Christian Schwitalla,
Mitglied der Development Community Leitung

Es gibt keine dummen (ADF-) Fragen

Die ADF-Community hat das Ziel, Informationen und Erfahrungen zum Oracle Application Development Framework (ADF) auszutauschen und damit die Entwicklungs-Plattform unter Entwicklern, Anwendern und IT-Dienstleistern bekannter zu machen. Sie wird von Oracle-Partnern, der DOAG sowie Oracle getragen und steht allen interessierten Anwendern offen. Zu den Aktivitäten der ADF-Community zählen folgende Punkte:

- ADF News Sessions: Eine Reihe von Online-News-Sessions, die in zweiwöchigem Rhythmus jeweils am Freitag von 8:30 bis 9:00 Uhr stattfinden. Die behandelten Themen sind sehr vielfältig, die Beiträge kommen sowohl von Oracle als auch von den Partnern. Derzeit läuft die sechste Staffel, Referenten sind jederzeit willkommen. Dank des kompakten Formats lassen sich die ADF-News-Sessions leicht in den beruflichen Alltag integrieren. Der Kreis der Teilnehmer wächst stetig (Infos bei annegret.warnecke@oracle.com).

- ADF Project Sessions: Eine fünfteilige, aufeinander aufbauende Workshop-Reihe, durchgeführt von erfahrenen Entwicklern und Projektleitern (siehe http://apex.oracle.com/pls/apex/f?p=38040:1). Sie richtet sich an Entwickler, Projektleiter und Architekten. Der Teilnehmer soll die Entwicklung von Rich-Internet-Applikationen mit dem Oracle Application Development Framework (ADF) kennenlernen, insbesondere die folgenden Punkte:

  - Applikationsplanung
  - Vorgehensmodell im Projekt
  - Entwicklung der Geschäftslogik
  - Gestaltung des User Interface
  - Deployment
  - Umsetzung von Sicherheitsanforderungen
  - Skalierbarkeitskonzepte

- XING-Gruppe „Oracle ADF Community“ (siehe http://www.xing.com/net/adfcomm/): Der Zugang zur Gruppe steht allen Interessierten offen und erfordert lediglich die Basis-Mitgliedschaft bei XING.

- Seit der DOAG-Konferenz 2009 finden regelmäßige Treffen von Oracle-Partnern statt, um Informationen und Erfahrungen auszutauschen und um weitere Aktivitäten zu planen.

Die ADF-Community sammelt derzeit Fragen für den Slot „Q&A panel with Oracle Application Tools Product Management“, der im Rahmen der DOAG 2011 Konferenz und Ausstellung in Nürnberg stattfinden wird. Es handelt sich dabei um ein Podiumsgespräch, in dem sowohl vorbereitete als auch spontane Fragen aus dem Publikum beantwortet werden. Die Teilnahme haben bisher bekannte und einflussreiche Persönlichkeiten aus dem Oracle-Development zugesagt:

- Bill Pataky, Vice President Product Management
- Duncan Mills, Senior Director Oracle Development
- Grant Ronald, Senior Group Product Manager

Somit bietet sich die Chance, Fragen, Wünsche und Anregungen bezüglich der breiten Palette der Oracle-Middleware-Development-Tools (JDeveloper, ADF, Oracle Enterprise Pack for Eclipse, NetBeans, Oracle Forms/Reports/Designer, JavaFx etc.) direkt an die Verantwortlichen des Oracle Developments zu richten. Dabei können sowohl technische als auch Marketing-, Support- oder Lizenz-Aspekte angesprochen werden. Zur Vorbereitung der Veranstaltung können bis spätestens zum 1. November 2011 Fragen per E-Mail an juergen.menge@oracle.com geschickt werden.

