



**sabadell
universitat**

INFORMACIÓ
REFLEXIÓ
DEBAT
CONEIXEMENT

TERCERA EDICIÓ DE SABADELL UNIVERSITAT
DEL 5 AL 9 DE JULIOL DE 2004

**Seguretat d'usuari
i de dades**

S3. Cityweb, portals de ciutat a Internet

Jordi Riera

Sabadell, 8 de juliol de 2004

organitzadors:



patrocinadors:



La seguridad en sistemas de mensajería

Versión v1.1

Jordi Riera Molina
jrm@nextret.net

Sabadell, 8 de Julio de 2004



BUSINESS IT SOLUTIONS

Índice

- Introducción: tendencias actuales
- Amenazas en los sistemas de mensajería
- Caso práctico

Introducción: tendencias actuales

Sistemas seguros de comunicaciones



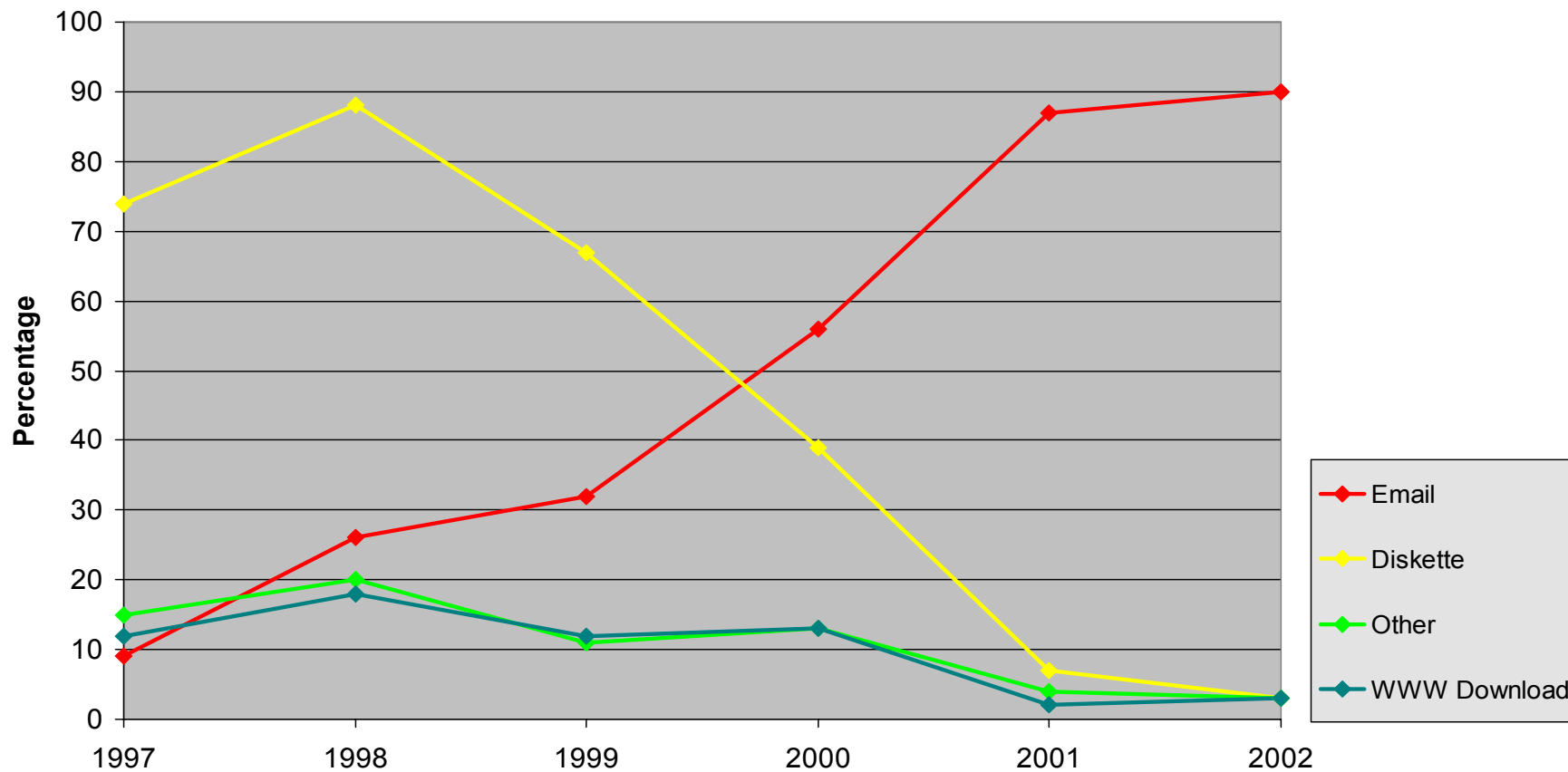
A considerar

- Los sistemas de mensajería son una parte vital en los procesos de negocio de las empresas:
 - Facilitan la comunicación interna
 - Es una herramienta de comunicación con los clientes, proveedores y usuarios
 - Mejoran los procesos internos
