SEGURIDAD INFORMÁTICA

PRINCIPIOS BÁSICOS

El ‘problema’ de la seguridad informática

- Cerca del 80% de los ‘ataques’ provienen del interior.
- No se notifican todos los ataques que se reciben.
- Muchos accidentes humanos se reportan como ataques.
- No es eficiente hacer una alta inversión puntual y olvidarse durante un tiempo.

- La seguridad es un proceso, un camino continuo.
- Se tiene que diferenciar de lo que hay que protegerse.

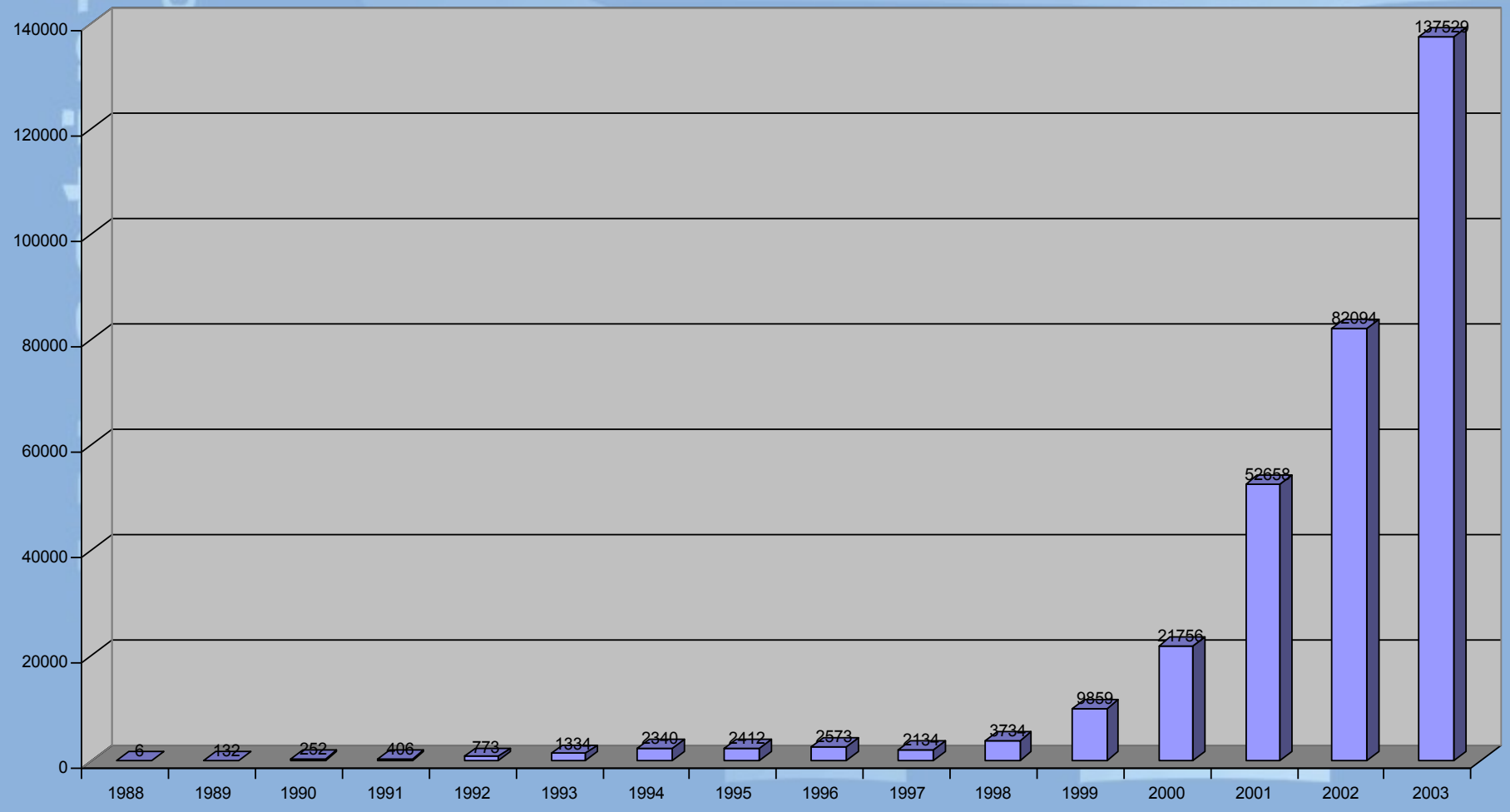
Ø Errores involuntarios. (Maquinaria y personal)

