Security Whitepaper

Novell eDirectory™ 8.6.1

April 2002

EUROSEC GmbH
Chiffriertechnik & Sicherheit
Mergenthalerallee 45−47
D−65760 Eschborn

INHALTSVERZEICHNIS

1 Einleitung

Durch das Wachsen des Internet und die Weiterentwicklung des e−Commerce müssen auch e−Business−Anwendungen und die Komponenten, auf denen diese basieren, immer neuen Anforderungen gerecht werden. Der Umgang und die Verarbeitung sensitiver Daten erfordert dabei ein Höchstmaß an Zuverlässigkeit und Sicherheit, damit Kunden− und Business−Daten vor unbefugtem Zugriff geschützt werden können. Als wichtige und zentrale Komponente in e−Business−Plattformen gilt der sogenannte Verzeichnisdienst, durch den Informationen und Ressourcen effizient verwaltet werden müssen. An die Verzeichnisdienstkomponente stellen sich daher besondere Anforderungen bezüglich Sicherheit bei gleichzeitiger Flexibilität und Leistungsfähigkeit.

Hier positioniert sich Novells eDirectory − derzeit in der Version 8.6.1 − als vielseitiges Verzeichnisdienstprodukt, welches neben adäquaten Sicherheitsmechanismen auch in der Lage ist, sich in heterogene Umgebungen zu integrieren. Vorteilhaft ist dabei insbesondere, dass das eDirectory nicht primär auf die Verwaltung von Rechnernetzen ausgerichtet ist, sondern als universeller Verzeichnisdienst auch beliebige Informationen verwalten kann. Dies erlaubt den Einsatz in e−Commerce−Applikationen ebenso wie traditionell zur Verwaltung von Rechnernetzen.

Novell besitzt seit 1993 mit der Einführung des Netware Directory Service (NDS, Netware Verzeichnisdienstes) langjährige Erfahrung in der Konzeption und Nutzung von Verzeichnisdiensten. Zu Beginn als erweiterbares Verwaltungswerkzeug für Benutzer und Dateisysteme von Netware 4 eingesetzt, vollzog sich im Laufe der Zeit der Wandel zu einem Verzeichnisdienst mit breitem Anwendungsspektrum. Die aktuelle Version 8.6.1 des eDirectory kann seine Verzeichnisdienstfunktion auch losgelöst von Netware−Systemen auf vielen Plattformen (z.B.: Windows NT, Windows 2000, Linux, Solaris, AIX) anbieten, so dass der Verzeichnisdienst auf den gängigen Betriebssystemplattformen verfügbar ist.

Verzeichnisdienste spielen insbesondere in e−Business−Applikationen eine wichtige Rolle, da sie als zentraler Informationsspeicher Daten von Benutzern und Ressourcen verwalten. Die Sicherheit der gespeicherten Daten ist dabei ein wichtiger Aspekt, da in der Regel neben personenbezogenen Daten auch Authentisierungs− und Berechtigungsinformationen im Verzeichnisdienst vorgehalten werden. Die durch ein Verzeichnisdienstprodukt angebotenen Sicherheitsmechanismen und Sicherheitsfunktionen sind daher von entscheidender Bedeutung bei der Wahl der Verzeichnisdienstkomponente für e−Business−Lösungen.

Für den erfolgreichen Einsatz von Verzeichnisdiensten stellen sich jedoch neben den Aspekten der Sicherheit auch weitere Anforderungen, die auf Erfolg und Misserfolge einer darauf basierenden e−Business−Applikation Einfluss nehmen können: Konformität zu etablierten Standards, Flexibiliät, Stabilität, Performanz, Wartbarkeit und effiziente Verwaltungsmöglichkeiten spielen für den praktischen Einsatz eine wichtige Rolle.

Mit eDirectory 8.6.1 ist es Novell gelungen, eine Verzeichnisdienstkomponente anzubieten, in die die langjährige Erfahrungen mit Verzeichnisdiensten eingeflossen sind. Durch die Entkopplung vom Betriebssystem Netware kann das eDirectory seine Funktionalität auch in anderen Umgebungen anbieten. Durch die Nutzung von etablierten Standards ist die Integration in verschiedene Umgebungen möglich, die oft durch Heterogenität gekennzeichnet sind und vielfach auch andere Verzeichnisdienste einsetzen. Um die Verwaltung mehrerer Verzeichnisdienste zu vereinfachen, ist es wünschenswert, dass der Zugriff auf die Daten und deren Wartung verzeichnisdienstübergreifend stattfinden kann. Hier kann durch den Einsatz weiterer Produkte, wie etwa Novell DirXML, auf einfache Weise der Datenaustausch zwischen eDirectory und anderen Verzeichnisdiensten erreicht werden. Das Novell eDirectory 8.6.1 ist ein vielseitiges Produkt,

welches einerseits das interne IT−Ressourcenmanagement einer Organisation mit heterogenem IT−Umfeld übernehmen kann, und andererseits auch als Internet−Informationsbasis mit gesicherten und standardisierten Zugriffsmöglichkeiten einsetzbar ist.

Im den folgenden Abschnitten werden, nach einer kurzen Einführung in das Thema "Verzeichnisdienste", die Sicherheitseigenschaften des eDirectory betrachtet. Die Darstellung wird abgerundet durch einen Kurzvergleich zwischen dem Novell eDirectory und anderen am Markt erhältlichen Verzeichnisprodukten.

2 Verzeichnisdienste

2.1 Überblick

Verzeichnisdienste werden dazu genutzt, Daten zu speichern und diese in strukturierter Form für Suchanfragen bereit zu halten. Daher stehen bei Verzeichnisdiensten im Gegensatz zu Datenbanken die Lese−Operationen aufgrund von Suchanfragen deutlich im Vordergrund. Ein typischer Anwendungsfall für einen Verzeichnisdienst in einem Unternehmen ist die Speicherung von Adressdaten aller im Unternehmen angestellten Personen. Durch die Weiterentwicklung der elektronischen Kommunikation und den darauf basierenden Anforderungen von e−Business−Anwendungen bezüglich Datenmenge und Datentypen, müssen Verzeichnisdienste auf die Speicherung unterschiedlichster Daten abgestimmt sein, wie zum Beispiel e−mail−Addressen oder elektronische Zertifikate. Ein Verzeichnisdienst kann jedoch auch eine Liste aller im Unternehmen verfügbaren (elektronischen) Ressourcen enthalten und damit auch zu deren Verwaltung und zur Speicherung der Zugriffsrechte benutzt werden. Daher ist ein Verzeichnisdienst ein durchaus komplexes Produkt, das aufgrund der gespeicherten Daten auch bestimmte Sicherheitsanforderungen erfüllen muss.

Aufgrund seiner Funktion muss ein Verzeichnisdienst für Suchoperationen optimiert sein. Daher sind Verzeichnisdienste baumartig und hierarchisch organisiert, denn diese Struktur erlaubt wesentlich effizientere Suchmöglichkeiten als eine flache Struktur.

Aufgrund der hierarchischen, internen Struktur können die meist hierarchisch organisierten Strukturen eines Unternehmens in die Verzeichnisdienststruktur abgebildet werden. Dies gilt inbesondere für den Fall, wenn der Verzeichnisdienst eine IT−Infrastruktur abbildet. Die aus einer Organisation ableitbaren Entitäten, wie Personen, Rechner, Peripheriegeräte, Dateiverzeichnisse, oder auch Anwendungen werden dabei als Verzeichnisdienstobjekte im hierarchisch organisierten Verzeichnisbaum gespeichert (siehe Abbildung 1).

