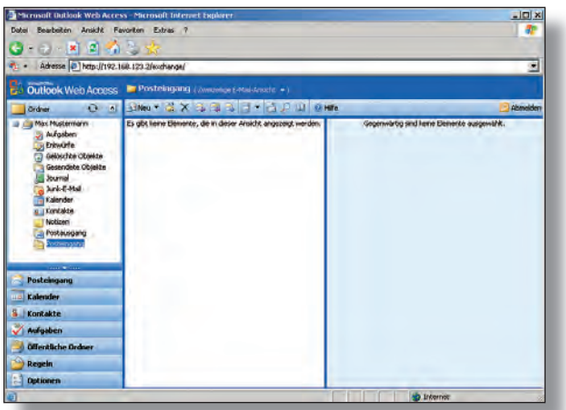
Internet Explorer als Mail-Client



Nachdem unsere Windows-Box in der letzten Ausgabe durch die Installation von Exchange die Fähigkeit bekam, Mails zu versenden/empfangen, steht heute die Erweiterung dieser Funktion an. Und zwar, indem OWA aktiviert und konfiguriert wird. Hinter dem Kürzel verbirgt sich Outlook Web Access und somit das Web-Front-End, mit dem man Vollzugriff auf die eigene Mailbox bekommt, selbst wenn kein Outlook auf der Workstation installiert ist - ein Browser reicht für diesen Zweck aus. Ideal also, wenn man von unterwegs schnell mal nachschauen möchte, ob diese oder jene e-Mail schon eingetroffen ist oder welcher Termin als nächstes ansteht.

von DI (FH) Christian Sudec

Leider muss ich Ihnen zu Beginn gleich die einzige schlechte Nachricht mitteilen: Sie können Outlook Web Access (OWA) leider nicht auf der bisher genutzten Windows-Box einrichten, welche seit dem letzten Mal bereits die Mail-Dienste von Exchange ausführt. Für uns bedeutet dies, dass spätestens jetzt ein zweiter Rechner notwendig ist, auf dem Windows 2003 Server und Exchange völlig analog zum ersten installiert werden müssen, wobei das Gerät aber diesmal als Mitgliedserver in die bestehende Domäne eingehängt werden sollte (in der Serververwaltungs-Konsole einzurichten).

Was dementsprechend mehr Aufwand und Lizenzen mit sich bringt, hat letztendlich aber auch ein paar Vorzüge: zum einen besitzen Sie mit einem zusätzlichen Server ab sofort eine aktuelle Kopie Ihrer Active Directory-Datenbank, an der Sie sich nun auch anmelden können, wenn der erste Server einmal down ist und zweitens lässt sich dessen Festplatte ebenfalls als Backup-Medium (siehe kommende Workshops) nutzen.

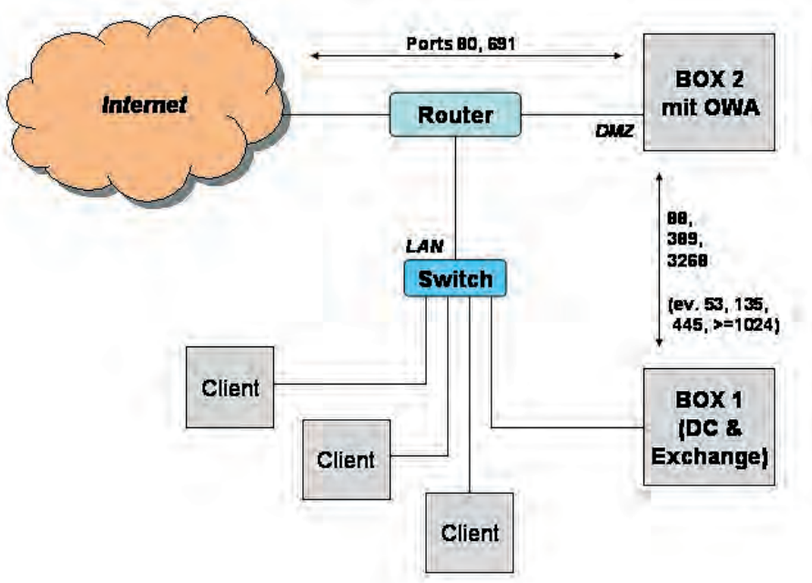
Ist der zweite Server endlich in Betrieb, sollten nicht nur die besagten Verzeichnisdienste repliziert worden sein, sondern auch die beiden Exchange-Instanzen. Dies bedeutet für Sie nichts anderes, als dass Sie mit dem Exchange-Verwaltungstool System-Manager auf der ersten Box weiterhin beide Mail-Server administrieren können.

