

IT-SICHERHEIT

Management der Daten- und Netzsicherheit



Sicherheit
durch Provisioning

Intrusion
Detection System

Absicherung
von Web-Servern

IT-Security-Management

Public-Key-Infrastruktur

Impressum

IT-SICHERHEIT

Management
der Daten- und Netzsicherheit

Verlag:

DATAKONTEXT-FACHVERLAG GmbH
Augustinusstraße 9d, 50226 Frechen
Telefon: (0 22 34) 9 66 10-0
Telefax: (0 22 34) 9 66 10-9
Internet: www.datakontext.com

Redaktion:

Ralf Herweg (Chefredakteur)

Ursula Coester, Dr. Peter Münch,
Wilhelm Kruth, Thomas Barthel,
Prof. Dr. Reinhard Voßbein,
Bernhard Adamski, Michael Hange,
Ass. iur. Jörg Becker
Telefon: (0 22 34) 9 66 10-0
Telefax: (0 22 34) 9 66 10-9
Email: herweg@t-online.de

Anzeigenleitung:

Anja Rohde, Datakontext Anzeigen
Marketing GmbH & Co. KG
Telefon: (0 22 34) 9 66 10-14
Telefax: (0 22 34) 9 66 10-9
Email: rohde@datakontext.com
z.Z. gilt Anzeigenpreisliste Nr. 1/2002

Abonnement:

Jahresabonnement:
EUR 60,- (für Studenten, RDV-Abonnen-
ten und GDD-Mitglieder: EUR 50,-)
Einzelheft: EUR 15,- zzgl. Versandkosten

Erscheinungsweise: sechs Ausgaben

Satz: Satzstudio Pohl, Bonn

Druck: Druckerei Roth, Solingen

© DATAKONTEXT-FACHVERLAG GmbH

Mit Namen gekennzeichnete Beiträge stellen nicht unbedingt die Meinung der Redaktion oder des Verlages dar. Für unverlangt eingeschickte Manuskripte übernehmen wir keine Haftung. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Verfasser alle Rechte, einschließlich der weiteren Vervielfältigung zu gewerblichen Zwecken. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektrischen Systemen.

Titelbild:

Frau Hennebühl, Verlag

Beilagen:

DATAKONTEXT-FACHVERLAG GmbH,
Frechen, datakontext-tagungen
GmbH & Co. KG, Frechen,
TÜV-Akademie Rheinland GmbH, Köln,
EUROFORUM Deutschland GmbH,
Düsseldorf,
Ostdeutscher Sparkassen- und
Giroverband, Potsdam

8. Jahrgang 2002, ISSN 0948-7328

Inhaltsverzeichnis

- ▶ **Editorial**
- Public-Key-Infrastruktur 3
- ▶ **Kurzmeldungen** 6
- ▶ **Provisioning**
- Sicherheit durch Provisioning** 12
- Ergebnisse des SIZ-Projektes
- „Fortschreibung Verzeichnisdienste in der Sparkassen Finanzgruppe“
- Michael Rogulla und Horst Walther, Bonn*
- ▶ **Management**
- Sicherheit muss in der Unternehmenskultur verankert sein** 15
- Gespräch mit Dr. Heinrich Kersten, Bonn*
- ▶ **CISO**
- Chief Information Security Officer (CISO)** 17
- Tätigkeitsschwerpunkte und Erfahrungen –
- ▶ **IDS**
- IDS am Wendepunkt** 20
- Aktuelle Entwicklung bei Intrusion Detection Systemen –
- Günter Busch, Düsseldorf*
- ▶ **Recht** 25
- Ass. iur. Jörg Becker, Bonn*
- ▶ **E-Business**
- Absicherung von Web-Servern** 26
- Sicherheit von E-Business-Systemen und Web-Applikationen
- Stefan Strobel, Heilbronn*
- ▶ **Literatur**
- Blick in unsere Fachbibliothek** 30
- ▶ **PKI**
- Mit Brief und Siegel** 32
- Sichere E-Mail mit Hilfe der Microsoft Certificate Services
- Jörg Folz und Uwe Wöhler, Hallbergmoos*
- Die Zukunft von Public-Key-Infrastrukturen** 38
- Dr. Norbert Pohlmann, Aachen*
- ▶ **IT-Budget**
- IT-Budgets – Lust oder Frust?** 44
- Anja Rohde, Frechen*
- ▶ **Unternehmen**
- Infodas** 45
- Software made in Cologne
- ▶ **Produktneuheiten** 46
- Dr. Peter Münch, Hamm*
- ▶ **Termine** 50

