könnte »nur zum Spaß« einmal das neue Benutzerprofil ausprobieren? Das Sicherheits-Toolkit enthält einen neuen Befehl, CHKDFTPWD (Check Default Password), der Benutzerprofile erkennt, deren Kennwort dem Namen des Benutzerprofils entspricht. Als Ergebnis erscheint entweder eine Liste der entsprechenden Benutzerprofile oder diese werden gesperrt.

2. Entfernung temporärer und hinfälliger Benutzerprofile

Möglicherweise existieren im System noch Benutzerprofile ehemaliger, längst ausgeschiedener Mitarbeiter oder temporäre Benutzerprofile für freie Mitarbeiter oder Servicetechniker. Inaktive Benutzerprofile bieten sich für nicht zu überwachenden Mißbrauch an. WEG DAMIT! Der neue Befehl CHGEXPSCDE (Change Profile Expiration Schedule Entry) aus dem Sicherheits-Toolkit gibt die Möglichkeit, ein bestimmtes Benutzerprofil zu einem bestimmten Datum zu deaktivieren

und/oder zu löschen.(Für die Vorversionen von V3R2 lautet der Befehl SCDPRFEXP – Schedule Profile Expiration). Diesen Befehl sollte man sofort verwenden und nicht erst für später in den Kalender eintragen. Sobald bekannt ist, daß ein Mitarbeiter seinen Bereich verläßt, sollte mit dem entsprechenden Befehl der Zeitpunkt des Löschens festgelegt werden. Bei einem temporären Benutzerprofil, kann gleichzeitig auch dessen „Ableben“ bestimmt werden. Eine weitere Verbesserung bietet der Befehl ANZPRFACT (Analyze Profile Activity). Man kann damit erkennen, welche Benutzerprofile lange Zeit nicht mehr aktiv waren (was »lange Zeit« bedeutet, wird individuell definiert.) Man kann diese Benutzerprofile stillegen, solange ist noch nicht entschieden, was damit passieren soll. Für die Vorversionen von V3R2 wird der Befehl PRCINACPRF verwendet.

3. Zeitliche Verfügbarkeit hochrangiger Benutzerprofile einschränken

Hacker surfen meist abends oder an Wochenenden, also zu Zeitpunkten, zu denen Versuche auf der Datenleitung und die dabei produzierten Fehlermeldungen nicht beobachtet werden können. Man kann zwar nicht alles vorhersehen, was ein Hacker versuchen könnte, aber so erreicht man wenigstens, daß sie sich nicht mit einem Benutzerprofil hoher Priorität anmelden können und damit alle Systemresourcen erreichen. Über den neuen Befehl CHGACTSCDE (Change Activation Schedule Entry) können bestimmte Benutzerprofile (z.B. QSECOFR) nur während bestimmter Tageszeiten zur Verfügung gestellt werden. (Für die Version des Sicherheits-Toolkits für Release-Stände vor V3R2 existiert der Befehl SCDPRFACT – Schedule Profile Activation). So lassen sich beispielsweise mit dem jeweiligen Befehl alle Benutzerprofile mit QSECOFR-Berechtigung jeden Morgen (Montag mit Freitag) um 8.00 Uhr aktivieren und automatisch um 17.00 Uhr sperren.

4. Sonderberechtigungen in den Griff bekommen

Sonderberechtigungen sind wie der Schlüssel zum Himmelreich. Ein Benutzer mit Berechtigung *ALLOBJ darf und kann alles im System, ob direkt, oder über ein anderes Benutzerprofil. Ein Benutzer mit Berechtigung *SPLCTL kann jede gespoolte Datei ansehen, kopieren oder löschen, ohne Rücksicht auf deren Wichtigkeit oder Vertraulichkeit. Ein Benutzer mit Berechtigung *SAVSYS hat die Möglichkeit, das komplette System (oder einen beliebigen Teil davon) auf Band abzuziehen, um firmensensible Dateien evtl. auf ein fremdes System zu übertragen.
Zumindest sollte man wissen, welche Benutzerprofile Sonderberechtigungen besitzen. Der neue Befehl PRTUSRPRF (bzw. PRTUSRINF vor V3R2) hilft dabei, alle Benutzerprofile aufzulisten, die eine bestimmte Sonderberechtigung wie z.B. *ALLOBJ besitzen, oder alle Benutzerprofile mit irgendeiner Sonderberechtigung.

