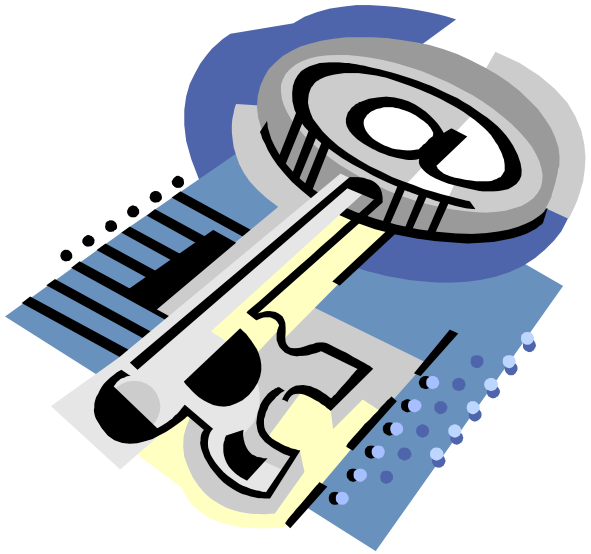
Seguridad informática

Una visión Global...

Pedro David Marco

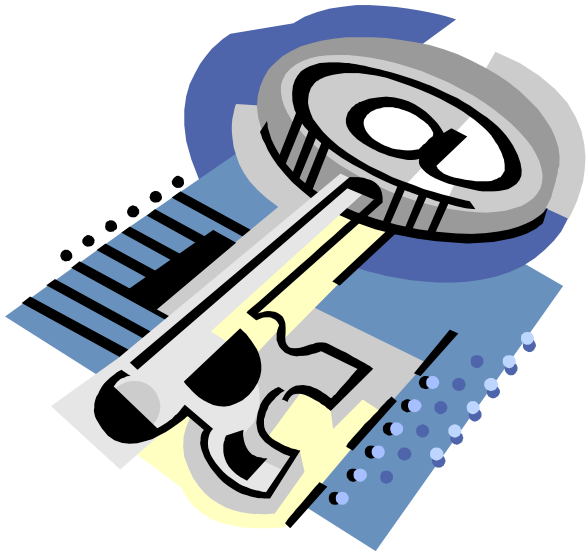
Agenda

- Introducción
- Estado, preocupaciones y riesgos actuales
- Costes de la seguridad
- Tecnologías



Agenda

Introducción



Introducción

¿Qué es la seguridad?

- **En Junio de 1942 un problema criptográfico japonés tuvo como consecuencia la destrucción de sus 4 mayores portaaviones y supuso el fin del dominio japonés del Pacífico.**

¡Bueno, esto es cosa de los militares y además ya forma parte del pasado!

Introducción

- **El 2 de Noviembre de 1988 un joven llamado Robert Morris escribió un pequeño programa capaz de, usando algunas vulnerabilidades de UNIX, transmitirse de unos sistemas a otros a gran velocidad infectándolos a su paso.**

  En unas horas miles de equipos tenían sus CPUs al 100% sin solución de continuidad.

  Se trataba del primer Gusano (Worm) de la historia.

¡Es cosa de “los locos del UNIX” y también es ya pasado, con un AntiVirus esto se habría evitado!

Introducción

- **En Junio de 2005 un hacker logró un listado de 40 millones de tarjetas de crédito.**

  Servired, Visa y 4B tuvieron que localizar y avisar urgentemente a más de 50.000 clientes en España del riesgo que corrían

¡Esto ya no hace tanta gracia!

Introducción

- **Históricamente la seguridad no ha sido nunca vista como una parte más de las tecnologías de la información, sino como algo propio de pequeños círculos de amistades, curiosos o gurús.**

- **En las universidades no existían (en muchas aún hoy no existen) asignaturas relacionadas con la seguridad**

- **En el mundo empresarial aun hoy existe esta tendencia en muchos casos**

Introducción

Existen varias razones por las que a todos los niveles no se le ha dado a suficiente importancia:

1. **El riesgo y las consecuencias de ignorarlo eran mínimos**
2. **Siempre ha sido incomoda: mucho esfuerzo -> poco resultado**
3. **Los posibles ataques requerían muy altos niveles de conocimiento.**
4. **El acceso al conocimiento y a las redes era muy limitado**

Introducción

¿Qué es el riesgo?