Sicherheit durch Provisioning

Ergebnisse des SIZ-Projektes „Fortschreibung Verzeichnisdienste in der Sparkassen-Finanzgruppe“

Michael Rogulla und Horst Walther, Bonn*

Erhöhte Sicherheitsanforderungen bei gleichzeitig steigender Komplexität der Benutzer-Administration schaffen in vielen Unternehmen aktuell einen besonderen Handlungsdruck. Die seit etwa zwei Jahren angebotenen Provisioning Systeme bieten hierbei die Möglichkeit, die Vorgänge der Vergabe, des Entzugs und des Reportings von Benutzerberechtigungen zu automatisieren und in einen Workflow einzubinden. Damit wird eine häufige Fehlerquelle, nämlich die manuelle Handhabung von Benutzerrechten, stark verkleinert.

Das Informatikzentrum der Sparkassenorganisation GmbH (SIZ) hat das Thema Provisioning im Rahmen der Fortführung seiner Aktivitäten zu Verzeichnisdiensten für die S-Finanzgruppe aufgearbeitet und stellt in diesem Artikel kurz die Ergebnisse zum Thema Provisioning vor. Die weiteren Ergebnisse aus dem Projekt zu Verzeichnisdiensten werden in einem später erscheinenden Artikel dargestellt.

1 Die Situation

Als zu Beginn dieses Jahres ein Hersteller von Provisioning Software zu einem Wettbewerb aufrief, die ungewöhnlichsten „Provisioning-Horror-Stories“ zu erzählen, kamen erstaunliche Kuriositäten zusammen:

- In einem Fall wurden einem Mitarbeiter, der in verantwortlicher Stellung zu einem Konkurrenzunternehmen wechselte, weder Zutrittskarten noch Rechnerzugriffsrechte

entzogen. Bei entsprechender Absicht hätte er seinem Ex-Arbeitgeber massiv schaden können.

- Realen Schaden angerichtet hatte in einem zweiten Fall ein ehemaliger Netzwerkadministrator, der sich selbständig gemacht und noch Jahre später fleißig die Rechnerkapazität (und wer weiß was noch?) seines ehemaligen Arbeitgebers genutzt hatte.
- In einem kuriosen Fall wurde ein Haus mit dem besonderen Vorzug eines kostenfreien Telefonanschlusses zum Kauf angeboten. Der Vorgänger des Hausbesitzers war ein ehemaliger Manager einer Telefongesellschaft. Bei seinem Ausscheiden war der Entzug seiner Privilegien schlicht vergessen worden.

Diese drei Beispiele zeigen deutlich, dass in der Praxis die Privilegien und Zugriffsrechte der Benutzer nicht immer wirksam verwaltet werden. Insbesondere werden häufig einmal erteilte Rechte nur verspätet oder gar nicht mehr zurückgenommen. Allgemein gesagt sind Verzögerungen (z.B. durch Benutzung eines Umlaufformulars) bei der Vergabe von Benutzerrechten zwar ärgerlich, aber nicht unbedingt sicherheitskritisch, wogegen der verspätete Entzug von Zugriffsrechten fatale Folgen haben kann.

2 Die kritische Funktionalität

Bei der wirksamen Verwaltung dieser Benutzerzugriffsrechte helfen seit kurzem sogenannte Provisioning Systeme.

- Provisioning heißt „die Versorgung von neuen Mitarbeitern mit all den Zugangsrechten zu den DV-Ressourcen, die sie für ihre Tätigkeit

benötigen“. Man spricht auch von „Ressource Provisioning“, „User Provisioning“ oder, im Trend der Zeit, von „eProvisioning“. Vorrangig geht es dabei um die automatisierte Zuweisung von Berechtigungen zur Benutzung von IT-Systemen.

- De-Provisioning, das Gegenstück dazu, ist fast noch bedeutsamer: die automatisierte Unterstützung von Wechseln in der Geschäftsrolle (Beförderungen, Abteilungswechsel) und beim Ausscheiden eines Mitarbeiters im Unternehmen und damit verbunden dem erforderlichen schnellen Entzug von Rechten.
- Weiterhin gibt es noch das so genannte „Reverse Provisioning“, bei dem, z.B. für Audit-Zwecke, ein Status der Zugriffsrechte zu einem bestimmten aktuellen oder in der Vergangenheit liegenden Zeitpunkt ermittelt wird.