Ein Verzeichnis besteht aus Objekten. Objekte können entweder andere Objekte enthalten, diese werden dann Containerobjekte genannt, oder können keine anderen Objekte enthalten. Solche Objekte werden dann als Blattobjekte bezeichnet. Ein Verzeichnisbaum besitzt immer ein ausgezeichnetes "Startobjekt", die sogenannte Wurzel, unter der alle anderen Objekte angesiedelt werden. Generell werden Objekte dazu benutzt, um Informationen zu speichern. Jedes Objekt besitzt einen eigenen Namen und ist von einem bestimmten Typ (z.B.: Benutzerobjekt, Rechnerobjekt, Containerobjekt), der im Wesentlichen bestimmt, welche Informationen das Objekt enthält. Alle Objekte in einem Verzeichnisbaum besitzen aufgrund ihrer Position im Baum (ausgehend von der Baumwurzel) eine eindeutige Adresse, die sich aus der Aneinanderreihung der Namen der Objekte ergibt, die auf dem Weg von der Baumwurzel zum jeweiligen Objekt liegen.

Die in einem Verzeichnisdienst gehaltenen Daten sind in der Regel sensitiv, da sie entweder personenbezogen oder vertraulicher Art sind. Zusätzlich liefert die aufgebaute

Verzeichnisbaumstruktur starke Hinweise auf die Organisationsstruktur oder IT−Struktur eines Unternehmens. Diese Daten müssen daher vor unbefugtem Zugriff geschützt werden und die Integrität muss gewährleistet werden. Generell können alle Daten hinsichtlich ihrer Schutzbedürftigkeit in unterschiedliche Klassen eingeteilt werden. Daher müssen Verzeichnisdienste auch geeignete Schutzmechanismen anbieten.
Auf der anderen Seite bestehen hohe Anforderungen bezüglich der Verfügbarkeit von Verzeichnisdiensten. Um eine entsprechende Verfügbarkeit zu gewährleisten, stellen Verzeichnisdienste spezifische Mechanismen zur Verfügung: durch das Anlegen von sogenannten Repliken, also Kopien der Verzeichnisdaten und die Nutzung von geeigneten Aufteilungen, sogenannten Partitionen des Verzeichnisbaumes auf mehrere physikalische Lokationen, kann die Ausfallsicherheit erhöht werden. Zusätzlich können Partitionen auch dazu genutzt werden, um die Verzeichnisdaten so aufzuteilen, dass Daten mit gleichen Sicherheitsanforderungen jeweils separat behandelt werden können. Die Verteilung sowie die Synchronisation der einzelnen Repliken und Partitionen ist Aufgabe des Verzeichnisdienstes. Nicht jede Directory−Lösung unterstützt die Partitionierung der Verzeichnisdaten, das Novell eDirectory enthält jedoch eine entsprechende Unterstützung.

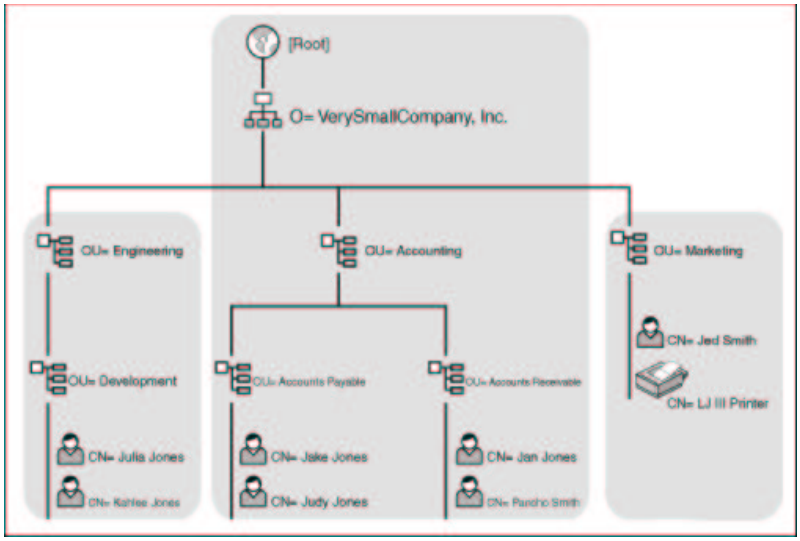

Abbildung 1: Hierarchische Struktur eines Verzeichnisdienstes

Um die in einem Verzeichnisbaum abgelegten Daten zu nutzen, wird ein spezielles Programm (der sogenannten Verzeichnisdienst−Client) benötigt, das mit dem Verzeichnisdienst über ein gemeinsam unterstütztes Protokoll kommunizieren kann. Als Clients kommen dabei Benutzer oder auch Applikationen in Frage. Insbesondere in Szenarien des e−Business findet der Zugriff auf einen Verzeichnisdienst in der Regel durch Programmkomponenten statt.

In Abhängigkeit von den in einem Verzeichnisbaum gespeicherten Daten ist es notwendig, dass vor einem Verzeichnisdienstzugriff eine geeignete Authentifizierung stattfindet, so dass auf Daten nur gemäß der eingestellten Zugriffsberechtigungen zugegriffen werden kann. Ohne vorherige Authentifizierung sollte nur eine sehr eingeschränkte oder überhaupt keine Zugriffsmöglichkeit bestehen. Ausnahmen bilden hier Verzeichnisse, die öffentliche Informationen anbieten, die für jeden zugreifbar sein sollten.

2.2 Standards

Im Umfeld der Verzeichnisdienste haben sich über die Jahre mehrere internationale Standards entwickelt. Diese standardisieren wichtige technische Aspekte von Verzeichnisdiensten, wie den

internen Aufbau oder auch Kommmunikationsprotokolle. Der in diesem Zusammenhang wichtigste Standard ist die Spezifikation X.500, ein ITU−Standard aus dem Jahre 1988. Dieser Norm sind zusätzlich verschiedene Erweiterungen zugeordnet (X.501, X.509, X.511, X.518, X.519, X.520, X.521 sowie X.525), die spezifische Einzelaspekte standardisieren.

Durch die Spezifikation X.519 sind mögliche Kommunikationsprotokolle standardisiert, darunter auch das sogenannte DAP (Directory Access Protocol). Aufgrund seiner Komplexität gibt es jedoch nur wenige Implementierungen dieses Protokolls. Zudem bestand die zusätzliche Schwierigkeit, dass zur Verwendung von DAP eine Implementierung der sogenannten OSI−Netzwerkprotokolle erforderlich war. Diese haben sich jedoch durch die Dominanz der Internet−Netzprotokolle TCP/IP nicht durchgesetzt. Anfang der 90er Jahre wurde deshalb das sogenannte LDAP (Lightweight Directory Access Protocol) entwickelt, welches auf dem Internetprotokoll IP aufsetzt. LDAP hat sich in der Folge als De−Facto−Protokollstandard für den Zugriff auf Verzeichnisdienste durchgesetzt, insbesondere auch deshalb, weil zahlreiche Web−Browser und E−Mail−Clients diese Schnittstelle unterstützen. Die aktuelle Version von LDAP ist die Version 3.