 - Etc...
- Pero....
 - Necesitamos controlar su uso
 - Aparecen nuevas amenazas: virus, spam..... Que pueden causar una denegación de servicio

Amenazas en los sistemas de mensajería

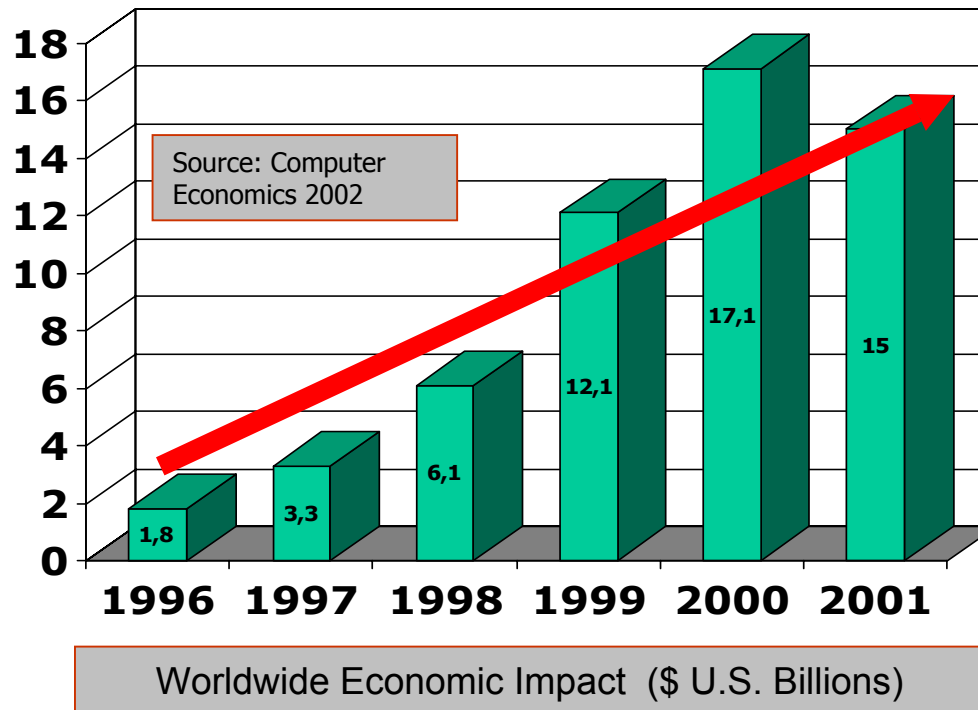
La amenaza de los virus

▪ De dónde vienen los virus?



La amenaza de los virus

- Los daños de los virus tienen un impacto muy negativo



La amenaza de los virus

- Estrategias de protección:
 - Protección en los puestos de trabajo
 - Antivirus
 - Control de las últimas versiones de sistema operativo y aplicaciones
 - Despliegue automático de clientes
 - Actualización automática de fichero de firmas
 - Administración centralizada
 - Entorno de puesto de trabajo y servidores controlado
 - Protección de servidores
 - Antivirus
 - Acceso a Internet
 - Antivirus en gateways
 - Antivirus en proxy
 - Control de la navegación Internet
 - Gestión del ancho de banda