Konfiguration

Dieses rufen wir sogleich auf, um die getätigte Behauptung zu überprüfen und dem zweiten Exchange-Dienst die Rolle eines Front-End-Servers für Outlook Web Access zuzuweisen. Dazu wechseln Sie in der Baumstruktur auf der linken Seite nach Administrative Gruppen – Erste administrative Gruppe – Server, wo mittels Rechtsklick auf den zweiten Exchange-Rechner (in unserem Fall WCM-BOX2) die Eigenschaften aufgerufen werden. Im Tabellenreiter Allgemein reicht es nun aus, ein Häkchen vor ‚Das ist ein Front-End-Server' zu setzen und mit OK zu bestätigen. Die Empfehlungen der nachfolgenden Dialogbox nehmen wir uns zu Herzen und starten den Server neu – Fertig!

Kurzinfo

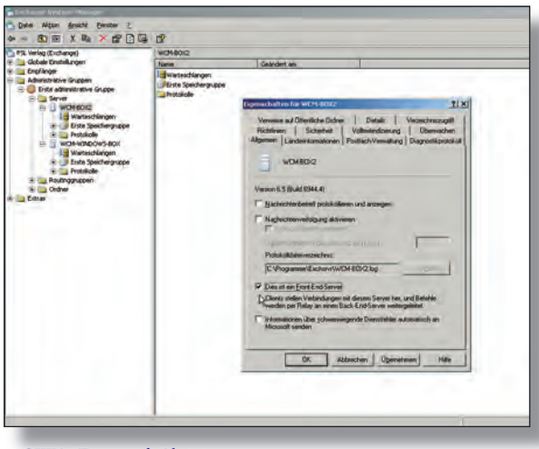
Mit Hilfe dieses Workshops und den noch geplanten werden aus Ihren Anwendern die viel und oft zitierten Information Worker, die jederzeit und von überall aus Zugriff auf relevante Nachrichten und Termine haben, die normalerweise nur im internen LAN zur Verfügung stehen.



Testlauf

Wenn Sie sich ab jetzt mit dem Internet Explorer zur zweiten Box verbinden (http://boxname/exchange/), sollte diese Ihnen einen Anmeldedialog präsentieren. Nach Eingabe von Username (Domänensuffix nicht vergessen; bei uns z.B. ‚mmustermann@wcm.local') und Passwort, landet der entsprechende User auf einer Oberfläche, die einem lokal installierten Outlook in nichts nachsteht. Zumindest solange der IE verwendet wird. Der Zugriff mit anderen Browsern ist zwar ebenfalls möglich, jedoch ist dann die grafische Darstellung eingeschränkt und die Nutzung des Kalenders oder der ToDo-Listen klappt nicht (richtig).

Ein kleiner, aber entscheidender Unterschied ist der Abmelden-Button in

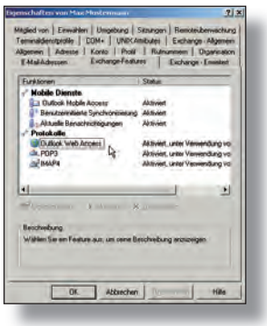


OWA_Frontend-Aktivierung

der rechten oberen Ecke. Sie sollten Ihre Anwender entsprechend schulen, dass sie nach Beendigung ihrer Arbeit, diesen auch anklicken. Andernfalls bleibt die Session (selbst nach Schließen des Browsers) bestehen. Dies ist besonders kritisch in Internet-Cafes, wo nachfolgende Personen einfach die URL erneut aufrufen brauchen, um die Identität des Anwenders zu übernehmen und in seinem Namen e-Mails zu verschicken und Termine zu ändern.

Troubleshooting

Im Vergleich zu anderen Workshops ist nicht die Installation von OWA (abgesehen vom Zeit- und Hardwareaufwand) das Problem, sondern der korrekte Betrieb an einem Router. Spätestens jetzt ist die Anschaffung eines solchen Gerätes dringend anzuraten, da man den Front-End-Server in



