

*Immer auf der Hut.
Die U.S.S. Enterprise
ist bekannt für ihre
wirkungsvollen
Schutzmechanismen*

Den Zugriff im Griff

Quelle: Paramount Pictures / MAC

Moderne PLM-Systeme bilden das Rückgrat der Produktentwicklung in weltweit vernetzten Unternehmen. Doch bergen deren weitreichende Zugriffsmöglichkeiten erhebliche Gefahren in Hinsicht auf Datensicherheit und Know-how-Schutz. CIM Database von Contact Software antwortet darauf mit einem ausgefeilten regelbasierten Berechtigungssystem, das Zugriffsrechte automatisch an Rollen und Inhalte koppelt.

Während die allgemeine Bedrohung der Computersicherheit durch Angriffe anonymer Hacker aus dem Cyberspace auch in der Öffentlichkeit große Aufmerksamkeit genießt, ist der Schutz vor unerlaubten Zugriffen durch reguläre Systembenutzer eher ein Expertenthema geblieben. Bei Tausenden, über den ganzen Globus verteilten Benutzern eines unternehmenskritischen Informationssystems lauern hier jedoch die größten Gefahren. Denn der Feind sitzt in diesem Fall in den eigenen Reihen. Er muss

gar nicht erst einbrechen, sondern kommt offiziell durch die Vordertür, ordnungsgemäß angemeldet und ausgewiesen! Der beste Schutz vor Trojanern, Viren, Würmern und anderer Malware, die im Internet lauern und dem Angreifer Hintertüren öffnen sollen, nützt daher nicht viel, wenn die Hausaufgaben nicht gemacht werden. Unbedingt notwendig ist, klar zu definieren, wer auf welche Daten wie zugreifen darf und wer nicht. Hierzu bedarf es eines IT-Systems, das diese obligatorischen Zugriffsregelungen auf einfache Weise umsetzen und kontrollieren kann.

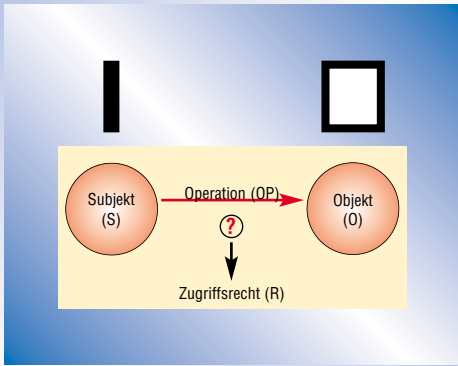
Bei der Einführung neuer IT-Sicherheitsmaßnahmen steht der (technische) Schutz geistigen Eigentums oftmals im Vordergrund. Dies freilich ist nur ein Aspekt. Allgemeiner formuliert lauten die Schutzziele: Sicherstellen der Integrität, Vertraulichkeit und Verfügbarkeit von Daten sowie der Verfügbarkeit von Systemfunktionen (siehe Glossar). Dateninte-

Rechteentzug sticht immer Rechtgewährung“

Achim Müller, Manager Strategic Product Development, Contact Software

grität und -vertraulichkeit sind nicht nur durch bewusste Angriffe von innen oder außen bedroht, sondern auch durch nachlässigen Umgang mit den Daten. Eine systematische Zugriffskontrolle nach zentralen Vorgaben kann dem vorbeugen und gehört deshalb zu den grundlegenden Sicherheitsmaßnahmen. Die folgenden Abschnitte widmen sich besonders dem Aspekt der Autorisierung. Eine ordnungsgemäße Identifizierung und Authentisierung von Benutzern werden vorausgesetzt und hier, wie auch andere grundlegende Sicherheitsmaßnahmen, nicht näher betrachtet.

Beispielszenario. Ein Automobilzulieferer hat mehrere Standorte in Deutschland mit fachbereichsübergreifenden Aufgaben, einen Entwicklungsstandort in Übersee sowie Produktionswerke in Osteuropa, Asien und Nordamerika. Als zentrale Informationsdrehscheibe für alle Unternehmensgliederungen fungiert ein PLM-System, das darüber hinaus auch Entwicklungspartnern im In- und Ausland Online-Zugang gewährt. Das PLM-System verwaltet neben den produktdefinierenden CAD-Daten und den daraus abgeleiteten Produktstrukturen sämtliche projekt- und prozessbegleitenden Daten und Dokumente aus Vertrieb, Entwicklung,



Quellen (3): Contact 2006

Zugriffskontrolle gehört zu den grundlegenden Sicherheitsmaßnahmen in IT-Systemen.