LDAP definiert drei verschiedene Möglichkeiten der Authentifizierung für Client−Zugriffe:
1. Den sogenannten "Anonymous Bind", bei dem keine Benutzerauthentifizierung stattfindet.
2. Den sogenannten "Cleartext−Password−Bind", hierbei ist die Verwendung eines Benutzernames und eines Passwortes erforderlich. Die Übertragung der Authentifizierungsdaten erfolgt dabei im Klartext.
3. Den sogenannten "Secure Bind", bei dem ebenfalls die Verwendung von Benutzername und Passwort notwendig ist, das Passwort wird dabei jedoch verschlüsselt übertragen.

Die unterschiedlichen Authentifizierungsarten müssen dabei von Client und Server unterstützt werden.

Zur Absicherung der bei einem LDAP−Zugriff übertragenen Daten definiert die LDAP V3−Spezifikation die sogenannte SASL Protokollerweiterung zur Authentifizierung und Verschlüsselung des LDAP−Zugriffs. In der Praxis wird jedoch an dieser Stelle hauptsächlich das SSL (Secure Socket Layer) Protokoll zur Wahrung der Integrität und Vertraulichkeit der Daten eines LDAP−Zugriffs eingesetzt. Die aktuelle SSL Spezifikation in der Version 3, die im Wesentlichen äquivalent zur TLS v1 (Transport Layer Security) Spezifikation ist, erlaubt entweder einseitige Authentifizierung des Servers oder auch gegenseitige Authentifizierung von Client und Server. Die dabei zur Authentifizierung und zur Absicherung der übertragenen Daten eingesetzten Verfahren werden zwischen Client und Server beim SSL−Verbindungsaufbau ausgehandelt. In der Regel erfolgt die Authentifizierung jedoch über Public−Key−Zertifikate oder über eine Benutzername/Passwort−Kombination.

2.3 Einsatzszenarien

Verzeichnisdienste können in unterschiedlichen Szenarien zum Einsatz kommen, wie zum Beispiel:

- Als unternehmensweites Verzeichnis beliebiger Ressourcen, wie beispielsweise Personaldaten oder zur Verwaltung von Meeting−Räumen.
- Zur Verwaltung von IT−Systemen und deren Ressourcen (z.B. Rechner, Benutzer, Berechtigungen).
- Als Verzeichniskomponenten innerhalb einer e−Business−Lösung.

Jedes Einsatzszenario stellt dabei individuelle Anforderungen an die Funktionen und Mechanismen eines Verzeichnisdienstes. Dies gilt insbesondere für die sicherheitsrelevanten Anforderungen, die je nach Einsatz auf unterschiedliche Gefährdungslagen abgestimmt werden müssen. Daneben spielen in allen Szenarien auch Anforderungen an die Verfügbarkeit, Administrierbarkeit und an

die Möglichkeiten zur Überwachung eine Rolle.

Die folgenden Kapitel beschäftigen sich im Wesentlichen mit den sicherheitsrelevanten Aspekten von Verzeichnisdiensten und beleuchten, wie das Novell eDirectory die identifizierten Themen umsetzt.

3 Novell eDirectory: Sicherheitsaspekte

Für das Novell eDirectory spielen die folgenden verzeichnisdienstspezifischen Sicherheitsaspekte eine wichtige Rolle:

- Der Datenschutz der im Verzeichnisdienst gespeicherten Daten muss gewährleistet werden. Der Verzeichnisdienst muss hier geeignete Mechanismen anbieten, um den Datenschutz umsetzen zu können.
- Die Verfügbarkeit der im Verzeichnisdienst gehaltenen Daten muss gewährleistet sein. Da hier oft auch Authentifizierungs− und Berechtigungsinformationen gespeichert werden, ist die Sicherheit auf Applikationsebene von der Verfügbarkeit solcher Daten und damit von der Verfügbarkeit des Verzeichnisdienstes abhängig.
- Zur Realisierung von Zugriffsbeschränkungen auf die Daten des Verzeichnisdienstes müssen geeignete Zugriffskontrollmechanismen vorhanden sein. Typischerweise ergibt sich daraus die Anforderung nach:
  - Zugriffsberechtigungen, die auf die einzelnen Verzeichnisdienstobjekte und auf die in ihnen enthaltenen Daten vergeben werden können.
  - Verschiedenen Arten der Netzanbindung, mit der auf einen Verzeichnisdienst über ein Netz zugegriffen werden kann. Hier stehen insbesondere die einsetzbaren Protokolle und deren Sicherheitseigenschaften (z.B.: Authentifizierungsmechanismen, Vertraulichkeit und Integrität der übertragen Daten) im Vordergrund.
  - Sicherheit bei der Benutzerauthentifizierung, von der insbesondere die Wirksamkeit der Zugriffsbeschränkungen abhängt.
- Unter administrativen Gesichtspunkten ist es wichtig, dass die Verwaltung einfach und effizient durchgeführt werden kann. Dies hat auch direkte Auswirkungen auf die Sicherheit, da komplexe und fehleranfällige Verwaltungsmechanismen schnell zu Sicherheitslücken führen können. Anspruchsvoll wird diese Anforderung dadurch, dass dennoch eine größtmögliche Flexibilität (z.B.: Delegation von Verwaltungsaufgaben, Partitionieren von Verzeichnisdatenbeständen) gewährleistet werden soll.
- Im laufenden Betrieb stellen sich zudem Anforderungen bezüglich der Überwachbarkeit. Ein Verzeichnisdienst sollte Überwachungsmechanismen anbieten, die es erlauben, nicht nur eine Überwachung im Sinne der technischen Systemüberwachung durchzuführen, sondern auch eine sicherheitsbezogene Überwachung.

Die folgenden Abschnitte gehen genauer darauf ein, welche Lösungen das Novell eDirectory zu den einzelnen Themengebieten anbietet und umsetzt.

3.1 Datenschutz

Beim Einsatz eines Verzeichnisdienstes in e−Business−Lösungen werden viele Daten im Verzeichnisdienst gehalten, denen im Sinne des Datenschutzes ein hoher Schutzbedarf zukommt. Dazu gehören nicht nur personenbezogene Daten, wie beispielsweise Addressinformation über Benutzer der e−Business−Applikation, sondern auch wichtige system− oder anwendungsbezogene Informationen, wie etwa Zertifikate oder Transaktionsinhalte.

Grundsätzlich ist im Rahmen des Designs einer e−Business−Lösung eine Schutzbedarfsfeststellung sowie eine Risikoanalyse für die im Verzeichnisdienst abgelegten Daten durchzuführen. Basierend darauf ergeben sich dann Anforderungen an die notwendigen Zugriffsbeschränkungen oder auch an den Ort der physikalischen Speicherung.

Das Novell eDirectory kann diese Anforderungen durch unterschiedliche Mechanismen und Eigenschaften unterstützen:

- Die Möglichkeiten der flexiblen Zugriffsberechtigungsstruktur (siehe 3.3 Zugriffsberechtigungen) erlauben es, den Zugriff auf Informationen entsprechend den notwendigen Zugriffsbeschränkungen zu vergeben.
- Das eDirectory bietet über die sogenannte "secret store" Technik die Möglichkeit der verschlüsselten Datenhaltung an. Dies bietet optimalen Schutz für besonders schutzbedürftige Daten.
- Um dem unterschiedlichen Schutzbedarf von Informationen gerecht zu werden, erlaubt das eDirectory die verteilte Datenhaltung. Dadurch können Daten einerseits auf unterschiedlichen physikalischen Servern mit unterschiedlichen Sicherheitseigenschaften gehalten werden und anderseits können die verschiedenen Partitionen mit unterschiedlichen Zugriffsberechtigungsstrukturen ausgestattet sein. Auf diese Weise läßt sich der über das eDirectory zugreifbare Datenbestand ideal auch unter unterschiedlichen Sicherheitsanforderungen verwalten.

3.2 Verfügbarkeit

Neben dem Schutzbedarf von Verzeichnisdaten spielt natürlich auch deren Verfügbarkeit eine wichtige Rolle. Dies ist insbesondere für den Einsatz in e−Business−Lösungen wichtig, wenn darüber wichtige Geschäftsabläufe abgewickelt werden.

Das eDirectory unterstützt erhöhte Verfügbarkeitsanforderungen dadurch, dass mehrere sogenannte Repliken − also Kopien − eines eDirectory−Servers betrieben werden können. Im Unterschied zu anderen Verzeichnisdiensten bietet das Novell eDirectory eine echte Multi−Master−Update−Fähigkeit, so dass alle Änderungen an Verzeichnisdaten an einem beliebigen Verzeichnisserver erfolgen können. Entsprechend der Konfiguration der Abgleichparameter übernimmt das eDirectory die Verteilung der Veränderungen an alle Serverkopien und löst widersprüchliche Änderungen (z.B: Veränderungen an Daten, die auf einer anderen Serverkopie gerade gelöscht wurden) automatisch auf.

3.3 Zugriffsberechtigungen

Um dem Schutzbedarf der im Verzeichnisdienst gespeicherten Daten gerecht zu werden, werden insbesondere Zugriffsberechtigungen auf Objekte des Verzeichnisdienstes eingesetzt. Von den Mechanismen und Verfahren, die ein Verzeichnisdienst bezüglich Zugriffsberechtigungen anbietet, hängt es ab, ob damit die Daten entsprechend ihres Schutzbedarfs geschützt werden können. Zusätzlich müssen die Verfahren auch geeignet sein, komplexe Zugriffsstrukturen effizient verwalten zu können, so dass oft auch intelligente Verwaltungsfunktionen für die Zugriffsberechtigungen (z.B.: Delegation, Rechtevererbung) notwendig sind. Dies ist auch unter Sicherheitsgesichtspunkten wichtig, da Fehler in Zugriffsberechtigungen in der Regel Sicherheitslücken bedeuten.

Das Berechtigungssystem des Novell eDirectory basiert im Wesentlichen auf den Zugriffsmechanismen, die schon unter NDS eingesetzt wurden. Diese haben sich in der Vergangenheit bewährt und bieten damit eDirectory−Administratoren einfache und zugleich

mächtige Möglichkeiten an, Berechtigungen innerhalb des Verzeichnisdienstes zu vergeben und zu verwalten.

Generell basieren alle Berechtigungen darauf, dass jedes Objekt im Verzeichnisbaum eine eigene Zugriffsliste (ACL, Access Control List) besitzt (siehe Abbildung 2), die die Zugriffsmöglichkeiten auf Objekt− sowie auch auf Attributebene festlegt.

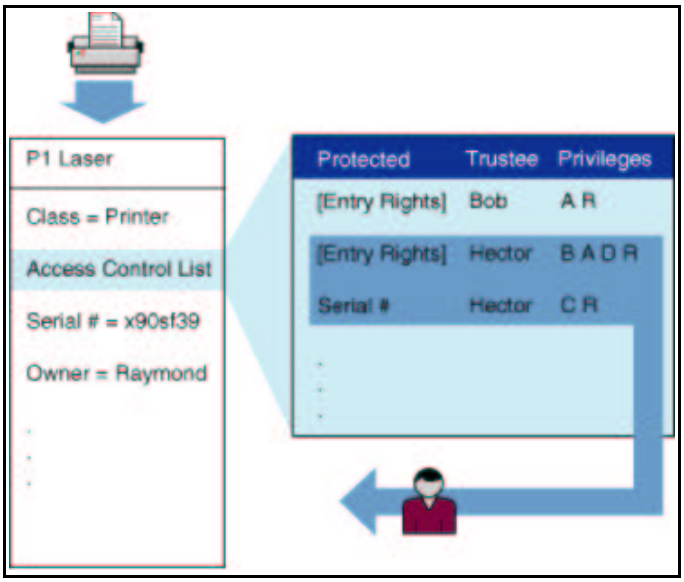

Abbildung 2: Jedes Objekt besitzt eine ACL

Die Konfiguration der Access Control Lists kann im Novell eDirectory auf verschiedene Arten erfolgen:

1. Direkt über sogenannte Trustee−Anweisungen,
2. Indirekt über den verwendeten Vererbungsmechanismus, oder
3. Indirekt über die Angabe von Zugriffsberechtigungsäquivalenzen.

Die einfachste Art Berechtigungen festzulegen, erfolgt direkt über die sogenannten Trustee−Anweisungen. Hierbei wird einem Zielobjekt direkt ein anderes Objekt zugeordnet, welches Zugriffsrechte auf das Zielobjekt besitzen soll. Die genauen Rechte bzw. Privilegien werden dabei explizit angegeben: Auf Objektebene sind dies die Rechte "Browse, Create, Delete, Rename und Supervisor". Auf Ebene der Attribute können die Rechte "Compare, Read, Add or Delete Self, Write, Supervisor sowie Inheritance Control" vergeben werden (siehe Abbildung 3 und Abbildung 4).

Um die Administration zu vereinfachen, lassen sich die Einstellungen jedoch auch über die Eigenschaften des zugreifenden Objektes vornehmen: dazu werden die Zielobjekte, auf die das Objekt Zugriffsrechte besitzen soll, im Eigenschaftsdialog mit den jeweiligen Rechten eingetragen.

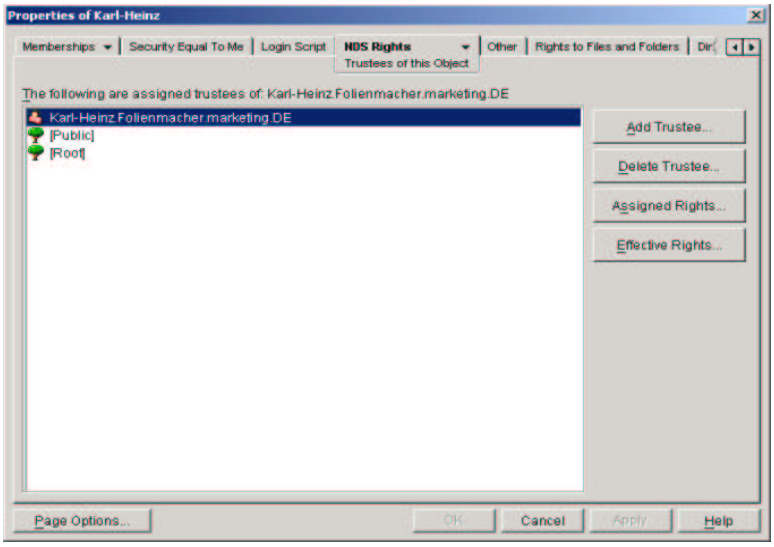

Abbildung 3: Zugriffsrechte auf Objekte und Attribute

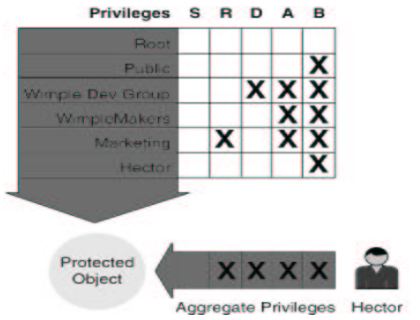

Abbildung 4: Zugriffsrechte (Schematisch)

Da Verzeichnisbäume auch sehr viele Objekte enthalten können und es aufwendig ist, für jedes einzelne Objekt Zugriffsberechtigungen zu definieren und anschließend notwendige Änderungen in die Zugriffslisten einzupflegen, stellt das eDirectory einen Vererbungsmechanismus zur Verfügung, so dass Zugriffberechtigungen implizit über die Vererbung auf untergeordnete Objekte vergeben werden können. Es ist hierbei auch möglich, die Vererbung dieser Zugriffberechtigungen durch die Definition von geeigneten Filtern ("Inherited Rights Filter" − IRF, siehe Abbildung 5) zu steuern:

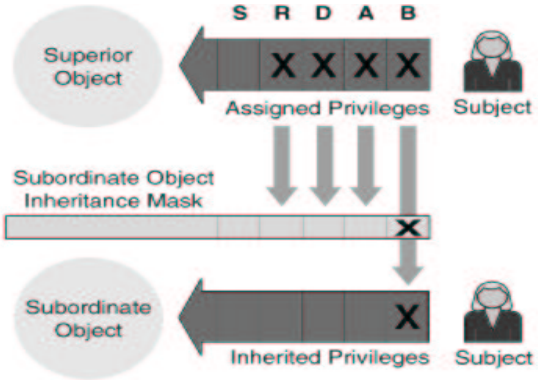

Abbildung 5: Inherited Rights Filter

Damit kann der Mechanismus der automatischen Rechtevererbung auf Objektebene gezielt beeinflusst werden. Zugriffberechtigungen auf Attributsebene vererben sich dagegen nicht automatisch auf untergeordnete Objekte, dies kann jedoch auch konfiguriert werden, falls es aufgrund der aufzubauenden Berechtigungsarchitektur notwendig und sinnvoll ist.

Als weitere Möglichkeit der Vergabe von Zugriffberechtigungen bietet das eDirectory die Zuweisung sogenannter "Sicherheitsäquivalenzen" an. Dadurch wird festgelegt, dass ein bestimmtes Objekt X mindestens die gleichen Zugriffsmöglichkeiten besitzt, wie ein anderes Objekt Y. Dies bietet die Möglichkeit, ein rollenartiges, hierarchisches Zugriffskonzept zu definieren.

Im Gegensatz zu anderen Verzeichnisdiensten, bietet das eDirectory dem Administrator standardmäßig die Möglichkeit an, festzustellen, welche effektiven Zugriffsrechte auf ein Verzeichnisobjekt bestehen. Dies ist notwendig, um die aus der Summe der Einstellungen resultierenden tatsächlich wirksamen Zugriffsmöglichkeiten festzustellen. Damit ist der

Administrator in der Lage, jederzeit Fehlkonfigurationen aufdecken zu können, so dass Sicherheitslücken, die auf Fehlkonfigurationen der Berechtigungen basieren, vermindert werden können.

3.4 Sicherheit beim Netzzugriff

Verzeichnisdienste werden in der Regel immer über ein Netz zugegriffen: ein Verzeichnisdienst−Client greift dabei mittels eines vom Verzeichnisdienst unterstützten Zugriffsprotokolls auf die Daten des Verzeichnisdienstes zu. Da insbesondere in e−Business−Anwendungen oft die Notwendigkeit besteht, die Daten des Verzeichnisdienstes auch über das Internet für bestimmte Kommunikationspartner zugreifbar zu machen, ist ein solcher Verzeichnisdienstserver prinzipiell zunächst für alle Internetnutzer zugreifbar. Aus Sicherheitsgründen muss daher schon der Verbindungsaufbau zu einen Verzeichnisdienstserver beschränkbar sein. Neben verschiedenen Möglichkeiten für die Authentifizierung von Zugreifer und Verzeichnisdienstserver, spielen hier auch Aspekte der Authentizität, Vertraulichkeit und Integrität von übertragenen Daten eine wichtige Rolle.

Das Novell eDirectory bietet hier verschiedene Möglichkeiten zur Absicherung des Netzzugriffes, so dass sich das eDirectory an unterschiedliche Einsatzszenarien anpassen kann. Generell können zwei unterschiedliche Zugriffsszenarien unterschieden werden:

1. Der Zugriff mittels NDAP−Protokoll über den Novell−Client, dies erfolgt in der Regel innerhalb eines Intranets.
2. Der Zugriff mittels LDAP−Protokoll, dies erfolgt in der Regel beim Zugriff über das Internet oder in Intranet Szenarien, in denen keine Novell−Clients zum Einsatz kommen.

Beim Zugriff über einen Novell−Client kommt das Novell−eigene NDAP (Novell Directory Access Protocol) zum Einsatz, welches auf dem NCP (Novell Core Protocol) aufsetzt. Eine Verbindung zum eDirectory ist einem Benutzer dabei nur möglich, sofern dieser im Verzeichnis als User−Objekt existiert. Ausserdem werden die Novell−eigenen Protokolle auch bei der Datensynchronisation zwischen einzelnen Partitionen und Repliken eingesetzt.

Erfolgt der Zugriff mittels LDAP, so unterstützt das eDirectory zum einen das anonyme Login (sofern dies nicht durch die Konfiguration ausgeschlossen wurde) und zum anderen den mit Benutzernamen und Passwort authentifizierten Zugriff. Dabei werden die Authentifizierungsdaten jedoch ungeschützt im Klartext zwischen den Kommunikationspartnern übertragen. Der sogenannte "secure bind", bei dem die Authentifizierungsdaten verschlüsselt übermittelt werden, wird durch das eDirectory derzeit nicht unterstützt. Da beim "secure bind" aber lediglich die Authentifizierungsdaten verschlüsselt werden, nicht jedoch die nachfolgend übertragenen Nutzdaten, ist der durch den "secure bind" erreichte Sicherheitsgewinn fraglich. Als weitaus sicherere Alternative unterstützt das eDirectory die Möglichkeit, Verbindungen mittels SSL/TLS abzusichern: hier werden dann Authentifizierungsdaten und Nutzdaten verschlüsselt übertragen. Dies ist speziell für Verzeichnisdienstinstallationen, die sensitive Informationen speichern, die zu präferierende Variante. Zusätzlich erlaubt die Verwendung der SSL−Clientauthentifizierung die Authentifizierung der zugreifenden Clients durch ein Client−Zertifikat. Diese Unterstützung ist insbesondere dann in e−Business−Lösungen sinnvoll, wenn die Verzeichnisinformationen ausschließlich einem eingeschränkten und bestimmten Benutzerkreis (z.B.: Zulieferer, Kooperationspartner) zugänglich gemacht werden sollen.

