von Carol Woodbury

Die letzten beiden Releases von OS/400 – V4R2 und V4R3 – enthalten diverse Ergänzungen und Erweiterungen in zentralen Bereichen, die das System noch sicherer machen. Diese Ergänzungen erleichtern zum Beispiel die Kontrolle über die Konfiguration der TCP Umgebung, machen e-Business sicherer und einfacher zu verwalten und unterstützen sofort die Installation eines ersten Sicherheitsplans mit der Option zur Detaillierung.

Der wachsende Einsatz von Internet-Technologien hat einige neue TCP/IP Anwendungen für die AS/400 und einige Ergänzungen zu bestehenden Anwendungen hervorgebracht. In V4R2 sind TCP/IP Anwendungen integriert, die das Point-to-Point Protocol (PPP) und Domain Name Service (DNS) enthalten. PPP bietet mehr Sicherheit als sein Vorgänger, das Serial Line Internet Protocol (SLIP). In PPP ist die Berechtigung des Anwenders direkt integriert und nicht von einem Script abhängig, das vom User selbst entwickelt wurde. PPP beinhaltet zudem Optionen im Bereich IP Adressenvalidierung und -konfiguration, um zu vermeiden, daß ein Anwender Sessions nutzt, die ein anderer Anwender vorher entwickelt hat. Die Verschlüsselung von User IDs und Passwörtern ist, falls von beiden Seiten unterstützt, ebenso möglich. In DNS ist die Übertragung von Hostnamen in IP Adressen integriert.

Künstler Burgy Zapp

Normalerweise sollte DNS über den Internet Service Provider (ISP) oder auf der Firewall laufen, um zwischen dem Internet Domainnamen (z.B. Fehler! Textmarke nicht definiert.) und der IP Adresse auf dem System zu vermitteln. Es bietet sich an, DNS auch auf einem internen Netzwerk zu betreiben, um die Übertragung von Hostnamen in IP Adressen im Intranet zu gewährleisten. Läuft DNS intern und extern, ist die Topologie des internen Netzes auch für Außenstehende sichtbar. Mit V4R2 stellt die AS/400 DNS für das Intranet zur Verfügung. Mit Telnet Exit Points läßt sich ein Programm erstellen, um Sitzungsanfragen zu akzeptieren oder zu verweigern, spezifische Optionsbeschreibungen für Anforderungen festzulegen, spezielle Benutzerprofile für Sessions festzulegen und Systemverbindungen und -trennungen über den Telnet Server zu definieren.
Die neuen TCP/IP Features in V4R3 sind Network Address Translation (NAT) und IP Packet Filtering.

Mit Hilfe von NAT können zwei Netzwerke miteinander verbunden werden, die inkompatible IP

Adressen-Schemata besitzen. Ebenso kann diese Funktion genutzt werden, um interne Adressen durch Verschlüsselung vor dem Zugriff über das Internet zu schützen (durch Übertragung zwischen einer internen IP Adresse, die für das Internet keine Gültigkeit besitzt und einer IP, die gültig ist). Wird die AS/400 als öffentlicher Web Server genutzt, der an das Internet angeschlossen ist, kann mit Hilfe von IP Packet Filtering das eigene System vor unerwünschtem IP Verkehr geschützt werden. Ebenso kann diese Funktion auf der AS/400 als ein weiterer Verteidigungslayer in der Internet-Sicherheitsstrategie dienen.
Obwohl NAT und IP Packet Filtering in Kombination zum Schutz des Systems eingesetzt werden können, sollten sie nicht anstatt einer Firewall zum Schutz der internen AS/400 genutzt werden. Falls das System tatsächlich via Internet attackiert werden sollte, könnte es dann nämlich mehr damit beschäftigt sein, Packet Filtering Funktionen zu betreiben, statt die normalen Anwendungen zu bearbeiten. Grundsätzlich ist es daher empfehlenswert, die Packet Filtering Funktionen auf der Firewall zu belassen. Beispiele für geeignete Implementierungen von NAT und IP Packet Filtering Funktionen auf der AS/400 oder einer Firewall gibt´s unter Fehler! Textmarke nicht definiert..

In der Version V4R3 hat der Hypertext Transfer Protocol (HTTP) Server (der umbenannte HTTP Server für die AS/400) nun einige Erweiterungen. Erstens ist er jetzt dahingehend konfiguriert, daß er Berechtigungen auf der Clientseite überprüfen kann, während der Secure Sockets Layer (SSL) läuft. (Das SSL Protokoll vernachlässigt die Berechtigungsprüfung auf der Serverseite, stellt aber die Option zur Prüfung auf der Clientseite bereit.) Ist der HTTP Server für die Berechtigungsprüfung konfiguriert, können Anwender nun digitale Zertifikate zur Identifizierung einsetzen. Ebenso kann vorher festgelegt werden, welche Anwender welche Web Seiten aufrufen können.
Soll mit dem HTTP Server für die AS/400 auch SSL eingesetzt werden, muß nicht mehr eine extra HTTP Server Lösung eingesetzt werden. Statt dessen muß eines von drei Kryptographie Produkten eingesetzt werden: Cryptographic Access Provider 40-bit (5769-AC1), Cryptographic Access Provider 56-bit (5769-AC2) oder Cryptographic Access Provider 128-bit (5769-AC3). Eines dieser drei Produkte wird den erforderlichen Level an Verschlüsselung für jedes IBM Produkt bereitstellen, das Kryptographie Funktionen auf der AS/400 einsetzt. Die Inhalte jedes Produktes entsprechen den Exportbestimmungen der US-Regierung für Kryptographieverfahren.

SOCKS Client Support

In dem Release V4R2 wird die AS/400 „firewallfreundlicher„ durch den Zusatz von nativem Sockets Security (SOCKS) Client Support. Das ermöglicht beispielsweise FTP-Transport von der AS/400 über eine Firewall auf einen Server im Internet.

Digital Certificate Manager

Da digitale Zertifikate einen so wichtigen Part im Internet und in der Internet-Sicherheit einnehmen, hat IBM in V4R2 die Option Digital Certificate Manager integriert. Damit lassen sich: