

Gruppenarbeit: Aber sicher!

Teamarbeit im Netz ist bequem und effizient, stellt aber mitunter ein Sicherheitsrisiko dar.

Die LAN-Vernetzung von Unternehmen und das Internet, das verschiedene Firmen untereinander verbindet, haben die Arbeitswelt unwiderprüflich verändert. Heute werden Projekte und Dokumente zwar immer noch in Teams bearbeitet, aber die Art der Zusammenarbeit ist nicht mehr mit früher zu vergleichen. Moderne Groupware, aber auch E-Mail-Systeme und sogar geteilte Laufwerke im LAN, vereinfachen die Kommunikation zwischen Teammitgliedern und ermöglichen eine bequeme und effiziente Zusammenarbeit in Projekten – unabhängig davon, wie sich die Gruppe aus internen und externen Mitarbeitern sowie Freelancern zusammensetzt. Allerdings entstehen durch die vereinfachte Zusammenarbeit auch ganz neue Sicherheitsprobleme.

Zahlreiche Aspekte zu berücksichtigen

Moderne Groupware ist komplex und bietet unzählige Funktionen. Entsprechend gibt es auch zahlreiche Aspekte, wie die Sicherheit der Lösung und der Daten unter Umständen kompromittiert werden könnten.

Im Vordergrund stehen dabei natürlich die klassischen Angriffspunkte: das Netzwerk, der Server sowie die Clients. So ist es heute eine Selbstverständlichkeit, dass Server und Netzwerk durch Firewalls, Intrusion-Detection-Systeme und andere Massnahmen bestmöglich geschützt sind, und die Anforderungen an die firmeninterne Netzwerk-Security werden durch Teamarbeit im Netz kaum

verändert. Allerdings ist dabei zu beachten, dass im Team nicht immer bloss interne Mitarbeiter mitwirken, sondern auch externe Beschäftigte sowie mobile Anwender involviert sind. Entsprechend gilt es, auch bei den Rechnern dieser User ein Höchstmass an Sicherheit zu erreichen – beispielsweise durch den Einsatz von Desktop-Firewalls und die Verschlüsselung von Festplatten.

Die bestgesicherten Hardwarekomponenten und Firmennetze nützen allerdings wenig, wenn Angreifer während der Kommunikation zwischen den einzelnen Mitarbeitern auf Daten zugreifen können. Dies ist insbesondere dann möglich, wenn Teammitglieder von ausserhalb des geschützten Firmennetzes auf die Serverdaten zugreifen oder sich per Mail austauschen. Abhilfe schaffen sichere Verbindungen per IPsec-VPN, die verschlüsselte Kommunikation über SSL oder HTTPS sowie die Verschlüsselung von E-Mails und anderweitiger netzgestützter Kommunikation. Dieselben Massnahmen helfen auch firmenintern, sensitive Projekte und Daten vor unerlaubtem Zugriff zu schützen.

Aktualität sichern

Ein wichtiger Sicherheitsaspekt bei Teamarbeiten sind die Zugangsberechtigungen: Nur in den seltensten Fällen wird jedes Teammitglied gleichberechtigt auf alle Daten zugreifen können. Entsprechend muss eine Groupware Möglichkeiten bieten, um Berechtigungen wie Lese-, Schreib- und Löschrechte granular zu verteilen. Während der Teamleiter gleichzei-

tig als Administrator fungieren kann und umfassende Rechte besitzt, sollten andere Mitarbeiter nur selektiv, das heisst im Rahmen ihrer Aufgaben, auf die Dokumente ihrer Kollegen zugreifen können. Wer Dokumente überarbeiten muss, braucht zwingend Schreibrechte, während gewisse Daten per Einschränkung der Leserechte auch innerhalb des Teams teilweise geheim gehalten werden können. Wichtig ist dabei, dass nicht nur der Administrator, sondern sinnvollerweise auch der Urheber eines Dokuments Rechte verteilen kann.

Löschrechte dagegen sollten – wenn überhaupt – nur sehr restriktiv vergeben werden, insbesondere, wenn innerhalb der Groupware eine Dokumentenmanagementfunktion dafür sorgt, dass die Daten aktuell sind und die verschiedenen Dateiversionen nicht überborden. Dafür sorgen etwa integrierte Check-in-Systeme, die überwachen, dass nur ein Anwender gleichzeitig an einem Dokument arbeiten kann. Dieselben Systeme sind für die Synchronisation von verschiedenen Dokumentversionen zuständig, etwa wenn eine Datei von einem mobilen Anwender ausserhalb der Groupware bearbeitet wurde.