Dr. Dietmar Neugebauer,
Vorstandsvorsitzender der DOAG

Fit für die Zukunft: Neustrukturierung der DOAG-Vereinsorganisation

Der Vorstand der DOAG hat eine Neuorganisation beschlossen. Um der breiteren Oracle-Produktpalette besser gerecht zu werden und um die Mitglieder besser informieren zu können, gliedert sich der Verein in vier eigenständige Communities, die bestimmte Themenbereiche repräsentieren:

- Datenbank
- Development und DWH
- Infrastruktur und Middleware
- Business Solutions

Bereits auf der Beiratssitzung im Februar 2011 zeichnete sich die Notwendigkeit ab, die DOAG nach Themen neu zu strukturieren. Zwei Arbeitsgruppen haben daraufhin auf Basis der Vereinssatzung und der Ziele der DOAG Vorschläge für die Neuausrichtung der Organisation erarbeitet. Die Ergebnisse wurden in mehreren Vorstandssitzungen abgestimmt und am 15. Juli 2011 vom Vorstand beschlossen.

Am 9. September 2011 stellte der Vorstand die Neuorganisation im Rahmen einer außerordentlichen Sitzung dem DOAG-Beirat vor. Sie fand eine große Zustimmung, sodass gleich die einzelnen Community-Leitungsteams gebildet wurden und diese ihre Arbeit aufnahmen.

Die Communities

Kern der Neuausrichtung sind die vier Communities. Diese werden aus mehreren SIGs gebildet, die gemeinsam bestimmte Themen adressieren. Der Vorstand hat basierend auf den positiven Erfahrungen mit der Business Solutions Community, die bereits Ende 2010 ins Leben gerufen wurde, drei weitere Communities eingerichtet: die Datenbank Community, die Development und DWH Community sowie die Infrastruktur und Middleware Community.

Der Vorstand hat auch die Community-Leiter benannt: Es sind Christian Trieb für die Datenbank Community, Stefan Kinnen für die Development und DWH Community sowie Björn Bröhl für die Infrastruktur und Middleware Community. Die Business Solutions Community wird bereits seit deren Einrichtung im vergangenen Jahr von Dr. Frank Schönthaler geleitet. Dem Vorstand war es bei diesem Vorgehen besonders wichtig, dass jede Community von einem Experten geleitet wird, der auch aus dem jeweiligen Fachgebiet kommt.

Der DOAG-Vorstand und die Leiter der Communities bilden zusammen die DOAG-Leitung. Dieses neu eingeführte Gremium stellt zukünftig den strategischen Kopf der DOAG dar. Sie entscheidet über alle Community-übergreifenden Themen und sichert die Konsistenz der Arbeit in der gesamten DOAG. Darüber hinaus sorgt sie dafür, dass alle relevanten Themen in der DOAG abgedeckt und den Communities zugeordnet sind. Der DOAG-Leitung sitzt der Vorstandsvorsitzende der DOAG vor.