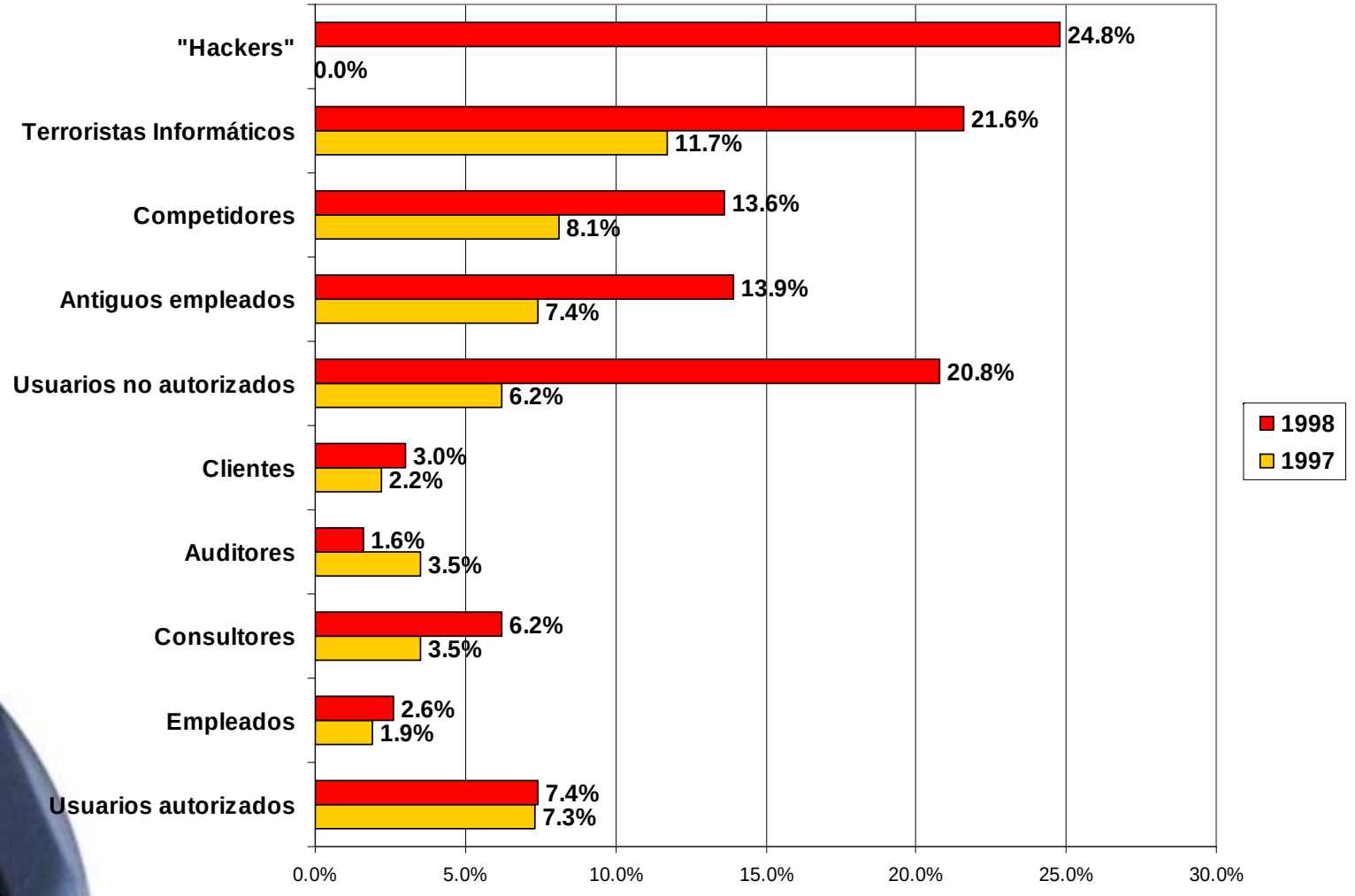
Riesgo* = *vulnerabilidades * amenazas

Si no hay amenazas no hay riesgo

Si no hay vulnerabilidades no hay riesgo

Introducción

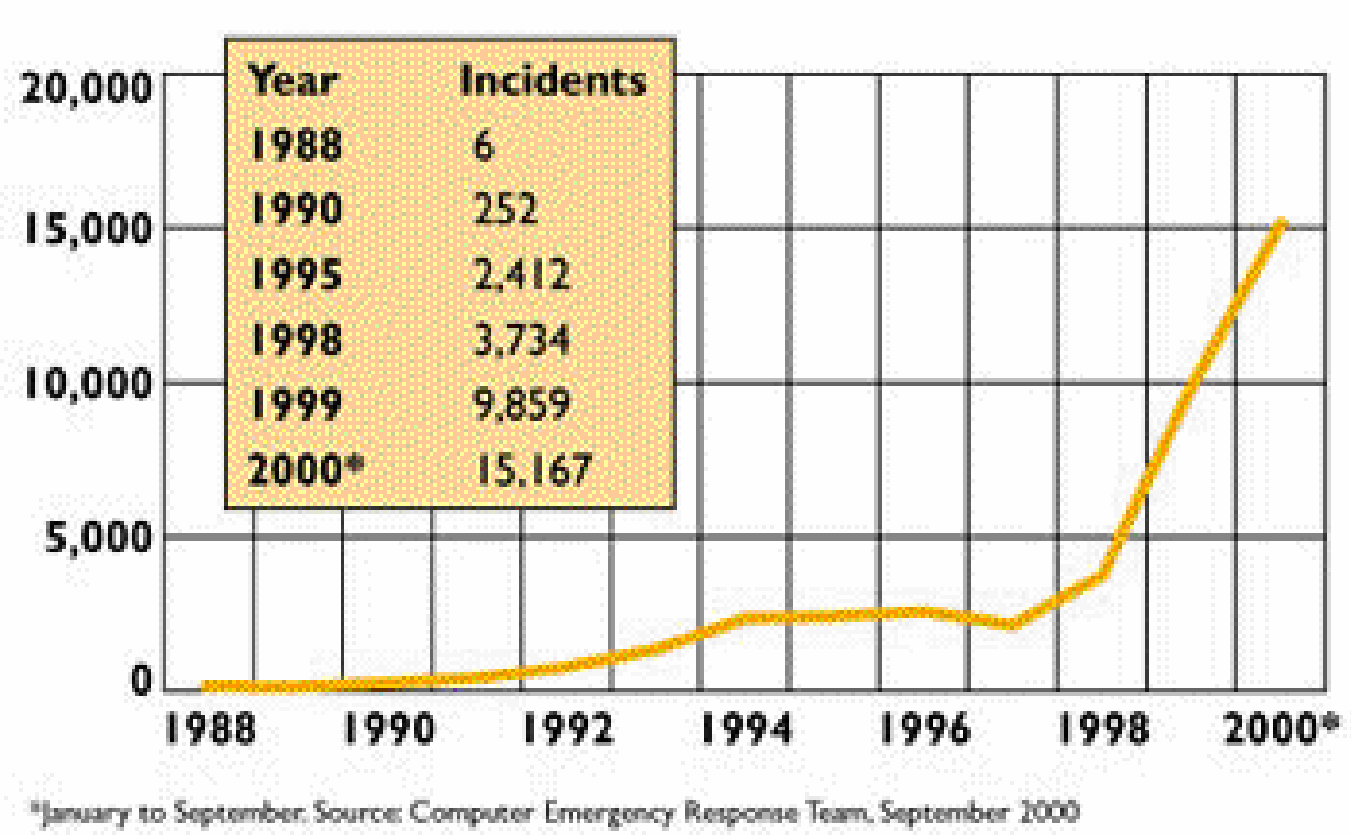