3.5 Benutzerauthentifizierung

Für den Zugriff auf einen Verzeichnisdienst und für dessen Nutzung (etwa für die Durchsetzung

von Zugriffsberechtigungen) spielt die Sicherheit der Benutzerauthentifizierung eine wichtige Rolle: Kann der Authentifizierungsmechanismus unterlaufen werden, so ist eine korrekte Durchsetzung der Zugriffsbeschränkungen nicht mehr möglich. Aus diesem Grund ist es wünschenswert, dass einerseits möglichst starke Authentifizierungsverfahren eingesetzt werden können und andererseits auch die Möglichkeit besteht, neue Authentifizierungsverfahren integrieren zu können.

Das Novell eDirectory bietet zur Benutzerauthentifizierung unterschiedliche Methoden an, die auch von der Art des Zugriffes abhängig sind. Es sind dies:

- Ein Novell−eigenes Zero−Knowledge−Verfahren, das beim Zugriff auf das eDirectory mittels Novell−Client zum Einsatz kommt.
- Die im Rahmen des LDAP−Protokolls definierten Authentifizierungsverfahren (siehe auch 3.4Sicherheit beim Netzzugriff):
  - Keine Authentifizierung,
  - Benutzername und Passwort Authentifizierung
  - Benutzername und Passwort Authentifizierung über SSL/TLS

Um neue Authentifizierungsverfahren in das eDirectory einbinden zu können, sind als Zusatzmodul die sogenannten Novell Modular Authentication Services (NMAS) erhältlich. Dies erlaubt die einfache Einbindung einer Reihe weiterer Verfahren zur Benutzerauthentifizierung: wie etwa Login−Methoden mittels privater RSA−Schlüssel auf einer Smartcard, mittels biometrischer Verfahren, über SecureID−Token, oder auch über RADIUS−Server. Insbesondere lassen sich mit NMAS verschiedene Authentifizierungsmethoden auch miteinander verketten. Für Business−Anwendungen besonders interessant ist die Möglichkeit, nun sogenannte "Security Label" auf NDS−Objekte vergeben zu können, wodurch Zugriffsrechte in Abhängigkeit von der verwendeten Login−Methode vergeben werden können.

Grundsätzlich besteht die Stärke eines Authentifizierungsverfahrens darin, dass die zur Authentifizierung notwendigen Daten möglichst geschützt werden und so geartet sind, dass sie nicht einfach erraten werden können. Im Idealfall müssen die eigentlichen Authentifizierungsdaten (z.B.: das Passwort) auch nicht im Rahmen der Authentifizierung übertragen werden, so dass das Verfahren auch gegen Abhörangriffe resistent ist. Auf diesem sogenannten Zero−Knowledge−Verfahren basiert die Authentifizierung beim eDirectory Zugriff mittels Novell−Client, so dass hier ein starkes Authentifizierungsverfahren verfügbar ist.

Aus Benutzersicht stellt sich das Verfahren als eine Benutzername & Passwort Authentifizierung dar: Der Benutzer der sich anmelden will, gibt seinen Benutzernamen und sein Passwort in die Eingabemaske ein.
Intern jedoch stellt sich der Ablauf wir folgt dar (siehe Abbildung 6): Der Benutzername wird dem Verzeichnisdienst überreicht und dort gesucht. Ist der Benutzer vorhanden, wird dessen "Private Key" extrahiert. Dieser ist mit dem Benutzerpasswort verschlüsselt im Verzeichnis abgelegt. Der verschlüsselte Private Key wird dem Clientrechner, zusammen mit zufällig erzeugten Sessiondaten, übermittelt. Auf dem Clientrechner wird der Private Key nun mit Hilfe des eingegebenen Passwortes entschlüsselt. Aus dem Private Key und den Sessiondaten werden nun sogenannte Credentials gebildet. Diese bestehen im Wesentlichen aus einer mit dem Private Key erzeugten Signatur der Sessiondaten. Der Private Key wird nach der Berechnung der Signatur sofort wieder aus dem Hauptspeicher des Clientrechners gelöscht. In der Folge werden nur noch die Credentials genutzt, womit sich der Benutzer bei weiteren Diensten anmelden kann. Damit ist implizit dem Single−Sign−On−Gedanken Rechnung getragen worden, analog zum Kerberos−Verfahren.

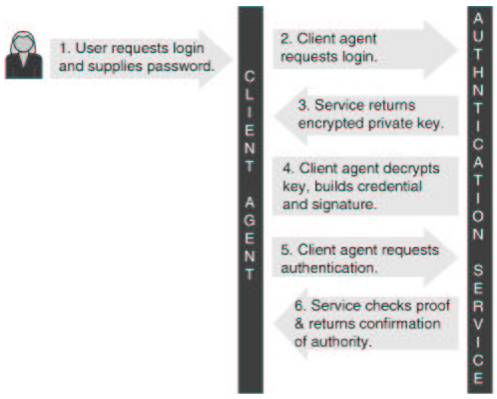

Abbildung 6: Benutzerauthentisierung

Neben dem Novell−eigenen Verfahren, kommt in e−Business−Anwendungen jedoch häufig der LDAP−basierte Zugriff auf des eDirectory zum Einsatz. Aus Sicherheitssicht kann hier nur die Nutzung des SSL/TLS−geschützten Zugriffes zur Anwendung kommen, wenn Zugriffe auf das eDirectory authentifiziert stattfinden müssen. Auf diese Weise kann die eDirectory−LDAP−Schnittstelle einen ausreichenden Schutz der Authentifizierungsdaten gewährleisten.

3.6 Administration

Das Novell eDirectory 8.6.1 erlaubt die zentrale Administration eines Verzeichnisbaumes. Als Administrationswerkzeug steht die ConsoleOne − eine Java−Applikation – zur Verfügung. Entsprechend der zu verwaltenden Funktionalitäten des Verzeichnisdienstes werden spezialisierte Module, sogenannte Snap−ins, in die ConsoleOne hinzugeladen.

Aus Sicherheitssicht sind auch für die Verwaltung eines Verzeichnisdienstes unterschiedliche Aspekte relevant, die wichtigsten sind:

- Auch ein Administrator sollte in seinen Berechtigungen eingeschränkt werden können. Dies verhindert, dass ein Administrator unbemerkt Sicherheitsverstöße begehen kann, indem er sich selbst Berechtigungen einräumt und Überwachungsmechanismen abschaltet oder die aufgezeichneten Daten verändert.
- Sicherheitskritische Daten (z.B.: Systemdaten, Passworte) sollten besonders schützbar sein.
- Im Idealfall kann die Administration rollenbasiert erfolgen, so dass insbesondere sicherheitskritische administrative Aufgaben nicht durch eine Rolle alleine ausgeführt werden können.
- Die Administration sollte einen Delegationsmechanismus unterstützen, so dass Verwaltungsaufgaben aufgeteilt werden können. Dies vereinfacht die Administration in großen Systemen wesentlich und unterstützt die hierarchischen Strukturen in vielen Organisationen.
- Die Administration muss durch geeignete Werkzeuge unterstützt werden, so dass Administrationsfehler möglichst vermieden oder festgestellt werden können.

Das Novell eDirectory bietet hier Mechanismen an, um diese wesentlichen Forderungen erfüllen zu können: Durch die Verwendung spezieller Rollen−Objekte (Rollen & Tasks) lässt sich eine rollenbasierte Administration durchsetzen. Dies bedarf jedoch einer vorherigen detaillierten Planung, um einen für Tagesbetrieb tragfähigen Kompromiss zwischen einfacher Administration und dem mit der Rollentrennung verbundenen Sicherheitsgewinn zu erreichen. Zusätzlich können einzelne Administrationsaufgaben an "Sub−Administratoren" delegiert werden.

Wesentlicher Bestandteil des Aufgabenbereichs eines Security−Administrators ist die Verwaltung des sogenannten Security−Containers, dieser enthält wichtige Systeminformationen, wie etwa das Schlüsselmaterial des Zertifikatservers, Security Policy Objects, Auditing Objects und weitere Objekte, deren Integrität für den sicheren laufenden Betrieb gewährleistet sein muss. Durch die

eDirectory Eigenschaften bzw. Mechanismen können diese Daten besonders geschützt werden: so können sie in einer eigenen Partition gehalten werden, die zusätzlich nur eine Read/Write − Replika (die Master−Replika) besitzt, welche sich auf einem physikalisch speziell gesicherten Rechner befindet.

3.7 Monitoring / Auditing

Die Sicherheitsüberwachung eines Verzeichnisdienstes ist ein wesentliches Mittel, um die Sicherheit im laufenden Betrieb aufrechtzuerhalten. Unberechtigte Zugriffe, die auf einen Angriff hindeuten, müssen frühzeitig erkannt werden, bevor beispielsweise sensitive Daten kompromittiert werden oder bevor ein Authentifizierungsverfahren durch einen Angreifer unterlaufen wird. Vorteilhaft ist in diesem Zusammenhang, wenn eine automatisierte Überwachung erfolgen kann, da bei der Übewachung großer Systeme bzw. von Systemen mit vielen Zugriffen große Datenmengen anfallen, die kaum mehr manuell ausgewertet werden können.

Das Novell eDirectory 8.6.1 definiert zu Überwachungszwecken eigene Ereignisse, sogenannte "Events". Diese können über das standardisierte Protokoll SNMP (Simple Network Management Protocol), unter Verwendung sogenannter SNMP Traps, an eine zentrale Überwachungsstation versandt und dort aufgezeichnet und ausgewertet werden. Dabei erlaubt das eDirectory Ereignisse auf einzelne Verzeichnis−Objekte zu definieren, was die gezielte Überwachung wichtiger Objekte erlaubt. Mit einer geeigneten SNMP−Console (z.B. das im Lieferumfang enthaltene iMonitor−Tool, siehe Abbildung 7) können diese Events manuell ausgewertet werden.

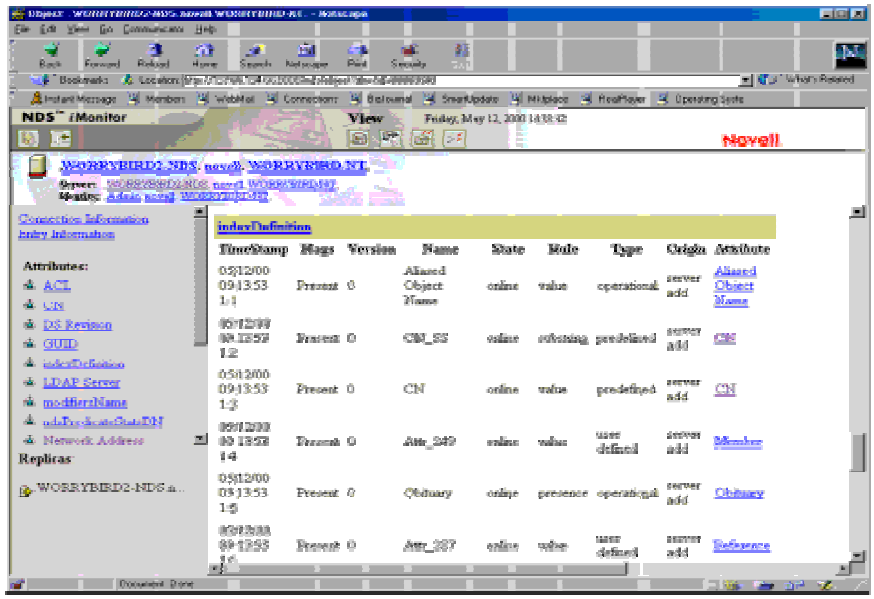

Abbildung 7: iMonitor Benutzungsschnittstelle

Die Applikation iMonitor ist dabei ein Service, auf den mittels HTTP zugegriffen werden kann. Wegen der Sensitivität der gesammelten Ereignisdaten sollte dieser Zugang zwingend über HTTPS erfolgen.

Als Zusatzmodul zum Novell eDirectory 8.6.1 ist der Novell Advanced Auditing Service − NAAS verfügbar, welcher ein Auditing−Framework zur automatisierten Auswertung der Überwachungsereignisse darstellt. Damit lassen sich sogenannte Search Criteria Policies,

Überwachungsrichtlinien (Audit Policies), sowie Benachrichtigungen (Real Time) für das Auftreten von bestimmten Ereignissen definieren und Log File Analyse sowie Performance Monitoring bewerkstelligen.

4 Kurzvergleich: eDirectory und andere Directory−Produkte

Aufgrund der Bedeutung des Directory−Konzeptes in heutigen IT−Strukturen zur Umsetzung skalierbarer und tragfähiger eBusiness−Lösungen tritt das Novell eDirectory gegen eine Reihe anderer Verzeichnisdienstlösungen an. U.a. sind dies:

- iPlanet™ Directory Server, von Sun/Netscape
- DirX™, von Siemens
- SecureWay Directory, von IBM
- Active Directory, von Microsoft

die von Novell mit dem eDirectory auch aus Sicherheitssicht verglichen wurden (siehe entsprechende "Competetive Guide" Artikel unter www.novell.com).

Einführend muss darauf hingewiesen werden, dass ein Vergleich von Verzeichnisdienstprodukten immer nur unter Berücksichtigung des konkreten Einsatzszenarios erfolgen kann. Zudem muss immer berücksichtigt werden, für welchen hauptsächlichen Einsatz die unterschiedlichen Produkte konzipiert wurden.

Die folgenden vier sicherheitstechnischen Hauptunterschiede zu anderen Verzeichnisdiensten können für das Novell eDirectory identifiziert werden:

- Durch die Verwendung der NMAS−Erweiterungen ist es prinzipiell möglich, dass durch das eDirectory beliebige Authentifizierungsverfahren unterstützt werden können. So lassen sich in einfacher Weise Chipkarten, Sicherheitstoken und auch biometrische Verfahren einbinden (z.B. Authentifizierung durch Fingerabdruck). Diese Variabilität und die sofortige Verfügbarkeit von alternativen Authentifizierungsverfahren findet sich derzeit nicht bei anderen Verzeichnisdienstprodukten. Zwar bietet auch das Active Directory die Möglichkeit Authentifizierungsverfahren modular einzubinden, eine standardmäßige Verfügbarkeit von biometrischen Verfahren ist jedoch nicht gegeben.
  Für die anderen Verzeichnisdienste gilt:
  - Die Authentifizierung des iPlanet Directory Servers kann zertifikatbasiert erfolgen.
  - IBMs SecureWay Directory nutzt die Benutzername/Passwort Authentifizierung und setzt das Kerberos−Protokoll ein.
  - Das DirX von Siemens nutzt ausschließlich Benutzername/Passwort Authentifizierung.
-
- Ein Vorteil des eDirectory bei der Durchsetzung der eingestellten Berechtigungen ist, dass die Berechtigungen bei jedem Zugriff neu ausgewertet werden. Auf diese Weise wird sichergestellt, dass Änderungen in Zugriffsrechten auch für Benutzer umgesetzt werden, die bereits eine Verbindung mit dem Verzeichnisdienst aufgebaut haben. Dieser Mechanismus unterscheidet das eDirectory von allen anderen Verzeichnisdiensten, durch die die Berechtigungen eines Benutzers zum Zeitpunkt der Authentifizierung ausgewertet werden. Veränderungen in der Berechtigungsstruktur werden daher vielfach erst beim nächsten Login wirksam.

