The BENCHMARK for Email Security™

Running the MXtreme Mail Firewall

Michael Kohl
Client-Server EDV
miko@client-server.ch

Wer ist BorderWare Technologies?

- Privates Unternehmen, gegründet 1994 als Border Network Technologies in Toronto/Canada
- Büros in London, Heidelberg, Stockholm, Kalifornien, Virginia, Dubai, Ottawa, > 150 Angestellte
- Erster Hersteller einer CC EAL4+ zertifizierten Firewall
- Erster Hersteller einer E-Mail Security Lösung in 2000
- In 2004 als erster Hersteller die CC EAL4+ Zertifizierung für eine E-Mail Security Appliance erreicht.

Ein paar Worte zu Email Security

- Eine aggressive, proaktive Herangehensweise an Email-Hygiene ist essentiell für Systemstabilität.
  Quelle: Meta Group, April 7, 2004
- Die Email-Umgebung gegen Viren, Malicious Codes und SPAM zu schützen muss heute als Kostenfaktor für das Business unbedingt eingeplant werden. Vernachlässigung wird zu garantierten System- und Produktivitätsausfällen und damit zu echten Verlusten führen.
  Gartner Group, 2004
- Viren bleiben die größte Einzelbedrohung für Email – permanente Wachsamkeit ist Pflicht.
  Quelle: Meta Group, April 7, 2004

- **Definition und Einsatz von Email-Hygiene Diensten**
  - **Viren**
  - **Spam**
  - **Security**
  - **Risiko**
  - **Verfügbarkeit**
- **Data-Center - Mentalität für Messaging anstreben**
  - **Streben nach den “fünf Neunen”**

Data Center Mentalität anstreben

- Downtime ist zunehmend inakzeptabel
- Email Management leidet unter “shared-file” Mentalität
- Email muss als Unternehmenskritische Applikation angesehen werden

Availability	Total Accumulated Outage per Year	(#9s)
90%	More than a month	1
99%	Just under 4 days	2
99.9%	Just under 9 hours	3
99.99%	About an hour	4
99.999%	A little over 5 minutes	5

Source: 2004 Aberdeen Group:

Email ist Unternehmenskritisch

Email ist mehr als Messaging; es ist die Plattform für Ihre Business Transaktionen:

- Bestellungen
- Aufträge
- Vertragsverhandlungen
- Private und Vertrauliche Dokumente
- Zeitkritische Inhalte

Sollten Sie Ihr Email nicht mit der Aufmerksamkeit behandeln, die es verdient?

Es sind nicht nur Spam und Viren…

- Wie hoch sind die Verluste, wenn Ihr Email Server nicht erreichbar ist? Was geschieht mit diesen verlorenen Transaktionen?

- Was geschieht, wenn Ihr Mail System mit Denial-of-Service Attacken überflutet wird?

- Spam repräsentiert mittlerweile bis zu 80% des Emailverkehrs. Das Email Volumen eines durchschnitllichen Unternehmens hat im letzten Jahr um über 300% zugenommen. Ihr MTA oder Mail Gateway ist steigender Belastung ausgesetzt; was geschieht wenn er ausfällt?

Sind Sie sicher, daß Ihr MTA und Ihre Email Infrastruktur der Anforderung gewachsen sind?

Die Kosten eines Internetausfalls

- Die Ökonomischen Auswirkungen eines einzelnen Internetausfalls oder Angriffes sind erschütternd:

	Small Business	Mid Tier Company	Global 5000 Company	Fortune 500 Company
Average Annual Revenues	$10 Million	$500 Million	$2.5 Billion	$30 Billion
Average Recovery Cost per Incident	$300	$15,000	$75,000	$900,000
Average Cost Per Incident Expressed as a % of Revenue	0.067%	0.067%	0.067%	0.067%
Median Revenue Losses For Each Internet Business Disruption	$6,700	$335,000	$1,675,000	$20.1 Million
Total Cost of Incident	$7,000	$350,000	$1,750,000	$21 Million