Musterbau, Werkzeugbau, Qualitätssicherung, Arbeitsvorbereitung, Fertigung, Service und Produktdokumentation. Das System unterstützt sowohl die kollaborative Erstellung der Daten und Dokumente im Rahmen von Entwicklungsprojekten als auch die Verteilung der geltungsgesicherten Projektergebnisse. Hierzu gehören auch kaufmännische und technische Betriebsgeheimnisse. Das Mengengerüst umfasst mehrere Millionen Dokumente und Teile, an die tausend Projekte sowie mehrere tausend Benutzer.

Im Spannungsfeld von Kooperation und Kontrolle – einerseits ist für die effiziente Kooperation mit den Partnern ein möglichst direkter Zugriff auf Informationen erforderlich, andererseits soll der Partner aber nur die jeweils für die Aufgabenerfüllung unbedingt erforderlichen Informationen erhalten – lautet die oberste Sicherheitsrichtlinie des Unternehmens: Zugriff auf Daten so weit wie nötig und so restriktiv wie möglich. Daraus wurden einige Detailregelungen für Dokumente abgeleitet:

Erstellung

- **Fachdokumente** (Dokumente bestimmter Kategorien) dürfen nur von Mitarbeitern der jeweils verantwortlichen Fachabteilung eingestellt und gepflegt (bearbeitet, freigegeben, fortgeschrieben) werden; Mitarbeiter von Kooperationspartnern werden als externe Mitarbeiter einer Fachabteilung geführt.
- **Projektbezogene Dokumente** dürfen nur von Mitgliedern des Projektteams eingestellt und gepflegt werden.
- **Dokumente** sind nur einem noch nicht abgeschlossenen Projekt zuweisbar und auch nur änderbar, solange das Projekt noch nicht abgeschlossen ist.
- **Projektstatusberichte** dürfen nur vom Projektleiter freigegeben werden.
- **CAD-Dokumente** dürfen nur von qua-

lifizierten Prüfern freigegeben werden.

- **Freigegebene Dokumente** sind nicht mehr änderbar oder löschbar; eine Fortschreibung ist nur als neue Dokumentversion möglich.

Bereitstellung

- **Dokumente** dürfen – sofern keine weitere Einschränkung definiert ist – von allen Benutzern gefunden werden (dies impliziert jedoch noch nicht das Recht, auf den Dokumenteninhalt zuzugreifen).
- **Dokumente** sind, abhängig von ihrer Kategorie und ihrer Zuordnung zu einer Produktgruppe, nur Mitarbeitern an bestimmten Standorten inhaltlich zugänglich (Herunterladen, Öffnen, Anzeigen von Neutralformaten). Für jede Dokumentkategorie ist definiert, welche Disziplinen (Entwicklung, Musterbau, Fertigung und andere) Zugriff bekommen. Für jede Produktgruppe ist definiert, welche Standorte welche Disziplinen übernehmen.
- **An Fertigungsstandorten** sind nur freigegebene Projektdokumente inhaltlich zugänglich, und das auch nur, wenn das entwickelte Produkt den Reifegrad „Vorserie“ erreicht hat. Zudem sind die Dokumente dort nur im Neutralformat verfügbar.

Ist ein Dokument als vertraulich klassifiziert, so bestimmt sein Vertraulichkeitsgrad die Sichtbarkeit. Für die aufeinander aufbauenden Grade „vertraulich“, „intern“ und „geheim“ gelten folgende Regelungen:

- **Vertrauliche Dokumente** sind nur Personen inhaltlich zugänglich, die als vertrauenswürdig gelten. Dazu zählen: (a) das Unternehmensmanagement, (b) Personen, die explizit als vertrauenswürdig eingestuft sind, und (c) Mitarbeiter der herausgebenden Fachabteilung (im Fall von nicht-projektbezogenen Dokumenten) beziehungsweise Mitglieder des Projektteams (im Fall von projektbezogenen Dokumenten).
- **Interne Dokumente** sind vertrauliche Dokumente und nur internen Mitarbeitern des Unternehmens inhaltlich zugänglich.
- **Geheime Dokumente** sind interne Dokumente und nur Personen zugänglich, die explizit als Geheimnisträger eingestuft sind. Geheime Dokumente sind auch nur von diesen Personen auffindbar.

