

Proaktiver Virenschutz im RWE-Netz

Der Versorgungsriese RWE hat sein Sicherheitskonzept gegen Computerviren auf der Basis von "proaktivem Outbreak-Management" modernisiert. Die Lösung sollte zentral administrierbar sein, um so für den entscheidenden Zeitvorsprung im Angriffsfall zu sorgen.

Von Jörg Lenuweit*

Steckbrief

Unternehmen: Energie- und Wasserversorger
Ziel: Restrukturierung des Sicherheitskonzepts zur Optimierung des Virenschutzes.
Projektumfang: Schutz vor digitalen Schädlingen für den ein- und ausgehenden SMTP-, HTTP- und FTP-Datenverkehr am Gateway, für sämtliche PCs und File-Server sowie 60 interne E-Mail-Server.
Herausforderung: Neue Antivirenlösung musste mit den bestehenden Lösungen harmonisieren, zwei unterschiedliche Exchange-Versionen bedienen können und sich dennoch über eine Schnittstelle zentral bedienen lassen.
Zeitraum: Projektstart Anfang 2003.
Stand heute: Im Produktivbetrieb.
Ergebnis: Zentralisierter Virenschutz für unterbrechungsfreien Informationsfluss auf Basis von "proaktivem Outbreak-Management".
Technische Basis: Interscan Virus-Wall, E-Manager, Scanmail for Exchange und Control Manager von Trend Micro; Antivirenprodukte von Symantec.
Realisierung: RWE Systems Computing und Networkers AG (Systemintegrator).

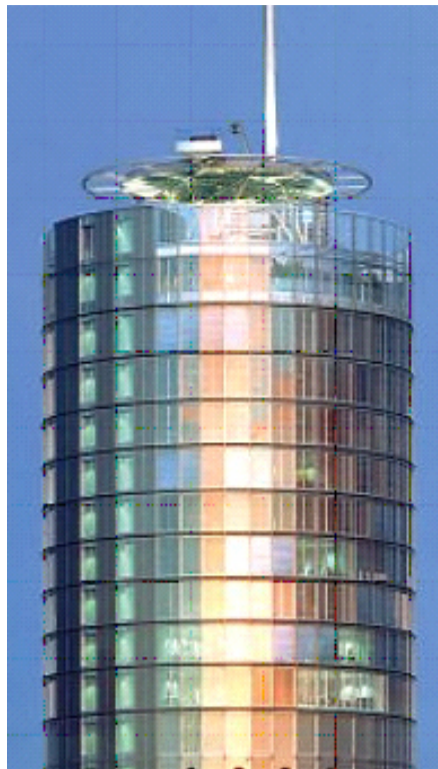
SEIT ÜBER 100 JAHREN versorgt der Großkonzern RWE Millionen Priv- und Geschäftskunden mit Strom, Gas, Wasser und einer Vielzahl von Dienstleistungen rund um die Energie. Ausfallsicherheit der Infrastruktur ist für den Anbieter ein entscheidendes Kriterium. Denn wird in einer sensiblen Branche wie der Energieversorgung der Datenfluss im Konzern unterbrochen, hat das Konsequenzen für den Kunden. Aus diesem Grund kommt dem vorbeugenden Schutz der Netze vor Computerviren bei RWE besondere Bedeutung zu.

Mit der Administration der IT-Umgebung des Konzerns ist RWE Systems Computing betraut. Rund 500 Mitarbeiter an 30 Standorten in Deutschland sind für den reibungslosen Netzwerkbetrieb mit allen Servern und Arbeitsplatz-PCs in einem komplexen Geflecht an Tochterunternehmen verantwortlich. Sie sorgen für den ungehinderten Datenstrom durch die verzweigten Netze und den fehlerfreien Dienst aller Programme. Rund 22.000 Rechner, 10.000 Internet-Zugänge und fast 30.000 E-Mail-Boxen werden vom IT-Stab des Dienstleisters installiert und gewartet.

Optimierter Schutz, leichte Administrierbarkeit

Bei der Restrukturierung des Sicherheitskonzepts für RWE zu Beginn des Jahres 2003 war nicht nur angesagt, den Virenschutz zu optimieren. Um die Effizienz zu steigern, war auch eine leichter administrierbare Lösung gefragt. "Wir waren auf der Suche nach einem ganzheitlichen Ansatz in puncto Virensicherheit", so Projektleiter Stefan Eesmann von RWE Systems. "Das vorhandene zweistufige Antivirenkonzept deckte unser Sicherheitsbedürfnis nicht mehr ausreichend ab."