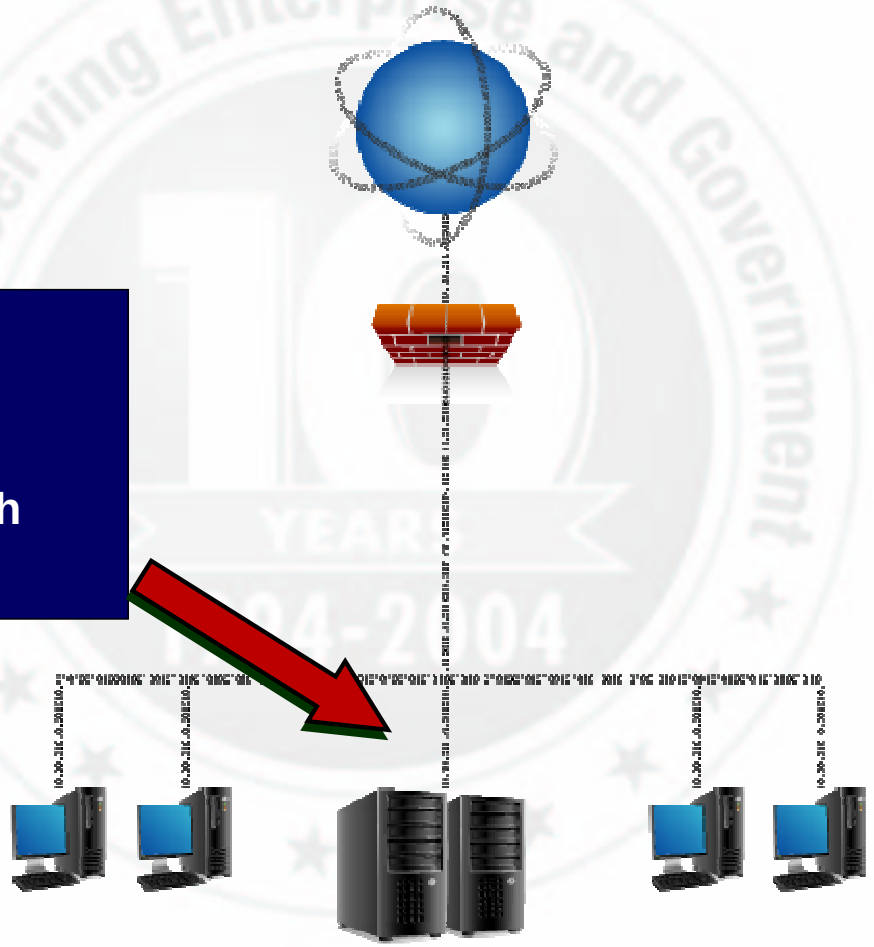
Quelle: © 2004 Aberdeen Group: The Internet Business Disruptions Benchmark Report

Die durchschnittlichen Kosten eines Ausfalls betragen $2 Millionen!

Existierende Mail Architektur

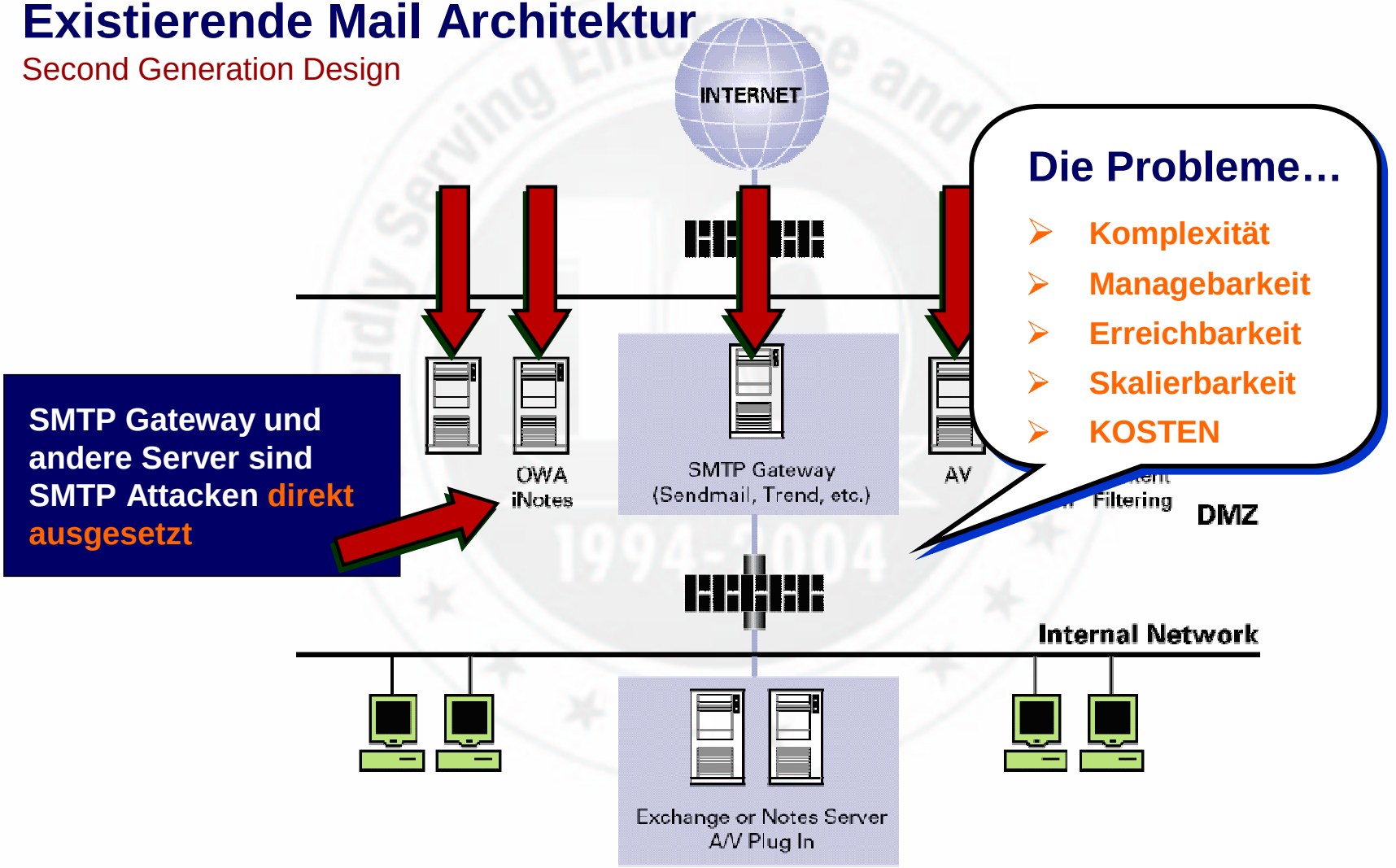
First Generation Design

Mail Server ist dem Internet SMTP Traffic direkt ausgesetzt, nur limitierter Schutz durch eine Firewall



