Über welche Sicherheitsvorkehrungen verfügen die Oracle Anwendungen?

Autor: Dr. Volker Thormählen

1. Definition, Überblick und Abgrenzung

Der Begriff *Datensicherheit* umfaßt alle Vorkehrungen (i. S. von Methoden, Verfahren, Algorithmen, etc.) in den Bereichen Hardware, Software, Netz und Organisation mit dem Ziel, das gesamte Informationssystem einschließlich seiner Daten gegen Schaden verursachende Störfaktoren zu schützen. Dazu zählen Notfälle, Katastrophen, Spionage durch Abhören von Leitungen, Sabotage mittels Computerviren, Vandalismus, Diebstahl, Verfälschung oder Vernichtung von Daten und Programmen, unbefugte Kenntnisnahme von Daten, unberechtigter Zugang zu sicherheitsrelevanten Bereichen, technisches Versagen, Eingabe- sowie sonstige Bedienungsfehler und dergleichen mehr.

Zur Vermeidung oder Minderung von Schadensfällen durch solche Gefahren, Bedrohungen oder Risiken werden gewöhnlich bauliche, hardwaretechnische, softwaretechnische, organisatorische sowie personelle Sicherheits- bzw. Schutzmaßnahmen ergriffen.

Im folgenden werden nur die möglichen Sicherheitsvorkehrungen auf der Ebene der Anwendungssoftware am Beispiel der *Oracle Anwendungen* betrachtet. Deshalb werden vorbeugende Maßnahmen auf der Datenbank- und Betriebssystemebene nicht behandelt. Auch mögliche Sicherheitsvorkehrungen auf der Ebene der Hardwarearchitektur sowie der Gebäude- und Netzinfrastruktur werden nicht weiter verfolgt.

Ein von Oracle herausgegebenes Dokument, das die Sicherheitsvorkehrungen des Anwendungssystems im einzelnen beschreibt, ist nach Wissen des Autors nicht verfügbar. Diese Informationslücke zu verkleinern, ist das Ziel der folgenden Ausführungen.

2. Benutzername und Paßwort

Die rechnergestützte Benutzeridentifikation und das Paßwortverfahren sind die beiden wesentlichen Bestandteile des Zugriffsschutzes der *Oracle Anwendungen*. Beide Funktionalitäten sind für alle jeweils eingesetzten Teilsysteme im Modul *'System Administrator'* zentralisiert.

In der Maske *'Benutzer definieren'* des Moduls *'System Administrator'* muß jedem Benutzer eine eigene Anmeldekennung (⇒ Benutzername) zugeordnet werden. Dafür kann auch ein Gültigkeitszeitraum festgelegt werden, denn eine Benutzerkennung sollte nur für den Zeitraum eingerichtet werden, in dem sie tatsächlich benötigt wird.

Außerdem kann in der erwähnten Maske definiert werden, ob das zur Anmeldung erforderliche Paßwort alle X Tage oder nach Y Zugriffen geändert werden muß. Das Paßwort sollte nur dem Benutzer bekannt sein.

Das System begrenzt die Zahl der Fehlversuche bei der Anmeldung. Nach 3 Fehlversuchen wird ein weiterer Versuch automatisch unterbunden. Mit der Meldung *'Erfolglose Anmeldeversuche seit der letzten Sitzung ...'* informiert das System den berechtigten Benutzer über das gerade genannte Ereignis.

Ob mehrfache und nur singuläre Anmeldungen je Benutzer zugelassen werden, kann nur auf der Ebene des Betriebssystems (⇒ Login) festgelegt werden.

Ob die Anmeldung eines Benutzers bereits auf der Ebene des Betriebssystems (neben dem Benutzernamen) ein Paßwort erfordern sollte, hängt von der Schutzbedürftigkeit der gesamten Anwendung ab.

