



Decus IT-Symposium 2006
Gateway Security: von der Policy bis zum sicheren rund um die Uhr Betrieb

Johann Lehner
Sales Business Project Manager
Senior Systems Engineer Symantec



Ausgangssituation für das Projekt

- ▶ Ein Netzwerk hat Verbindungen über das Internet zu
 - Vielen eigenen weit verstreuten Anwendungen wie Mail und B2B Funktionen
 - Zu Lieferanten
 - Zu Shops und Vertriebsniederlassungen
 - Zum Aussendienst
- ▶ Jedes Land hat seine eigenen (gewachsenen) Regeln
 - Business critical
 - Unantastbar
- ▶ Das Firmen - LAN ist separat als Frame-Relay Netz gebaut
 - Keine Default Route
 - Kein DNS im LAN
 - Internet Verkehr soll das LAN möglichst wenig belasten



Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.


Die Ausschreibung

- ▶ Geographische Kompetenz
- ▶ Technische Kompetenz
- ▶ Größe der Lieferanten
- ▶ Geräteauswahl nicht vorgegeben
- ▶ Serviceprovider Auswahlverfahren



Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

Das Projekt



symantec.

Matrix: Funktionen x Implementierung durch

Design Phase

	MSSP	Consulting	Device	PM
Questionnaires		R		S
FW Ops	R	S	SGS	
IDS			SGS	
Monitoring	R		SGS, Proxy	I
...	R			

Preparation Phase

	MSSP	Consulting	ISP	PM
DNS		R	R	I
...	R			I

R - Responsible
A - Accountable
S - Supportive
C - to be Consulted
I - to be Informed
Free Format

Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Die Projektleitung

- ▶ 4 Projektleiter
- ▶ > 120 Tasks je Site
- ▶ Details - Details - Details
 - Trade - Compliance
 - Spannungen, Kabel, Racks, ...
 - Consulting Tasks
 - Nummern ohne Ende
 - ...



Region	Country	City	MSS Device Type	ID	MSS Device Name	Billing and Sale	Internal processes for Symc devices	Device Part on Site/Device	Device Date	Migration Date	Device Migration to	Status Information
Africa	South Africa	Cape Town	D	508	SGS_CapeTown	open	internal processes for Symc devices	Symantec			not needed	pending
Middle East	UAE	Dubai	D	51	SGS_Dubai	open	max 300 report license needed	all three			not needed	not needed
Caption:			1 of 2 in 1000 - had changed from previous version 1 of 2 in 1000 - changed from previous version									

Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Bereitstellung der Geräte / Trade Compliance

- ▶ Gleiche Ausrüstung überall, zentral beschafft
- ▶ Klassifizierung der verwendeten Geräte
- ▶ Export
 - Encryption Gesetzgebung > 56 Bit dann volle Nachverfolgung
 - Dual – Use Goods / Militärische Ausrüstung
 - Einzellizenzen – End Use Undertaking (EUU)
 - Abhängig vom Ort des Versenders
- ▶ Versand
 - Incoterms
 - Tracking
 - Warenannahme und Aufbewahrung
- ▶ Import
 - Encryption Gesetzgebung
 - Telekommunikations-Gesetzgebung
- ▶ Lizenzen sind landesspezifisch
 - Betriebslizenzen
 - Einfuhrlicenzen



Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Consulting: Schreiben einer Security Policy

- ▶ Welche Elemente sollen geregelt werden
- ▶ Verantwortung für die Policies
- ▶ Verantwortung für die Einhaltung
- ▶ Wer muss sie kennen
- ▶ Überlegungen zur Wahrscheinlichkeit
- ▶ Regelmäßige Reviews und Updates
- ▶ Festlegen von Maßzahlen wie Security bewertet wird
 - Security ist nicht Availability
 - 99,9 % Verfügbarkeit ist **keine** Maßzahl für Internet Verfügbarkeit
 - Nicht erfassbare Fremdeinflüsse
 - Stromausfälle
 - Leitungsprobleme
 - DNS Probleme




Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Mögliche Information Security Policies