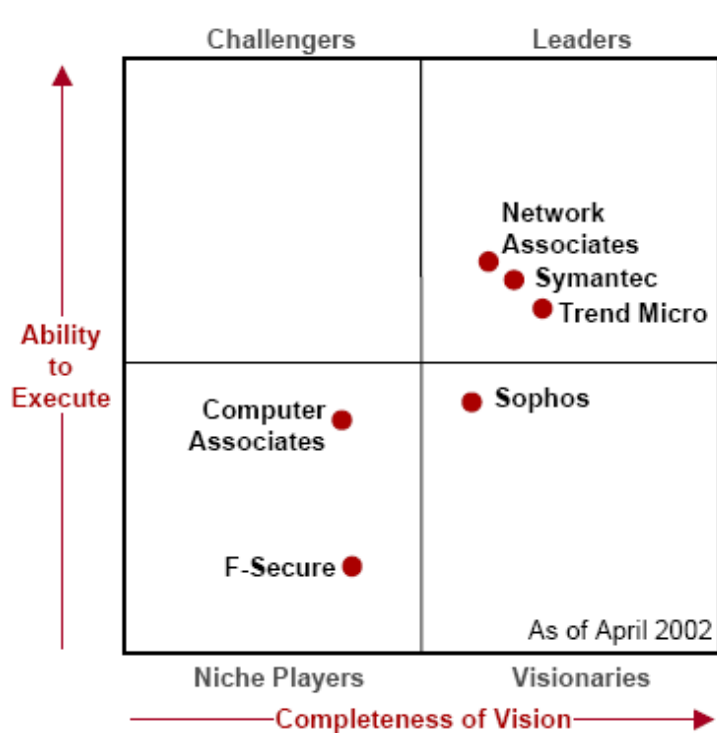
La amenaza de los virus

- Estrategias de protección:
 - Correo electrónico
 - Antivirus
 - Protecciones antispam
 - Generales
 - Heterogeneidad de proveedores de antivirus
 - Productos especialistas

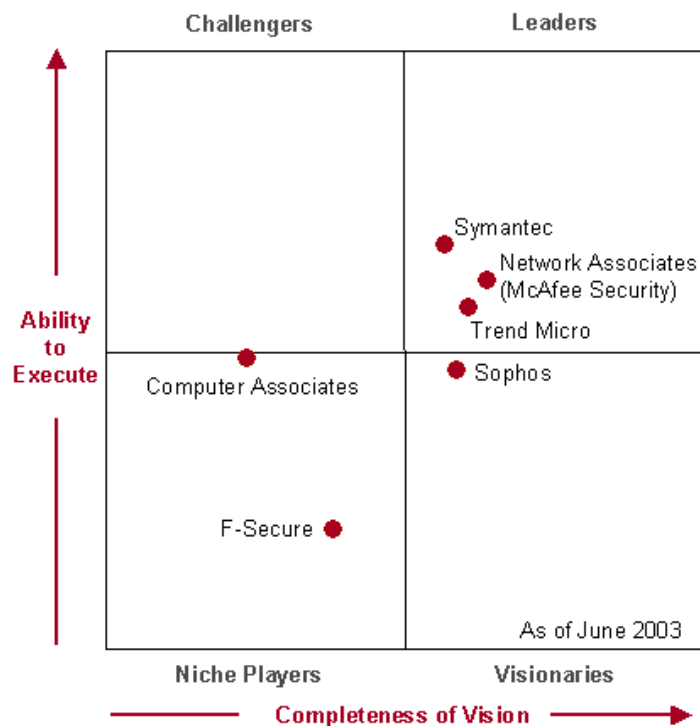


La amenaza de los virus

- Cual es la mejor solución? Según Gartner:



2Q02



1H03

La amenaza de los virus

▪ Cual es la mejor solución? Virus Bulletin (www.virusbtn.com)



• ESET

Result summary: 21 passes / 3 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.nod32.com/>

• Norman

Result summary: 20 passes / 8 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.norman.com/>

• Sophos

Result summary: 19 passes / 9 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.sophos.com/>

• Symantec

Result summary: 19 passes / 6 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.symantec.com/>

• Kaspersky

Result summary: 17 passes / 11 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.kaspersky.com/>

• VET

Result summary: 16 passes / 12 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.vet.com.au/>

• CA Iris

Result summary: 14 passes / 8 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.ca.com/etrust>

• Dialogue Science

Result summary: 12 passes / 12 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.antivir.ru/english/>

• NAI (McAfee)

Result summary: 10 passes / 16 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.networkassociates.com/>

• F Secure

Result summary: 10 passes / 11 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.fsecure.com>

• Trend Micro

Result summary: 4 passes / 7 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.antivirus.com/>

• Panda Software

Result summary: 1 pass / 3 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.pandasoftware.com>

• Alladin (eSafe)

