2

Zugriff nur durch die Anwendung: Umsetzung der Strategie

Wenn Sie sich einmal den PC genauer ansehen, der mit Ihrer AS/400 vernetzt ist, dann sehen Sie ein harmlos wirkendes Werkzeug, das unauffällig seinen Dienst versieht. Denken Sie aber einmal daran, wozu eine Person fähig sein könnte, die sich dieses Werkzeugs bedient und Sie beginnen, den PC als eine Art Wolf im Schafspelz zu betrachten, eine weit offene Sicherheitslücke für die Daten auf der AS/400.

Kapitel 1 beschreibt die allgemein bekannten Methoden für den Schutz der Daten, die jedoch Ihre AS/400-Daten in einer Netzwerkumgebung nur ungenügend schützen. Werkzeuge wie ODBC, FTP und Client Access eröffnen viele Wege, um an Ihre Daten zu kommen. Dabei ist es schwierig, wenn nicht unmöglich, den Zugriff von den PCs aus über die Einschränkung der verfügbaren Menüoptionen zu kontrollieren. Sie brauchen eine neue Methodologie, die Ihnen dieses Kapitel vorstellen soll.

Während meiner Arbeit mit Klienten an der Sicherheit ihrer Systeme erkannte ich dieses Problem und entwickelte eine neue Strategie, den Exklusivzugriff durch die Anwendung. Der Exklusivzugriff verwendet die Sicherheitsfunktionalität der AS/400 auf Sicherheitsstufe 30 und höher, um den Zugriff auf die Produktionsdaten außerhalb einer Anwendung einzuschränken. In diesem Kapitel werden die Details des exklusiven Datenzugriffs beschrieben und einige der Probleme vorgestellt, auf die Sie stoßen können.

DIE STRATEGIE DES EXKLUSIVEN DATENZUGRIFFS DURCH DIE ANWENDUNG

Mit dieser Strategie erhalten die Benutzer nur dann Zugriff auf die Produktionsdaten, wenn sie mit Produktionsanwendungen arbeiten. Um das zu erreichen, sollten die Benutzer der Anwendung über kein Gruppenprofil verfügen, das ihnen Zugriff auf Produktionsdaten gewährt.

Diese Strategie verhindert Änderung und Zugriff auf Daten außerhalb der Produktionsanwendungen, doch die Benutzer müssen nach wie vor innerhalb der Produktionsanwendungen auf Daten zugreifen können. Die Benutzer erhalten daher ein Start-

programm, das die erforderliche Zugriffsberechtigung für die Produktionsbibliotheken übernimmt. Die übernommene Berechtigung des Eingangsprogramms ermöglicht den Benutzern, von der Anwendung aus auf Daten zuzugreifen, wobei die Anwendung die Operationen kontrolliert, die der Benutzer ausführen darf. Die Benutzer haben auf Daten außerhalb der Anwendung, wie es z. B. bei PC-Dateiübertragung, Remote-Befehlen oder FTP der Fall ist, keinen Zugriff.

Die Anwendungen erlauben häufig interaktiven Zugriff auf Menüoptionen, die Stapeljobs auslösen können. Diese Stapeljobs müssen ebenfalls Zugriffsberechtigung durch Berechtigungsübernahme erhalten, wobei dies nur für die Eingangsprogramme der Stapelprozesse gilt. Es kann jedoch schwierig sein, die Startpunkte aller Stapeljobs zu finden.

Wenn es nicht möglich ist, alle Eingangsprogramme für die Stapelprozesse zu finden, kann das Problem gelöst werden, indem man alle Systemprogramme in Produktion so ändert, dass sie Berechtigung übernehmen. Diese Änderung ermöglicht es, dass die übergebenen Jobs die benötigten Zugriffsrechte für die Produktionsdaten übernehmen. Wenn möglich, empfehle ich jedoch, nur die Eingangsprogramme für die Stapeljobs Berechtigung übernehmen zu lassen.

Ein Sicherheitsbeauftragter kann mit dem Befehl CHGPGM Programme mit sogenannter Observability so ändern, dass sie Berechtigung übernehmen, ohne dass eine Rekompilierung des Programms erforderlich ist. Programme, die über keine Observability verfügen, müssen neu kompiliert werden. Wenn Sie mit kommerziellen Programmen arbeiten, deren Funktionen für die Observability entfernt wurden, können Sie diese Strategie ohne die Kooperationsbereitschaft Ihres Softwarelieferanten nicht verwirklichen.