3. Benutzername und Zuständigkeiten

In der Maske *'Benutzer definieren'* des Moduls *'System Administrator'* müssen jedem Benutzer seine Zuständigkeiten individuell zugeordnet werden. Eine Zuständigkeit erlaubt die Ausführung definierter Funktionen des Systems im Sinne von Menüpfaden und damit aufrufbaren Masken. Je Benutzer und Zuständigkeit kann ein Gültigkeitszeitraum festgelegt werden. Somit können vorher und nachher die mit der jeweiligen Zuständigkeit verbundenen Systemfunktionen nicht mehr ausgeführt werden.

Zuständigkeiten werden gewöhnlich gemäß den Kompetenzen eines Benutzers abgestuft. Je höher (niedriger) der jeweilige Rang eines Benutzers in der Strukturorganisation ist, desto größer (kleiner) ist gewöhnlich die Zuständigkeit. Eine typische Abstufung könnte je Modul wie folgt lauten:

- Information (nur für Abfragen innerhalb eines Moduls)
- Sachbearbeiter (nur für bestimmte Teilfunktionen eines Moduls)
- Administrator (für alle Funktionen eines Moduls einschließlich Einrichtung)

In der Maske *'Zuständigkeiten definieren'* des Moduls *'System Administrator' können die zu einem Modul gehörigen* Zuständigkeiten definiert und mit einem Anfangs- und Enddatum versehen werden. Gleichzeitig erfolgt hier die Verknüpfung mit den Menüpfaden des Systems im Sinne des gesamten Menübaums oder bestimmter Teile davon.

Da die im Standardsystem enthaltene Menüstruktur der Module vom Anwender relativ leicht an seine Anforderungen angepaßt werden kann, ist je Modul eine Vielzahl von Zuständigkeiten definierbar. Aus praktischer Sicht ist es jedoch empfehlenswert, die Abstufungen der Zuständigkeiten nicht zu übertreiben, um den Pflegeaufwand möglichst gering zu halten.

Die Zuordnung von Zuständigkeiten zu Benutzern, die nur der Systemverwalter vornehmen kann, sollte beantragungspflichtig sein. Diese Prozedur stellt eine empfehlenswerte organisatorische Sicherheitsmaßnahme dar.

Über den Menüpfad *Navigieren-Sicherheit-Zuständigkeit-Auswertungen-Gruppen* des Moduls *'System Administrator'* kann die Maske *'Auswertungs-Gruppen definieren'* erreicht werden. Die hier definierten Sicherheitsgruppen für Auswertungen können mit Zuständigkeiten verbunden werden. Auf diese Weise wird festgelegt, welche Benutzer welche Auswertungen abrufen dürfen.

4. Modulübergreifende Sicherheitskonzepte

Sicherheit und Flexibilität der Oracle Anwendungen wird unter anderem durch das Konzept der *Flexfelder* gewährleistet. Vgl. dazu [VT96] und [VT99].

Bei den Flexfeldern handelt es sich im Grunde um benutzerdefinierte Verbundnummern mit bis zu 30 Nummernteilen. Die klassifizierenden und/oder identifizierenden Nummernteile werden als *Segmente* bezeichnet. Die Inhalte der Segmente werden *Segmentwerte* genannt, die im Form von *Wertesets* zusammengefaßt werden.

- Werden Flexfelder für kaufmännische Ordnungsbegriffe (z. B. Artikelnummer) oder ähnliches verwandt, dann handelt es sich um *Schlüsselflexfelder* .
- Werden die Flexfelder dagegen zur Speicherung von (betriebs-) individuellen Zusatzinformationen benutzt, dann wird von *Infoflexfeldern* oder *Beschreibenden Flexfeldern* gesprochen.

Ein spezielles *Schlüsselflexfeld* stellt das *Kontoflexfeld* dar. Mittels der Segmente eines Kontoflexfelds können benutzerdefinierte Kontierungsbegriffe (⇒ Segmentwerte) miteinander verbunden werden, um eine mehrdimensionale Kontierung im Rechnungswesen zu erzielen.

Das Konzept der *Flexfelder* in den Oracle Anwendungen wird ergänzt durch dazugehörige Gültigkeits- und Sicherheitsregeln, die im folgenden behandelt werden.