Result summary: No passes / 9 fails
 Performance graph: - Success / Failure / No Entry
 Vendor website: <http://www.ealaddin.com/>

La amenaza de los virus

	Windows NT Feb 03	RedHat Linux May 03	Windows XP Professional Jun 03	Netware 6.0 Aug 03	Windows 2003 Server Nov 03
AhnLab	X	□	X	□	☑
Aladdin Knowledge Systems	□	□	□	□	□
Alwil	X	☑	☑	□	X
CAT Quickheal	X	□	☑	□	☑
Command Software Systems	☑	□	☑	X	□
Computer Associates (InoculateIT/eTrust)	☑	□	☑	X	X
Computer Associates (Vet)	☑	□	☑	☑	☑
DialogueScience	☑	X	X	☑	☑
Eset	☑	□	☑	☑	☑
F-Secure	☑	X	☑	□	☑
Frisk	X	X	☑	□	☑
GDATA	☑	□	☑	□	X
GeCAD	☑	X	☑	□	□
Ggreat	X	□	X	□	□
Grisoft	X	□	☑	□	☑
H+BEDV	□	X	□	□	□
Hauri	X	□	☑	□	□
Ikarus	□	□	□	□	□
Kaspersky	☑	X	X	☑	☑
Leprechaun VirusBuster II	□	□	□	□	□
McAfee	□	□	□	□	□
MicroWorld	X	□	☑	□	☑
Network Associates (McAfee)	☑	□	☑	☑	☑
Norman	☑	X	☑	☑	X
Panda Software	□	□	□	□	□
Proland Software	□	□	□	□	□
Softwin	X	□	☑	□	☑
Sophos	☑	X	☑	☑	☑
Symantec	☑	□	☑	☑	☑
Trend Micro	☑	☑	☑	□	☑
Virus Chaser	☑	□	X	□	X
VirusBuster	☑	X	☑	☑	☑

EL SPAM

- SPAM es el correo electrónico no solicitado
- En Junio de 2003 el SPAM representaba el 40% del tráfico de correo en EEUU, con un coste anual de 10.000 M\$ a las empresas
- El porqué del SPAM:
 - Cuesta sólo....
 - \$100 obtener un 1M de direcciones de correo electrónico...**
 - El coste, por dirección de e-mail es de:
 - \$0.0001 / e-mail**
 - Para un producto que se venda a:
 - \$12.95 con un beneficio de \$4.00...**
 - Y con una respuesta de:
 - 1 de 40,000 ...**
 - OBTENEMOS un punto muerto a partir del cual se obtienen beneficios.....



Los sistemas sencillos no funcionan

- Maneras distintas de escribir "Viagra"

V I @ G R A , V--1.@--G.R.a, \./iagra, Viiagra, V?agr?, V--i--a--g--r-a,
V!agra, V1agra, VI.A.G.R.A, vi@gra, vIagr.a, via-gra, Via.gra,
Vriagra, Viag*ra, vi-agra, Vi-ag.ra, v-iagra, Viagr-a, V^I^A^G^G^A,
V'i'a'g'r'a', V*I*A,G,R.A, VI.A.G.R.A..., Viag\ra!, Vj@GRA, V-i:ag:ra,
V'i'a'g'r'a, V/i;a:g:r:a, V i a g r @, V+i\algl\ra, Viag[ra, V?agra,
V;l;A*G-R-A, V-i-a-g-r-a, V*I*A*G*R*A , V-i-@-g-r-a, VI@AGRA,
Vi@gr@, V^i^ag-ra, VIAGRA, Vi\la.g.r.a, V1@GRA, v_r_i_a_g_r_a,
V\la:g:r:a, V^i^a^g^r^a, V-i-@-g-r-@, Viag(ra.