- Das eDirectory erlaubt über Erweiterungen die verschlüsselte Speicherung von beliebigen Daten im Benutzerobjekt. Dies wird durch die secret store Technologie unterstützt. Für den praktischen Einsatz bedeutet dies, dass z.B. zusätzliche Authentifizierungdaten von

Applikationen im Benutzerobjekt geschützt abgelegt werden können. Andere Verzeichnisdienste sind hier weniger variable und erlauben entweder keine verschlüsselte Speicherung (z.B. des Passwortes) oder können keine weiteren Authentifizierungsdaten im Benutzerobjekt speichern.

- Insbesondere im Vergleich mit dem Active Directory zeigt sich, dass die Erzeugung der sogenannten Security−Principals getrennt ist von deren Verwaltung. Dies erlaubt eine besser kontrollierbare Delegation der Verwaltung und verhindert so Sicherheitsprobleme. Durch die Trennung wird verhindert, dass ein neues Security−Principal−Objekt durch einen Administrator erzeugt werden kann und diesem dann beliebige Rechte zugeordnet werden können .

Der sicherheitstechnische Kurzvergleich zeigt, dass das eDirectory neben einer Vielzahl funktionstechnischer Vorteile auch sicherheitstechnische Vorteile aufweist, so dass diese je nach Einsatzszenario und Sicherheitsanforderungen sinnvoll genutzt werden können.

5 Zusammenfassung

Mit dem Novell eDirectory in der Version 8.6.1 ist ein universell einsetzbarer Verzeichnisdienst verfügbar, der auch unter Sicherheitsgesichtspunkten eine Reihe von Vorteilen anbietet. Daneben ergeben sich auch rein technische Vorteile, die beim Einsatz von eDirectory genutzt werden können.

Das eDirectory kann auf vielen Betriebssystemplattformen betrieben werden, was auch den Einsatz in heterogenen Umgebungen möglich macht. Dadurch braucht nur ein Verzeichnisdienstprodukt administriert werden und die Notwendigkeit von Konvertierungen zwischen verschiedenen Verzeichnisdienstprodukten entfällt. Kann auf den Einsatz anderer Produkte nicht verzichtet werden, so kann das eDirectory auch über die Novell Dir−XML Schnittstelle als Meta−Directory eingesetzt werden. Durch die Verwendung und die Unterstützung relevanter Verzeichnisdienst− und Internet−Standards wird die Einbindung in existierende Umgebungen vereinfacht, so dass das eDirectory auch als Verzeichnisdienstkomponente in beliebigen e−Business−Installationen genutzt werden kann.

Aufgrund der eDirectory−eigenen Mechanismen zur Partitionierung und Verteilung von Verzeichnisbäumen ergeben sich nicht nur Vorteile bezüglich Performanz und Ausfallsicherheit, sondern es ist auch möglich, Verzeichnisteilbäume mit unterschiedlichen Sicherheitsanforderungen optimal zu unterstützen, indem diese nicht nur logisch, sondern auch physikalisch getrennt behandelt werden können. Dabei sorgen die internen Abgleichmechanismen dafür, dass die Informationen immer zeitnah aktualisiert werden. Die Version 8.6.1 unterstützt nun ein Backup−Verfahren, dass im laufenden Betrieb des Verzeichnisdienstes eingesetzt werden kann, so dass Ausfallzeiten für die Datensicherung nicht auftreten. Dies ist insbesondere in e−Commerce−Applikationen vorteilhaft, die hohe Verfügbarkeitsanforderungen stellen.

Aus Sicherheitssicht sind insbesondere folgende Merkmale hervorzuheben, die einen positiven Einfluss auf die eDirectory−Sicherheit haben:

- Unter Verwendung der Secure−Store−Erweiterung ist es Applikationen möglich, beliebige Daten in Benutzerobjekten verschlüsselt abzuspeichern. Dies erlaubt beispielsweise die Nutzung des eDirectory zur sicheren Speicherung von applikationsbezogenen Authentifizierungsdaten für Benutzer. Da die Daten verschlüsselt vorgehalten werden, können sie auch nicht durch privilegierte Benutzter (z.B.: Administratoren) eingesehen werden.

- Zur Absicherung des eDirectory Zuganges können PKI−basierte Authentifizierungsverfahren eingesetzt werden. Vorteilhaft ist dabei, dass bei Nutzung der NMAS−Erweiterungen auch andere Authentifizierungsmethoden (Chipkarten, Biometrie) zum Einsatz kommen können. Zusätzlich erlaubt das sogenannte "Graded Login", die Zugriffsrechte vom verwendeten Login−Mechanismus abhängig zu machen. Dies gilt jedoch nur für den eDirectory−Zugriff über einen Novell−Client. Erfolgt der Zugriff mittels LDAP, so steht insbesondere der SSL−geschützte Zugriff zur Verfügung. Für Applikationen oder Dienste, die eine entsprechende eDirectory−Anbindung unterstützen, kann eine automatisierte Benutzerauthentifizierung durch das eDirectory erfolgen, so dass ein einmal gegen das eDirectory authentifizierter Benutzer, im Sinne eines Single−Sign−On, auch automatisch gegenüber weiterer Diensten authentifiziert wird.
- Die Mechanismen zur Rechtevergabe bieten mehrere Vorteile. Die Wesentlichen sind: es ist möglich, rollenbasiert zu arbeiten und administrative Aufgaben zu delegieren. Dies kann dazu genutzt werden, ein Berechtigungsmodell aufzubauen, dass die Sicherheit der im Verzeichnisbaum gespeicherten Daten wesentlich dadurch erhöht, dass kein "allmächtiger" Administrator existiert. Durch die Prüfung der Zugriffsrechte bei jedem Zugriff ist zudem sicher gestellt, dass Änderungen in den Berechtigungen zeitnah wirksam werden. Dies wird durch die Multi−Master−Update−Fähigkeit unterstützt, da damit auch Berechtigungsänderungen auf beliebigen Verzeichnisservern durchgeführt werden können.
- Neben den eigentlichen Sicherheitsmechanismen, bietet das eDirectory auch flexible Überwachungsmöglichkeiten an, die für das Aufrechterhalten der Sicherheit wichtig sind. Durch die verfügbaren Zusatzprodukte zur automatisierten Auswertung können auch große Systeme geeignet überwacht werden.

Zusammengefasst ergibt sich für die aktuelle Version von eDirectory eine positive Bilanz bezüglich der angebotenen Sicherheitseigenschaften. Zudem zeigt sich die langjährige Verzeichnisdiensterfahrung von Novell in den vom eDirectory oder durch mögliche Erweiterungen angebotenen Funktionalitäten. Mit dem eDirectory steht damit ein Verzeichnisdienst zur Verfügung, der nicht nur universell in e−Business−Anwendungen zum Einsatz kommen kann, sondern sich zudem auch im Bereich von Meta−Directory−Lösungen gut zu positionieren weiß.