Existierende Mail Architektur

Second Generation Design



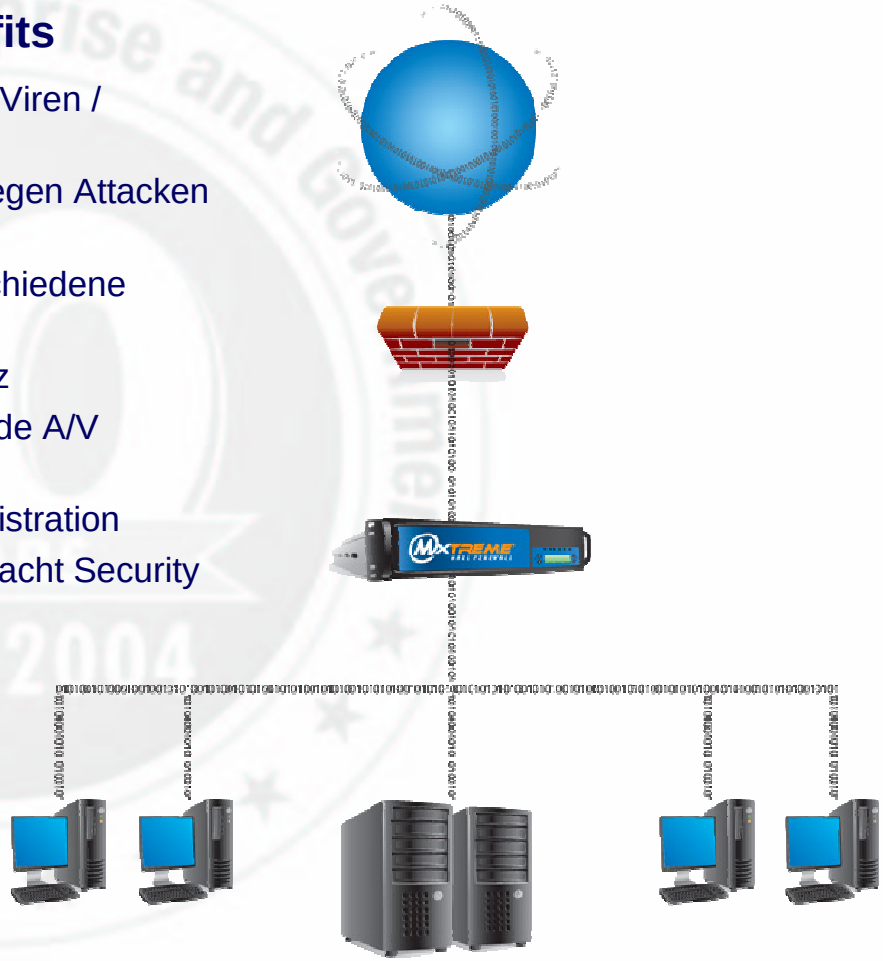
Konsolidierung mit MXtreme

Key Features

- Anti-Spam / Anti-Fraud / Anti-Virus
- End-User Kontrolle (Whitelisting / Quarantäne Mgmt)
- Malformed Message Protection
- Enterprise Policy Management
- Attachment Control
- High Performance MTA
- Content Filtering
- Sicherer OWA/iNotes Access
- Echte High-Availability mit Stateful Failover (Queue Replication)
- Granulares Reporting
- SNMP Logging
- Baut auf BorderWare's S-Core™ OS (10 Jahre "Felderfahrung")
- Zentralisiertes Management & Reporting

Business Benefits

- Eliminiert Spam / Viren / Phishing
- Email Systems gegen Attacken geschützt
- Konsolidiert verschiedene Email Services
- Rationaler Einsatz
- Reduziert dauernde A/V Kosten
- Einfachste Administration
- Erzwingt & überwacht Security Policies



MXtreme - Umfangreicher Schutz

- Liefert einen hoch skalierbaren und robusten MTA sowie Enterprise Mail Gateway.
- Umfangreiches Email Abwicklungs-Management
- Blockiert Email - bezogene Angriffe an der Netzwerkgrenze.
  - Spam, Viren, Trojanische Pferde, Würmer, DoS, DHA
- Content und Policy Control
  - Sensitivität und Vertraulichkeit werden aufrecht erhalten
  - Audit Report und Management
  - Schützt Ihre verwundbaren Informationen

Common Criteria EAL4+ CERTIFIED

Common Criteria EAL4+Certification

- MXtreme ist die einzige Email Firewall der Welt mit einer Common Criteria EAL4+ Zertifizierung.
- Common Criteria EAL4+ Zertifizierung ist der von 16 führenden Nationen und dem US Department of Defense, dem US Department of Homeland Security und der NATO geforderte Sicherheitsstandard
- Common Criteria evaluiert die Sicherheit des Produktes, die Entwicklungsarbeit des Unternehmens und den Support Prozess

ZERTIFIZIERTE SICHERHEIT

Common Criteria EAL4+ CERTIFIED

MXtreme Sicheres Mail Processing

Verschiedene Spam Filter

- MXtreme verwendet eine umfassende Mischung von Technologien um Spam und unerwünschte Inhalte zu filtern:
  - Objektive Filter
  - Subjektive Filter
  - Content Filter und Anti-Virus Scanning
- 98% Spam Erkennungsrate mit 1 : 100,000 False Positive

Symantec Brightmail Anti-Spam Technologie

Probe Network

- Patentierte Technik: verwendet Spam Fallen als Real-Time Datenquelle für die Erstellung von Regeln
- Inhalt der Spam Fallen wird automatisch an BLOC weitergeleitet

Symantec Brightmail Logistics & Operations Center (BLOC)