GRENZEN DER BIBLIOTHEKSSICHERHEIT

Bei meinem ersten Versuch, den exklusiven Datenzugriff durch die Anwendung zu implementieren, arbeitete ich mit der Bibliothekssicherheit. Die Datendateien und Programme in der Bibliothek verfügten über *PUBLIC-Zugriff, aber die Produktionsbibliotheken, in denen sich die Daten und Programme befanden, hatten allgemeinen Zugriff mit *EXCLUDE. Um auf die Daten zuzugreifen, übernahmen die Programme die Berechtigung des Bibliothekseigners für die Produktionsbibliotheken. Die Sicherheit über Bibliotheken kann problemlos umgesetzt werden und das ist der Grund, warum ich mich für diese Alternative entschieden habe. Trotzdem weist diese Strategie einige Schwächen auf.

Für interaktive Benutzer ist die Bibliothekssicherheit gut geeignet. Wenn interaktive Benutzer die Anwendung öffnen, übernimmt ein Eingangsprogramm die Berechtigung des Bibliothekseigners und fügt die Produktionsbibliotheken der Bibliotheksliste hinzu. Dies ermöglicht den Benutzern, auf die Produktionsbibliotheken zuzugreifen.

Wenn jedoch ein interaktiver Benutzer eine Menüoption auswählt, die einen Stapeljob an die Warteschlange übergibt, erben die damit übergebenen Stapeljobs nicht die übernommene Berechtigung des interaktiven Jobs, sondern der Stapeljob wird nicht starten, weil er für den Zugriff auf die Produktionsbibliotheken nicht berechtigt ist.

Die Produktionsbibliotheken befinden sich in der Bibliotheksliste für den übergebenen Job, da der Befehl SBMJOB - Job übergeben - standardmäßig auf die Bibliotheksliste des interaktiven Jobs zurückgreift, um den Stapeljob zu starten. Der Stapeljob verfügt jedoch über keinen Mechanismus, um die Berechtigung

für diese Produktionsbibliotheken zu übernehmen. Da die Stapeljobs so nicht ausgeführt werden können, muss für den Schutz der Produktionsdaten eine andere Strategie gewählt werden.

Wenn die interaktiven Benutzer der Anwendungen keine Jobs an die Warteschlange übergeben und die Systembediener alle Stapeljobs starten, kann vermieden werden, dass Stapeljobs fehlschlagen. Die Bibliothekssicherheit allein würde ausreichen, denn die Anfangsbibliotheksliste für die von den Benutzern übergebenen Stapeljobs würde keine Produktionsbibliotheken enthalten. Selbst in diesem Szenario besteht jedoch die Möglichkeit, dass Anwendungen in der Zukunft den Benutzern die Übergabe von Produktionsstapeljobs an die Warteschlange gestatten. Deshalb empfehle ich eine flexiblere Strategie als die Bibliothekssicherheit.

EXKLUSIVER ZUGRIFF DURCH DIE ANWENDUNG AUF OBJEKTEBENE

Das Problem bei der Begrenzung des Zugriffs auf Produktionsbibliotheken war, dass die Stapeljobs abgebrochen wurden, bevor sie die Berechtigung für den Zugriff übernehmen konnten. Wenn der individuelle oder allgemeine Zugriff auf die Produktionsbibliotheken mit *USE erfolgt, können die Stapeljobs starten. Nach dem Start können die Eingangsprogramme in den Stapeljobs die für den Dateizugriff erforderliche Berechtigung übernehmen.

Da der individuelle Benutzer oder die Allgemeinheit auf die Bibliotheken mit *USE zugreift, muss es einen Weg geben, um die Benutzer am Datenzugriff zu hindern. Wenn Sie verhindern möchten, dass die Produktionsdaten jedermann zugänglich sind und beliebig geändert werden können, müssen Sie die individu-

ellen Benutzerprofile und den allgemeinen Zugriff auf alle Produktionsdatendateien auf den Wert *EXCLUDE setzen.