4.1 Gültigkeitsregeln für Schlüsselflexfelder

Gültigkeitsregeln für *Schlüsselflexfelder* können bzw. sollten in der Maske *'Segment-Validierungen definieren'* angelegt werden.

Die Segmentwerte eines *Schlüsselflexfelds* können einer automatischen Kontrolle auf gegenseitige Verträglichkeit unterworfen werden. Dadurch kann sichergestellt werden, daß der Benutzer nur gültige Kombinationen von Segmentwerten in das betreffende Schlüsselflexfeld eingeben kann. Demgemäß wird die Erfassung ungültiger Kombinationen vom System abgelehnt. Auf diese Weise kann die Eingabesicherheit erheblich erhöht werden.

Die Komplexität der Gültigkeitsregeln für Schlüsselflexfelder steigt (sinkt),

- je mehr (weniger) Segmente definiert werden,
- je mehr (weniger) zusammenhängende Nummernbereiche bei der Planung der Nummernsysteme vorgesehen werden.

Daher beeinflußt auch die Gestaltung betrieblicher Nummernsysteme die Eingabesicherheit in erheblichem Ausmaß.

4.2 Sicherheitsregeln für Flexfelder

Durch die Definition von Sicherheitsregeln für *Flexfelder* läßt sich folgendes erreichen**:**

- Begrenzung der Segmentwerte, die ein bestimmter Benutzer eingeben darf (das bedeutet in der Praxis eingeschränkte Auswahllisten zur Belegung der einzelnen Segmente eines *Flexfelds* mit zulässigen Werten).
- Verhinderung der Eingabe von Segmentwerten, die ein bestimmter Benutzer nicht verwenden darf.

Sicherheitsregeln werden mit der Maske *'Sicherheitsregeln definieren'* angelegt. Die Verknüpfung einer Sicherheitsregel mit Zuständigkeiten erfolgt mit der Maske *'Sicherheitsregeln zuordnen'.* Nach Durchführung dieses Einrichtungsschritts sind die Sicherheitsregeln für *alle* Benutzer aktiv, deren jeweilige Zuständigkeit mit einer Sicherheitsregel verbunden wurde.

Zwei Voraussetzungen sind notwendig, um Sicherheitsregeln für *Flexfelder* nutzen zu können:

- In der Maske *'WerteSets definieren'* muß der Schalter *'Sicherheitsregeln'* auf *'Ja'* gesetzt werden.
- In der Maske *'Schlüssel-FlexFeld-Segmente definieren'* muß der Schalter *'Sicherheit aktiv'* ebenfalls auf *'Ja'* gesetzt werden. Ähnlich ist in der Maske *'Info-FlexFeld-Segmente definieren'* vorzugehen.

4.3 Aliasnamen für Flexfeldkombinationen

In der Maske *'Alias definieren'* kann der Benutzer Aliasnamen für ein Schlüsselflexfeld definieren. Ein Aliasname dient dazu, die Belegung des betreffenden Schlüsselflexfelds mit einer

bestimmten *Kombination* gültiger Segmentwerten ganz oder teilweise zu automatisieren. Die Eingabe eines definierten Aliasnamen in ein entsprechendes Bildschirmfenster genügt, um automatisch die *vollständige* oder *teilweise* Belegung der Segmente des betreffenden Schlüsselflexfelds mit vorher festgelegten Segmentwerten zu erzielen. Die Verwendung von Aliasnamen stellt deshalb eine Erfassungshilfe dar, die dazu dient, gültige Kombinationen oder Muster von Segmentwerte schnell und sicher einzugeben.

