Ausgabe 6-2007 November/**Dezember**

€ 20,–

itsecurity

itsecurity

Free- und Shareware:
Sicherheitssoftware im Überblick

Schwerpunkt
IT-Security effizient einführen

Management
SAP Business ByDesign löst SAP A1S ab

Praxis
IE7 jetzt auch für Raubkopien

Produkt
Sicherheits-lücken in Handy-software

itverlag

Performance sowie zentrale Administration und Monitoring mit Clavister Firewall-Lösung

Service-Center im Einsatz: Der erste Cluster soll die DMZ-Infrastruktur für konzerninterne Daten wie E-Mails, Webhosting und „Surf"-Traffic schützen.

Sichere Versorgung mit Security Appliance-Clusterlösungen

Die N-ERGIE Aktiengesellschaft ist ein Unternehmen, das Energie- und Wasserlieferungen sowie Lösungen, Leistungen und Produkte rund um die Energieversorgung anbietet. Das Tochterunternehmen itecPlus GmbH hat dabei die Aufgabe, den reibungslosen und ausfallsicheren IT-Netzwerkbetrieb zwischen den zentralen Rechenzentren, den Außenstandorten sowie den Tochtergesellschaften sicherzustellen. Darüber hinaus müssen der gesicherte Internetzugang und der Zugriff aus dem Web auf Server im internen Netz gewährleistet werden. Diese Maßgaben veranlassten den Dienstleister zu der Entscheidung, eine Clavister-Firewall-Lösung zu implementieren.

Bei der N-ERGIE Aktiengesellschaft handelt es sich um ein Multi-Utility-Unternehmen, das seinen 650.000 Kunden Strom, Erdgas, Fernwärme und Wasser sowie Dienstleistungen bereitstellt. Im Fokus steht hierbei für N-ERGIE insbesondere auch die regionale Verantwortung sowie aktives Engagement für die Umwelt.

Ausgangssituation und Herausforderung

Gesucht wurde eine Lösung, die zuverlässig vor Viren, Würmern, Rootkit-, Trojaner-, Phishing- und anderen Internet-Attacken schützt. Für den Bereich Netzwerksicherheit sollte ein entsprechendes Modul zur Abwehr sämtlicher Angriffe bereit-

stehen. Zudem sollte die Lösung weitere wichtige Anforderungen erfüllen. Die Außenstellen bzw. Standorte der N-ERGIE sind zum Teil mit sehr hohen WAN-Bandbreiten (>100 MBit) angebunden. Daher musste bei der Evaluierung einer geeigneten IP-Sicherheits-/Firewall-Lösung besonderes Augenmerk auf die Performance gelegt werden. Benötigt wurde eine Lösung mit mehreren GBit-Anschlussmöglichkeiten. Zudem sollte eine einfache Erweiterung der Performance bzw. der Anschlussmöglichkeiten durch ein Lizenzmodell erfolgen. Darüber hinaus musste sichergestellt werden, dass bei zentralen IT-Lösungen kein „Single Point of Failure" entstehen kann. Hinzu kam die Anforderung, dass bei allen im Konzern eingesetzten Lösungen eine zentrale Administration und Monitoring möglich sein sollen.

Evaluation und Entscheidung

Als Kunde des Dienstleistungs- und Systemhauses EDV-Partner folgte die itecPlus GmbH dessen Empfehlung und entschied sich für den Einsatz der Technologie des schwedischen Herstellers IP-basierter Security-Lösungen Clavister. Nach der Entscheidung, ausschließlich die Lösungen des Herstellers einzusetzen, wurden die passenden Modelle ausgewählt. Die Clavister Security Appliance der Serie 4230 und 3110/50 stellte aufgrund der zu erfüllenden Anforderungen die ideale Lösung dar.

Lösung und Anpassung

Die itecPlus GmbH entschloss sich für den ausschließlichen Einsatz von vier Clavister Security Gateway-Clustern als reinen Statefull-Inspection Firewall-Cluster.

