



Foto: fi online

Sicherheit

Festung gegen moderne Raubritter

Unternehmen mit vielen Niederlassungen und Außendienstmitarbeitern sind in verstärktem Maße auf Sicherheit angewiesen. Ein leistungsfähiges EDV Netzwerk und die Anbindung an das Internet birgt viele Risiken. Nur ein umfassendes Sicherheitskonzept und die ständige Pflege und Wartung der Technologie vermögen den Angriffen zu trotzen.

Wie schützte man im Mittelalter Ländereien und Schätze gegen unliebsame Angreifer? Durch den Bau von Burgen. Eine langwierige und strapaziöse Arbeit. Über all die Jahrhunderte mussten ständig neue Mauern gezogen, Türme errichtet und aufgebrochene Löcher ausgebessert werden. Je dichter das Netz der Verteidigungslinien, desto größer die Chance, die immer listigeren und mit schweren Waf-

fen beladenen Horden vom Tafelsilber fernzuhalten. Unternehmen heute müssen zwar keine Landstriche verteidigen. Das wertvollste Gut der Informationsgesellschaft sind die Daten, die auf Festplatten lagern und daraufwarten, über das weitverzweigte Verkehrsnetz an Glasfaserkabeln geschickt zu werden. Die Raubritter von heute sind Hacker und Virenprogrammierer, die auf ihren trojanischen Pferden angeritten kom-

men. Das Schlimme ist, dass man die Feinde im Gegensatz zu früher nicht sehen kann und nicht einmal weiß, woher sie kommen. „Gefahren drohen von Außen und Innen, wobei meiner Meinung nach die Angriffe durch eigene Mitarbeiter häufiger vorkommen und schwerer zu beherrschen sind“, sagt Jürgen Terpin, Leiter im Bereich Informationstechnologie bei der Amadeus AG. „Die Angriffsmethoden werden immer komplizierter, variabler und subtiler. Verschiedene Angriffsmethoden werden kombiniert und massiv verschleiert“, ergänzt Matthias Krauß, Abteilungsleiter Network Security und Network Technology bei Networkers. Was müssen die Unternehmensfürsten tun, um ihre digitalen Kostbarkeiten effizient zu schützen?

„Sicherheit muss endlich als Prozess verstanden werden, der kontinuierlich weitergeführt wird“, so Krauß. Viele Firmen würden den Fehler machen, sich nur gegen einzelne Eingriffsarten zu schützen. Dadurch gebe es zu viele Lächer, durch die Feinde unbemerkt hindurch schlüpfen können. Notwendig ist der Aufbau eines Abwehrbollwerks, das mit einem Verbund von Sicherheitsmaßnahmen Datendieben den Garaus macht.

Bei dem Personal-Dienstleister Amadeus liegt das Kerngeschäft im Finanz- und Rechnungswesen. Es wird mit äußerst sensiblen Daten hantiert. Neben dem Hauptsitz in Frankfurt am Main gibt es in Deutschland 20 Niederlassungen und jeweils eine in Österreich, England und den Niederlanden. Daher besteht ein hoher Kommunikationsbedarf unter allen Außenstellen und der Zentrale. Auch die Nutzung des Internet darf nicht fehlen. Damit steigt das Risiko, dass Unbefugte von Außen Zugang auf Interna bekommen und Mitarbeiter ihre Rechte missbrauchen.

Sicherheit als Gesamtkunstwerk

„Bei Amadeus hat man die Zeichen der Zeit erkannt“, sagt Krauß. „Dort wollte man keine Schnellschüsse und Teillösungen, sondern ein gut geplantes Gesamtkunstwerk.“ Mit diesem Anliegen wandte sich Amadeus Anfang 2000 an die Networkers AG. Die Neu-Ulmer sind unter anderem Spezialisten für die Realisierung, Planung und den Betrieb von IT-Sicherheit in Unternehmen und Organisationen. Die Anforderungen waren hoch: Zunächst sollte das Netzwerk der Firmenzentrale umstrukturiert und ein großes Corporate Network mit allen Niederlassungen errichtet werden. Neben der Absicherung des Netzwerkes lag das Hauptaugenmerk auf der Revisions-sicherheit der IT, um auch den Wirtschaftsprüfer von Amadeus zufrieden zu stellen. Da der Personal-Dienstleister nur einen Partner bei der Umsetzung des Konzeptes haben wollte, kam Networkers als 'Full-Service'-Anbieter gerade recht. „Entscheidungsfaktoren waren der komplette Service, das tiefe technische Verständnis, das umfassende Si-

cherheitskonzept und die konzeptionelle Kompetenz der Networkers AG“, sagt Terpin.