Denkbar ist auch, dass Sie die Anzahl der Benutzer begrenzen möchten, die Anwendungsprogramme ausführen dürfen und die Programme mit allgemeiner (*PUBLIC) Berechtigung mit *EXCLUDE ausstatten. Damit die Benutzer die Erlaubnis für die Ausführung der Programme erhalten, wird für die Programmausführung im Gruppenprofil GRPAPP01 der Wert *USE ACCESS gesetzt. (Nur das Eingangsprogramm benötigt die Berechtigung für GRPAPP01. Auf die anderen Programme kann mit Hilfe der Berechtigungsübernahme zugegriffen werden.)

Die Änderung der Berechtigung für alle Produktionsobjekte klingt nach einem umfangreichen Vorhaben, ist aber nicht schwierig. Der Befehl GRTOBJAUT - Objektberechtigung erteilen - verfügt über eine generische Option, mit der die Berechtigung aller Objekte in einer Bibliothek mit einem einzigen Vorgang geändert werden kann. Die neue Option REPLACE des Befehls GRTOBJAUT, mit der V3R2 und V3R7 erweitert wurden, entfernt weitere Zugriffberechtigungen, die der Benutzer eventuell bereits besitzt.

Ich empfehle die Verwendung von Berechtigungslisten, um die Produktionsdatendateien zu schützen. Die Berechtigungslisten haben den Vorteil, dass Änderungen der Sicherheit selbst dann zulässig sind, wenn die Dateien offen sind. Das einzige Problem ist es, einen Zeitpunkt für das Hinzufügen der Berechtigungslisten zu finden, zu dem die Dateien in der Bibliothek nicht bearbeitet werden. Weitere Informationen zu Berechtigungslisten finden Sie in Kapitel 3.

IMPLEMENTIERUNG DES EXKLUSIVEN DATENZUGIFFS DURCH DIE ANWENDUNG

Die Implementierung des exklusiven Zugriffs durch die Anwendung wird in Abb. 2-1 gezeigt. Das Benutzerprofil PRDOWN01 hat kein Kennwort und besitzt die Eigentumsrechte an allen Produktionsprogrammen, Dateien und Bibliotheken. Die Eingangsprogramme übernehmen die Zugriffsberechtigung von PRDOWN01, um den Benutzern den Zugriff auf die Produktionsobjekte zu gewähren.

