



**Unternehmensgruppe
Graf von Oeynhausen-Sierstorpff
GmbH & Co. KG**

REFERENZ PROJEKT

IT-Security und Vernetzungskonzept

Immer häufiger werden interne Unternehmensdaten auch von unterwegs aus aktuell benötigt. Dabei kommt dem Zugriff von extern auf das zentrale Unternehmensnetzwerk eine immer größere Bedeutung zu. Die moderne Computing-Welt erstreckt sich bereits weit über den mobilen Mitarbeiter mit Laptop hinaus und umfasst inzwischen auch Telearbeiter, freie Mitarbeiter, Servicetechniker und Kunden. Mit der steigenden Bedeutung mobiler Arbeitsplätze steigt auch der Bedarf an sicheren Lösungen für den Remote-Zugriff auf Unternehmensdaten.

Die Schwierigkeit liegt dabei in der Einhaltung der internen Sicherheitsstandards und gleichzeitiger Öffnung des Netzwerks zum Internet.

Projektanforderungen:

Implementierung und Konfiguration einer Sicherheitslösung - den neuesten Datenschutz-Richtlinien entsprechend - die das gesamte Unternehmen von der Zentrale über die Außenstellen bis zu Arbeitsplätzen zuhause und unterwegs integriert. Wichtiger Bestandteil der Lösung soll ein sicheres Einwählen der mobilen Mitarbeiter und ein Rundum-Schutz vor externen und internen Sicherheitsbedrohungen sein. Dabei muss eine optimale Netzwerkproduktivität gewährleistet sein.

Sicherheitslösungen müssen mehrere Funktionen erfüllen - vor allem, wenn sie direkt am Gateway eingesetzt werden.



Die Graf von Oeynhausen-Sierstorpff Unternehmensgruppe

ist einer der führenden privaten Anbieter von Dienstleistungen im Gesundheitsbereich. Die Unternehmensgruppe gliedert sich in die drei Geschäftsbereiche: Bad, Kliniken und Brunnen. Die drei Bereiche beschäftigen zusammen über 1000 Mitarbeiter und erreichten einen Jahresumsatz von 65,9 Mio. (Stand 2006). Im zentralen Rechenzentrum in Bad Driburg bündelt sich die gesamte Informationstechnologie der Holding. Die nahe liegenden Standorte – Caspar-Heinrich-Klinik, Marcus-Klinik, Park-Klinik (www.ugos.de) Bad Driburger Naturquellen und der Gräfliche Park – sind durch Lichtwellenleiter-Verkabelung miteinander vernetzt. Die entfernten Standorte – Bad Klosterlausitz und Langelsheim – sind mittels VPN an das Rechenzentrum angebunden.



REFERENZPROJEKT

**Unternehmensgruppe
Graf von Oeynhausen-Sierstorpf
GmbH & Co. KG**

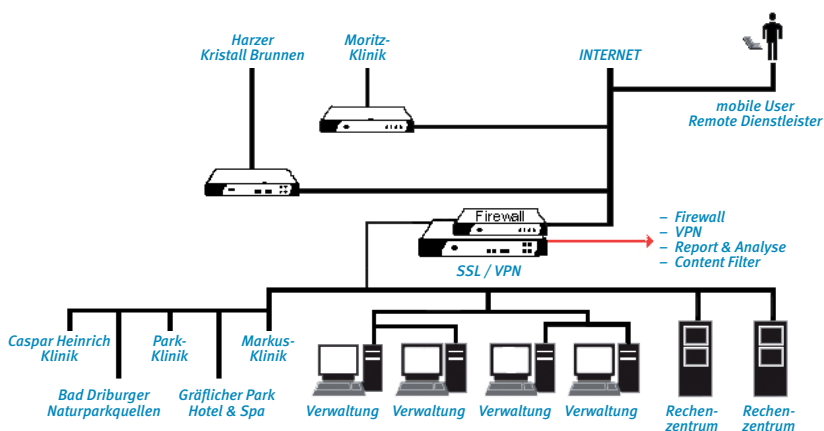
Lösungskonzept:

Die von EGGENET implementierte appliancebasierte Lösung integriert Anti-Virus, Anti-Spyware und Intrusion Prevention in einem einzigen, umfassenden Paket und eignet sich für drahtlose und kabelgebundene Netzwerke jeder Größe.

Die mit dem Ziel zur Verbesserung der Sicherheit und zur Reduzierung der Komplexität entworfenen Internet Security Appliances minimieren die Kosten und die Komplexität der Installation und Verwaltung von verschiedenen Geräten und Softwarepaketen. Mit der strukturierten, überschaubaren Lösung wird eine umfassende Sicherheit gewährleistet.

Der Zugang für mobile User erfolgt über kleine Token (Lösung zur Vergabe von Einmal-Kennwörtern) per Remote-Access.

EGGENET übernimmt den Fernwartungs-Support für die Gesamtlösung, wie z. B. das Einspielen sicherheitskritischer Updates und die Entstörung.



„Das EGGENET-Konzept besteht durch seine leistungsstarke Sicherheitsplattform und ist speziell für die kritischen Sicherheitsanforderungen unseres Unternehmens ausgelegt.“

Wir denken, mit dieser Lösung einen wichtigen Schritt zu mehr Sicherheit in sich öffnenden IuK-Systemen getan zu haben.“

Dieter Gerling
Chief Information Officer (CIO)
der Unternehmensgruppe
Graf von Oeynhausen-Sierstorpf
GmbH & Co. KG.

Die eingesetzte Lösung von EGGENET beinhaltet:

- › EAL 4+-zertifizierte Firewall-UTM-Appliance inkl. Intrusion Prevention und Anti-Virus/Anti-Spyware
- › Remote Access über SSL VPN Gateway
- › Einmal-Kennwörter über Token
- › Zentrales Management und Überwachung
- › Fernwartungs-Support von EGGENET 24 x 7

EGGENET
eine Marke der Teleos GmbH & Co. KG
Rolandsweg 80 | 33102 Paderborn
Tel.: 0 52 51 / 89 88 80
Fax.: 0 52 51 / 89 88 98
E-Mail: info@eggenet.de

EGGENET
Eine Marke der Teleos.