Factores que se consideraban fuentes de amenazas:



Fuente: Ernst&Young

Introducción

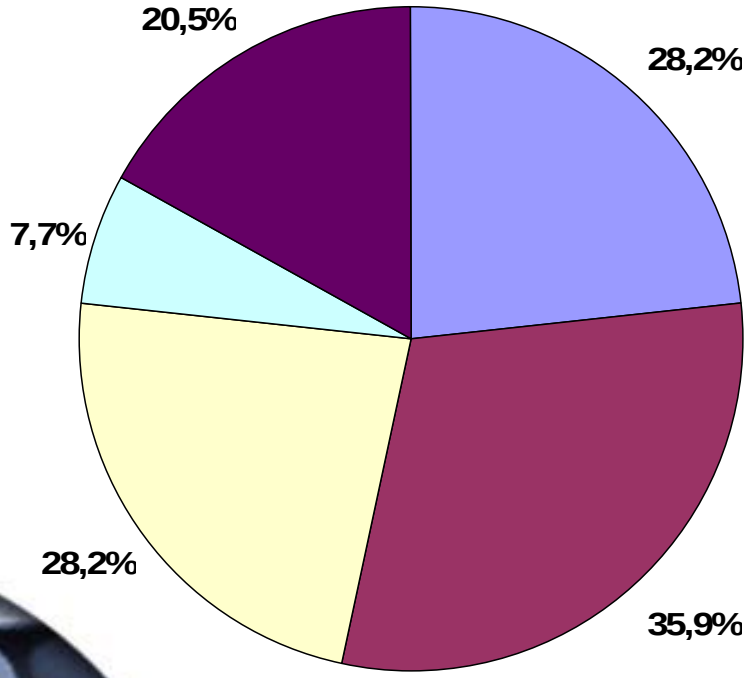
Evolución mundial de las vulnerabilidades