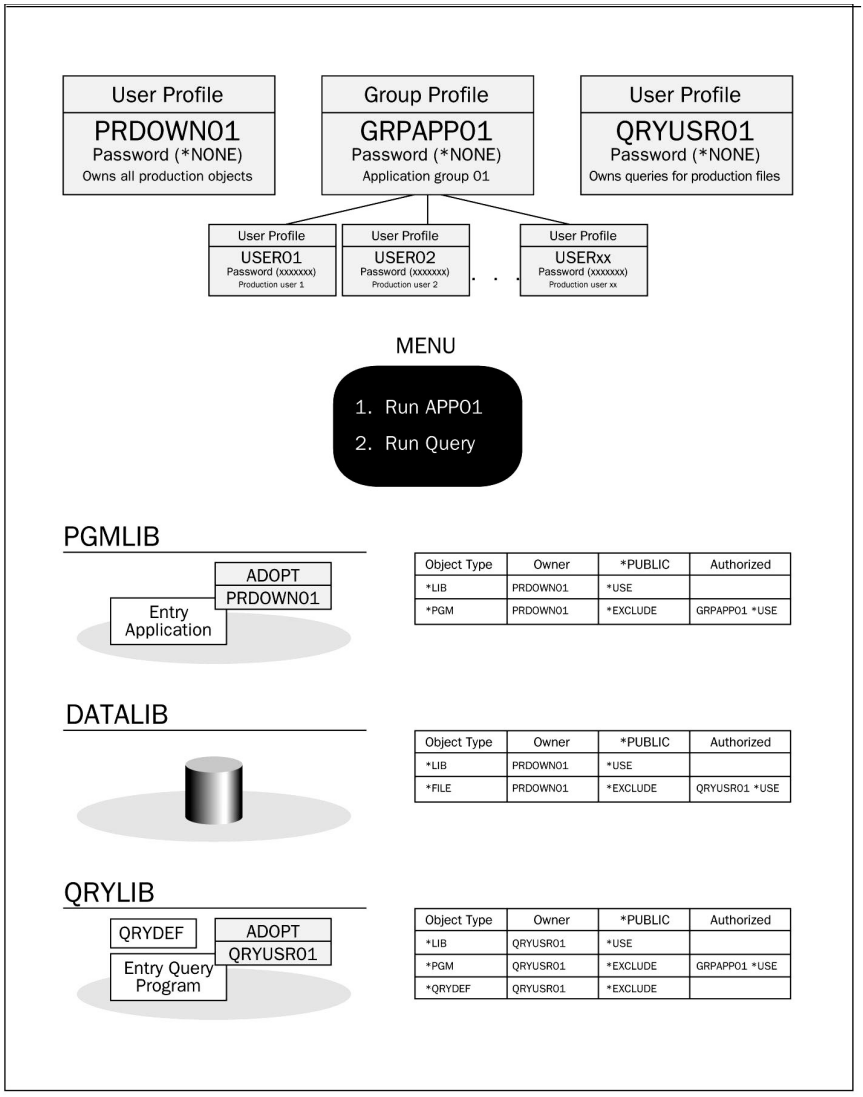

Abb. 2-1: Exklusivzugriff durch die Anwendung

Wenn ein Benutzer in GRPAPP01 die Menüoption 1 wählt, wird ein Eingangsprogramm aus PGMLIB aufgerufen. Dieses Programm übernimmt die Eigentumsrechte von PRDOWN01, die dem Benutzer Zugriff auf die Produktionsdaten gewähren. Das Eingangsprogramm ist ein Shell-Programm, das die eigentliche Anwendungsfunktion aufruft. Im Fall von gekaufter Software ist es möglich, dass Sie das übergebene Programm nicht steuern können. Deshalb wird jedes Programm in der Anwendung so geändert, dass es die Berechtigung des Produktionseigners (PRDOWN01) übernimmt.

BERICHTSERSTELLUNG

Häufig bieten die Systeme über Query, ODBC oder ein Tool für die Berichtserstellung zusätzliche Möglichkeiten zu den Berichten, die die Anwendungen zur Verfügung stellen. Da die Benutzer keinen Zugriff auf die Daten haben, muss ihnen eine Methode angeboten werden, um diese Berichte zu erstellen. Eine Möglichkeit besteht darin, den Benutzern Datenzugriff mit *USE zu erlauben. Damit könnten sie jedoch Produktionsdaten kopieren. Wenn das Kopieren nicht erwünscht ist, darf den Benutzern Zugriff mit *USE nicht gewährt werden.

Die Benutzer müssen nach wie vor Abfragen ausführen, um Berichte zu erstellen. Das ist weiterhin möglich, wenn das Benutzerprofil QRYUSR01 für Abfragen übernommen wird, während die Benutzer Query ausführen.

QRYUSR01 verfügt über kein Kennwort und ist der Eigner des Eingangsprogramms und der Abfragedefinitionen. Wenn der Benutzer die Menüoption 2 auswählt, wie in Abb. 2-1 gezeigt, wird das Eingangsprogramm in QRYLIB aufgerufen. Damit wird die Zugriffsberechtigung von QRYUSR01 übernommen.

QRYUSR01 greift auf Produktionsdateien mit *USE zu, womit der Nur-Lese-Zugriff ermöglicht wird. Damit werden die Query-Anwender an der Änderung der Produktionsdaten gehindert.

Die Bibliotheken PGMLIB und DATALIB erhalten Zugriffsberechtigung mit dem Wert *USE für *PUBLIC, so dass die übergebenen Jobs starten. Die Benutzer erhalten nur über die Menüoptionen 1 oder 2 Zugriff auf die Datendateien oder Programme.

Die Zugriffsrechte, die QRYUSR01 erteilt wurden, können entweder persönliche Berechtigungen sein oder mit einer Berechtigungsliste erteilt werden. Ich empfehle, die in V3R1 neu integrierte Unterstützung für die primäre Gruppenprofilberechtigung (PGP) einzusetzen. Mit dieser Berechtigung wird die Leistung im Vergleich mit persönlicher Berechtigung oder mit Berechtigungslisten verbessert.