Ø Ataques voluntarios. (Internos y externos)

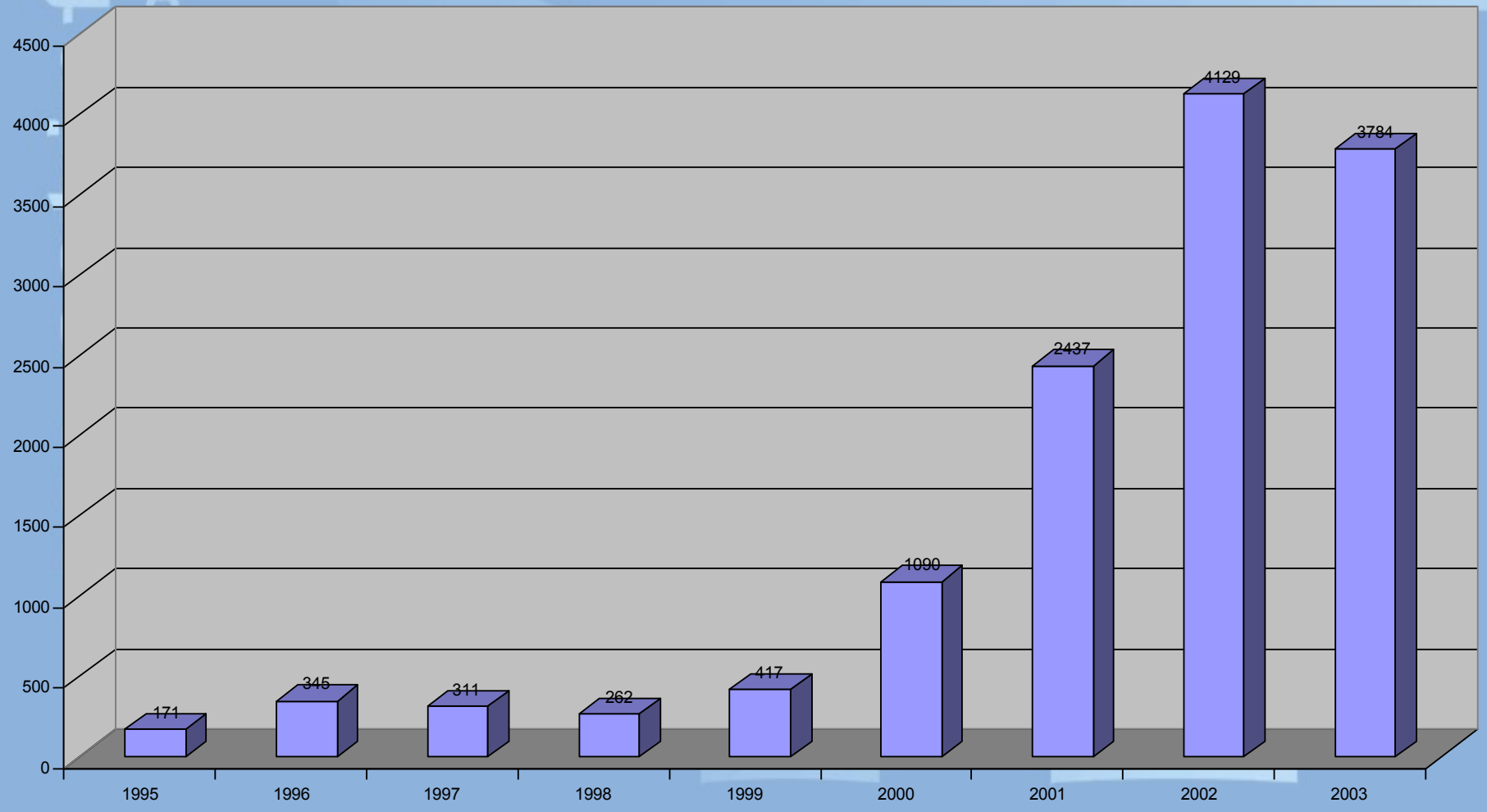
Ø Desastres naturales.