Lösungen vorhanden

Ein nicht zu unterschätzender Punkt ist schliesslich das Backup. Dass die komplette Ordner- und Dokumentenstruktur regelmässig gesichert werden muss, dürfte dabei wohl jedem einleuchten. Oft vergessen werden allerdings die weniger offensichtlichen Daten,

die für das Projekt aber ebenso entscheidend sein können, darunter etwa Bookmarks vom Browser oder die gesamte E-Mail-Kommunikation. Es ist natürlich von Vorteil, wenn auch diese Daten in eine automatisierte Backup-Strategie eingebunden werden können.

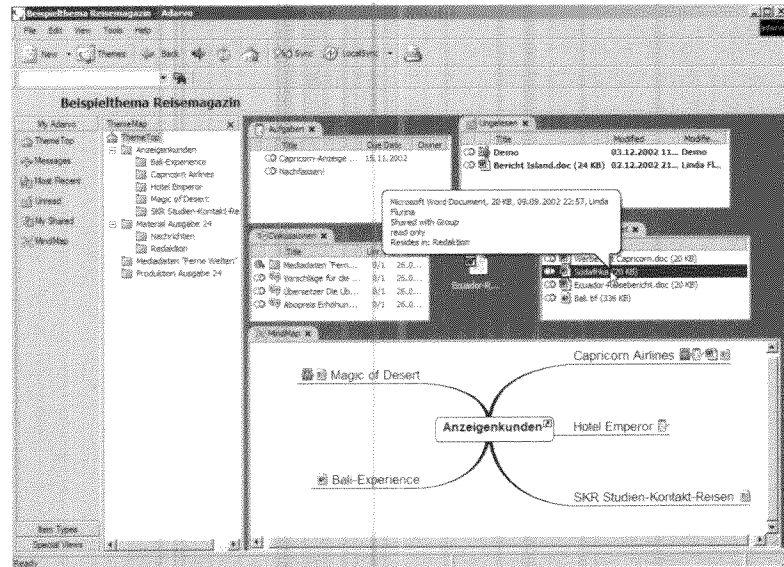
Grundvoraussetzung dafür, dass all diese sinnvollerweise bereits in der Groupware-Lösung integrieren Massnahmen greifen, ist die Benutzer-Authentifizierung, die auch heute noch vielfach über die gute alte Kombination aus Benutzername und Passwort sicherge-

stellt wird. Höheren Sicherheitsanforderungen, insbesondere auch im Zusammenhang mit Fernzugriff über das Internet, vermag diese Lösung allerdings nicht mehr zu genügen – ähnlich wie beim E-Banking wird deshalb in modernen Lösungen auf ein dreistufiges Zugangskonzept gesetzt, bei dem neben Username und Passwort ein sogenanntes Token zum Einsatz kommt. Dieses kann beispielsweise aus einer Nummernkarte (Streichliste) oder einem USB-Token mit Zertifikat be-

stehen. Dass moderne Zusammenarbeit im Netz mehr bedeutet als den blossen Austausch von Dokumenten, die gemeinsame Verwaltung von Terminen und die Kommunikation per E-Mail, ist auch den Herstellern nicht entgangen. Aktuelle Lösungen wie Themeware von Adarvo, eRoom von Documentum oder Livelink von Opentext bieten in der einen oder anderen Form all die angesprochenen Anforderungen an sichere Datenhaltung und Kommunikation. (mva)

Sicherheitsaspekte für Teamarbeit

- ▶ **Login:** Grundanforderung sind ein Benutzername und Passwort, nach Bedarf ergänzt durch ein persönliches Token (USB-Dongle, Nummernliste).
- ▶ **Rechtevergabe:** Lese-, Schreib- und Löschrechte müssen durch den Administrator und den Dokumentbesitzer granular verteilt werden können.
- ▶ **Verschlüsselung:** Sicherheit für mobile Daten wird durch die Chiffrierung der Festplatte und verschlüsselte Kommunikation erreicht.
- ▶ **Versionierung:** Der Zugriff auf die aktuellste Version aller Dokumente und Daten muss durch Dokumentenmanagement, Check-in-Systeme und Synchronisation jederzeit gewährleistet sein.
- ▶ **Datenhaltung:** Schutz für den Server durch Firewall, Intrusion-Detection-Systeme, Spamfilter und Virens Scanner sollte heute ebenso selbstverständlich sein wie eine automatisierte Backupstrategie, die neben den Daten auch Bookmarks und Mails umfasst.
- ▶ **Fernzugriff:** Die teaminterne netzgestützte Kommunikation sollte ausschliesslich über gesicherte Verbindungen (VPN, SSL, HTTPS) sowie mit verschlüsselten Mails erfolgen.



Moderne Kollaborationsprogramme wie das webbasierte Adarvo ThemeWare bieten nicht nur bequeme Zusammenarbeit, sondern erfüllen auch hohe Sicherheitsanforderungen.