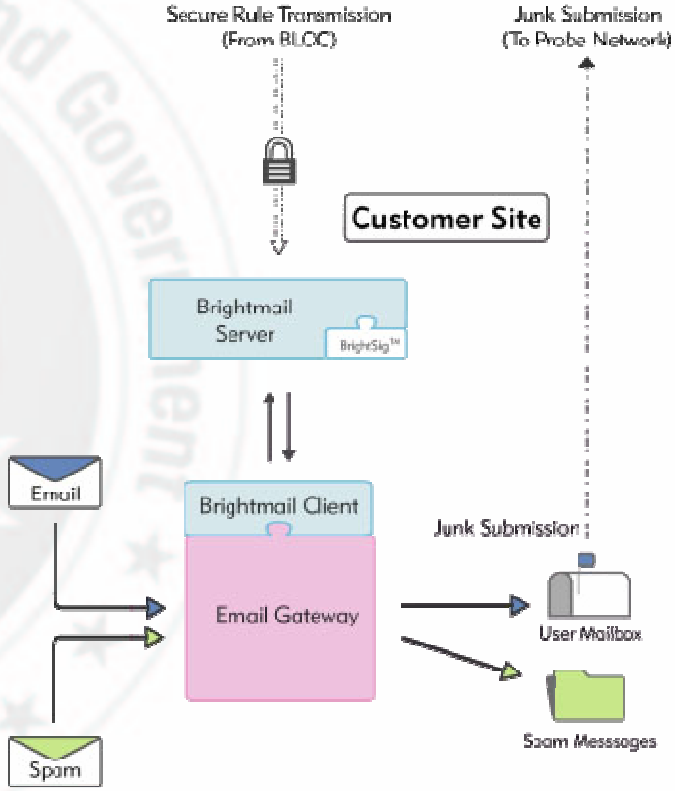
- Spam kontrolliert und Regeln erstellt
- 24x7x365

#1 Genauigkeit

- Niedrigste False Positive Rate auf dem Markt (weniger als 1 : 1,000.000)

Bietet Echtzeit - Spamfilter ohne IT Administration oder Eingriffe

- Regelupdate alle paar Minuten
- 300 Millionen Mailboxen geschützt



symantec.

Content und Policy Control

- Hoch performantes Content Scanning
  - Scant Header, Body, Attachment Typ, Größe, Verschlüsselung
- Zahlreiche Verfahrensoptionen
  - Forward, Strip Attachment, Administrator benachrichtigen, Return to Sender, oder Quarantäne.
- Umfang der Policy Control mit LDAP
- Policies können Global, nach Gruppen oder pro Domain erstellt werden

Content Scanning

- MXtreme scannt sowohl inbound als auch outbound Content
- Verringert das Risiko von Verlust geistigen Eigentums durch das interne Netzwerk
  - Scan nach “company confidential” Schlüsselworten
  - Report über die Email Aktivität und Verstöße
- Beugt Copyrightverstößen vor
  - Hindert Files wie movs, mp3s, avi, wav, xvid, divx, vcd daran in Ihr Unternehmen zu gelangen
- Industrievorschriften
  - MXtreme unterstützt Unternehmen bei der Einhaltung von Sarbanes Oxley, HIPAA, PIPEDA etc.

Integriertes Anti-Virus

SC MAGAZINE GLOBAL AWARDS 2004 WINNER

Kaspersky Anti-Virus gibt den Administratoren ein kraftvolles Werkzeug gegen Viren, Trojaner und Würmer in die Hand und schafft eine zusätzliche Verteidigungslinie

KASPERSKY ANTI-VIRUS

Defense In Depth - Anti-Virus

Integrierte Kaspersky Anti-Virus Engine

- Hoch performantes In-Line Scanning
- **Unlimited User** Lizenzen für MXtreme
- MXtreme prüft automatisch alle 15 Minuten nach Updates

Umfassender Schutz

- Schützt vor allen Arten Malicious Code
- Polymorphe oder Selbstausführende Viren
- Getarnte oder unsichtbare Viren
- Viren für Windows 9x, Windows NT, UNIX, OS/2
- Neue Viren für Java Applets
- Makro-Viren für Word Dokumente, Excel Sheets, PowerPoint Präsentationen, Help Files etc.
- Netzwerk Würmer und
- Trojaner