3 Der Handlungsdruck

Die Aufgabe der Benutzerverwaltung ist seit jeher für Unternehmen von hoher Bedeutung und war bislang mit hohem administrativem Aufwand verbunden (manuelle Eingriffe oder Versand von eMails mit der Aufforderung Änderungen vorzunehmen etc.). Dies ist weder im Hinblick auf den

INHALT:

- 1 Die Situation
- 2 Die kritische Funktionalität
- 3 Der Handlungsdruck
- 4 Anforderungen und Anbieter
- 5 Identity Management
- 6 Aspekte des Einsatzes
- 7 Empfehlung

* Michael Rogulla ist Produktmanager im Ressort Sicherheitstechnologie des Informatikzentrums der Sparkassenorganisation GmbH (SIZ) in Bonn. Dr. Horst Walther ist Geschäftsführer der SiG Software Integration GmbH.

getriebenen Aufwand noch auf die erreichte Geschwindigkeit befriedigend. Gleichwohl ist sie in vielen großen Unternehmen nach wie vor nicht zufriedenstellend gelöst. Diese unerfreuliche Situation wird durch aktuelle Entwicklungen noch verschärft:

- Steigende Dynamik – Der Wechsel wird zum Normalzustand. Mitarbeiter bleiben für kürzere Zeit als früher mit einer Geschäftsrolle verknüpft. Sie wechseln Abteilungen, arbeiten in Projekten oder gehen für einige Wochen zu einer Niederlassung. Normal ist auch der zeitweilige Einsatz externer Kräfte, die meist Zugriff auf bestimmte interne Ressourcen benötigen.
- Stärkere IT-Durchdringung – Büroarbeit bringt heute fast immer die Nutzung von IT-Ressourcen wie PC, e-Mail, Firmen-Intranet mit sich.
- Höheres Sicherheitsbewusstsein – Erfahrungen mit den Gefahren des Internet, die hohe IT-Abhängigkeit und nicht zuletzt aktuelles Weltgeschehen haben zu einer erhöhten Security Awareness geführt. Ein „Leih’ mir ‘mal Dein Passwort!“ wird heute nicht mehr akzeptiert.
- Externe Auflagen – Die elektronische Verkettung von Geschäftsprozessen zu einem Online Business birgt Risiken. Behördliche Regelungen nehmen sich immer intensiver dieser Risiken an und definieren entsprechende Anforderungen. Beispielsweise müssen sich Banken nach den Plänen des Basel Accord II darauf einrichten, für die operativen Risiken (operational risks) ihrer internen Abläufe Rückstellungen zu bilden. Diese lassen sich nur dann reduzieren, wenn nachgewiesen werden kann, dass die internen Abläufe geringere Risiken bergen als pauschal unterstellt wird.

4 Anforderungen und Anbieter

Wo das bisher übliche „händische“ Vorgehen in der Vergangenheit gera-

de noch akzeptabel war, wird man künftig schnellere und wirtschaftlichere Vorgehensweisen benötigen.

In der Praxis hängen Arbeitsfähigkeit und Informationssicherheit häufig von Fleiß, Organisationstalent und Vertrauenswürdigkeit einiger weniger, häufig stark überlasteter Administratoren ab. Aber auch in gut organisierten Unternehmen ist beispielsweise ein automatisierter Abgleich der Zugriffsrechte aller – wesentlichen – Zielsysteme über Schnittstellenmodule, so genannte Konnektoren, heute noch selten realisiert.

Regelmäßige Audits aktueller und historischer Berechtigungen werden ebenfalls nur in den wenigsten Fällen durchgeführt, da diese aufgrund der fehlenden Automatisierung mit einem hohen Aufwand verbunden wären. Reverse Provisioning könnte hier für eine entscheidende Verbesserung sorgen.

In der Sparkassen-Finanzgruppe sehen sich die Institute mit der Situation konfrontiert, dass sie neben der Verwaltung von Zugriffsrechten auf internen Systemen auch verantwortlich sind für die Zuweisung solcher Rechte auf Systemen, die bei einem externen Dienstleister stehen. Eine Vereinheitlichung der Berechtigungsdadministration wäre hier von Vorteil. Die Installation und der Betrieb von Provisioning-Systemen sowie die technischen Aspekte (und nur diese) der Festlegung von Berechtigungsprofilen können auch von einem betreuenden Verbandsrechenzentrum wahrgenommen werden. Die inhaltliche Definition der Berechtigungsprofile auf Basis der Geschäftsprozesse sowie die Zuweisung der einzelnen Mitarbeiter zu diesen Profilen jedoch gehört zu den hoheitlichen Aufgaben jedes einzelnen Institutes und muss daher auch bei diesem verbleiben. Es empfiehlt sich, soweit möglich, vordefinierte Templates zu verwenden, um so den damit verbundenen Aufwand zu minimieren. Weiterhin gehört zu den Aufgaben, die nicht an einen externen Dienstleister vergeben werden dürfen, die Auslösung des Prozesses zur Berechtigungsverga-

be und ggf. die gesonderte Zustimmung zur Vergabe von Einzelberechtigungen.

Aus Sicherheitsgesichtspunkten muss eine Provisioning-Lösung mindestens folgende Funktionen unterstützen:

- Policy-basierte Berechtigungsverwaltung. Das heißt, die Regeln, nach denen der Dienstleister zu verfahren hat, gibt das Institut vor.
- Berechtigungsevidenz: Die Institute haben die volle Transparenz der aktuellen Berechtigungssituation.
- Flexibler Genehmigungs-Workflow: Die Aktivierung einer Berechtigungsvergabe an einen Institutsmitarbeiter durch direkte oder höhere Vorgesetzte muss möglich sein.

Seit kurzem sind Werkzeuge auf dem Markt, die diese Aufgaben zufriedenstellend zu unterstützen versprechen. Anbieter solcher Systeme sind z.B. BMC, Access360, Business Layers, Courion, Systor, Thor, Waveset und M-Tech. Die Übernahme von Access360, einem der führenden Anbieter von User Provisioning Systemen, durch IBM im September 2002 macht deutlich, dass dieses Marktsegment inzwischen auch von den Großen der Branche für bedeutsam gehalten wird. Man erwartet eine weitere Konsolidierung einer Vielzahl kleiner und mittlerer Unternehmen.

5 Identity Management

Das unternehmensinterne Identity Management besteht aus drei Gruppen von Prozessen (siehe Abbildung 1):

- Identity Administration – Verwalten digitaler Identitäten von Personen, deren Beziehungen zur Organisationseinheit und die Zuweisung von Ressourcen. Die Prozesse des Provisioning implementieren die Funktionen der Zuweisung, Änderung und Auditierung.
- Community Management – Authentisieren, Bereitstellen / Publizieren und Autorisieren von Personen anhand ihrer digitalen Identitätsinformationen.

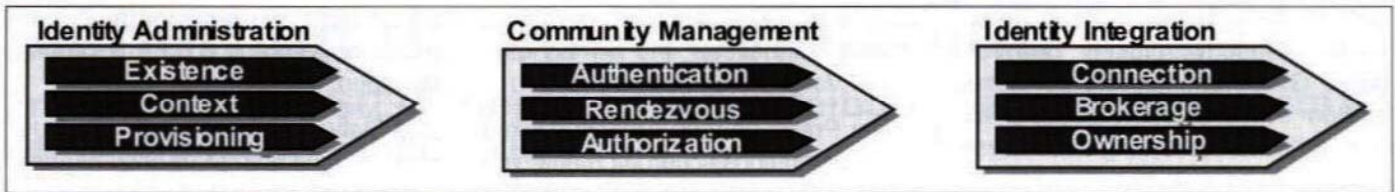


Abbildung 1: Prozessgruppen des Identity Management

□ Identity Integration – Mechanismen für die Aktualisierung und Synchronisation von digitalen Identitäten, die verteilt und teilweise redundant gehalten werden.

Die Aspekte des aktuell vieldiskutierten federated identity management, wie es Microsoft mit dem Passport-Dienst oder die Liberty Alliance behandeln und die primär auf die digitale Identität im Internet abzielen (B2C), sind nicht Gegenstand dieses Beitrages.

6 Aspekte des Einsatzes

Nach Aussagen der Gartner¹-Analysten ist die Einführung eines systemunterstützten Provisioning aktuell eine der wenigen IT-Investitionen, deren schnelle Amortisation unmittelbar nachgewiesen werden kann.

Gleichwohl sind Installation und Einrichtung mit erheblichem Aufwand verbunden. Insbesondere der Aufwand für Definition und Abstimmung von Mitarbeiterrollen im Unternehmen darf nicht unterschätzt werden und nimmt in Projekten oft eine unerwartet große Zeitspanne in Anspruch. Klar strukturierte und dokumentierte Prozesse sind eine notwendige Voraussetzung für die Ausarbeitung des Rollen- und Rechte-Modells. Diese Aspekte sollten im Vorfeld eines Provisioning Projektes angemessen berücksichtigt werden.