- ▶ **Eigene Application Security**
 - Sicherheit in der Programmierung
 - Ausschluss bestimmter Programmiersprachen
 - Risikobewertung
 - Zugriffsrechte
 - Logging und Alarmer
 - Notfallpläne
 - Standards
- ▶ **Host Security**
 - Herkunft von HW
 - Was muss auf jedem Rechner sein
 - Was darf nicht installiert sein
 - Behandlung von Produktiv-, Entwicklungs- und Test-Rechnern
 - Server Virtualisation Regeln
 - Gast Accounts
 - Hardening
 - Passwort Verwaltung
 - Datenklassifizierung und Regeln (vertraulich bis ...)
- ▶ **Network Security**
 - Eigene Folie
- ▶ **VPN Security**
 - Abstimmung mit den Netzwerk and FW Policies
 - Gruppenbildung
 - Endpunkte
 - Mehrfaktorauthentisierung
 - Active Directory und Zertifikate
- ▶ **Partner Security**
 - Vertragsbestandteil
 - Checkliste
 - Approval Process
 - Netzwerk Anforderungen
 - ICSA certified FW
 - Mit IDS System
 - Mit Vulnerability Assessment
 - OS Anforderungen
 - Mit Host based IDS
 - Mit Vulnerability Assessment
 - Applikations - Anforderungen
 - Ausschluss bestimmter Programmiersprachen
 - Vulnerability Assessment



Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Generelle Network Security Policy

- ▶ Network Usage Policy
- ▶ Trennung von Netzwerk - Arten
 - Engineering Netz
 - IT-Management Netz
 - Produktions-Netzwerk
- ▶ Mehrstufigkeit
- ▶ WLAN Zugriffspolicy
- ▶ Policy für Zweigstellen und Niederlassungen
- ▶ Policy für VPNs der Zweigstellen und Niederlassungen




Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Welche Elemente des Netzwerks fallen unter die Policy

- ▶ Internet Gateways mit ihren Funktionen
 - FW
 - Intrusion Detection
 - Spam
 - AV
 - Contentfilter
- ▶ Internet access links
 - ISPs und Border Router
 - IP Adressplanung
 - DNS
 - Network Operation
- ▶ Anwendungen die über das Gateway laufen



Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Detaillierte Firewall Policies oder besser Perimeter Policies

- ▶ IP Adress Segmentierung / Subnetze
- ▶ Eigene DMZ Segmente
- ▶ Evtl. 2-stufiges FW Konzept
- ▶ Application Proxies mit Login
- ▶ 24x7 Betrieb und Support
- ▶ Mit AV und Intrusion Detection



- ▶ Business geht irgendwann mal nicht mehr vor Security
- ▶ Fragebogen zur Planung der Regeln
- ▶ FW Policy Dokument

Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

FW Policy Dokument

Table of Contents

- 1. INTRODUCTION..... 5
 - 1.1 Purpose..... 5
 - 1.2 Relationship to other Documents..... 5
 - 1.3 Definitions and Abbreviations..... 6
- 2. IMPLEMENTATION CONTACTS AND RESPONSIBILITIES 7
- 3. SITE SPECIFIC DETAILS..... 8
 - 3.1 Site details..... 8
 - 3.2 Site network diagram..... 8
- 4. ACTION STEPS DURING CUT OVER..... 8
- 5. INITIAL FW RULESET..... 8
 - 5.1 General Internet connectivity..... 8
 - 5.2 Mail-services – in and outbound..... 8
 - 5.3 VPN-C oncentrator in DMZ..... 8
 - 5.4 General AntiVirus Policy Settings..... 8
 - 5.5 Customer PAC-File Download..... 8

5.2 Mail-services – in and outbound

Rule	inbound IP	inbound IP	source	destination	ports	Outgoing
1	eth1	eth2	any	172.16.1.2	SMTP	yes
2	eth2	eth1	172.16.1.2	any	SMTP	no
4	eth2	eth1	172.16.1.2	128.16.1.40	SMTP	no
5	eth0	eth2	128.16.1.40	172.16.1.2	SMTP	yes

NAT (address translation)

NAT eth1 on 128.237.223.131 for Rule 1
 NAT eth1 on 128.237.223.131 for Rule 2
 NAT eth0 on 128.68.1.19 for Rule 4

Meistens 4 bis 6 Versionen vor der Migration bei kleinen Standorten

Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

Installation

- ▶ Standortdetails
 - Besichtigung der Baustelle vor Ort
 - Out-of-Band Leitungen
 - Aufbauanleitung
 - Dispatch Notes
 - Synchronisation aller Beteiligten
 - Sehr landesspezifisch
 - Ein PL hat's am schwersten
- ▶ Echte Kosten falls ‚3rd Party On Site‘ kommt.

