



Inhaltsverzeichnis

Teil I

Datensicherheit

Kapitel 1

Exklusiver Zugriff durch die Anwendung: Sicherheitsrisiken erkennen S. 1

HINTERGRUND S. 3

Methoden für die Zuweisung der
Eigentumsrechte: S. 4

DATENZUGRIFF IM NETZWERK S. 9

RESSOURCEN-SICHERHEITSSTRATEGIE S. 12

Zugriffsmethoden blockieren S. 12

Datenzugriff einschränken S. 14

WÄHLEN SIE EINE STRATEGIE S. 16

Kapitel 2

Zugriff nur durch die Anwendung:

Umsetzung der Strategie S. 1

DIE STRATEGIE DES EXKLUSIVEN DATENZUGRIFFS DURCH DIE ANWENDUNG	S. 2
GRENZEN DER BIBLIOTHEKSSICHERHEIT	S. 4
EXKLUSIVER ZUGRIFF DURCH DIE ANWENDUNG AUF OBJEKTEBENE	S. 5
IMPLEMENTIERUNG DES EXKLUSIVEN DATENZUGRIFFS DURCH DIE ANWENDUNG	S. 7
BERICHTSERSTELLUNG	S. 9
ES IST ALLES IN DER ANWENDUNG ENTHALTEN	S. 10
GRENZEN DES EXKLUSIVZUGRIFFS DURCH DIE ANWENDUNG	S. 12

Kapitel 3

Verleihen Sie der Ressourcen-Sicherheit

mehr Klasse S. 1

RESSOURCEN-SICHERHEIT S. 2

ORGANISIEREN LOHNT SICH S. 3

BERECHTIGUNGSLISTEN FÜR ALLE FÄLLE S. 5

BERECHTIGUNGSLISTE PLANEN S. 9

BERECHTIGUNGSLISTE - ERSTE SCHRITTE S. 10

ZUSAMMENFASSUNG..... S. 13

Kapitel 4

Automatisieren Sie Ihre

Berechtigungslisten S. 1

BERECHTIGUNGSLISTEN „ZU FUß“

ERSTELLEN S. 2

DER EINFACHERE WEG S. 3

SO FUNKTIONIERT CVTOBJAUT S. 5

OBJEKTBERECHTIGUNG KOPIEREN S. 9

AKTUELLE BERECHTIGUNG ABRUFEN S. 14

ANWENDUNG IN DER PRAXIS S. 15

Kapitel 5	
Datensicherheit - Fragen und	
Antworten	S. 1
BENUTZERPROFILE FÜR PROGRAMMIERER	S. 2
Berechtigung *ALLOBJ kann nicht eingeschränkt werden	S. 6
SENSIBLE DRUCKAUSGABE SCHÜTZEN	S. 6
AUSGABEDATEIEN IN QUERY/400 VERHINDERN	S. 9
PROGRAMM FÜR DIE GÜLTIGKEITS- PRÜFUNG HINZUFÜGEN	S. 14
BENUTZERÄNDERUNGEN IN DATAFILE UTILITY (DFU) ÜBERWACHEN	S. 16
BEFEHLSZEILE MIT PROTOKOLLIERUNG	S. 19
BEFEHL FÜR DAS SETZEN DES GRUPPENPROFILS VERWENDEN	S. 26
ANMELDUNG ALS QSECOFR UMGEHEN	S. 28
INTERAKTIVE ABFRAGEN VERHINDERN	S. 30
JOBS IN DEN STAPELBETRIEB ÜBERGEBEN	S. 34
MIT PHYSISCHER DATEI ZUGRIFF AUF LOGISCHE DATEIEN EINSCHRÄNKEN	S. 36

