

Doppelte Absicherung gegen 50.000 Viren

Zur Optimierung der Viren-Abwehr setzt der TÜV Rheinland auf eine Doppelte Absicherung. Unterstützt vom Bremer Security-Spezialisten Ampeg wurde eine neue Anti-Viren-Strategie aufgesetzt, die komplementäre Lösungen verschiedener Hersteller verwendet und so doppelten Schutz bei weniger Administrationsaufwand bietet.

TÜV Rheinland ist heute ein Synonym für geprüfte Sicherheit und Zuverlässigkeit, egal ob es um Stromanlagen, Kraftfahrzeuge, Kraftwerke, Brandschutz, Aufzüge, Umweltschutz oder Produktsicherheit geht. Die wenigsten regelmäßigen Kunden des TÜV Rheinland machen sich allerdings klar, dass aus den Überwachungsvereinen in den letzten Jahrzehnten überaus erfolgreiche Unternehmen geworden sind. So erwirtschaftet die Kölner Konzerngruppe, hervorgegangen aus den entsprechenden Organisationen Rheinland, Berlin und Brandenburg, heute mit ihren über 10.000 Mitarbeitern 800 Millionen Euro Umsatz, davon etwa 40 Prozent im Ausland. Das Unternehmen verfügt über 300 Niederlassungen in 58 Ländern, allein in Deutschland werden 100 Prüfstellen betrieben.



Ein guter Ruf, wie ihn der TÜV Rheinland in Sachen Sicherheit ohne Zweifel hat, will natürlich gepflegt sein – selbstverständlich muss der TÜV selbst "sicher" sein und den hohen Maßstäben gerecht werden, die er bei anderen überwacht. Würden beispielsweise die Dienstfahrzeuge oder Personenaufzüge eine technische Überprüfung des TÜV nicht bestehen, also nicht "durch den TÜV" kommen, so wäre ein erheblicher Imageschaden mit entsprechendem publizistischen Echo die Folge. Technische und bauliche Anlagen, eingesetzte Systeme, aber auch Betriebsabläufe jedes TÜV Unternehmens müssen daher den besonders hohen Ansprüchen genüge leisten.

Dies gilt selbstverständlich auch für die eigene IT des TÜV Rheinland, die hier wie überall in modernen Unternehmen alle Geschäftsprozesse und die gesamte Kommunikation trägt. Entsprechend dem weltweiten Engagement des TÜV Rheinland ist die gesamte IT des Unternehmens hoch integriert, alle Niederlassungen und Tochtergesellschaften sind in einem globalen Netzwerk mit einem einheitlichen Active Directory abgebildet. Um die weltweit verteilten Standorte zu administrieren, betreibt der TÜV Rheinland ein komplexes WAN. Selbstverständlich gibt es seit dem Eintritt ins Internet-Zeitalter eine entsprechende Firewall, um unberechtigte Zugriffe auf die Netze zu unterbinden.

Blaster eskaliert Sicherheitsthema

Das Thema Sicherheit eskalierte vor einigen Jahren in Zusammenhang mit dem mittlerweile schon legendären Virus "Blaster". Dieser infizierte auch einige Systeme des TÜV Rheinland, was sich insbesondere auf den Datendurchsatz im Netz negativ auswirkte. Blaster verstopfte die Datenleitungen und da die weltweit verteilten Standorte bei ihrer täglichen Arbeit nicht zuletzt von der verfügbaren Bandbreite abhängig sind, störte der Virus das Unternehmen an einer empfindlichen Stelle. "Insgesamt mussten wir rund hundert Manntage zur Bereinigung von befallenen PCs aufwenden", berichtet Norbert Tesch von der TÜV Rheinland Service GmbH und für die Virenabwehr im gesamten Unternehmen zuständig. Der Vorfall war Anlass für die Einführung eines systematischen Patch-Managements und eines flächendeckenden Virenschutzes, der nicht nur alle Desktops weltweit sondern vor allem auch alle Mobilcomputer umfasste. Neben einigen tausend Notebooks sind das etwa 400 Blackberrys, sowie zahlreiche Tablett-PCs, und diverse PDAs im Einsatz.

Die getroffenen Abwehrmaßnahmen waren erfolgreich, so dass das Unternehmen den – vorläufigen – Höhepunkt der Virenschwemme, der vor etwa zwei Jahren zu verzeichnen war, ohne jegliche Beeinträchtigungen überstand. Aber auf Dauer zeigte sich jedoch, dass die für verschiedene Teilaufgaben der Virenbekämpfung unterschiedlichen Tools nur schwer zu koordinieren waren und einen großen Administrationsaufwand mit entsprechend hohen Kosten verursachten. "Wir mussten dringend die Werkzeuge konsolidieren und dabei auch die Anzahl der unterschiedlichen Hersteller reduzieren", erläutert Tesch. "Ziel war ein globales Management mit standardisierten Produkten, das vor allem auch die mobilen Systeme abdeckt."