Provisioning Systeme lohnen sich aktuell typischerweise für größere Organisationen wie Landesbanken, größere Sparkassen oder Verbandsrechenzentren mit den von ihnen betreuten Instituten. Hier können sie sich dann aber in 1 bis 2 Jahren amortisieren und zu einem deutlich

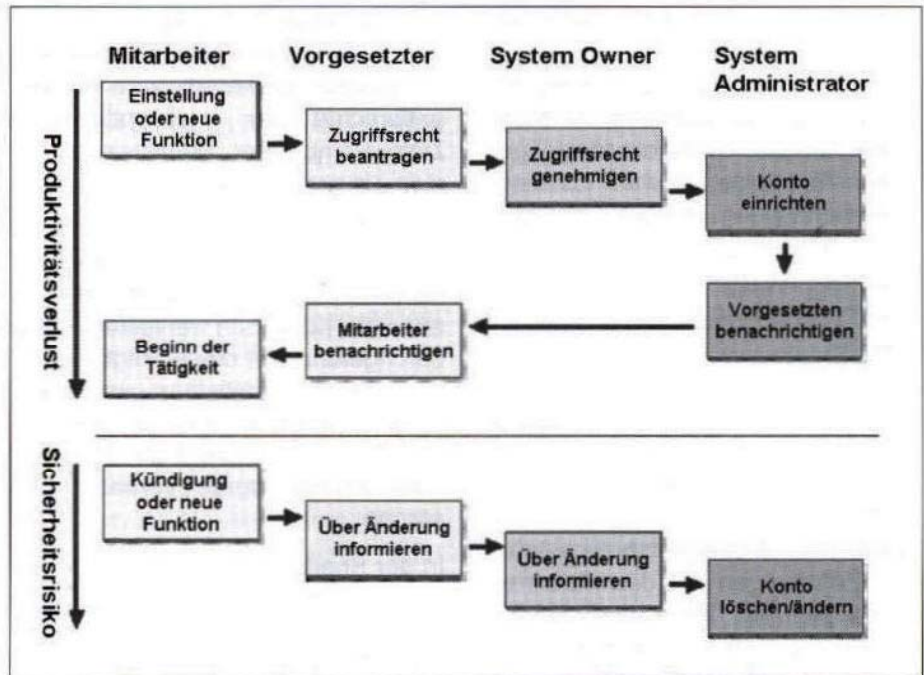


Abb. 2: Produktivitätsverlust und Sicherheitsrisiko (Quelle: M-Tech). Bei der manuellen Vergabe von Rechten entsteht eine Wartezeit für den Anwender und damit ein Verlust an Produktivität. Beim Entzug von Zugriffsrechten besteht während der Bearbeitungszeit die Gefahr eines unberechtigten Zugriffes.

höheren Sicherheitsniveau beitragen. Dieser Nutzen ist auch für kleinere und mittlere Institute erreichbar, wenn die Technik von den betreuenden Rechenzentren zur Verfügung gestellt wird. Bereitgestellte Mustervorlagen für Benutzer-Rollen, Berechtigungsprofile und Genehmigungs-Workflow können helfen, auch den fachlichen Definitionsaufwand in überschaubaren Grenzen zu halten.

Mit der OASIS-Initiative zur Definition der XML-basierten Provisioning Services Markup Language (PSML) liegt ein Entwurf vor, der ein standardisiertes Austauschformat für Provisioning-Informationen definiert. Das wird dann wichtig, wenn User Provisioning Systeme über Unternehmensgrenzen hinweg, etwa zu Lieferanten oder Kunden, wirken sollen. Auch Fu-

sionen und Unternehmensübernahmen erfordern in der Folge interoperable User Provisioning Systeme.

7 Empfehlung

Der Einsatz von User-Provisioning Systemen in Unternehmen der Finanzdienstleistungsbranche sollte erwogen werden. Einerseits hat der Handlungsdruck für viele Unternehmen stark zugenommen. Andererseits haben die angebotenen Systeme inzwischen Einsatzreife erlangt. Bei Einhaltung der oben geschilderten Hinweise und Maßnahmen lassen sich erhebliche Verbesserungen des Sicherheitsniveaus und eine Reduktion der Administrationsaufwände erzielen, sodass Investitionen in Provisioning Systeme auch in wirtschaftlich schwierigen Zeiten gerechtfertigt werden können. □

¹ „User Provisioning – Automating Accounts and Access“, 02. October 2002 – Roberta Witty