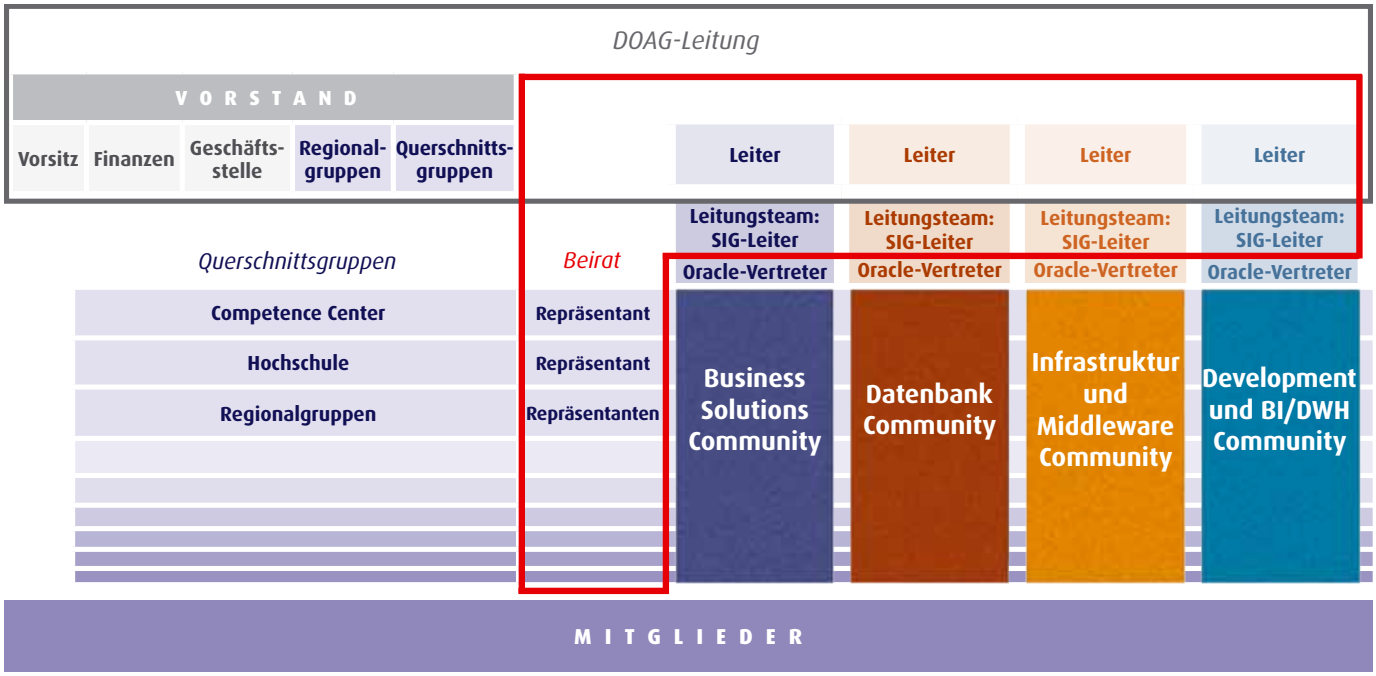
Der Leiter einer Community benennt die weiteren Mitglieder seines Community-Leitungsteams. Insbesondere die SIG-Leiter sind Mitglied dieses Community-Leitungsteams, hinzu kommen ein Ansprechpartner von Oracle und weitere berufene Mitglieder. Die Definition der Ziele und Aktivitäten sowie die weitere Gliederung der Community liegen in der Verantwortung der Community-Leitung.

Die Querschnittsgruppen

Regionalgruppen, Competence-Center und Hochschulgruppen sind Querschnittsgruppen in der neuen DOAG-Struktur. Sie laufen thematisch über mehrere oder alle Community-Themen. Diese Gruppen erhalten zukünftig noch mehr Bedeutung. Die Zusammenarbeit zwischen Querschnittsgruppen und den einzelnen Communities findet eng vernetzt statt. Ein Regionalleiter wird daher in der neuen Organisation zum regionalen Repräsentanten der DOAG aufgewertet. Er ist erster Ansprechpartner für die Mitglieder und Interessenten in einer Region und wird in alle Aktivitäten der DOAG in seiner Region eingebunden.

Der Vorstand

Die Aufgaben des Vorstands konzentrieren sich zukünftig auf die satzungsgemäß vorgegebene Verantwortung für Finanzen und die Geschäftsstelle sowie auf die Steuerung der Querschnittsthemen. Darüber hinaus ist der Vorstand für die Community-übergreifende Zusammenarbeit zuständig. Er klärt die Zuordnung der Themen zu den Communities und stellt sicher,



Die Neuorganisation der DOAG im Überblick

dass die Arbeit in den Communities im Sinne des Vereins funktioniert. Da sich die im Vorstand verbliebenen Zuständigkeiten deutlich verringern, wird der nächsten Mitgliederversammlung vorgeschlagen, die Zahl der Vorstandsmitglieder von heute acht auf fünf zu reduzieren.

