

Mit Energie ans Ziel

rhenag Rheinische Energie AG

Historie

Die rhenag Rheinische Energie AG wurde als Erbauer und Betreiber von Gas- und Wasserwerken im Jahr 1872 gegründet. Bereits 1929 folgten erste Kooperationen mit anderen Energieversorgern in Form einer Kapitalbeteiligung durch rhenag.

Heute betreibt rhenag als nunmehr 100%ige Tochtergesellschaft der RWE Rhein-Ruhr AG ihr Energiegeschäft überwiegend im rechtsrheinischen Rhein-Sieg-Kreis und im Westerwald. Sie versorgt diese Gebiete mit Gas, teilweise auch mit Strom und Wasser und erstellt für die Kommunen auf Wunsch auch die Abwasserabrechnung in Betriebsführung.

Die Kooperation mit anderen Energieversorgern wurde im Laufe der Zeit auf 14 kommunale Versorgungsunternehmen erweitert. rhenag verfolgt hierbei das Prinzip der operativen Zusammenarbeit in Kombination mit einer Minderheitsbeteiligung. Nicht die beherrschende Einflussnahme ist das Ziel, sondern eine Effizienzsteigerung.

Gebündeltes Know-how für Stadtwerke

Zunehmend an Bedeutung gewinnt das Dienstleistungsgeschäft. Mit diesem neuen, eigenständigen Geschäftsfeld reagiert rhenag auf die Nachfrage nach speziellen Stadtwerk-lösungen, die sie immer mehr auch von Nicht-Beteiligungsgesellschaften erreicht. Basis dieser Dienstleistungen, die bundesweit angeboten werden, ist das umfassende energiewirtschaftliche Know-How, das rhenag durch die jahrzehntelange Tätigkeit als stadtwerkeähnliches Versorgungsunternehmen besitzt.

Hierbei ist es gerade für kleine und mittelgroße Stadtwerke interessant auf sogenannte Overhead-Funktionen, wie beispielsweise Finanz- und Rechnungswesen, Einkauf, Personal und Recht, zurückzugreifen, die im eigenen Hause nicht im nötigen Umfang und vor allem nicht zu vertretbaren Kosten vorgehalten werden können. Mit einem gemeinsam mit der THÜGA betriebenen Rechenzentrum, einer auf Energieversorger zugeschnittenen Softwarelösung und ca. 40 IT-MitarbeiterInnen unterstützt rhenag andere Unternehmen insbesondere auch im Schlüs-



rhenag Firmenhauptsitz in Köln

selbereich Informationsmanagement. Im Rahmen der Netzwerktechnik arbeitet rhenag dabei seit dem Jahr 2001 eng mit der MAGELLAN Netzwerke GmbH zusammen. Bei dem jüngst erfolgreich umgesetzten Projekt handelte es sich um die Einrichtung von Internet Security Services, in dessen Umsetzung die MAGELLAN Netzwerke GmbH von Anfang an eingebunden wurde.



Blick auf Bauteile des Rechnertyps der IBM i5 Serie, seit Ende 2004 bei rhenag im Einsatz

Ausgangssituation

Ziel des Projekts war die Einführung einer wirksamen Lösung zur Virenabwehr sowie die Gewährleistung einer sicheren, ungestörten Email-Kommunikation und Internet-Nutzung für rhenag und ihre zahlreichen, an das Rechenzentrum angebundenen IT-Kunden.

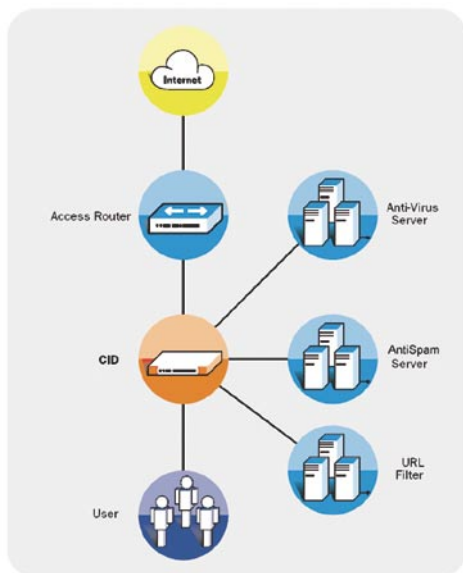
Das System sollte zudem problemlos mit den bereits vorhandenen IT-Komponenten zusammenarbeiten und ausreichende Ressourcen bieten, um weitere Kunden anbinden zu können.

Die Projektbeteiligten der rhenag und MAGELLAN Netzwerke GmbH entschieden sich zu einer proaktiven Gesamtlösung mit den Produkten eSafe Gateway von Aladdin, Kaspersky AntiSpam/Virus und Smartfilter von Secure Computing. Installiert wurden diese Komponenten auf Servern in einem redundant ausgelegten Bladecenter der Firma IBM. Kernstück der Internet Security Services, kurz ISS genannt, sollten zwei CID von Radware darstellen.

Deutlich beschleunigte Prüfungsgeschwindigkeit

Der „Content Inspection Director“ (CID) von Radware unterscheidet automatisch zwischen zu prüfenden und vertrauenswürdigen Daten. Nur die kritischen Daten werden zur Überprüfung weitergeleitet. Der Vorteil: Firmennetzwerke werden entlastet, weil Viren-Scanning und Content Filtering direkt an die entsprechenden Instanzen geroutet wer-

den. Bisher nahm die Überprüfung von Inhalten auf Viren eine hohe Prozessorleistung in Anspruch und sorgte damit für Engpässe in der Netzwerkperformance. Durch einen vorgeschalteten Screening-Algorithmus ist der CID in der Lage, eingehende Daten zu differenzieren. Unkritische Daten passieren ungehindert die Kontrollen, während potenziell zu prüfende Inhalte wie z.B. SMTP und HTTP zu den Antiviren-Gateways geleitet und überprüft werden. Die bekannten Flaschenhälse bei Datentransfers werden so aufgelöst.