Incidencias reportadas al CERT.

(CERT: Centro de coordinación de emergencias telemáticas.)



Vulnerabilidades reportadas al CERT.



¿Cómo se puede proteger bien la empresa?

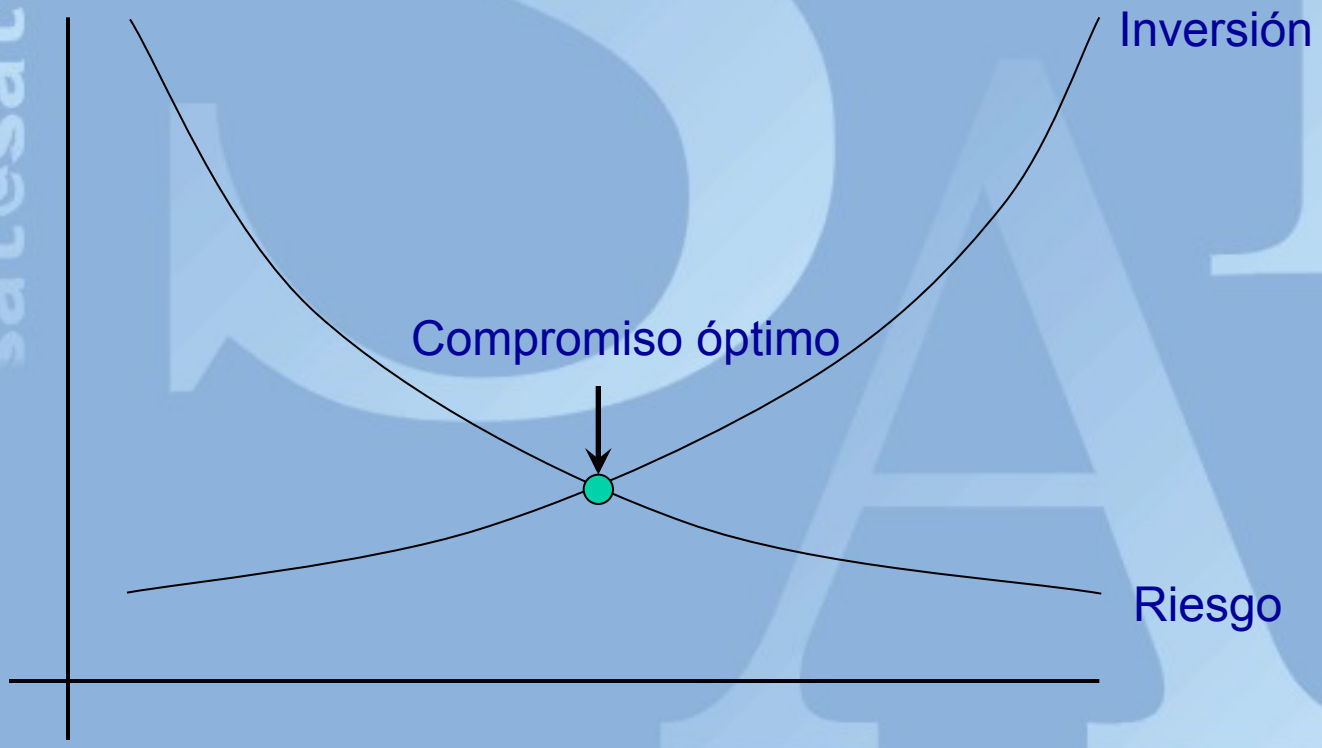
- Antivirus que controle todas las posibles entradas de datos. (Internet, discos, ...)
- Firewall perimetral. (Control de accesos)
- Separar físicamente redes diferentes. (Subnetting)
- Auditorias externas puntuales.
- Formación continuada del encargado(s) de seguridad.
- Política estricta de seguridad del personal.