Ausnahmen von diesen Regelungen sind möglich, müssen aber im Einzelfall begründet und von einem Sicherheitsverantwortlichen genehmigt werden. Offensichtlich kommt man hier mit der herkömmlichen manuellen Vergabe von Zugriffsberechtigungen durch einen Systemadministrator oder gar durch einzelne Benutzer nicht sehr weit. Im vorgestellten

Glossar

IT-Sicherheit/Computersicherheit: Konzepte und Maßnahmen zum Schutz eines IT-Systems oder Computers mit dem Ziel, Vertraulichkeit, Integrität und Verfügbarkeit von gespeicherten beziehungsweise verarbeiteten Daten sowie die Verfügbarkeit von Systemfunktionen in ausreichendem Maß sicherzustellen.

Datensicherheit: Teilaspekt von IT-Sicherheit, konzentriert sich auf die Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit von Daten.

Datensicherung: Maßnahme zur Sicherstellung der Verfügbarkeit von Daten. Synonym für Backup.

Datenschutz: Maßnahme zum Schutz der Vertraulichkeit personenbezogener Daten gemäß gesetzlicher Bestimmungen.

Zugriffskontrolle: Maßnahme, die sicherstellen soll, dass nur autorisierte Subjekte (Benutzer oder Prozesse im Namen von Benutzern) auf Objekte (Daten oder Systemressourcen) zugreifen können. Sie beinhaltet Identifizierung, Authentisierung und Autorisierung.

Bei einer benutzerbestimmten Zugriffskontrolle (Discretionary Access Control, DAC) liegt es im Ermessen des Benutzers, Zugriffsberechtigungen für „seine“ Daten zu vergeben. Bei einer obligatorischen Zugriffskontrolle (Mandatory Access Control, MAC) erfolgt die Rechtevergabe nach zentralen Sicherheitsvorgaben, zumeist basierend auf allgemeinen Regeln und Eigenschaften von Subjekten und Objekten.

Zugangskontrolle: Physische und logische Kontrolle des Rechnerzugangs. Sie beinhaltet Identifizierung und Authentisierung des Benutzers.

Zugriffsrecht: Privileg eines Subjekts, auf ein Objekt in einer bestimmten Art und Weise zuzugreifen zu dürfen. Es wird auch als Zugriffsberechtigung bezeichnet.

Autorisierung: Vergabe von Zugriffsberechtigungen. Oft ist damit zugleich auch deren Überprüfung gemeint.

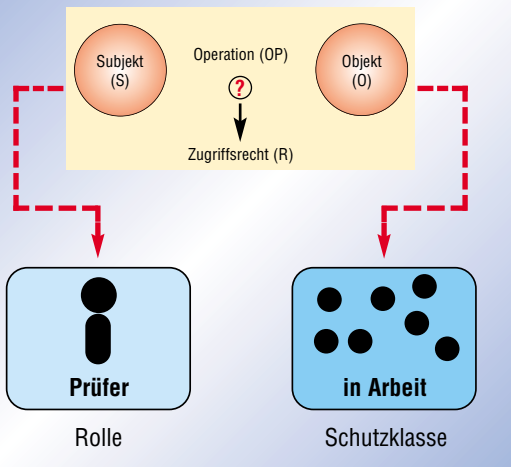
Authentisierung: Überprüfung der Identität eines Benutzers: Ist er tatsächlich derjenige, der er vorgibt zu sein? Häufig geschieht dies durch Abfrage eines Passworts oder einer PIN.

Integrität: In Bezug auf Daten die Eigenschaft, unverändert und damit vollständig, unversehrt und korrekt zu sein.

Vertraulichkeit: Eigenschaft einer Information, nur für autorisierte Empfänger zugänglich zu sein.