Bisher baute RWE Systems auf ein Konzept, bei dem unterschiedliche Einfallstore durch Antivirenprodukte abgesichert wurden. Die Unternehmensrichtlinien sahen vor, dass der ein- und ausgehende SMTP-, HTTP- und FTP-Datenverkehr am Gateway geschützt wurde. Unabhängig davon waren die einzelnen PCs und File-Server abgesichert. Vom Einsatz heterogener Antivirensoftware versprach sich der Konzern einen Zeitgewinn im Fall eines Virenausbruchs. Je nach Reaktionszeit erhielt man das aktuelle Viren-Pattern zuerst für den Schutz am Gateway oder am PC beziehungsweise File-Server. Dadurch wurde zumindest für einen Bereich die kürzestmögliche Latenzzeit



zwischen dem Bekanntwerden eines neuen Virus und der Abhilfe durch das Pattern-Update garantiert. Nachteil dieser Sicherheitspraxis: zweifacher administrativer Aufwand wegen Pflege und Wartung unterschiedlicher Produkte.

Hilfestellung bei der Überarbeitung der RWE-Sicherheitspraxis leistete der Systemintegrator Networkers AG. Dessen Konzept sicherte nicht nur zwei mögliche Einfallstore, sondern berücksichtigte auch den bis dato ungeschützten internen Mailverkehr unter den vielen RWE-Beteiligungsfirmen. Die zusätzliche Einführung von zentral verwaltbaren "Outbreak Prevention Services" (OPS) gewährte darüber hinaus den gewünschten Handlungsspielraum. Michael Voss von Networkers erklärt: "OPS stellen ein Schutzkonzept dar, bei dem ein Unternehmen während der Wartezeit selbst aktiv werden kann. Das bedeutet wesentliche Vorteile im Kampf gegen die Zeit zwischen der Virenwarnung des Herstellers und dem entsprechenden Pattern-Update."

Die Networkers AG suchte zur Umsetzung dieser Strategie ein Produkt für den Schutz der 60 internen E-Mail-Server und nach einer zentralen Management-Konsole für das gesamte Antivirensystem. Die Mail-Server abzudecken war notwendig, da die interne Ansteckungsgefahr durch E-Mail-Viren mit der großen Zahl von Notebook-Usern stieg. Die Notebook-Mailboxen wurden nach dem Außeneinsatz nicht am Gateway durchsucht, sondern direkt an das Netzwerk angeschlossen: Hier öffnete sich ein potenzielles Einfallstor. Die zentrale Management-Konsole wurde für das proaktive Outbreak-Management geplant. Über deren Funktionalität sollte zukünftig auf

zusätzlicher Ebene ein Schutz über das gesamte Netzwerk ausgebreitet werden: Wenn nach Auftreten eines neuen Computervirus das spezifische Pattern-File noch nicht vorliegt, kann das Unternehmen nach der ersten Benachrichtigung über die Gefahr durch den Antiviren-Hersteller dennoch selbst reagieren. Denn verdächtige E-Mails werden aufgrund von allgemeinen Eigenschaften, beispielsweise dem Format angehängter Dateien, geblockt.

Lovegate erleichterte die Entscheidung

Als die Evaluierungsphase für die geplanten Neuerungen begann, waren bei RWE die folgenden Produkte im Einsatz: Auf Ebene des Gateways untersuchte die "Interscan VirusWall" des Anbieters Trend Micro den ein- und ausgehenden Datenverkehr nach Computerviren. Zusätzlich blockte deren "eManager" unerwünschte Attachments und filterte Spam. Die Arbeitsplatzrechner und File-Server wurden durch Produkte von Symantec geschützt. Diese sollten mit der neuen Lösung harmonisieren. Die gesuchte Software musste darüber hinaus eine technische Herausforderung bewältigen. Bei RWE waren unterschiedliche Exchange-Versionen auf den Mail-Servern im Einsatz. Die Antivirensoftware musste sowohl Exchange 5.5 als auch Exchange 2000 bedienen. "Beide Versionen nutzen unterschiedliche Application Programming Interfaces (APIs), über die die Antivirensoftware direkt auf die Postfächer zugriff", so Rainer Schneider, technischer Berater bei Networkers. "Das RWE-Netzwerk benötigte eine Lösung in zwei unterschiedlichen Versionen, die sich dennoch über eine Schnittstelle zentral verwalten ließ."