A más seguridad, más coste.

A más seguridad, menos facilidad para el usuario.

No hay sistema conectado 100% seguro.

Se establece un compromiso de seguridad.



¿Cómo valorar la información a proteger?

¿Cuánto dinero dejaría de ganar en caso de estar 1 hora sin conexión a Internet?

¿Y un día?

¿Qué pasaría si pierde la información de un día de trabajo?

¿Y si su competencia tiene acceso a sus archivos?

Hay que valorar económicamente estos y todos los riesgos posibles con las preguntas adecuadas.

5 PASOS A SEGUIR EN

SEGURIDAD INFORMÁTICA

1- Asegurar la situación.

- Instalar los sistemas operativos esenciales y **TODOS** sus parches.
- Eliminar todos los privilegios y añadirlos solamente si se necesitan (Primero deniega, luego permite)
- Organizar mecanismos de autentificación de usuarios, copias de seguridad, detección y eliminación de virus, administración remota y acceso físico.
- Recabar y guardar de forma segura información de chequeo de integridad.

2- Prepararse.

- Identificar y priorizar los activos críticos, nivel de protección necesarios, amenazas potenciales, acciones de detección y reacción y autorización de actuación.
- Identificar la información a recabar y los mecanismos.
- Identificar, instalar y comprender las herramientas de detección y reacción.
- Determinar la mejor forma de recabar, tratar, proteger y guardar toda la información que se tiene.

3- Detección.

- Asegurar que el software usado para examinar los sistemas no ha sido comprometido.
- Vigilar y monitorizar la actividad de la red y los sistemas.
- Inspeccionar archivos y directorios por cambios inesperados.
- Investigar hardware y software no autorizado.
- Buscar signos de acceso físico no autorizado.
- Iniciar procedimientos de respuesta.

4- Reacción.

- Analizar toda la información disponible. Saber qué es lo que ha pasado.
- Distribuir la información por políticas determinadas, usar canales seguros.
- Guardar y conservar las evidencias.
- Contener el daño.
- Restaurar los sistemas a su status normal.

5- Mejorar / aprender.

- Identificar las lecciones aprendidas, recoger información del caso sucedido.
- Instalar nuevos parches (Reasegurar), desinstalar parches problemáticos.
- Actualizar la configuración de los mecanismos de alerta, logs y recogida de información.
- Actualizar la información de los activos de la empresa.
- Instalar una herramienta nueva, desintalar una vieja.
- Actualizar políticas, procedimientos y formación.

FIREWALLS

¿Qué es un Firewall?

• Elemento de red cuya finalidad es asegurar que solamente las comunicaciones autorizadas son las permitidas a pasar entre redes. Bloquear las comunicaciones no autorizadas y registrarlas.

¿De qué puede proteger un Firewall?

- Ataques externos.
- Virus que usen instrusismo. (Lovsan, SQLSlammer, ...)
- Accesos no deseados.

¿De qué **NO** puede proteger un Firewall?

- Ataques internos en la misma red.
- Mala configuración de zonas desmilitarizadas.
- Falta de mantenimiento de las políticas.
- Inexperiencia del administrador.
- Bugs de los S.O.
- Virus informáticos.

¿Firewall de hardware o de software?