Verfügbarkeit: Eigenschaft von Daten, IT-Systemen oder Systemfunktionen, in einem definierten Zeitraum mit einer bestimmten Wahrscheinlichkeit zur Verfügung zu stehen.

www.contact.de

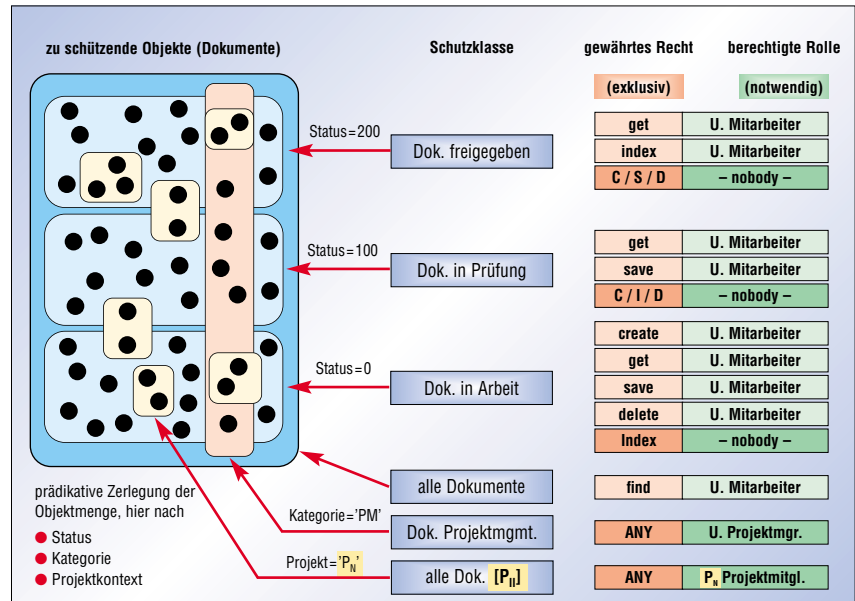


Rollen und Schutzklassen dienen der Zusammenfassung von Personen oder zu schützenden Objekten.

Szenario sind verbindliche, mehrdimensionale Vorgaben des Unternehmens bezüglich Datensicherheit und Know-how-Schutz durchzusetzen. Und das geht nur durch automatische Interpretation von Regeln!

Das PLM-System CIM Database von Contact Software GmbH mit Sitz in Bremen knüpft Berechtigungen regelbasiert an Rollen und Dateninhalte. Das oben definierte Regelwerk lässt sich damit nahezu 1:1 im System abbilden – und zwar ohne die Regeln fest im Code programmieren zu müssen. Die Lösung kann jede einzelne Operation (Suchen/Finden, Laden/Anzeigen, Speichern, Neuanlegen, Freigeben, Fortschreiben und weitere) des aktuellen Benutzers (Subjekt) auf einem Datensatz oder Dokument (Objekt) vom Vorhandensein eines spezifischen Rechts abhängig machen. Da sich jedoch Sicherheitsvorgaben im Allgemeinen nicht auf konkrete Benutzer und Datensätze beziehen, sondern auf Gruppen von Personen und Objekten mit bestimmten Eigenschaften, bietet das Berechtigungssystem flexible Möglichkeiten der Klassifizierung von zugreifenden Subjekten wie auch von zu schützenden Objekten:

- **Rollen** dienen der Gruppierung und Abstraktion von konkreten Personen. Sie modellieren üblicherweise Funktion, Qualifikation oder Organisationszugehörigkeit einer Person. Rollen können nicht nur von Personen, sondern auch wiederum von Rollen besetzt werden. So lassen sich Personen nach unterschiedlichen Kriterien hierarchisch gruppieren. Ein Benutzer nimmt normalerweise mehrere Rollen ein. Alle Inhaber einer berechtigten Rolle hinsichtlich des Zugriffsrechts gleich behandelt.
- **Schutzklassen** fassen zu schützende Objekte anhand ihrer Eigenschaften wie Bearbeitungsstatus, Kategorie



Rechtevergabe über Schutzklassen bilden den Kern des Rechtesystems von CIM Database. Sie fassen Objekte anhand ihrer Eigenschaften regelbasiert zusammen und gewähren Zugriffsrechte rollenbezogen.

oder Vertraulichkeitsgrad regelbasiert zusammen. Es sind beliebig viele Schutzklassen definierbar. Objekte können auch in mehrere Schutzklassen fallen. Alle Objekte einer Schutzklasse werden rechtemäßig gleich behandelt.

