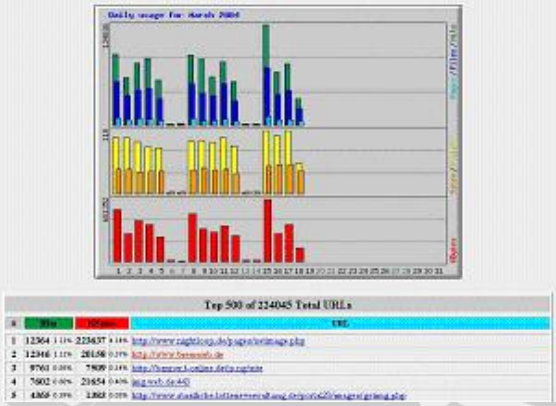
DECO_SecureNet

Heutige Unternehmen sehen sich zunehmend mit der Anforderung konfrontiert ihre Geschäftsprozesse über das Internet laufen zu lassen, um kostengünstige und effiziente Kommunikationswege erschließen zu können. Die Sicherheit spielt dabei eine entscheidende Rolle, da man sich nicht in die internen Daten schauen lassen möchte. Eine Absicherung gegenüber dem Internet durch eine Firewall ist dabei heute Standard, stellt aber längst nicht das Allheilmittel gegenüber Hackern dar. Zunehmend werden nämlich auch interne „Einbruchsversuche" auf Server wahrgenommen; man spricht sogar von einem Verhältnis von 70:30. Hinzu kommt, dass an der Firewall vorbei evtl. noch ganz andere Kommunikationswege offen sind, die entweder aus Unkenntnis oder aufgrund der Einfachheit der Installation unsichere Öffnungen des Unternehmensnetzes darstellen. Deshalb ist hier eine ganzheitliche Betrachtung gefragt, die den Schutz von extern nach intern, aber auch in die andere Richtung gewährleistet und alle Kommunikationswege berücksichtigt.



Die DECOIT GmbH hat für den Schutz eines Unternehmens vor dem Internet sowie der sicheren Kommunikation zwischen Außenstellen eine ganzheitliche Lösung entwickelt, die auf Open Source Software (OSS) basiert und daher ohne zusätzliche Lizenzen auskommt. Dabei muss man keine Einschränkung in der Leistungsfähigkeit hinnehmen. Das Firewall-System lässt sich beispielsweise im Clusterbetrieb völlig ohne Unterbrechungen betreiben. Zusätzlich wird eine VPN-Funktionalität (Virtual Private Network) angeboten und das interne Netz auf Angriffe über ein IDS-System (Intrusion Detection System) untersucht.

Es sind unterschiedliche Module zu beachten:

a. *Sicherheitskonzept:* das Sicherheitskonzept stellt sicher, dass alle relevanten Sicherheitslücken erkannt und abgeschaltet wurden. Es wird ein Dienst- und Nutzerprofil erstellt, welches das Kommunikationsprofil des Unternehmens festlegt. Dieses Profil mündet in eine Security Policy, die sich in dem Regelwerk der Firewall widerspiegelt.

b. *Firewall-System:* das Firewall-System schützt vor unbefugten Zugriff von außerhalb des Firmennetzes. Es wird in zwei Stufen angeordnet (Paket- und Stateful-Inspection-Filter), um den Zugriff zu erschweren und eine De-Militarisierte Zone (DMZ) für öffentliche Serversysteme (z.B. E-Mail- und FTP-Server) zu schaffen.

c. *Proxy-Server:* der Proxy, der auch als sog. Stellvertreter bezeichnet wird, regelt den Zugriff der Benutzer auf das Internet oder andere Dienste. Hier kann eine wirkungsvolle Schwelle für alle installierten Dienste geschaffen werden, wodurch z.B. der Zugriff limitiert wird oder nur ganz bestimmte Webseiten abgefragt werden können. Es werden Benutzerprofile eingegeben, die individuell angepasst werden können.

d. *VPN-Gateway:* um den sicheren Zugriff auf Außenstellen oder Kundensysteme ermöglichen zu können, sind VPN-Gateways notwendig. Diese bündeln den Verkehr, der auf verschiedene Außenstellen gehen soll, verschlüsseln diesen und Authentifizieren die Teilnehmer. Dabei ist insbesondere auf Kompatibilität, Sicherheit, Performance, Ausfallsicherheit und Quality-of-Service (QoS) zu achten.

e. *IDS-System:* diese Systeme schauen sich die Kommunikationsprozesse innerhalb des Unternehmens an und sichern insbesondere Serversysteme ab. Neben der Erkennung von Sicherheitslücken können auch Monitoring- und Response-Funktionen implementiert werden. Eine gute Ergänzung stellt IDS im Zusammenspiel mit einer Firewall dar, wenn eine DMZ zusätzlich abgesichert werden soll.

Alternativ werden von uns auch Standardlösungen wie von Checkpoint oder Enterasys angeboten. Ergänzt werden kann das DECO_SecureNET durch unseren DECO_LogWatcher zur Auswertung der Logfiles. Die Module können ebenfalls einzeln angeboten werden.

Komponenten:

- Betriebssystem: SuSE 8.2 oder SuSE 9.0
- Firewall-System: basiert auf eigener Konfiguration der *iptables* (ab Linux-Kernel 2.4)
- Proxy-Server: basiert auf *Squid* inkl. Proxy-/Cache-Funktionen sowie Zugriffskontrolle; Statistik-Auswertung über den Webalizer
- VPN-Gateway: basiert auf FreeS/WAN.
- IDS-System: basiert auf Snort, inkl. Angriffsmustererkennung, Filter-Regeln, Alarme etc.

Systemanforderungen:

- Server: Linux-Betriebssystem mit 2 GHz CPU, 1 GByte RAM, RAID, 2x80 GByte EIDE Festplatten (für jedes System erforderlich)

© DECOIT GmbH • Fahrenheitstraße 9 • D-28359 Bremen
Alle Rechte und technische Änderungen sind vorbehalten.
Die verwendeten Hard- und Softwarenamen sind Handelsnamen.