- El hardware no puede ser desactivado por un virus o programa nocivo.
- La integridad del software puede ser comprometida.
- El hardware suele ser más potente y con más recursos.
- El hardware no consume recursos del sistema (CPU y memoria) y no es dependiente del S.O.
- ...

Siempre es más aconsejable una opción de hardware.

ANTIVIRUS

¿Qué es un virus informático?

- Programa informático que se reproduce a sí mismo y ataca al sistema.
- Puede abrir accesos (Backdoors) a atacantes externos.
- Puede reproducirse por la red (Worms)
- Puede ser programado para dañar gravemente un sistema (Bombas lógicas)
- Puede camuflarse en programas 'conocidos' (Troyanos)

¿De qué me protege un antivirus?

- Alteración del correcto funcionamiento del equipo por parte de virus informáticos.
- Ejecución de códigos nocivos en el equipo.

¿De qué **NO** me protege un antivirus?

- Agujeros del S.O.
- Accesos no deseados (Intrusismo)
- Uso malintencionado o erróneo del equipo
- Recibir correo basura (Spam)

Otras consideraciones a tener en cuenta (I)

- Copias de seguridad periódicas.
- Copias de seguridad en ubicación remota.
- Cambio periódico de las contraseñas.
- Evitar los usuarios genéricos (admin, invitado, ...)
- Evitar las contraseñas fáciles (admin, 1234, ...)
- Uso de SAIs (Sistemas Alimentación Ininterrumpida)
- Uso de estabilizadores de corriente.

Otras consideraciones a tener en cuenta (II)

- Usar programas con menos vulnerabilidades. (Netscape, Eudora, Pegasus, ... frente a Outlook)
- Desconfiar del remitente del correo, aunque parezca 'conocido'. Se puede falsear el remitente.
- Encriptar información sensible.
- Encriptar canales de comunicación sensibles. (VPN)
- Alta disponibilidad y mirror en servidores críticos.
- Usar firmas digitales para autentificar mensajes.

Algunas webs de interés:

- http://www.satinfo.es - Mayorista español de seguridad informática.
- http://www.nai.com - Fabricante del antivirus McAfee.
- http://www.clavister.com - Fabricante sueco de cortafuegos.
- http://www.spi-a.com - Fabricante de cortafuegos AlphaShield.
- http://www.cert.org - Centro de coordinación de emergencias en redes telemáticas.
- http://escert.upc.es - Centro español del CERT.
- http://www.hispasec.com - Portal hispano de seguridad informática.
- http://www.eicar.org - Instituto europeo para la investigación de antivirus.
- http://www.infohackers.org - Asociación para la información de Hackers.
- http://www.pgpi.com - Web internacional del protocolo de encriptación PGP.
- http://www.microsoft.com/security - Guías de ayuda de Microsoft sobre seguridad.

Bibliografia de interés:

• Stuart McClure & Joel Scambray, George Kurtz. Hacking Exposed (Network Security Secrets & Solutions), Osborne/McGraw-Hill, 1999

• Stephen Northcutt & Judy Novak. Network Intrusion Detection An Analyst's Handbook Second Edition, New Riders Publishing, 2001

• Guang Yang. Introduction to TCP/IP Network Attacks, Department of Computer Science, Iowa State University

• R.T. Morris. *A Weakness in the 4.2BSD UNIX TCP/IP Software*, CSTR 117, 1985, AT&T Bell Laboratories, Murray Hill, NJ.

• Steven M. Bellovin. *Defending Against Sequence Number Attacks*, 1996, AT&T Research

• Postel, J. *Transmission Control Protocol*, STD 7, RFC 793, September 1981.

• Atkinson, R. *Security Architecture for the Internet Protocol*, RFC 1825, August 1995.

• Joncheray. *A Simple Active Attack Against TCP*, 1995, Proc. Fifth Usenix UNIX Security Symposium

www.satinfo.es

sat@satinfo.es

Muchas gracias por su atención.

Servicio técnico SATINFO.