Teil 2

Systemsicherheit

Kapitel 6

Zweistufige Anmeldung S. 1

ÜBERBLICK S. 2

TECHNISCHE EINZELHEITEN S. 4

KONTROLLE S. 7

RISIKOMANAGEMENT S. 8

ANMELDEBILDSCHIRM DER AS/400

 ÄNDERN S. 9

Kapitel 7

Inaktive Arbeitsstationen

abmelden S. 1

INAKTIVITÄTSINTERVALLE S. 2

Inaktivitätsnachrichtenwarteschlange S. 3

Kapitel 8

Anleitung für die Änderung von

QSECURITY S. 1

SETZEN SIE SICH IHR ZIEL S. 2

VON STUFE 20 AUF STUFE 30 WECHSELN S. 7

VON STUFE 30 AUF STUFE 40 WECHSELN S. 13

ÜBERSTÜRZEN SIE NICHTS S. 18

Kapitel 9	
Vorteile und Gefahren der Berechtigungsübernahme	S. 1
SO ÜBERNEHMEN PROGRAMME	
BERECHTIGUNG	S. 2
DIE LÖSUNGEN	S. 4
SICHERHEITSRISIKEN DER	
BERECHTIGUNGSÜBERNAHME	S. 5
EMPFEHLUNGEN	S. 8
Beschränken Sie den Zugriff	S. 8
Kategorisieren Sie die Objekte	S. 9
Beschränken Sie die Benutzeraktionen auf bestimmte Menüs	S. 10
Geben Sie für die meisten Benutzerprofile den Wert LMTCPG(*YES) an	S. 11
Hüten Sie sich vor Startprogrammen, die Berechtigung übernehmen	S. 11
Verwenden Sie systemeigene Menüs anstelle von CL-Programmменüs	S. 11
Vorsicht vor CL-Programmменüs, die Berechtigung übernehmen!	S. 12
Vorsicht bei Befehlen, mit denen Dateiwerkzeuge ausgeführt werden!	S. 12
Versuchen Sie, den Umfang der Berechtigungsübernahme zu begrenzen	S. 13
Verwenden Sie anstelle von CALL den Befehl TFRCTL	S. 13

Im Stapelbetrieb und nicht interaktiv verarbeiten	S. 14
Lassen Sie sich von Zeit zu Zeit die Berechtigungsübernahme anzeigen	S. 14
Vertrauen ist gut, Kontrolle ist besser	S. 14
Schützen Sie Ihre Bibliotheksliste	S. 15
Angabe von LOG(*NO) und ALWRVSRV(*NO)	S. 15
Sezifizieren Sie für OVRDBF-Befehle SECURE(*YES)	S. 16
SCHÜTZEN SIE IHRE DATEN UND IHRE MITARBEITER	S. 16

Teil 3

Interne Sicherheit

Kapitel 10

Fragen und Antworten zur

Systemsicherheit S. 1

BENUTZERPROFILE ANZEIGEN S. 2

EIGENTUMSRECHTE DER BENUTZER S. 3

VERTRAULICHE AUSGABEWARTESCHLANGE ERSTELLEN S. 4

EIGENTUMSRECHTE AN GESPOOLTEN DATEIEN S. 9

F22 VOM WRKSPLF-BILDSCHIRM AUSEINSCHRÄNKEN S. 10

IM BENUTZERPROFIL BLÄTTERN S. 12

SYSTEMWERT QCRTAUT ÄNDERN S. 13

EIN CL-PROGRAMM, DAS DIE BERECHTIGUNG DES SICHERHEITSCHEAUFTRAGTEN ÜBERNIMMT S. 14

ORDNER UND DOKUMENTE SCHÜTZEN S. 16

BENUTZERPROFIL QSECOFR S. 17

BENUTZERPROFIL UMBENENNEN S. 18

DEAKTIVIERTE BENUTZERPROFILE SUCHE S. 20

ZUGRIFF AUF DAS SYSTEMANFRAGENMÜNÜ EINSCHRÄNKEN S. 21

LETZTES SPEICHERN DER BENUTZER- PROFILE ANZEIGEN	S. 23
JOBAKTIONEN ÜBERWACHEN	S. 24
ÜBERGANGSPHASE ZU VERBESSERTER SICHERHEIT	S. 25
RICHTLINIEN FÜR BENUTZER- PROFILNAMEN	S. 27
BERECHTIGUNG *PUBLIC FÜR NACHRICHTEN ÄNDERN	S. 28
BENUTZERPROFILE UND BERECHTIGUNGEN KONSOLIDIEREN	S. 30
SICHERHEITSJOURNALDATEN ANZEIGEN LASSEN	S. 33
BERICHTS- UND JOURNALVERWALTUNG	S. 37
DRUCKER VERWALTEN	S. 38
ÄNDERUNGEN AN DEN BENUTZER- PROFILN PROTOKOLLIEREN	S. 44
MIT LMTCPB ARBEITEN	S. 46
IST DIESE ÄNDERUNG ERFORDERLICH?	S. 46
SOLL ICH *CHANGE ÄNDERN?	S. 47
EREIGNISSE FÜR INDIVIDUELLE BENUTZER ODER SYSTEMWEIT ÜBERWACHEN	S. 48
HAT DIESE ÄNDERUNG NEBENWIRKUNGEN?	S. 51
BERECHTIGUNG FÜR DAS SICHERHEITSJOURNAL ÄNDERN	S. 52
INAKTIVE BENUTZERPROFILE FINDEN	S. 54