4.4 Sonstige modulübergreifende Sicherheitsvorkehrungen

Ohne Anspruch auf Vollständigkeit sollen abschließend noch drei weitere modulübergreifende Sicherheitsvorkehrungen kurz erwähnt werden:

- Das System verhindert konkurrierende Aktualisierungen. Dadurch wird die gleichzeitige Bearbeitung eines Datensatzes durch mehrere Benutzer automatisch unterbunden.
- Das System umfaßt diverse Sicherheitsabfragen, die zum Beispiel wie folgt lauten: *"Sollen die Änderungen gespeichert werden?"*
- QuickCodes stellen entweder fest vorgegebene oder benutzerdefinierte Schlüssel mit einer bestimmten Bedeutung dar. Sie erscheinen gewöhnlich als Auswahlliste im einem QuickPick-Fenster zwecks Belegung eines Maskenfelds. Die Menge der eingerichteten Quickcodes begrenzt ihre Auswahlmöglichkeit im QuickPick-Fenster und verhindert dadurch Fehleingaben im betreffenden Maskenfeld.

5. Modulspezifische Sicherheitskonzepte

Für 8 häufig eingesetzte Module der Oracle Anwendungen werden im folgenden wichtige oder bemerkenswerte Sicherheitsvorkehrungen geschildert. Eine vollständige Beschreibung der zahlreichen modulspezifischen Sicherheitsmechanismen (i. S. von sicherheitsrelevanten Geschäftsregeln und Geschäftsprozessen, Einzel- und Kombinationsprüfungen, etc.) ist hier *nicht* beabsichtigt. Anhand von repräsentativen Beispielen wird jedoch versucht zu verdeutlichen, was damit gemeint ist und welche praktische Bedeutung sie besitzen.

5.1 Modul '*General Ledger*'

Zwei Beispiele für Sicherheitskonzepte, die im Modul *Rechnungswesen* genutzt werden können, beinhalten folgendes:

- Buchungsbelege können durch automatische Numerierung (⇒ Zählnummer) gesichert werden.
- Mittels Profiloptionen kann festgelegt werden, welche Benutzer die Verbuchung oder Stornierung von Buchungsstapeln on-line vornehmen dürfen (seit Release 11).
- Die Abstimmung von Buchungsstapeln kann mit dynamisch aktualisierten Kontrollsummen erfolgen.

5.2 Modul '*Assets*'

Zu den Sicherheitskonzepten des Moduls *Anlagenbuchhaltung* zählen folgende Einrichtungen:

- Im Rahmen der Systemsteuerung kann eine fortlaufende Anlagennumerierung festgelegt werden.
- Mittels Flexfeldern für Anlagenstandorte, Anlagengruppen, Anlagenschlüsseln und Kontenkombinationen kann die Zuordnung von Anlagen zuverlässig vorgenommen werden.

5.3 Modul '*Receivables*'

Das Modul *Debitoren* besitzt u. a. folgende Sicherheitsvorkehrungen*:*

- Kreditprofile (einschließlich Kreditlimit) können für alle Kunden anlegt werden zwecks Kreditprüfung bei der Auftragserfassung und beim Warenversand. Das Kreditrisiko kann dadurch begrenzt werden.
- Je Benutzer können Genehmigungsgrenzen (von-bis Betrag) für Korrekturen festgelegt werden. Nur innerhalb dieser Grenzen ist ein Benutzer befugt, den delegierten Entscheidungsspielraum auszunutzen.
- Die Gefahr fehlerhafter Kontierung der Ausgangsrechnungen und -gutschriften kann durch die Speicherung von Kontierungsregeln im System vermindert werden. Durch die Verwendung von Kontierungsregeln läßt sich die Kontierung automatisieren und damit systematischer, schneller und sicherer durchführen.
- Die baumartige Struktur des Kundenstamms mit den zugehörigen Adressen, Banken, Kontaktpersonen, etc. bewirkt eine auf den Hauptkunden/Verband begrenzte Auswahlmöglichkeit und demnach mehr Sicherheit als ein flacher Kundenstamm. Dies wirkt sich positiv aus bei der Rechnungs- und Zahlungserfassung bis hin zur Anzeige der *'Offenen Posten'* .
- Die Möglichkeit zur Zuordnung von Rechnungen bei der Gutschriftserfassung stellt sicher, daß keine Gutschrift ohne vorhergehende Rechnung erstellt werden kann. Hinzu kommt, daß die Daten der jeweiligen Rechnung bei der Gutschriftserstellung zur Wiederverwendung angeboten werden. Das mindert das Risiko von Erfassungsfehlern.
- Auch die System- und Profiloptionen des Moduls lassen eine Vielzahl von sicherheitsrelevanten Einstellungen zu. Zum Beispiel unterbindet der Schalter 'Rechnungen löschen/ändern', daß Rechnungen unberechtigt storniert oder modifiziert werden.