5. Systemumgebung der Anwender überwachen

Die Systemumgebung eines Benutzerprofils (wie z.B. Ausgabewarteschlange, Jobwarteschlange, Startprogramm und Abrufprogramm), ist ein wichtiges Werkzeug des Sicherheitsbeauftragten. Mit dem Aufbau der Umgebung wird festgelegt, wie Anforderungen des Benutzers behandelt werden. Mit dem Parameter *ENVINFO des Befehls PRTUSRPRF wird die Benutzerumgebung eines jeden Benutzerprofils ausgedruckt. Dieser Bericht ist für den Sicherheitsbeauftragten ein schnelles und effektives Werkzeug, falls er die Erstellung und Pflege der Benutzerprofile delegiert hat.

6. Arbeit mit Benutzerprofilen überwachen

Wenn auch andere mit der Pflege der Benutzerprofile beauftragt sind, besteht der Bedarf, eventuell getätigte &AUMLnderungen sofort zu erkennen oder bei bestimmten Arbeiten mit Benutzerprofilen benachrichtigt zu werden. Außerdem kann der Sicherheitsbeauftragte festlegen, daß beim Neuanlegen eines Benutzerprofils bestimmte Werte automatisch vom System vergeben werden.

Beginnend ab V3R2 stellt das System Exit Points (Austrittspunkte) für die Befehle zur Verfügung, die mit Benutzerprofilen arbeiten. So können Exit-Programme zur Überwachung, Steuerung und Vereinfachung der administrativen Arbeiten mit Benutzerprofilen eingesetzt werden. Jedem neu erstellten Benutzerprofil können zudem bestimmte Werte zugeordnet werden. Nach Ausführung eines Benutzerprofil-Befehls (oder vor dessen Ausführung im Falle von DLTUSRPRF – Delete User Profile) ruft das System das Exit-Programm auf und übergibt ihm den Namen des Benutzerprofils. Das Exit-Programm kann die Werte des erstellten oder geänderten Benutzerprofils erkennen und, falls nötig, verändern. So kann man z.B. ein Exit-Programm schreiben, das einem neuen Benutzerprofil die Umgebungswerte zuweist, die für das Gruppenprofil gelten, oder das &AUMLnderungen an Benutzerprofilen auf andere Systeme innerhalb Ihres Netzwerkes überträgt. Das Programm kann außerdem alle Objekte erstellen, die der Anwender benötigt, und ihm die Berechtigung für die benötigten Anwendungen erteilen. Exit Points stehen bei folgenden Befehlen zur Verfügung:
Erstellen eines Benutzerprofils – CRTUSRPRF &AUMLndern eines Benutzerprofils – CHGUSRPRF Löschen eines Benutzerprofils – DLTUSRPRF Zurückspeichern eines Benutzerprofils – RSTUSRPRF

7. Systemwerte überprüfen

Sicherheitsbezogene Systemwerte sind ein wichtiges Werkzeug im Sicherheitsrepertoire. Prüfer fragen häufig, inwieweit die Systemwerte den geforderten Werten entsprechen, und Manager könnten wissen wollen, welche Sicherheitsrichtlinien verfolgt werden. Sicherheitsbezogene Systemwerte bilden die erste Verteidigungslinie der AS/400. Es wäre daher keine schlechte Idee, diese Parameter ab und an zu überprüfen, um sicherzugehen, daß sie wirklich das bewirken was sie sollen. Der neue Befehl PRTSYSSECA (Print System Security Attributes) erstellt einen Bericht, der zeigt, inwieweit die sicherheitsrelevanten Systemwerte mit den von IBM empfohlenen übereinstimmen. Diese befinden sich im Handbuch „Tips and Tools for Securing your AS/400“ (siehe auch Tip 19). Zusätzlich kann man den Befehl CFGSYSSEC (Configure System Security) dazu verwenden, um Systemparameter den vorgeschlagenen anzupassen.