Mitten in der Evaluierungsphase unterschiedlicher Produkte trat bei RWE der Ernstfall ein. Der Virus "Lovegate" verbreitete sich im Februar 2003 in Windeseile über die ungeschützten Mail-Server innerhalb des Netzwerks. RWE Systems musste die Server herunterfahren, um die sich rasch über Outlook-Adressen verbreitende E-Mail-Flut einzudämmen. Erst nach zwei Stunden fiebriger Arbeit der Systemadministratoren konnten die Server wieder gestartet werden. Eine erste Schadensbilanz zeigte, dass 2000 Rechner und 50 Mail-Server mit dem Virus infiziert waren. Stefan Eesmann testete mit dem Networkers-Team zu dieser Zeit unter anderem die Lösung "Scanmail for Exchange" von Trend Micro und die darin enthaltenen Features für die

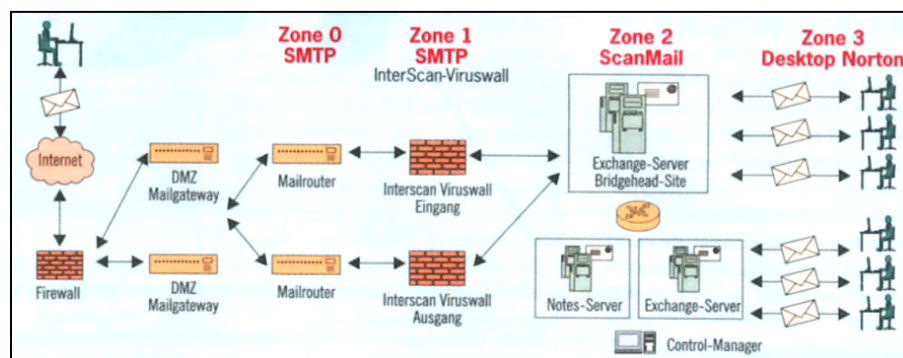
zentrale Antiviren-Systemverwaltung. Die Management-Eigenschaften des "Control Managers" bewährten sich bei der Entfernung des Lovegate-Virus aus den infizierten Mail-Servern: Innerhalb eines Mantages wurden die Lösungen zu Testzwecken an einem der befallenen Exchange Server installiert. Diese Kombination konnte überzeugen.

Handeln statt Warten

Ausschlaggebend für die Wahl waren zum einen die Funktionalität und die leichte Administrierbarkeit des Control Managers. Über ihn werden Pattern-Files zentral aktualisiert. Die Einstellungen der Antivirensoftware an den Servern lassen sich aus der Ferne über einen Web-Browser konfigurieren. Zum anderen ist nun die Grundlage für ein proaktives Outbreak-Management bei einem Virenausbruch geschaffen. Sobald die ersten Informationen über einen neuen Computervirus vorliegen, werden Gegenmaßnahmen eingeleitet - auch ohne das eigentliche Pattern. Im Zuge der produktübergreifenden Enterprise-Protection-Strategie (EPS) von Trend Micro sind über das Tool angriffsspezifische Einzelheiten und Richtlinienempfehlungen über Internet automatisch verfügbar. Diese lassen sich über die Software zentral für das gesamte Netzwerk einsetzen.

Schnelle Realisation

Der Vorteil einer derartigen Absicherung während der Latenzzeit liegt auf der Hand: Das Beispiel Lovegate hat gezeigt, dass die kurze Zeit zwischen Virenalarm und Verfügbarkeit des Pattern-Updates für einen Computervirus zur Verbreitung ausreicht. Der Control Manager kann das Unternehmen für diese Zeitspanne vor der Ansteckung mit dem neuen Virus schützen. Das Netzwerk wird schnell und effizient abgeschottet, ohne dass Verfügbarkeit und Leistung eingeschränkt sind. Aufbauend auf der ersten Bewährungsprobe vollzog man den Rollout der neuen Lösung auf allen Exchange-Servern des RWE-Netzwerks innerhalb weniger Wochen.



Quelle:
 COMPUTERWOCHE
 Ausgabe 38/2003
 Seite 30f.

*Jörg Lenuweit ist freier Autor in München.