5.4 Modul '*Payables'*

Die folgenden Funktionen des Moduls *Kreditoren* beruhen u. a. auf praxistauglichen Sicherheitskonzepten:

- Die Prüfung auf doppelte Lieferantenrechnungen (⇒ mehrfache Eingabe einer bestimmten Rechnungsnummer eines Lieferanten) ist systemseitig gewährleistet.
- Lücken bei der (automatischen) Numerierung der Buchungsbelege können mittels Standardbericht erkannt und überprüft werden.
- Versehentlich mehrfach angelegte Lieferanten können systemunterstützt gesucht werden.
- Lieferanten können für den Zahlungsausgang gesperrt oder mit Obergrenzen und ähnlichen Bedingungen eingeschränkt werden. Ähnliche Begrenzungen können auch auf weiteren Ebenen genutzt werden, beispielsweise bei eigenen Bankkonten, Obergrenzen für automatische Zahlungsläufe, etc.
- Systemfunktionen zur Zahlungsabstimmung für Lieferanten, die zugleich Kunden darstellen, sind verfügbar.
- Bei der Rechnungseingabe kann die Abstimmung entsprechender Stapel mittels Kontrollsumme und Belegzähler sichergestellt werden.
- Die Möglichkeiten zur Einrichtung der 2-, 3- oder 4-Wege-Abstimmung von Einkaufsaufträgen, Lieferantenrechnungen, Wareneingängen und Empfangsbestätigungen der internen Bedarfsträger können eine Rechnungsgenehmigung unter falschen Voraussetzungen wirksam verhindern. Definierte Toleranzen können dabei berücksichtigt werden.

Die programmierten Kontrollen des lokalisierten Moduls umfassen keine Prüfung auf gültige Bankleitzahlen und keine Prüfziffernberechnung für Bankkontonummern, vgl. dazu [VT95]. Die *Änderungshistorie* dieser beiden Daten kann von einem dazu berechtigten Benutzer auf Anwendungsebene *nicht* on-line abgefragt und überprüft werden. Mithin kann eine kriminelle Manipulation dieser Daten vor und nach einem Zahlungslauf mit den verfügbaren Funktionen des Standardsystems nur zufällig entdeckt bzw. verhindert werden. Ist die Gefahr erkannt,

kann die entsprechende Sicherheitslücke durch eine wohlüberlegte Definition und Zuordnung der Zuständigkeiten geschlossen werden. Zusätzlich oder statt dessen kann mit dem Modul *Alert* (siehe weiter unten*)* eine Ausnahmemeldung über die Änderungsereignisse ausgelöst werden.

5.5 Modul '*Purchasing'*

Die wichtigsten Sicherheitskonzepte des Moduls *Einkauf* lassen sich mit den Stichworten *Positions-, Sicherheits- und Genehmigungshierarchie* sowie *Befugnisgrenzen* umreißen:

- Eine Positionshierarchie kann sowohl als Sicherheits- als auch als Genehmigungshierarchie benutzt werden.
- Sicherheits- und Zugriffsebenen können für alle Dokumentenarten (z. B. Anforderungen, Anfragen, Bestellungen, etc.) festgelegt werden.
- Genehmigungswege können ebenfalls je Dokumentenart bestimmt werden.
- Kontrollfunktionen können mit Tätigkeiten oder Positionen verbunden werden.
- Kontrollgruppen führen Kontrollfunktionen aus und werden dafür durch Befugnisregeln bevollmächtigt.
- Befugnisregeln wiederum beinhalten Betragsgrenzen, Kontenbereiche, Artikelbereiche, Artikelgruppenbereiche und/oder Auslieferungsadressen.