Der erste Cluster soll die DMZ-Infrastruktur für konzerninterne Daten (E-Mails, Webhosting, „Surf"-Traffic) schützen. Der zweite Cluster hat die Aufgabe, die DMZ-Infrastruktur für konzernfremde IT-Dienstleistungen (kundeneigener Web-Server, Datenbank-Server, Mail-Server) zu sichern. Der Schutz des „Dial-in"-Traffics der mobilen Mitarbeiter per Analog/ISDN/VPN ist Aufgabe des dritten Clusters. Die VPN-Tunnel werden hier nicht am Cluster aufgebaut, sondern am Cisco VPN-Konzentrator vor dem Firewall-Cluster. Der vierte Cluster übernimmt die Sicherung des Datenverkehrs vom zentralen Rechenzentrum zu den Tochterunternehmen und Beteiligungen, die über mehrere GB-Datenanbindungen auf das Rechenzentrum zugreifen können.

Management und Monitoring erfolgen überwiegend mit Clavister Finetune, dem zentralen Firewall-Managementprogramm von Clavister. Das Unternehmen verfolgt insgesamt eine grundsätzlich zweistufige Sicherheitsstrategie:

1. Stufe: Der Border-Router, der die Anbindung der WAN-Strecken realisiert, übernimmt neben reinen Routing-Funktionen auch eine erste IP-Adress-Filterung.

2. Stufe: Clavister Firewall Cluster

Hierbei werden folgende Features der SG genutzt: HA, Stateful-Inspection, NAT-Rules, SAT-Rules. Bei den geschützten Servertypen handelt es sich um Windows, AIX, Linux, Unix und Novell.

Einsatz des Produktes

Zunächst wurde der erste Cluster an einer nicht so kritischen Anwendung in Betrieb genommen, um so erste Erfahrungen mit dem Clavister-System zu sammeln. Die Implementierung wurde im Rahmen eines Workshops durchgeführt, bei dem alle im anschließenden laufenden Betrieb für dieses System verantwortlichen Mitarbeiter beteiligt waren. Somit konnten kostenintensive Schulungen weitestgehend vermieden werden. Erste Erfahrungsergebnisse ergaben, dass im Fail-over-Fall des Clavister-Clusters keinerlei Verzögerungen bzw. Ausfälle im IP-Datenverkehr festzustellen waren. Nach mehreren Monaten des Betriebs des „Pilot-Clusters" wurden dann weitere Cluster in Betrieb genommen. Dabei zeigte sich jedoch zunächst ein Problem: Die jeweils angeschlossenen Netzwerk-Switches waren nicht in der Lage, auf Layer 2-Ebene den Portwechsel im Fail-over-Fall schnell genug zu registrieren. Die Lösung bestand darin, das Spanning-Tree-Protokoll auf den beteiligten Switch-Ports auszuschalten.

Situation und Ausblick

Mittlerweile funktionieren die Cluster einwandfrei. Durchgeführt wird ein permanentes Monitoring der Firewall-Cluster über SNMP-Tools (MRTG) bezüglich Performance und Auslastung. Eine Log-File-Analyse wird im Fehlerfall bzw. nach einer Konfigurationsänderung vorgenommen.

Darüber hinaus hat der Kunde itecPlus GmbH im Labor auch die neuen Clavister xUTM Features getestet. Da eine einfache Integration/Aktivierung von IDP auf dem Cluster möglich wäre, sind derzeit Pläne in der Diskussion, dieses Feature auf den „Haupt"-Clustern einzuführen, um damit die Netzwerksicherheit noch weiter zu erhöhen.

Fazit

Die Clavister-Technologie hat sich im Praxiseinsatz bei N-ERGIE bewährt. Insbesondere die Möglichkeit der zügigen und einfachen Konfiguration hat sich als großer Vorteil herausgestellt. Auch bei insgesamt acht Appliance Firewalls (vier Cluster) ist, wie gewünscht, eine übersichtliche zentrale Administration möglich. Durch das unternehmensweite Netzwerkmonitoring-Tool ist eine optimale Überwachung erreichbar. Positiv bewertet wurden zudem das übersichtliche und effektive Fehleranalyse-Tool in der mitgelieferten Management-Software sowie die äußerst gute Performance der Appliances. Es entstehen im Fail-over-Fall keinerlei Einbußen mehr im TCP/IP-Datenfluss.

Oliver Raabe