Die Konzeptarbeiten richteten sich unter anderem nach den im Grundschrift-handbuch und im IT-Sicherheits-handbuch dokumentierten Vorgehens-empfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI). Gerade wenn ein Unternehmen den umfassenden Ansatz für ein Sicherheitskonzept sucht, sind die beiden Werke, die häufig fälschlicherweise als Gesetz angesehen werden, eine solide Grundlage: „Die Empfehlungen decken alle relevanten Bereiche ab, sowohl technisch als auch organisatorisch. Die notwendigen Maßnahmen werden sehr transparent dargestellt und belegt“, sind sich Terpin und Krauß einig. Damit war ein sehr gutes Gerüst für den Bau der Festung vorhanden.

Sensibilisierung der Mitarbeiter

Insgesamt zehn Personen (sechs von Networkers und vier von Amadeus) machten sich an die Arbeit. Nach der Analyse der IT-Infrastruktur wurde nach den Maßgaben des BSI der Schutzbedarf der Amadeus festgestellt. Ergänzend dazu fand eine Untersuchung der möglichen Bedrohungen und Risiken statt. Nach der Anlage des Sicherheitskonzeptes ging man in die Realisierungsphase über. Zunächst wurde im lokalen Netz wie auch im Weitverkehrsbereich eine moderne Netzwerkinfrastruktur geschaffen, welche neben der zuverlässigen und schnellen Kommunikation auch die Integration einer Netzwerksicherheitslösung ermöglicht. Anschließend kümmerte man sich um die Absicherung des zentralen Internet-Zugangs in Frankfurt am Main.

Ähnlich wie bei einer Burg ist es von großer Wichtigkeit die Tore zur Außenwelt als natürliche Schwachpunkte zu schützen. Als Wächter platzierte das Projektteam ein High-End Firewallsystem. Dieses wurde selbst noch einmal durch paketfilternde Router abgesichert. Damit realisierte man einen mehrstufigen Schutz des lokalen Netzwerkes gegenüber externen Netzen wie dem Internet. Damit auch kein moderner Raubritter

durchschlüpfen kann, wurde gegen Hacker ein Intrusion Detection System (IDS) installiert, das bei einem Angriff sofort Alarm schlägt. Nun bestünde noch die theoretische Möglichkeit, dass Angreifer über den Postweg gefährliche Viren in die Festung einschleusen. Dagegen sind Firewall und IDS in der Regel machtlos, da eingehende E-Mails nicht auf ihre Inhalte überprüft werden. Deshalb wurde an der zentralen Pforte und allen Servern des Netzes sowie an den einzelnen Arbeitsstationen Virens Scanner eingebaut. Werden neue Viren bekannt, findet eine automatische Aktualisierung der Scanner statt, um auch den neuen Listen der Feinde zu begegnen.

Damit auch die Angestellten keine Chance haben, mit den Daten - absichtlich oder unabsichtlich - Unfug zu treiben, wurden sie durch Schulungen und Informationsveranstaltungen für das Thema Sicherheit sensibilisiert und entsprechende Authentifizierungslösungen etabliert. Außendienstmitarbeiter und Telearbeiter wählen sich mittels Einmalpasswörtern (Token) in ein speziell abgesichertes Netzwerk-Segment ein. „Die Zugriffe passieren hierbei zwingend die zentralen Sicherheitssysteme, wo eine entsprechende Kontrolle und Protokollierung erfolgt“, beschreibt Krauß den Ablauf.

Finanzielle Schäden vermeiden

Sicherheit hat seinen Preis. Die Amadeus AG hat insgesamt rund 300.000 Euro in ihr Bollwerk investiert. Viele schrecken vor den Ausgaben zurück, weil sich ein direkter Gewinn nicht ermitteln lässt. Solange nichts passiert, mag dieser Leichtsinngerechtfertigt sein. Wird ein Unternehmen aber doch überfallen, erlebt es häufig einen finanziellen Supergau, ganz zu schweigen vom Vertrauensverlust bei den Kunden. Da ist es doch besser, gewappnet zu sein und für präventive Maßnahmen gesorgt zu haben: „Wir sind mit der Lösung von Networkers sehr zufrieden. Sie erfüllt ihren Zweck und hat uns schon mehrfach vor Schaden bewahrt“, sagt Terpin.

CYbiz

Alexander Pradka
(alexander.pradka@cybiz.de)