Vorteile für die Mitglieder

Die neue Organisation bringt eine Menge an Vorteilen für die Mitglieder der DOAG. So sind die Interessen der Anwender themengerecht in den einzelnen Communities adressiert. Dies erleichtert das Networking und den gezielten Erfahrungsaustausch. Die DOAG kann damit jedes Thema gezielt an die entsprechende Zielgruppe adressieren.

Durch die Community-Struktur sind alle Oracle-Themen gleichwertig in die Vereinsarbeit eingebunden. Das bedeutet, dass auch für neue Themen, für die es noch wenige Interessenten gibt beziehungsweise diese für die DOAG erst gewonnen werden müssen, eine hohe Sichtbarkeit entsteht. Dies hat die Business Solutions Community in diesem Jahr schon bewiesen. So ist es gelungen, die Zahl der Teilnehmer an der DOAG 2011 Applications von 188 im Vorjahr auf 427 Teilnehmer mehr als zu verdoppeln.

Die Inhalte der Themen werden von Community-Leitern und ihren Teams getrieben, die als Experten die Bedürfnisse der Anwender gut kennen. Damit sind die inhaltlichen Schwerpunkte der DOAG sichtbarer und die Qualität der fachlichen Arbeit wird deutlich gesteigert. Im Gegenzug ist die Vorstandsarbeit weniger inhaltlich und stattdessen mehr koordinativ, organisatorisch und strategisch.

Das neue DOAG-Internet

Parallel zur Neustrukturierung hat die DOAG einen neuen Web-Auftritt entwickelt. Dieser ist bereits entsprechend der neuen Struktur gegliedert. Auf www.doag.org und bsc.doag.org finden Sie weitergehende Informationen zur neuen Struktur – in einem neuen Layout, übersichtlich und informativ.

Die Teilnehmer der Beiratssitzung am 9. September 2011

Wir begrüßen unsere neuen Mitglieder

Firmenmitglieder

Georg Bertler	Tognum AG
Roland Ehry	Tognum AG
Stefan Ring	Tognum AG
Thomas Gutacker	Tech Springer GmbH
Andreas Schulz	Tech Springer GmbH
Gustav Müller	Bayern Invest Kapitalanlagegesellschaft mbH

Persönliche Mitglieder

Martin Frech	Paul Abbing
Stefan Sack	Tilo Metzger
François Lange	Franz Drey
Horst Heineck	Werner Wendt
Thomas Starlinger	Jörg Weber
Holger Bartnick	Andreas Tophofen
Yann Neuhaus	Alexander Kleber
Hervé Schweitzer	Volker Klös
Georg Konopik	Volker Silinus

Franz Hüll, DOAG-Vorstand und Leiter des Competence-Centers Securityfragen

„Sicherheit kostet meistens Bequemlichkeit“

Daten so zu sichern, dass sie nicht verloren gehen oder in fremde Hände gelangen – das ist die Herausforderung eines jeden Datenbank-Administrators. Dabei ist es Konsens: 100 Prozent Sicherheit gibt es nicht. Doch wer besser informiert ist, kann auch besser vorbeugen. Oftmals zählen nur drei bis sieben Prozent aller gespeicherten Daten zu den „Kronjuwelen“ einer Firma. So nennt man die Daten, die für ein Unternehmen überlebenswichtig sind.

In der SIG Security am 7. September in Leipzig, hat Franz Hüll, DOAG-Vorstandsmitglied und Leiter der SIG Security, diverse Aspekte dieser komplexen Thematik unter die Lupe genommen. Für Interessierte, die beiden Veranstaltungen nicht beiwohnen konnten, hat die DOAG die zwei Tage zusammengefasst.

Jedes Sicherheitssystem kann umgangen werden. Dies meint jedenfalls Alexander Kornbrust von der Red Database Security GmbH in seinem Vortrag über Forensik. Seine Erfahrung habe gezeigt, dass Angreifer meistens von Innen kommen. Oftmals nehmen es Mitarbeiter mit dem Datenschutz nicht so erst. Neugier hat schon mal den einen oder anderen dazu gebracht, zu erforschen, was denn der Chef verdient. Das ist ein Verstoß gegen das Bundesdatenschutzgesetzt und ist strafbar. Doch wen kümmert es?

Das kriminelle Potenzial von den eigenen Mitarbeitern sollten Unternehmer und CIOs nicht unterschätzen. Besonders IT-versierte Mitarbeiter tendierten dazu, wenn sie das Unternehmen verlassen, Daten mitzunehmen. Dann gibt es auch noch die „Spielkinder“ – diese Mitarbeiter, die ohne böse Absichten Hacker-Tools oder Hintertüren gegen die Produktion anwenden. Einfach so aus Spaß, weil sie es schon immer mal ausprobieren wollten. Erst dann kommen die externen Hacker, die organisierte Kriminalität und die Geheimdienste. Dabei seien Hacker oftmals gut erkennbar, weil sie sich immer besonders coole Benutzernamen vergeben, wie etwa HappyHacker.

Geheimdienste hingegen verwenden oft die größte Schwachstelle eines Unternehmens: ihre Mitarbeiter. Ob Naivität, Auskunftsfreudigkeit, persönliche Enttäuschungen und Ressentiments oder sogar Stolz und Patriotismus – es gibt für einen Mitarbeiter viele Gründe, eine Information weiterzugeben, die er geheim halten sollte.

Während des Kalten Krieges praktizierten Regierungen Spionage hauptsächlich aus politischen Gründen. Inzwischen hat sich das Interesse verlagert: Regierungen betreiben zunehmend Industriespionage und konzentrieren sich immer mehr auf Gebiete der Wirtschaft, Wissenschaft und Technik. Dies betrifft vor allem die Branche der regenerativen Energien, die Informations- und Kommunikationstechnik und die Rüstungsindustrie. In diesem Bereich sind die aktivsten Länder die Volksrepublik China und die Russische Föderation, sagt Andrea Müller vom Bundesamt für Verfassungsschutz (BfV) in ihrem Vortrag zur Wirtschaftsspionage.

Besonders Russland gehe laut Müller dieser Aktivität sehr offensiv nach, was unter anderem daran liegt, dass die Beschaffung von Informationen in der russischen Verfassung verankert ist. Der damalige Ministerpräsident Wladimir Putin sagte 2007 in einer Rede: „Unser Nachrichtendienst muss seine Anstrengungen verstärken, um die russische Wirtschaft und die Interessen russischer Unternehmen im Ausland aktiver zu unterstützen.“

Der Aufwand, den diese Länder zur Beschaffung von Wirtschaftsgeheimnissen betreiben, ist manchmal beachtlich: Nachrichtendienstoffiziere werden in diplomatische Mission geschickt oder in Medienorgane eingeschleust. Manchmal gründen Nachrichtendienste sogar Tarnunternehmen, die sich dann mit verlockenden Aufträgen an Firmen wenden, die im Besitzt vom wertvollen Wissens sind. Sollte ein Nachrichtenoffizier in die Firma eingeladen werden, macht er womöglich eine Besichtigung des Firmengeländes, die er nutzt um Maschinen unter allen Blickwinkeln abzufotografieren oder sich auf dem Weg zur Toilette in den Serverraum zu verirren.

Die Nachrichtendienste nutzen auch sogenannte Non-Professionals – Studenten, Praktikanten, Gastprofessoren, die sich nur für eine begrenzte Zeit in Deutschland aufhalten und aufgrund ihrer Position an Informationen herankommen. Diese Methode wendet China gern an: „Der Patriotismus ist in China so stark, dass diese Leute nicht mal unter Druck gesetzt werden müssen“, meint Müller.