Usereinstellungen

eine DMZ (demilitarisierte Zone) hängen sollte, um ihn vom Internet aus erreichen zu können (siehe Grafik). Da der Domänencontroller jedoch im internen Netz verbleibt, sind die häufigsten Probleme, die man sich bei der Verwendung von OWA einhandeln kann auf Schicht 3 zu suchen. Nämlich da, wo Windows-Firewall und/oder der integrierte IP-Filter im Router den Datenverkehr sicherheitstechnisch beschneiden. Für Sie bedeutet dies nun, dass die entsprechenden Ports freigeschaltet und/oder weitergeleitet werden müssen. Im Detail sind dies 80 (TCP) und 691 (TCP) für eingehende Verbindungen. Diese machen das Mail-Front-End aus dem Internet erreichbar. Danach benötigt man noch 88 (TCP & UDP), 389 (TCP & UDP), sowie 3268 (TCP) für Verbindungen zwischen DMZ und LAN, um Mail-User gegen das Active Directory am Domänencontroller authentifizieren zu können. Hapert es daran, dass sich die beiden Server überhaupt einmal gegenseitig finden, bedarf es je nach Routermodell/Firewalltechnologie/LAN-Topologie noch zusätzlicher Ports. Dabei handelt es sich um DNS (53, UDP & TCP), Netlogon (445, TCP) und RPC (135 & 1024-65535, TCP).

Da dieser Haufen an Ports doch einige Fehlerquellen bei der Konfiguration beherbergt, sollten Sie unbedingt systematisch mit dem Freischalten vorgehen: also genau dokumentieren, was, wann und wo geöffnet wurde. Beschränken Sie sicherheitshalber den Datenaustausch zwischen DMZ und LAN auch noch auf die IP-Adressen der beiden Server, um die Löcher so gering wie möglich zu halten.

Administration

Natürlich besteht auch die Möglichkeit, den Sicherheitshebel auf einer höheren Ebene anzusetzen und nur einzelne User vom Webzugriff auszunehmen. Die notwendigen Einstellungen sind wieder in den Eigenschaften des jeweiligen Kontos in Active Directory-Benutzer und –Computer vorzunehmen. Der dazu notwendige Tabellenreiter hört auf den Namen Exchange-Features, in dem man Outlook Web Access de- & reaktivieren kann. Standardmäßig besitzen nämlich alle - nach der Installation von Exchange - erstellten Benutzer das OWA-Zugriffsrecht.

Ab hier

Bei verstärkter Nutzung von Outlook Web Access werden sich bei Ihren Anwendern mit ziemlicher Sicherheit weitere Wünsche auftun. Der erste wird sicherlich der nach Verschlüsselung der Daten sein, da jeder Browser diese im Normalfall im Klartext überträgt. Dazu bedarf es der Aktivierung von SSL, das wiederum ein gültiges Sicherheits-Zertifikat voraussetzt. Dieses kann man von einer öffentlichen, aber kostenpflichtigen Certificate Authority (CA) wie z.B. VeriSign beantragen oder selbst generieren. Dann muss allerdings eine eigene CA im internen LAN installiert werden, die diese Aufgabe übernimmt. Keine Sorge, dies wird in einem kommenden Workshop abgehandelt.

Weiters lässt sich dann auch die Forms-basierte Authentifizierung von Exchange aktivieren. Damit können Time-Outs via Cookies übermittelt werden, die der Browser nutzt, um Anwender, die (wieder mal) vergessen haben, sich abzumelden nach einer gewissen inaktiven Zeitspanne aus OWA rauszukicken. Somit wäre das oben erwähnte Sicherheitsrisiko bei der Nutzung von OWA in Internet-Cafes sehr stark reduziert worden. ■

OWA-Tuning

Um den Datenverkehr zwischen Domänencontroller (auch erster Exchange-Server) und Front-End-Server gering zu halten, hat es sich bewährt, die zwei folgenden Registry-Einträge vorzunehmen:

HKLM\System\ccs\services\MSExchangeDSAccess
DWORD: LdapKeepAliveSecs WERT: 0

HKLM\System\ccs\services\MSExchangeDSAccess
DWORD: DisableNetlogonCheck WERT: 1

Zusätzlich ist es ratsam, die nicht benötigten Dienste am Front-End-Server abzuschalten. Erstens um die Performance zu erhöhen (vor allem, wenn der PC etwas schwächer ist) und zweitens, um eine möglichst geringe Angriffsfläche gegenüber Crackern zu bieten. So benötigt OWA genau vier Services, um korrekt zu funktionieren. Dies wären der WWW-Publishingdienst, das Simple Mail Transfer Protocol (SMTP), die Microsoft Exchange-Systemaufsicht und das Microsoft Exchange-Routingmodul. Je nach Einsatzzweck der zweiten Box können Profis natürlich auch die Windows-eigenen Dienste mehr oder weniger drastisch einschränken. Achten Sie aber unbedingt darauf, dass die Abhängigkeiten weiterhin erfüllt sind.