Ende 2005 wurde daher nach ausführlichen Pilottests beim TÜV Rheinland eine neue Anti-Viren-Strategie implementiert, die im Einzelnen folgende Aufgaben abzudecken hat:

- Das Scannen von Mails auf den Mail-, Hub- und Gateway-Servern
- Das Filtern der eingehenden Mails auf Spam
- Das Scannen von HTTP und Downloads
- Den Schutz der Clients
- Den Schutz der Fileserver
- Ein systematisches Patch-Management

Dabei sollten weltweit die jeweils gleichen Virens Scanner für die verschiedenen Anwendungsbereiche, also ein Virens Scanner für Clients, ein Virens Scanner für Fileserver usw. eingesetzt werden. Zur Vereinfachung der Administration sollte darüber hinaus eine einheitliche Konsole, die Daten über den Status der Antivirus-Server und der daran angeschlossenen Clients und Server erfassen und so eine schnelle Reaktion in Notsituationen weltweit ermöglichen. Auf diese Weise sollte außerdem ein einfacheres und dennoch aussagefähigeres Reporting ermöglicht werden.

Schutz durch Zwei-Produkte-Strategie

Mit Unterstützung des Bremer Security-Spezialisten AMPEG entwickelte der TÜV Rheinland eine konsolidierte Virenabwehr auf Basis einer Zwei-Produkte-Strategie mit den Anti-Viren-Tools von Trend Micro und von Symantec. Tesch erklärt die Vorteile dieser Strategie so: "Wir setzen die Werkzeuge dieser Hersteller komplementär ein. Jedes Dokument und jede E-Mail wird mit zwei unterschiedlichen Produkten geschützt. Ein Virus müsste daher immer die Technologien von zwei Herstellern überwinden, ehe er Schaden anrichten kann. Durch diese doppelte Absicherung erreichen wir ein besonders hohes Sicherheitsniveau." Auf den verschiedenen Ebenen beziehungsweise Plattformen wurden schließlich ab Frühjahr 2006 folgende Tools implementiert:

- E-Mail-Server: Trend Micro ScanMail für Domino
- Domino-Hub-Server: Symantec
- Clients: Trend Micro OfficeScan
- Fileserver: Symantec
- Netzwerk: Patch-Management und Desktop-Firewall

So wird jeder Vorgang mit unterschiedlichen Produkten doppelt abgesichert. Ein Dokument wird beispielsweise am Client mit Trend Micro und auf dem Fileserver mit Symantec überprüft; eine E-Mail am E-Mail-Server mit Trend Micro und auf dem korrespondierenden Domino-Hub-Server mit der Symantec-Technologie.

Diese Struktur gilt einheitlich für den gesamten Konzern an allen verteilten Standorten und umfasst auch die mobilen Systeme. Durch die Standardisierung und Konsolidierung der Produkte auf nur noch sechs Anti-Viren-Server weltweit, konnte der TÜV Rheinland nicht nur eine Kosteneinsparung erreichen, sondern auch ein globales Incident-Management und ein verbessertes Reporting einführen. "Wir wissen nun immer, welche Abwehrmaßnahmen auf welchen Systemen getroffen wurden oder noch erforderlich sind", erklärt Tesch. "In Störfällen können wir damit wesentlich schneller reagieren als bisher."

Nahezu alle Clients des TÜV Rheinland werden hinsichtlich des Virenschutzes in derselben Konfiguration betrieben, es gibt auch für besonders kritische Aufgaben keine "extra sicheren" Systeme, was die Administration erheblich erleichtert. Die Vereinfachung der Administration wird aber auch von den nun verwendeten Produkten selbst unterstützt. So sind die Produkte von Trend Micro webbasiert, weshalb für ihre Steuerung keine spezielle Konsole benötigt wird. "Die Empfehlungen von AMPEG haben sich bestens bewährt", hebt Tesch hervor. "ScanMail und Office-Scan haben sich im Praxiseinsatz als sehr schnell und stabil erwiesen." Zudem beanspruchen sie die CPU nur in geringem Umfang, so dass die laufende Arbeit in keiner Weise beeinträchtigt wird."

Das vom TÜV Rheinland regelmäßig durchgeführte Reporting zeigt, dass der mit der Virenabwehr getriebene Aufwand nur allzu angebracht ist. Auf den E-Mail-Servern werden im Durchschnitt mehr als 10.000 Viren pro Monat identifiziert und unschädlich gemacht, auf den Clients sind es noch rund 1.000, die hauptsächlich über das Internet eingeschleust werden. "Wir hatten aber auch schon bis zu 50.000 Viren im E-Mail-Bereich", erläutert Tesch. "Heute spielt das Thema Spyware eine immer größere Rolle. Etwa 50 Prozent der Client-Viren gehören nach unseren Beobachtungen derzeit zur Spyware."

Auch über Konzeption und Implementierung der Anti-Viren-Tools hinaus erhält der TÜV Rheinland durch AMPEG Unterstützung im Rahmen eines regelmäßigen Consulting. "AMPEG hat uns sehr gut bei Trend Micro vertreten und uns bei den anfänglichen Problemen, die auf Grund unserer komplexen WAN-Struktur entstanden sind, ausgezeichnet unterstützt", resümiert Tesch. "Wenn wir uns hinsichtlich der Viren-Gefahr heute so sicher fühlen, dann liegt das nicht zuletzt daran, dass alle an der Viren-Abwehr Beteiligten einen guten Job gemacht haben." Beim Viren-Schutz kann der TÜV Rheinland damit auch gehobenen Ansprüchen gerecht werden.

Die Lösung wurde realisiert bei:

TÜV Rheinland Group
Am grauen Stein
51105 Köln

Kontakt

AMPEG Technologie und Computer Service GmbH
Flughafenallee 24
28199 Bremen
Tel. 0421-52587-0
Fax 0700 – 267 34 329