Die konsequente Anwendung dieser Sicherheitsvorkehrungen schützt weitgehend vor Fehlbeschaffungen und Kompetenzüberschreitungen und verkürzt insgesamt die Ausführungs- und Entscheidungsprozesse im Einkaufsbereich.

Ähnliche Genehmigungsverfahren sind in den *'Work Flow'* anderer Module integriert.

5.6 Modul '*Inventory'*

Im Modul *Lager* sind vielfältige Sicherheitsvorkehrungen integriert, von denen an dieser Stelle nur einige wenige erwähnt werden:

- Der Aufbau der Lagerorganisation kann bis hinunter zu den Lagerplätzen flexibel abgebildet werden. Durch die Nutzung der Lagerplatzkontrolle kann das Auffinden von Artikeln zwecks Entnahme oder Inventur besser sichergestellt werden.
- Die Möglichkeit zur zentralen Verwaltung der Artikelstammdaten ist gegeben. Die Artikel können dann in beliebig vielen Lagerorganisationen einheitlich benutzt werden. Erfassungsaufwand und Erfassungsfehler werden dadurch minimiert.
- Attribute eines Artikels können *entweder* auf Artikelebene *oder* in Verbindung mit einer Lagerorganisation festgelegt werden. Im zuletzt genannten Fall kann die einheitliche Festlegung der Artikelattribute über alle Lagerorganisationen hinweg sichergestellt werden.
- Bestimmte Attribute eines Artikels können einer *Statussteuerung* unterliegen. Das bedeutet, daß die eingestellten Werte von Benutzer nicht geändert werden können.
- Die Reservierung von Artikeln für Kundenaufträge ist möglich, falls entsprechender Lagerbestand verfügbar ist (⇒ Verfügbarkeitsprüfung).
- Das Bestandsrisiko in den Lägern kann durch automatische Lagerdisposition auf der Grundlage alternativer Lagerhaltungsmodelle reduziert werden. Zugleich kann die Zahl der Fehlmengensituationen (⇒ Servicegrad) optimiert werden.

5.7 Modul '*Order Entry'*

Fünf repräsentative Beispiele für die diversen Sicherheitskonzepte des Moduls *Auftrag* werden im folgenden kurz umrissen:

- Die Vorbelegung der Masken zur Auftragserfassung mit sinnvollen Anfangswerten kann der Benutzer durch die Definition von Regeln zur Auswahl von Standardwerten festlegen. Das wirkt sich erfahrungsgemäß positiv auf Geschwindigkeit und Sicherheit der Auftragsbearbeitung aus.
- Die Profiloptionen des Moduls umfassen verschiedene Sicherheitsvorkehrungen. Zum Beispiel kann mittels Schalter eingestellt werden, ob die Änderung von Umsatzsteuerschlüsseln durch den Benutzer zulässig ist. Ähnliches gilt für die diversen Masken zur Einrichtung des Moduls. Zum Beispiel kann in der Maske *'Rabatte definieren'* festgelegt werden, ob Preisnachlässe vom Benutzer überschrieben werden dürfen.
- Durch die Bonitätsprüfung bei der Auftragserfassung läßt sich das Kreditrisiko begrenzen.
- Durch die Verfügbarkeitsprüfung kann das Risiko nicht oder nicht rechtzeitig erfüllbarer Lieferverpflichtungen vermieden werden.
- Durch die Möglichkeit zur Definition von Auftragsarten, -zyklen und -schritten kann der Ablauf der gesamten Auftragsbearbeitung sicherer gestaltet werden. Beispielsweise können definierte Auftragsschritte vom Benutzer nicht ohne weiteres übersprungen werden. Eine termintreue Auftragsabwicklung wirkt sich in der Regel positiv auf die Kundenzufriedenheit aus und schützt damit vor der Gefahr, Kunden wegen unzuverlässiger Auftragsabwicklung zu verlieren.

5.8 Modul 'Alert'

Im Zusammenspiel mit den erwähnten Lösungen für das Rechnungswesen und die Logistik (⇒ Warenwirtschaft) ist dieses Modul maßgeschneidert für die Unternehmensführung nach dem *Prinzip der Ausnahme:*

- Geschäftsregeln bzw. Ausnahmeereignisse können vom Benutzer definiert werden.
- Die sofortige Benachrichtigung bestimmter Benutzer oder Benutzergruppen mittels elektronischer Post ist möglich, sobald sich Ausnahmen ereignen.
- Auf Ausnahmeereignisse kann das System im Sinne vollständig automatisierter Geschäftsprozesse reagieren. Dadurch lassen sich Routineaufgaben ohne manuellen Eingriff ausführen.

Kurz, dieses Modul kann die ausführende Ebene von Routineaufgaben befreien und die dispositive Ebene bei der Ausführung der Kontrollaufgaben entlasten. *Deswegen ist es für systematisches Risikomanagement ideal geeignet!*

6. Sicherheitslücken und zusätzliche Sicherheitsvorkehrungen

Zählt man mögliche Bedienungsfehler des Systems zu den Risiken, dann wird sofort deutlich, daß hundertprozentige Sicherheit trotz umfangreicher Vorkehrungen in der Praxis kaum erreichbar ist.

Gegen mangelndes Sicherheitsbewußtsein der Anwender bzw. Benutzer ist kein Schutz möglich. Man denke in diesem Zusammenhang zum Beispiel an den Menüpfad *\Benutzer-Werkzeuge*, der im Standardsystem (Release 10) enthalten und damit jedem Benutzer zugänglich ist. Die Auswahl des Werkzeugs *'Shell'* ist nicht durch Paßwort gesichert. Folglich kann der Benutzer auf die Ebene des Betriebssystems gelangen und dort eigene und fremde Dateien ändern oder löschen, sofern die Dateizugriffsrechte das erlauben. Die Stillegung dieses Menüzweigs ist daher aus Sicherheitsgründen empfehlenswert. Die Option *'Shell'* gibt es in Release 11 *nicht* mehr! Alle Systemfunktionen sind angeblich mittels Paßwort geschützt, die neuerdings über den Menüpfad *\Hilfe-Tools* erreichbar sind.

Im allgemeinen sind die im Standardprogramm enthaltenen Sicherheitsvorkehrungen vollkommen ausreichend. Je nach der angenommenen oder tatsächlichen Risikosituation kann

es ggf. erforderlich sein, die Sicherheit der Anwendung an den als kritisch beurteilten Stellen durch individuelle Zusatzprogramme zu ergänzen.

7. Schlußbemerkung

Der Verfasser gibt in diesem Artikel sein persönliches Verständnis und seine persönliche Beurteilung der Sicherheitsvorkehrungen der Oracle Anwendungen wieder.

Literatur:

[VT95] THORMÄHLEN, V., Tabellengesteuerte, modulare Prüfziffernberechnung bei Bankkontonummern, Version 2, Nov. 1995, 18 Seiten, 13 Tabellen, Selbstverlag, Schutzgebühr 180,-- DM.

[VT96] THORMÄHLEN, V., Die Kontierungsleiste eines mehrdimensionalen Rechnungswesens in internationalen Konzernen, in: Betriebswirtschaftliches Controlling, Planung - Entscheidung - Organisation, Hersg. Bernd Rieper, Thomas Witte, Wolfgang Berens, Gabler Verlag, Wiesbaden 1996, Seite 235 - 257, ISBN 3-409-12909-X

[VT99] THORMÄHLEN, V., Grundsätze der Gestaltung des Kontoflexfelds in den Oracle Anwendungen, in: DOAG News, Ausgabe 2, Stuttgart Febr. 1999, Seite 49-53, ISSN 0936-0360

Dr. Volker Thormählen
in Firma Bull GmbH
Theodor-Heuss-Str. 60-66
D-51149 Köln-Porz
Tel. + 49 (2203) 305-1719
Fax: + 49 (2203) 305-1699
Email: v.thormaehlen@bull.de