BENUTZERPROFILZUGRIFF AUF EINE SPEZIFISCHE EINHEIT EINSCHRÄNKEN	S. 55
ZUGRIFFSBERECHTIGUNG FÜR EIN OBJEKT ERTEILEN UND ENTZIEHEN	S. 57
INDIKATOR FÜR EIGNER- BERECHTIGUNG	S. 58
ANZAHL DER OBJEKTARTEN EINSCHRÄNKEN, DIE DER BENUTZER WIEDERHERSTELLEN KANN	S. 59
OPTIONEN FÜR DIE VERHINDERUNG VON TIME-OUTS	S. 60
PROGRAMM FÜR DIE GÜLTIGKEITS- PRÜFUNG HINZUFÜGEN	S. 64
ZUGRIFF AUF BEFEHLSZEILENEBENE BEGRENZEN	S. 65
AUF GESCHÜTZTE DATENBANKEN ÜBER EINEN JOBSTAPEL ZUGREIFEN	S. 70

Kapitel 11	
Sicherheitsdesign für die Systemleistung	S. 1
SICHERHEITSGRUNDLAGEN	S. 2
ZUGRIFF AUF OBJEKTE	S. 5
OBJEKTSTRUKTUR	S. 8
REIHENFOLGE DER BERECHTIGUNGS- SUCHE	S. 10
TIPPS FÜR DAS SICHERHEITSDSIGN	S. 13
Tipp 1	S. 13
Tipp 2	S. 14
Tipp 3	S. 15
Tipp 4	S. 16
Tipp 5	S. 16
Tipp 6	S. 18
Tipp 7	S. 19
TECHNISCHE EINZELHEITEN	S. 20
REFERENZLITERATUR	S. 22

Kapitel 12

Berechtigungslisten –

Grundlagen S. 1

BERECHTIGUNGSLISTEN-KONZEPT S. 2

BERECHTIGUNGSLISTEN KONKRET S. 4

BERECHTIGUNGSPRÜFUNG FÜR
BERECHTIGUNGSLISTEN S. 7

BERECHTIGUNGSLISTEN RICHTIG
EINSETZEN S. 8

Dateien schützen, die längere Zeit geöffnet sind S. 9

Datenbankdateien mit mehreren Teildateien
schützen S. 9

Mit Berechtigungslisten persönliche
Berechtigungen berücksichtigen S. 11

Dokumente und Ordner schützen S. 12

EIN LEISTUNGSFÄHIGES WERKZEUG S. 13

Kapitel 13

Interne Sicherheit:

Fragen und Antworten S. 1

UNTERSTRICHE ENTFERNEN S. 2

ZUGRIFF DURCH EIN HINTERTÜRCHEN S. 3

ZUGRIFF AUF EIN OBJEKT

 KONTROLLIEREN S. 6

ALLGEMEINE BERECHTIGUNG FÜR

 EIN OBJEKT S. 7

SICH AUF BERECHTIGUNGSÜBERNAHME

 VERLASSEN S. 8

Programme S. 10

Daten S. 10

Teil 4

Netzwerksicherheit

Kapitel 14
Internetsicherheit
für die AS/400 S. 1

INTERNETGRUNDLAGEN S. 2

AS/400-LÖSUNGEN S. 4

NETZWERKLÖSUNGEN S. 6

ZUSAMMENFASSUNG S. 8

REFERENZLITERATUR S. 8

Kapitel 15
AS/400-Sicherheit in einer
vernetzten Welt S. 1

UNTERNEHMENSKULTUR..... S. 2

RASANTE TECHNOLOGISCHE
ENTWICKLUNG S. 5

HÜTEN SIE SICH VOR DEM AUDITOR S. 8

FÜR DIE ZUKUNFT S. 13

Kapitel 16
Das 20-Fragen-Spiel zur
Netzwerksicherheit S. 1

FRAGE 1 S. 2

FRAGE 2 S. 3

FRAGE 3 S. 4

FRAGE 4 S. 4

FRAGE 5 S. 5

FRAGE 6 S. 6

FRAGE 7 S. 6

FRAGE 8 S. 7

FRAGE 9 S. 7

FRAGE 10 S. 8

FRAGE 11 S. 8

FRAGE 12 S. 9

FRAGE 13 S. 9

FRAGE 14 S. 10

FRAGE 15 S. 10

FRAGE 16 S. 11

FRAGE 17 S. 11

FRAGE 18 S. 12

FRAGE 19 S. 12

FRAGE 20 S. 12

SCHLIEßEN SIE DIESE TÜR S. 13

Kapitel 17

Netzwerksicherheit:

Fragen & Antworten S. 1

ANMELDEBILDSCHIRM UMGEHEN (AS/400S).....	S. 2
ANMELDEBILDSCHIRM UMGEHEN (S/36S UND S/38S)	S. 3
UNTERSCHIED ZWISCHEN ENDPASTHR UND SIGNOFF	S. 3
PC-DATEIÜBERTRAGUNGS-PROGRAMME	S. 6
DLOS GEMEINSAM NUTZEN.....	S. 7
KONFIGURATION IHRES SYSTEMS FÜR DDM-SICHERHEIT	S. 8
SECURELOC ANGEBEN	S. 12
DATEN SCHÜTZEN	S. 15
ZUGRIFF AUF AS/400-OBJEKTE ÜBER DAS IFS BESCHRÄNKEN	S. 16
BENUTZERPROFILE GEMEINSAM NUTZEN.....	S. 19
STANDARDBENUTZERPROFILE	S. 22
EXPLIZITE EINHEITENSPEZIFIKATION ERSTELLEN	S. 24
STANDARDBENUTZER ENTFERNEN	S. 26

Teil 5

Sicherheitsaudit

Kapitel 18

So überleben Sie ein

AS/400-Sicherheitsaudit S. 1

STRESS REDUZIEREN S. 2

ZIEL DES EDV-AUDITS S. 3

DANACH SUCHEN AUDITOREN S. 4

TYPISCHES AUDIT S. 6

Gespräche S. 6

Installation der Audit-Software S. 8

PHYSISCHE ANLAGEN S. 9

DOKUMENTATION UND SICHERHEITS-
KONFIGURATION S. 9

PRÜFBERICHT S. 15

EIN AUDIT ÜBERSTEHEN S. 16

Einen Monat vor dem Audit S. 17

Eine Woche vor dem Audit S. 18

Während des Audits S. 19

ERSTELLUNG DER AUDIT-TOOLS S. 21

REFERENZLITERATUR S. 26

Kapitel 19

Checkliste Sicherheitsaudit S. 1

DOKUMENTATION	S. 2
PHYSISCHE SICHERHEIT	S. 3
SYSTEMWERTE UND NETZWERK- ATTRIBUTE	S. 4
ÜBERPRÜFUNG DER KENNWORT- SICHERHEIT	S. 10
BENUTZER- UND GRUPPENPROFILE	S. 13
GRUPPENPROFILE UND OBJEKT EIGNERPROFILE	S. 16
BERECHTIGUNGSKONTROLLE	S. 17
BERECHTIGUNG FÜR SYSTEME UNTERHALB VON SICHERHEITSSTUFE 40 ODER 50	S. 18
BIBLIOTHEKEN UND BIBLIOTHEKSLISTEN	S. 19
PROGRAMME	S. 20
BERECHTIGUNGSÜBERNEHMENDE PROGRAMME	S. 21
BEFEHLE	S. 22
Den Zugriff überwachen	S. 22
Kommunikation	S. 23
CLIENT ACCESS	S. 26
INTERNET UND TCP/IP-SICHERHEIT	S. 28
ZUSÄTZLICH	S. 32

CHECKLISTEN FÜR DIE DOPPELTE
KONTROLLE S. 33
REFERENZLITERATUR S. 33

Index