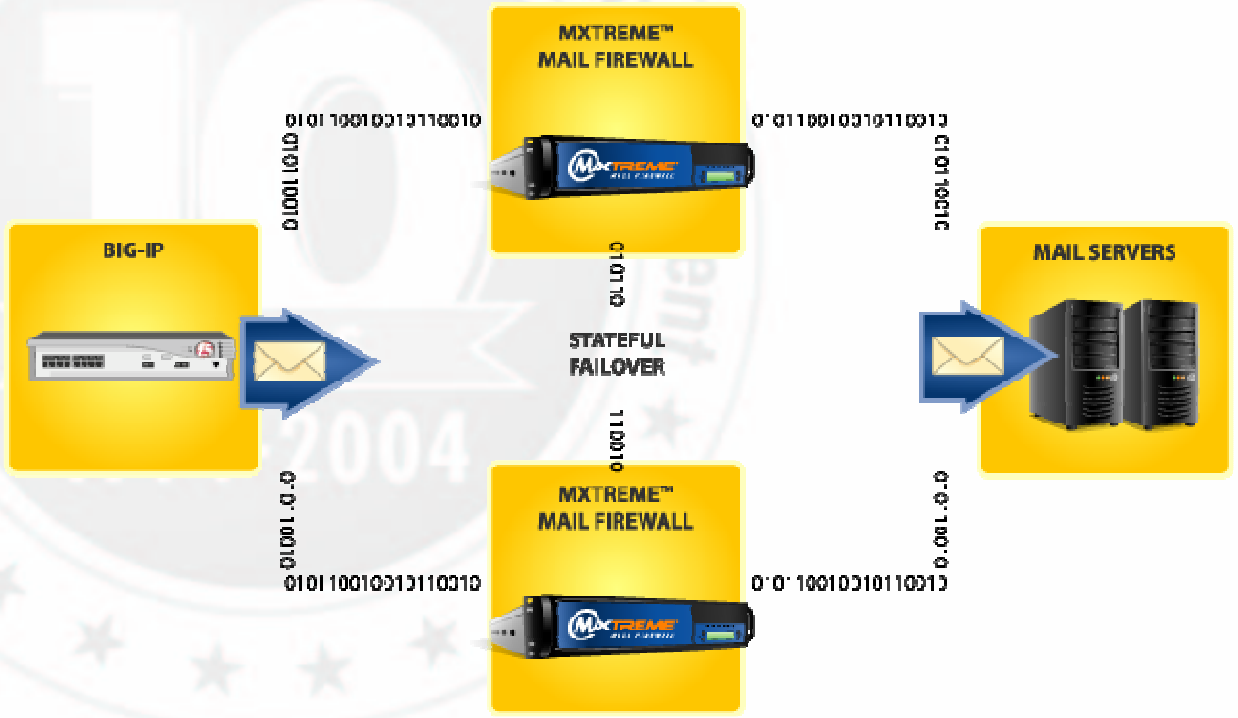
Laut einer Untersuchung des FBI haben 99% aller Unternehmen einen Virenschutz. Dennoch erlagen 2003 82% einer Virenattacke – der Schaden betrug $200 Mrd.

KASPERSKY ANTI-VIRUS

Stateful Failover™ - HALO™

Echte High-Availability implementiert um Verzögerungen und Downtime zu vermeiden – und dem Verlust wertvoller Nachrichten vorzubeugen

- Clustering
- Stateful-Failover
- Queue Replication
- Kompatibel mit Load Balancern
- Integration mit F5 BigIP
- Ausfallsichere Hardware