Während die Besetzung der Rollen mit einzelnen Personen (oder anderen Rollen) im allgemeinen manuell vorgenommen wird, geschieht die Zusammenfassung von Objekten zu Schutzklassen vollautomatisch durch das System. Dazu sind den Schutzklassen Prädikate zugeordnet, die logische Aussagen über beliebige Objekteigenschaften (Attribute) treffen. Hierzu einige Beispiele:

- das Dokument ist freigegeben
- das Dokument gehört zur Kategorie CAD-Unterlage
- das Dokument besitzt einen Projektbezug und ist vertraulich.

Alle Objekte, auf die ein Prädikat zutrifft, fallen automatisch in die zugehörige Schutzklasse. So zerlegen Schutzklassen die gesamte Menge der vom System verwalteten Objekte virtuell in Teilmengen, die sich auch überlappen können. Diese Zerlegung läuft sehr dynamisch ab, so dass sich jede Änderung eines Objekts wie ein Statuswechsel unmittelbar in der Schutzklassen-Abbildung widerspiegelt. Diese Schutzklassen bilden den Kern des Rechtesystems: Sie definieren, welche Rolle und welches Zugriffsrecht (auf die enthaltenen Objekte) zu gewähren ist. So kann ein Benutzer über die Rollen, die er einnimmt, verschiedene Rechte in verschiedenen Schutzklassen erlangen.

Diese rein additive Rechtevergabe hat jedoch ihre Grenzen. Oft ist es nötig, Rechte auch gezielt entziehen zu können. Zu diesem Zweck kann CIM Database die

Vergabe eines Rechts in einer Schutzklasse exklusiv an eine bestimmte Rolle knüpfen, wodurch alle Nicht-Inhaber der Rolle automatisch vom fraglichen Zugriff auf ein Objekt der Schutzklasse ausgeschlossen sind. Die Einnahme der Rolle ist in diesem Fall also für die Gewährung des Rechts zwingend notwendig. Relevant ist dieses für Objekte, die in mehrere Schutzklassen fallen, und so auf anderem Wege möglicherweise doch für einen Benutzer zugreifbar werden könnten. Rechteentzug sticht immer Rechtgewährung!

Beispiele. Die umfassende Schutzklasse „Alle Dokumente“ gewährt das Finderecht für alle Dokumente pauschal allen (internen und externen) Unternehmensmitarbeitern, die spezielle Schutzklasse „Geheime Dokumente“ schränkt dieses Recht jedoch für geheime Dokumente exklusiv auf Geheimnisträger ein. Die Schutzklasse „Freigegebene Dokumente“ stellt mit der exklusiven Vergabe des Rechts zur Pflege an eine unbesetzte Rolle grundsätzlich sicher, dass niemand freigegebene Dokumente verändern kann.

Darüber hinaus ermöglicht CIM Database eine kontextbezogene Rechtevergabe für Objekte mit Bezug zu organisatorischen Einheiten wie Projekten, Abteilungen oder Standorten. In diesen Fällen vergibt eine generische Schutzklasse Rechte an generische Rollen, die jeweils im Kontext einer organisatorischen Einheit besetzt werden können. Der Organisationsbezug eines Objekts bestimmt dann dynamisch, welche Rollenbesetzung jeweils für die Rechtevergabe wirksam wird. Auch hierzu ein Beispiel: Die Schutzklasse „Vertrauliche Projektdokumente“ gewährt das Recht auf inhaltlichen Zugriff auf ein ebensolches Dokument exklusiv

den Mitgliedern des Projekts, in dessen Kontext das Dokument steht.

Mit diesen Basismechanismen ist eine mehrdimensionale Rechtevergabe gemäß eingangs skizzierter Sicherheitsvorgaben leicht möglich. Die hier zu berücksichtigenden Dimensionen lauten

- **Grundlegende Bearbeitungsrechte**, abhängig vom Bearbeitungsstatus
- **Bearbeitungsrechte**, abhängig von der Unterlagenart (Kategorie) und der Organisationszugehörigkeit
- **Berechtigung zum Herunterladen** eines Dokuments (das heißt zum Zugriff), abhängig von der Bedeutung (Produktgruppe, Unterlagenart) und dem Standort
- **Recht zum Zugriff** auf den Dokumentinhalt, abhängig vom Vertraulichkeitsgrad.

Zu beachten ist dabei besonders die Schnittmengenbildung bei der exklusiven Rechtevergabe. Es bleiben nur Personen übrig, denen in allen Dimensionen das fragliche Recht gewährt wird. So sind im aufgeführten Beispiel vertrauliche Projektdokumente der Kategorie „CAD-Unterlage“ nur Personen zugänglich, die sowohl Mitarbeiter im Bereich Entwicklung als auch Mitglied im Projektteam sind.

Die komplexe Autorisierung von Benutzern reduziert sich so im täglichen Betrieb auf die gezielte Besetzung einer überschaubaren Zahl von Rollen, während das System die zu schützenden Ob-

jekte automatisch nach inhaltlichen Gesichtspunkten in vordefinierten Schutzklassen arrangiert. Damit wird die Rollenbesetzung selbst zum Knackpunkt. Manuelle Rollenbesetzungen sollten deshalb nur dem Systemadministrator oder anderen besonders berechtigten Personen überlassen bleiben. Weil die Zuordnung einer Person zu einer Rolle in CIM Database aber auch nichts anderes ist als ein (Beziehungs-)Objekt, kann die Rollenbesetzung selbst wiederum mit den vorgestellten Schutzmechanismen kontrolliert werden. Üblich ist beispielsweise, dass die Besetzung weiterer Projektrollen der Rolle Projektleiter im jeweiligen Projekt vorbehalten bleibt.

Die definierten Rollen sollten wegen ihrer zentralen Bedeutung für die Rechtevergabe die für die Sicherheitsregelungen relevanten Eigenschaften und Verantwortlichkeiten von Personen im Unternehmen möglichst genau widerspiegeln. Hierzu gehören die Zugehörigkeit zu einer Organisationseinheit, die Funktion innerhalb einer Organisationseinheit oder die Qualifikation der einzelnen Anwender.

Keine Regel ohne Ausnahme! In der Praxis können Fälle auftreten, die im Regelwerk nicht berücksichtigt sind. Wichtig ist, dass diese ebenfalls kontrolliert behandelt werden können, da sonst schnell der Überblick verlorengehen kann und schließlich das gesamte Sicherheitsregelwerk zur Makulatur wird. Das Konzept

ermöglicht es deshalb, Rollen „ausnahmsweise“ zu besetzen. Eine Ausnahmeberechtigung knüpft die Vergabe einer Rolle an Bedingungen. Sie gilt nur

- **bezogen auf** explizit aufgelistete Objekte
- **bis zu einem** angegebenen Verfallsdatum.

Damit kann beispielsweise ein externes Ingenieurbüro in Bezug auf einzelne Dokumente befristet wie ein interner Standort behandelt werden, ohne dass dafür grundlegende Änderungen am Regelwerk vorzunehmen sind. Ausnahmeberechtigungen und damit verbundene bedingte Rollenbesetzungen werden zentral definiert, während die Zuordnung der freizuschaltenden Objekte rechtegesteuert und protokolliert den jeweils verantwortlichen Fachanwendern überlassen bleibt.

Fazit. Die Kontrolle der Zugriffe regulärer Benutzer auf Daten und Dokumente gehört zu den grundlegenden Sicherheitsmaßnahmen, insbesondere in standortübergreifenden Systemen. Eine systematische Zugriffskontrolle erfordert jedoch ein leistungsfähiges, dynamisches Rechtssystem, das auch mit großen Datenmengen umgehen kann. CIM Database kann Berechtigungen regelbasiert an Rollen und Inhalte knüpfen und so komplexe Sicherheitsvorgaben des Unternehmens automatisch durchsetzen.

ACHIM MÜLLER

Die korrekte Entscheidung erfordert zuverlässige Quellen.

info@cadplus.de

www.cadplus.de

In CADplus / digitalPLANT werden Sie ständig informiert über:

- Product Lifecycle Management
- IT Strategien im Anlagenbau - digitalPLANT
- Engineering Workflow
- Supply Chain Management
- Trends bei Workstation und Server
- CAD/CAM/CAE - Tools der neuesten Generation



Bestellen Sie noch heute Ihr persönliches Probeexemplar