Qué deben hacer los sistemas AntiSpam ideales

- Eliminar o detectar el máximo del SPAM (sin intervención humana!!!)
- No detectar falsos positivos
- No generar carga administrativa
- Garantizar la privacidad
- Control centralizado / individualizado
- Distintas técnicas a aplicar
 - Listas negras
 - Filtros heurísticos
 - Filtros bayesianos
 - Filtros de contenido
 - Servicios gestionados con firmas de correo

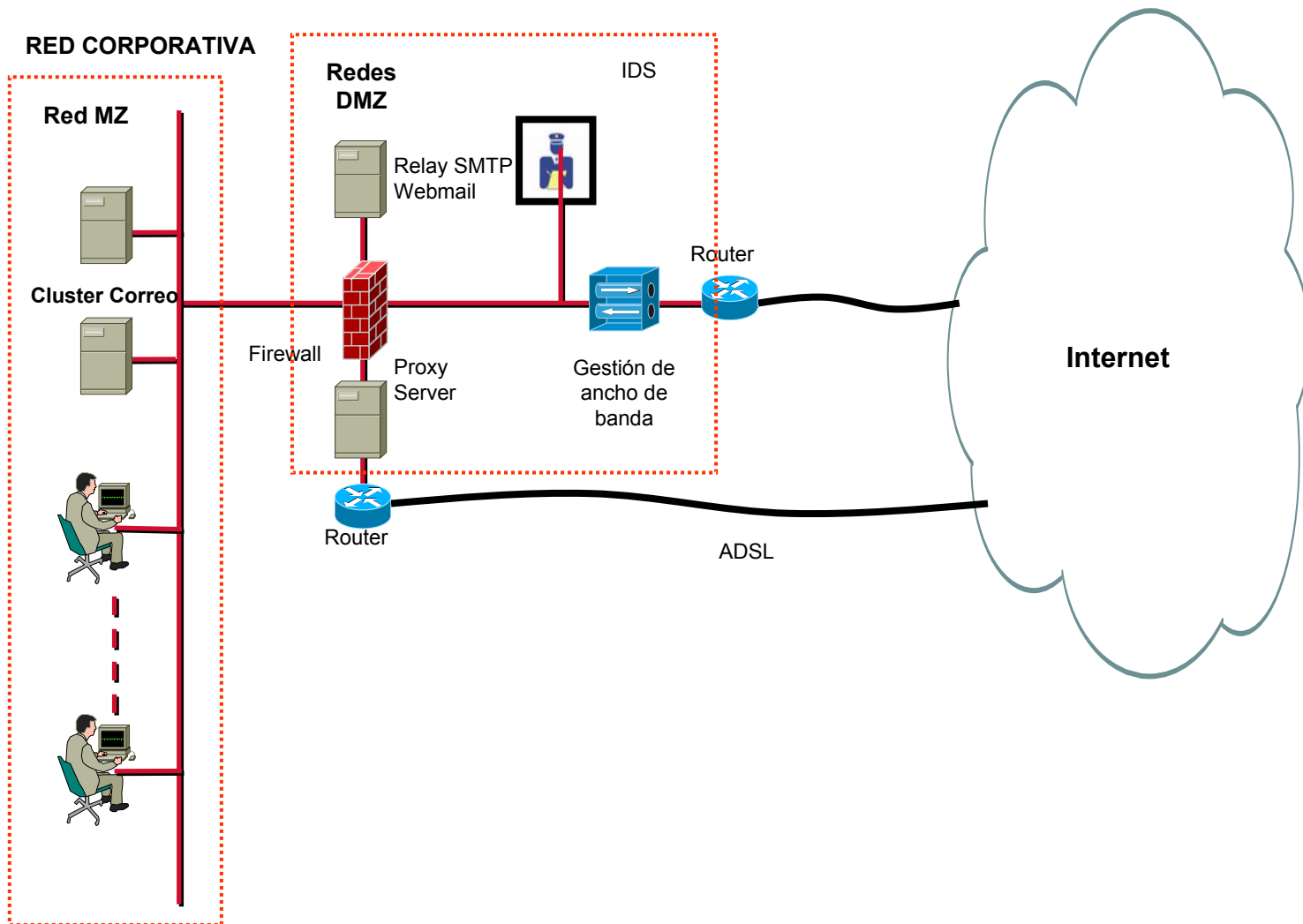


Caso práctico: infraestructura de mensajería segura

Caso práctico: infraestructura de mensajería segura

- Requerimientos:
 - Alta disponibilidad
 - Gestión de ancho de banda
 - Gestión centralizada de la información
 - Buena protección frente ataques
 - Buena protección frente a virus
 - Buena protección AntiSpam

Caso práctico: infraestructura de mensajería segura



- Paseo Bonanova, 9
- 08022 **Barcelona**
- T. 932 541 530
- F. 934 175 062



- Calle Fortuny, 3
- 28010 **Madrid**
- T. 917 021 645
- F. 913 198 453

Gracias por su atención
¿ Preguntas ?