Null Downtime **Null Verzögerung** **Null Nachrichtenverluste**

Manage, Monitor und Audit

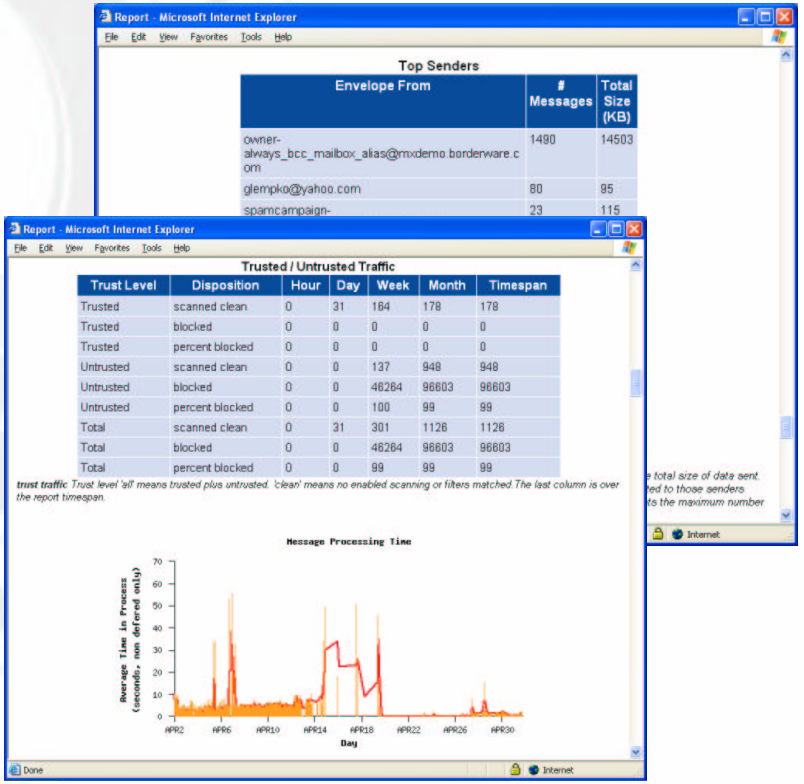
Reduziert die Kosten der Administration, erhöht die Sicherheit und bietet echte Kontrolle durch eine zentral zusammengefasste Lösung.

- Integrierte Content Kontrolle & Anti-Spam
- Policy - Steuerung mit LDAP
- Zentralisierte Konsole
- Zentralisiertes Reporting
- Integriert sich in die SNMP Management Tools des Unternehmens

Email Intelligenz und Übersicht

MXtreme Mail Firewall hat die fortschrittlichste Datenbank und Reporting Engine

- Trackt Email Verwendung im Cluster
- Identifiziert Anomalien und erlaubt Policy Fine-Tuning
- Unterstützt Kapazitäts-Planung
- Reduzierte interne Bandweiten-Kosten
- Entdeckt und identifiziert gegenwärtige und aufkommende Bedrohungen
- Verteilt Reports und Daten an das Management und die Administratoren
- Individuelle und Gruppenbasierende Reporting-Möglichkeiten

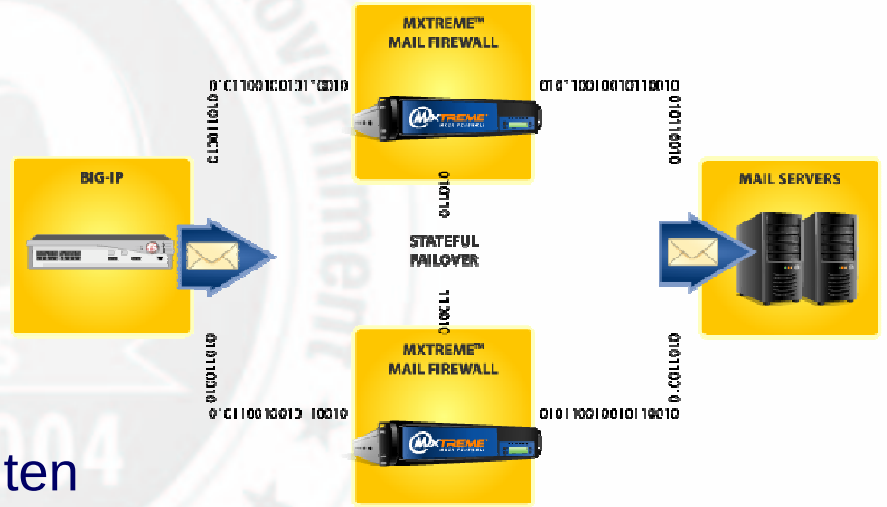


Message Geschwindigkeit steuern

MXtreme und BIG-IP ermöglichen Kunden ihren SMTP Traffic zu priorisieren und effektiver zu steuern.