A. Before starting ..

- Delivery complete?
 - Shipping list (please check if the shipment you received contains the following items; multiple shippings possible):
 - ◆ 1 Symantec Gateway Security Appliance (5600 series)
 - ◆ 1 CDV Port Authority OOB-Device (model 4488) (incl. AC power supply unit and serial/Net. cables)
 - ◆ 1 CDV Power Control Module (incl. 'cold' plug extension)
 - Additionally you'll need network cables (RJ45) (straight/crossed) to connect the system to your network infrastructure!

D1. Connection diagram: Firewall appliance

Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

symantec.

Migration

- ▶ DNS Problem
 - TTL und alte DNS Server Software bei manchen Providern
- ▶ Alles was im Installation Questionnaire vergessen wurde kommt jetzt raus
- ▶ Fehlende Regeln sind in Abstimmung mit der Change Control Prozedur noch während der Migration zu erstellen oder anzupassen
- ▶ Vieles kommt erst am 2. Tag
- ▶ Manches auch erst beim Monatsabschluss

5.2 Mail-services – in and outbound

NAT (redirections)						
From	to	ports				
123.237.223.131	172.16.1.2	all				
128.68.1.19	172.16.1.2	all				
Rule	inbound IF	outbound IF	source	destination	ports	Action(s)
1	eth1	eth2	any	172.16.1.2	SMTP	yes
2	eth2	eth1	172.16.1.2	any	SMTP	no
4	eth2	eth0	172.16.1.2	128.16.1.40	SMTP	no
5	eth0	eth2	128.16.1.40	172.16.1.2	SMTP	yes



NAT (address transform)
 NAT eth2 on client IP for Rule 1
 NAT eth1 on 123.237.223.131 for Rule 2
 NAT eth0 on 128.68.1.19 for Rule 4

Decus IT-Symposium 2006
Gateway Security bis zum 24x7 Betrieb


symantec.

Monitoring und Betrieb durch das Security Operations Center (SOC)

- ▶ Hinter allem steht das SOC (Security Operations Center)
 - Global Netz von ‚state of the art‘ Security Operation Centers
 - Sicher, Skalierbar, Zuverlässig
 - Überwachung von über 600 Kunden mit über 4000 Devices
 - Ein SOC ist auditiert und BS7799 zertifiziert von einem unabhängigen Prüfer
 - Fail over Prozesse sind entwickelt und getestet
 - Redundante Stromversorgung und Netzanbindung
 - Strenge Zugangskontrollen

Decus IT-Symposium 2006
Gateway Security bis zum 24x7 Betrieb

Was wurde am Ende erreicht

- ▶ Zeitplan war mit geringer Verzögerung zu halten
- ▶ mehr Ordnung, Change Management
- ▶ Weniger Betriebsprobleme, nur noch einen critical Incident im letzten Monat
- ▶ Synergien durch häufige Wiederholung, Jeder Fehler vielleicht nur zweimal
- ▶ Zentrales, dokumentiertes **Device Management** mit SLA
- ▶ **24x7 Monitoring** mit 10 min Vorfalls-SLA
- ▶ das log Volumen war bereits über 200 Mio Logeinträge im ersten Monat mit ca 70% der Last
- ▶ Einen zufriedenen Kunden



Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb

Zusammenfassung

Das Problem Internet Gateways und deren Sicherheit samt ihren Compliance Anforderungen ist erst mal für die nächsten Jahre für diesen Kunden gelöst

Vielen Dank für ihr Interesse

johann_lehner@symantec.com



Decus IT-Symposium 2006 | Gateway Security bis zum 24x7 Betrieb