Schematische Darstellung der Sicherheitslösung

Der CID als Management von Antivirensystemen ist die erste Lösung ihrer Art, die Virenschutz bei gleichzeitiger und vor allem gleich bleibender Netzperformance ermöglicht.

Schutz vor Spam-Mails auf verschiedenen Ebenen

Am „Eingang“ des Unternehmensnetzwerks wurde Kaspersky installiert, ein Filter, der den eingehenden Email-Verkehr auf Spam-Inhalte und Viren durchsucht.

Kaspersky Anti-Spam funktioniert als Email-Pufferspeicher, welcher Emails vor ihrer Bearbeitung durch den Mail-Server überprüft. So wird eine maximale Kompatibilität der Anti-Spam-Lösung mit der bereits bestehenden Netzwerk-Infrastruktur erzielt. Die hohe Effizienz von Kaspersky Anti-Spam wird durch die Analyse der eingehenden Emails auf vier Ebenen erzielt.

Auf der ersten Ebene wird die Email durch einen „intelligenten“ Kernel zur Inhaltserkennung von Emails überprüft, welcher selbstständig verschiedene Spam-Typen von normaler Geschäftskorrespondenz unterscheiden kann. Auf der zweiten Ebene wird eine Signatur-Methode verwendet, wobei jede Email mit bestehenden Vorlagen in der täglich aktualisierten Datenbank verglichen wird. Diese Datenbank enthält Muster uner-

wünschter Emails und ermöglicht das Erkennen von Spam sogar, wenn die eingehende Email sich von der Vorlage unterscheidet.

Auf der dritten Ebene werden die Emails nach formalen Attributen analysiert. Hierzu gehören unter anderem die Email-Adresse und die IP-Adresse. Das Produkt enthält ein umfassendes Set an „intelligenten“ Regeln, mit welchen eine Spam-Mail nach äußeren Kennzeichen (Art der Versendung, Adresse, Pfad und anderen Attributen) erkannt werden kann.

Auf der vierten Ebene benutzt Kaspersky Anti-Spam die „Black-List“-Methode, welche standardmäßig zur Filtrierung von Emails auf Adressen verwendet wird, die als notorische Spam-Quellen bekannt sind und in öffentliche, ständig aktualisierte „schwarze Listen“ eingetragen werden.

Kaspersky AntiVirus überprüft zusätzlich alle eingehenden Mails auf Viren. Der Virens Scanner aktualisiert sich automatisch durch stündliches Herunterladen der neusten Virenpattern des Herstellers. Kaspersky Labs gehört zu den weltweit führenden Entwicklern von Antiviren-Software und besitzt eine anerkannt führende Position im gesamten Bereich der Informationsschutz-Technologien.

Doppelter Schutz vor Viren...

Zusätzlich zu Kaspersky AntiVirus kommt mit eSafe Gateway von Aladdin eine Komplettlösung mit mehrschichtigen Schutzmechanismen zum Einsatz. Sie untersucht den gesamten eingehenden Email- und www-Datenverkehr nach Anzeichen für zerstörerische oder produktivitätshemmende Inhalte.

eSafe Gateway erfordert keine zusätzliche Client-Software auf dem Arbeitsplatzrechner oder Änderungen an der Hardware. Nach der Installation von eSafe Gateway werden sämtliche HTTP-, FTP- und SMTP-Datentransfers gescannt.

...bei niedrigen Kosten

Infizierte Dateien werden gesäubert, abgeblockt oder in den Quarantäne-Bereich umgeleitet, saubere und reparierte Dateien dem gewünschten Empfänger zugestellt. Ungefährliche Dokumente werden unverzüglich weitergesendet, um den Datendurchsatz nicht unnötig zu beeinträchtigen. Mit dieser speziellen Architektur bietet diese Lösung größtmöglichen Schutz und Performance bei niedrigen Verwaltungskosten.

rhenag arbeitet mit dieser Lösung seit nunmehr einem Jahr und konnte deshalb auch die Würmer- und Viren-Attacken der letzten Wochen schadensfrei überstehen. „Jeder ein-



Andreas Weingarten, Geschäftsführer der rhenag-Thüga Rechenzentrum GBR

zelle Mitarbeiter profitiert bei der täglichen Arbeit am PC von einem umfassenden Schutz gegen die Schädlinge aus dem Web. Solche Systeme sind nicht nur zur Gefahrenabwehr absolut notwendig, sondern auch zur Produktivitätssteigerung relevant“, meint Dipl. Physiker Andreas Weingarten, Geschäftsführer der rhenag-Thüga Rechenzentrum GBR.

ContentFiltering für „sauberes“ Surfen

Alle Zugriffe auf Webseiten durchlaufen zuerst SmartFilter und werden anschließend sofort anhand der Webrichtlinie des Unternehmens und der SmartFilter-Kontrollliste bewertet. Die SmartFilter-Kontrollliste enthält über 2 Millionen kategorisierte Sites mit breiter internationaler Abdeckung. In Abhängigkeit vom Seitenaufwurf werden die Anforderungen zugelassen, blockiert, verzögert oder mit einer Warnung weitergeleitet.

Zuverlässige Partnerschaft

Durch die gute Zusammenarbeit mit der MAGELLAN Netzwerke GmbH konnte das komplexe Projekt zügig und problemlos umgesetzt werden. ■

Weblinks:
www.rhenag.de
www.magellan-net.de