Natürlich nimmt auch die elektronische Wirtschaftsspionage zu. Ein Großteil der Angriffe erfolgt über E-Mails, die Trojaner im Anhang, in einem verlinkten Dokument oder verlinkter Webseite enthalten. Der Absender ist dabei absolut unauffällig: Meistens handelt es sich um eine nur leicht gefälschte E-Mail-Adresse etwa von einem wohlbekannten Partner oder Mitarbeiter, die nur ein Underscore mehr beinhaltet. Kaum sichtbar, wenn man nicht aufpasst. Der Inhalt ist auf die Person zugeschnitten, die die E-Mail aufmachen soll: Es sind faktische Ausschreibungen, produkt- oder geschäftsbezogene Texte. Es wird alles unternommen, um das Interesse zu wecken. Gegen diese Art der Wirtschaftsspionage hilft nur eins: Aufmerksamkeit. Deswegen ist die Öffentlichkeitsarbeit der Bundesbehörde besonders wichtig.

Im Datenbank-Bereich sind die Gefahren jedoch nicht auf E-Mails begrenzt. Die Möglichkeiten, an Informationen heranzukommen sind vielfältiger und Hacker zeigen oftmals viel Kreativität. Eine Option, um seine Daten zu schützen, ist in diesem Zusammenhang die Verschlüsselung. Die

SFNT Germany GmbH bietet mit einer Reihe von Hardware-Sicherheitsmodulen (HSM), die Datenbank-Administratoren ermöglichen, die verschlüsselten Daten von der eigentlichen Kryptografie zu trennen. Der Master Key wird bei diesem Ansatz in ein Stück Hardware abgelegt. Im Banking-Bereich sowie in Behörden sei es bereits eine beliebte Methode, sagt der Referent Andreas Gatz von SFNT Germany.

Weiter besteht die Möglichkeit, nur eine Spalte zu verschlüsseln, was im Falle eines Audits die Arbeit erleichtere, da die sensiblen Daten dann nicht mehr im Wege stünden. Für ein Stück mehr Sicherheit gibt es die Technologie der Tokenization, mit der sensible Daten durch eine Art Alias, ein sogenanntes „Token", ersetzt werden. Die sensiblen Daten werden dann offshore gespeichert. Dieses Verfahren ist besonders geeignet für kurze Daten wie Kreditkarten- oder Sozialversicherungsnummern.

Natürlich kann man sich gegen Angriffe schützen. Doch jedes Sicherheitssystem kann umgangen werden und Hilfe bekommen die Hacker ganz einfach im Internet. „Google ist dein Freund", meint Kornbrust. Da fände man nämlich alles an Informationen, was man so braucht, um einen solchen Angriff durchzuführen. Das Gute ist: Angreifer hinterlassen Spuren. Kornbrust hat sich in seinem Vortrag auf forensische Daten konzentriert, die auch ohne Einschaltung des Auditings vorhanden sind. Es sind Listener.log, Tabellen, Redo Logs oder Datenbank-Blöcke.

Beispiele für typische Spuren sind der Missbrauch von Kennungen, das Erraten von Passwörter oder Benutzernamen, der Export einer Datenbank oder eines Schemas sowie die Verwendung von nicht-autorisierten Programmen oder Anwendungen. Wer zum Beispiel in der Spalte „sql-text" der Tabelle „sys.wrh$_sqltext" einen Insert oder Delete in einer User-Session vorfindet, hat vielleicht eine heiße Spur. Ähnlich interessant ist die Spalte „Icount" in „sys.user$": Ist die Anzahl von ungültigen Login-Versuchen in dieser Spalte besonders hoch oder wurde nach einem gültigen Login das Passwort zurückgesetzt, ist zu vermuten, dass ein Angriff stattgefunden hat.

Schwierig sei herauszufinden, wann und wo Daten manipuliert worden sind. Wenn man interessante Spuren gefunden hat, ist es dann einfach. Sobald der Zeitpunkt feststeht, können per logminer die ausgeführten Kommandos gefunden werden. Deswegen ist das Erstellen einer Timeline (auch „Bauertrick" genannt) ein triviales, aber nützliches Mittel, um Spuren nachzugehen.

Wer die Unterstützung von einer Software-Lösung haben möchte, kann ein Database Activity Monitoring einsetzen. Für Thomas Drews und Eckard Bogner von Imperva Inc. ist es wichtig, die gespeicherten Daten nach Wichtigkeit einzustufen. Ihre Lösung, Imperva SecureSphere Database Monitoring ermöglicht, durch netzwerkbasierte Scans Assets zu finden und neu auszuweisen. So kann eine Datenklassifizierung stattfinden. Die Software erkennt auch Schwachstellen und ermöglicht ein zentrales Management der Risiken. Auch das Erfassen und die Analyse der Berechtigungen werden mit der Lösung einfacher. Zusätzlich zu der Rechtevergabe erkennt Imperva auch den physischen Nutzer, der sich über eine Applikation einloggt.

Eine ähnliche Lösung bietet IBM mit seinem InfoSphere Guardium Database Security. Die Datenbanküberwachung erfolgt in Echtzeit und ermöglicht nicht nur die Protokollierung eines Events, sondern auch eine aktive Zugriffsbeschränkung in Echtzeit, betont Holger Seubert von IBM Deutschland GmbH.

Die Software von McAfee Database Activity Monitoring funktioniert ähnlich. Im Gegensatz zu Anti-Virus-Programmen, die auf Blacklists basieren, funktioniert die Datenbanklösung auf dynamischem Whitelisting, das definiert, welche Programme aufgeführt werden sollten. Mit der Lösung haben Datenbank-Administratoren zudem die Möglichkeit, mit der Installation von Patches zu warten und das Virtual Patching zu nutzen. So können sie ihr System vor bekannten oder Zero-Day-Schwachstellen ohne Downtime oder Änderungen im Code schützen.

Natürlich hat auch Oracle ein entsprechendes Produkt: Die Oracle Database Firewall ist überwacht Datenbank-Aktivitäten auf dem Netzwerk in Echtzeit. Die Besonderheit der Lösung ist laut Heinz-Wilhelm Fabry von Oracle Deutschland B.V. & Co. KG ihre hochpräzise SQL-basierte Grammatik. „Die Engine versteht SQL-Sprache", meint der Referent, was ihr ermögliche, nicht autorisierte Transaktionen zu blockieren, bevor der Angriff die Datenbank erreicht.

Wenngleich diese Lösungen die Arbeit eines Datenbank-Administrators erleichtern können, sind sie kein Wundermittel. Hacker überlegen sich immer wieder neue Wege, um an Daten heranzukommen. Deswegen muss die Sicherheit an der Basis gewehrleistet werden, meint Müller. Darüber hinaus sei es besonders wichtig, die eigenen Mitarbeiter für diese Thematik zu sensibilisieren. Welche Daten müssen besonders geschützt werden? Welche Mitarbeiter dürfen darauf zugreifen? Welche Mitarbeiter greifen tatsächlich darauf zu? Dies sind die Kernfragen, die ins Sicherheitskonzept einfließen sollen. Dass ein strenges Sicherheitskonzept in der Praxis negative Auswirklungen haben kann, kommentiert Müller so: „Sicherheit kostet meistens Bequemlichkeit".

Mylène Diacquenod
mylene.diacquenod@doag.org

Errata

In der letzten Ausgabe muss es auf Seite 33 in der Tabelle unter „SQL Server 2008 R2 Express" bei Datenbankgröße heißen „10 GB" und unter „IBM DB 9.7 Express-C" bei Datenbankgröße „keine Beschränkung".

Auf Seite 38 oben rechts war die Bedeutung der Smilies fehlerhaft. Richtig ist: ☺ optimal / komfortabel, :| aufwändig / lückenhaft und 😑 sehr aufwändig / unzureichend.

Wir entschuldigen uns für das Versehen.