

# Mehr Sicherheit im Intranet+Extranet

Aus dem digital business magazin, Ausgabe 1-2007



*Leistungsfähige Directory Services zur Authentifizierung und Autorisierung von Benutzern sind die entscheidende Voraussetzung für Intra- und Extranet-Anwendungen. Heterogene Directory-Landschaft in den Anwenderunternehmen (LDAP, Domino Directory, Microsoft Active Directory/MSAD), Handling von diversen User-Passwörtern sowie oft restriktive Password Expiration Policy erschweren den effektiven Betrieb.*

*Mit SecureDomino lassen sich Anwendungen auf Basis von Domino nicht nur für den Anwender leichter, sondern vor allem auch sicherer betreiben.*

## Domino Directory im Einsatz im Intranet

Bereits in den 90er Jahren ist das Domino Directory von vielen Lotus Notes Anwendern als globales Corporate Directory mit teilweise deutlich über 100.000 Personen und tausenden von Berechtigungs- und Mailgruppen implementiert worden. Im Intranet konnten somit schnell Anwendungen mit individuellen Berechtigungen und Zugriffsbeschränkungen implementiert werden. Alle potenziellen Benutzer der Anwendungen wurden ja für die Mailkommunikation bereits stets aktuell im Domino Directory vorgehalten. Die Pflege der Berechtigungsgruppen konnte leicht von der IT-Abteilung direkt an die verantwortlichen Fachabteilungen delegiert werden. Die Datenqualität des Domino Directory hat daher bei der Wahl der Plattform oftmals den Ausschlag zugunsten von Domino gegeben. Auf die Durchführung vorgeschalteter Directory Infrastrukturprojekte konnte somit verzichtet werden.

## Domino als Plattform für Extranet Anwendungen

Auch für Extranet-Anwendungen waren die Voraussetzungen schnell geschaffen. Hier konnte oftmals sogar die Pflege der Benutzer vollständig an die verantwortliche Fachabteilung oder an den Extranet-Anwender selbst delegiert werden. Zum Erfolg von Domino als Plattform für Extranet Anwendungen hat darüber hinaus sicher auch der attraktive Preis des Domino Utility Express Servers beigetragen, der viel Leistung zu vergleichsweise geringen Kosten liefert.

Zudem konnte das Domino Directory seit jeher flexibel an spezifische Anforderungen angepasst werden. Individuelle Erweiterungen der Personenattribute oder die Automatisierung der Gruppenpflege hat fast jeder Lotus Kunde vorgenommen. Kein Wunder, dass Intra- und Extranet-Anwendungen auf Basis von Lotus Domino sich bereits in den 90er Jahren schnell verbreitet haben.

## Directory-Inseln im Microsoft Umfeld

Ganz anders war zu der Zeit das Bild im Microsoft Umfeld. Mit dem Security Accounts Manager (SAM) in Windows NT konnte Microsoft nur vergleichsweise kleine Directory-Inseln vorzuweisen. Globale Corporate Directories ließen sich mit SAM ebenso wenig realisieren wie individuelle Erweiterungen oder leistungsfähige Schnittstellen zu anderen Systemen. Trotzdem haben fast alle Mitarbeiter in Unternehmen eine Microsoft Benutzererkennung erhalten. Damit hatten die Mitarbeiter allein für Mail-, File- und Print-Services bereits zwei Benutzer-Kennungen, ganz zu Schweigen von ERP, CRM und anderen Systemen.

# Mehr Sicherheit im Intranet+Extranet

Aus dem digital business magazin, Ausgabe 1-2007

## **Effektiv Authentifizieren oder wie viele Namen und Kennungen braucht ein Benutzer?**

Mit der Einführung des Microsoft Active Directory (MSAD) und der Konsolidierung der Directory-Inseln hat sich das Umfeld in den meisten Unternehmen mittlerweile deutlich geändert. In dem MSAD wird oftmals eine strikte Password Expiration Policy definiert, die die Mitarbeiter dazu zwingt ihr Passwort alle paar Wochen zu ändern. Trotz der oftmals eingesetzten "Active Directory Synchronization" müssen sich die Anwender zwei, zumindest temporär unterschiedliche, Passwörter merken. Auch die "Domino Directory Assistance" bietet aus dem Dilemma keinen Ausweg. Schließlich nützt es wenig, wenn ein Anwender unter Domino mit seiner MSAD Benutzerkennung bekannt ist, da die Autorisierung, d.h. die Zuweisung von Berechtigungen durch ACLs und Gruppen, immer auf Basis des Benutzernamens im Domino Directory erfolgt.

Mit der Nutzung der MSAD auch für Domino Browser-Anwendungen ließe sich wenigstens ein Benutzerkennung / Passwort für den Anwender eliminieren. Sicher würde das zu einer höheren Akzeptanz der Anwendungen und geringerem Supportaufkommen führen. Darüber hinaus würde damit aber auch gleich eine effektive Password Expiration Policy implementiert, die für das Domino http Passwort oftmals sträflich vernachlässigt wird.

## **Authentifizierungs- & Security Tool für Domino Server**

Ein Ausweg aus diesem Dilemma bietet das Produkt SecureDomino, das das Kölner Unternehmens TIMETOACT kürzlich auf der Lotusphere 2007 in der Version 6.0 vorgestellt hat. SecureDomino ermöglicht die Authentifizierung gegen ein beliebiges LDAP Directory und übersetzt den LDAP Namen in den Lotus Domino Benutzernamen. Damit funktioniert auch die Autorisierung mit den ACLs und den Gruppen im Domino Directory. Die Version 6.0 bietet zudem ein Logging sämtlicher Authentifizierungsversuche und ermöglicht somit erstmals z.B. dem Benutzer die letzte Anmeldung anzuzeigen.

## **Domino Intrusion Prevention**

Ein weiteres Problem der Domino Directory Services ist, dass es keinen Schutz vor den gefürchteten Brute Force Attacken mit "Password Recovery Tools" bietet. Selbst unbedarfte Anwender können mit diesen zahlreich frei verfügbaren Tools Brute Force Attacken gegen Domino Server fahren. Das Knacken des Passwortes ist somit nur eine Frage der Zeit – ein Wochenende sollte ausreichen bis ein Hacker selbst komplexe Passwörter "knackt" und z. B. vertrauliche Informationen lesen oder Mails im Namen Dritter versenden kann.

Der Schutz vor diesen Gefahren - Intrusion Prevention – ist seit der ersten Version Kernfunktionalität von SecureDomino. Zum Funktionsumfang gehören zudem die IP-basierte Authentifizierung, die Definition von Anmeldezeiten, die Beschränkung des http-Zugriffs auf einzelne Datenbanken oder Verzeichnisse und vieles mehr. Der DSAPI-Filter ist für die Domino Plattformen Windows, Linux (x86), AIX und SUN (SPARC) verfügbar.

Mehr zum Thema auf <http://SecureDomino.de>