Inbound und Outbound Routing Rules können basieren auf:

- Source Server
- IP Addresse der SMTP Connection
- Outbound Mail Prioritisierung
  - Unterstützt zeitkritische Mailings.
  - Isoliert einzelne User oder Nachrichten von Effekten anderer Mail-Handling Aktivitäten, welche auf anderen Systemen im MXtreme Cluster stattfinden könnten.



f5 NETWORKS

MXtreme Modelle

MX-1000 für Umgebungen mit sehr hohem Traffic; 2U Rack ; RAID 0+1; redundant power; 4x Gigabit

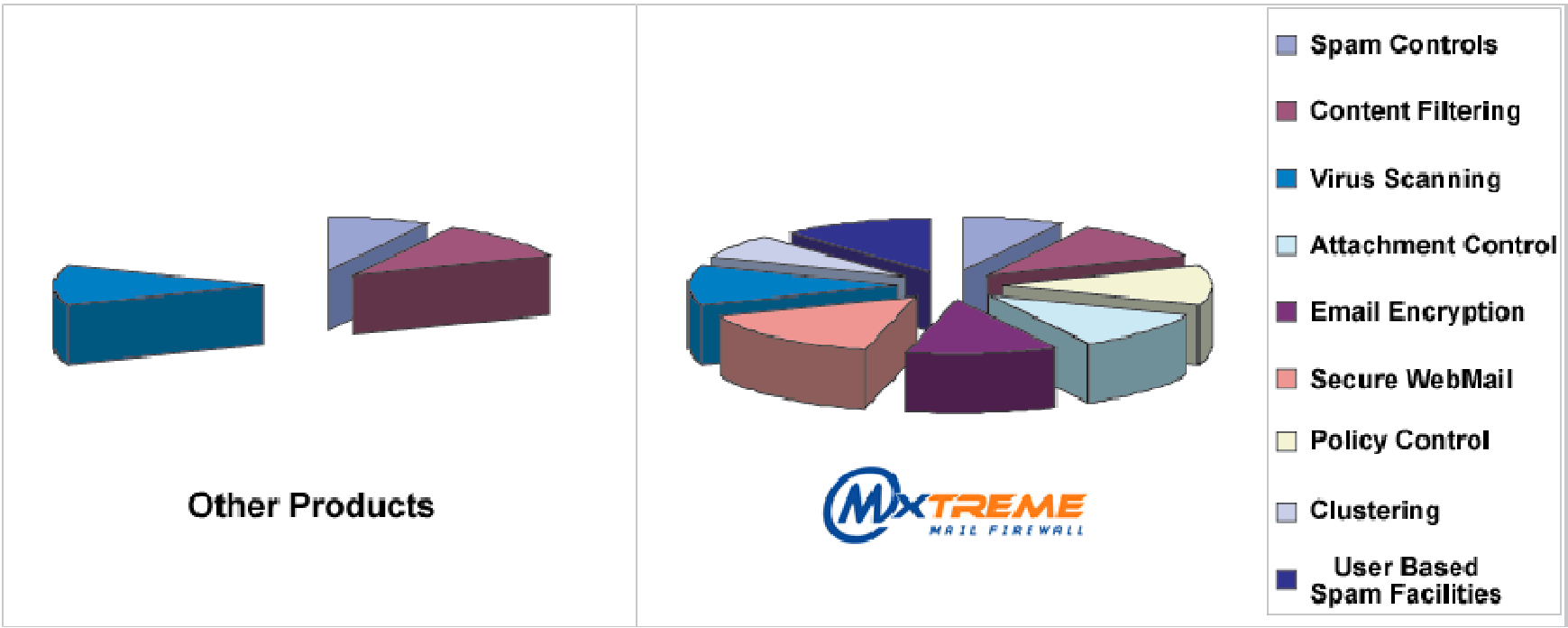
MX-800 für große Unternehmen; 2U Rack; RAID 0+1; redundant power; 2x Fast Ethernet; 2x Gigabit

MX-400 für Mittelständische Unternehmen: mittlerer Traffic;1U Rack; RAID 1; 2x Fast Ethernet; 1x Gigabit

MX-200 für Kleine Unternehmen und Zweigniederlassungen; 1U Rack; 2x Fast Ethernet

Warum ist die MXtreme anders?

- Die meisten Produkte/Lösungen decken nur einen Teil der Anforderungen an eine E-Mail Security Lösung ab.



MXtreme Kunden

Weitere Kunden

Vielen Dank!

Michael Kohl
Client-Server EDV
miko@client-server.ch
www.client-server.ch
http://document@client-server.co.at