*January to September. Source: Computer Emergency Response Team, September 2000

Introducción

Incidentes denunciados por empresas. España. 1999.



Fuente: CDI, Guardia Civil

Introducción

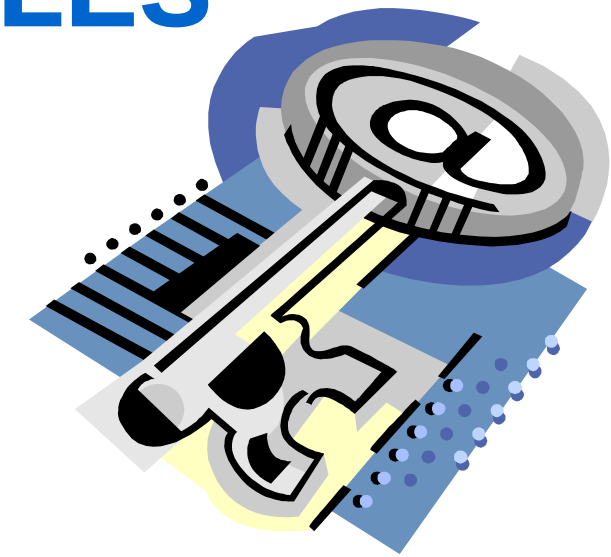
Hoy en día el escenario ha cambiado

¡¡ RADICALMENTE !!

Agenda

Estado, preocupaciones y riesgos

ACTUALES



¿Cuál es el nivel de riesgo en la actualidad?

1. Las vulnerabilidades se disparan todos los años:

Vulnerabilities reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2005

Year	2000	2001	2002	2003	2004	1Q-3Q,2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	4,268

Total vulnerabilities reported (1995-3Q,2005): **23,868**

Fuente: Cert

¿Cuál es el nivel de riesgo en la actualidad?

2. **Las amenazas también aumentan:**

Cada vez es necesaria menos especialización y menos conocimiento técnico para llevar a cabo ataques, robar y/o modificar información o cometer fraudes.

No sólo está disponible y al alcance de todos la información sobre los fallos y las vulnerabilidades sino que también lo están los "exploits" y las herramientas para llevar a cabo todo tipo de acciones.

Preocupaciones y riesgos actuales

Si además tenemos en cuenta que:

1. **Hoy día todo esta conectado con todo**
2. **El número de usuarios de la red crece exponencialmente**
3. **Cada vez hay más sistemas y servicios en la red**

El nivel de riesgo es suficientemente alto como para empezar a pensar en la seguridad como algo imprescindible

Tipos de ataques actuales: Ataques híbridos

Son ataques en los que se mezclan más de una técnica:

DOS, DDOS, Exploits, Escaneos, Troyanos, Virus, Buffer Overflows, Inyecciones, etc.

Suelen ser de muy rápida propagación y siempre se basan en alguna vulnerabilidad de algún sistema.

Por ejemplo los gusanos Blaster, Sasser, o Slammer se propagaron por todo el planeta en cuestión de pocas horas gracias a una mezcla de técnicas de “uso de vulnerabilidad”, Buffer Overflows, escaneado de direcciones, transmisión vía Internet, y mimetización en los sistemas.

Como curiosidad: el 75% de los ataques tienen como telón de fondo técnicas de Buffer Overflow

¿no podrían ser evitadas?

Tipos de ataques actuales: **Ingeniería social**

Son ataques en los que se intenta engañar a algún usuario para hacerle creer como cierto algo que no lo es.

- Buenos días, ¿es la secretaria del Director del Departamento?
- Si digame, ¿que desea?
- Soy Pedro, técnico informático del Centro de Apoyo a Usuarios y me han avisado para reparar un virus del ordenador del director pero la clave que me han indicado para entrar no es correcta, ¿podría ayudarme, por favor?

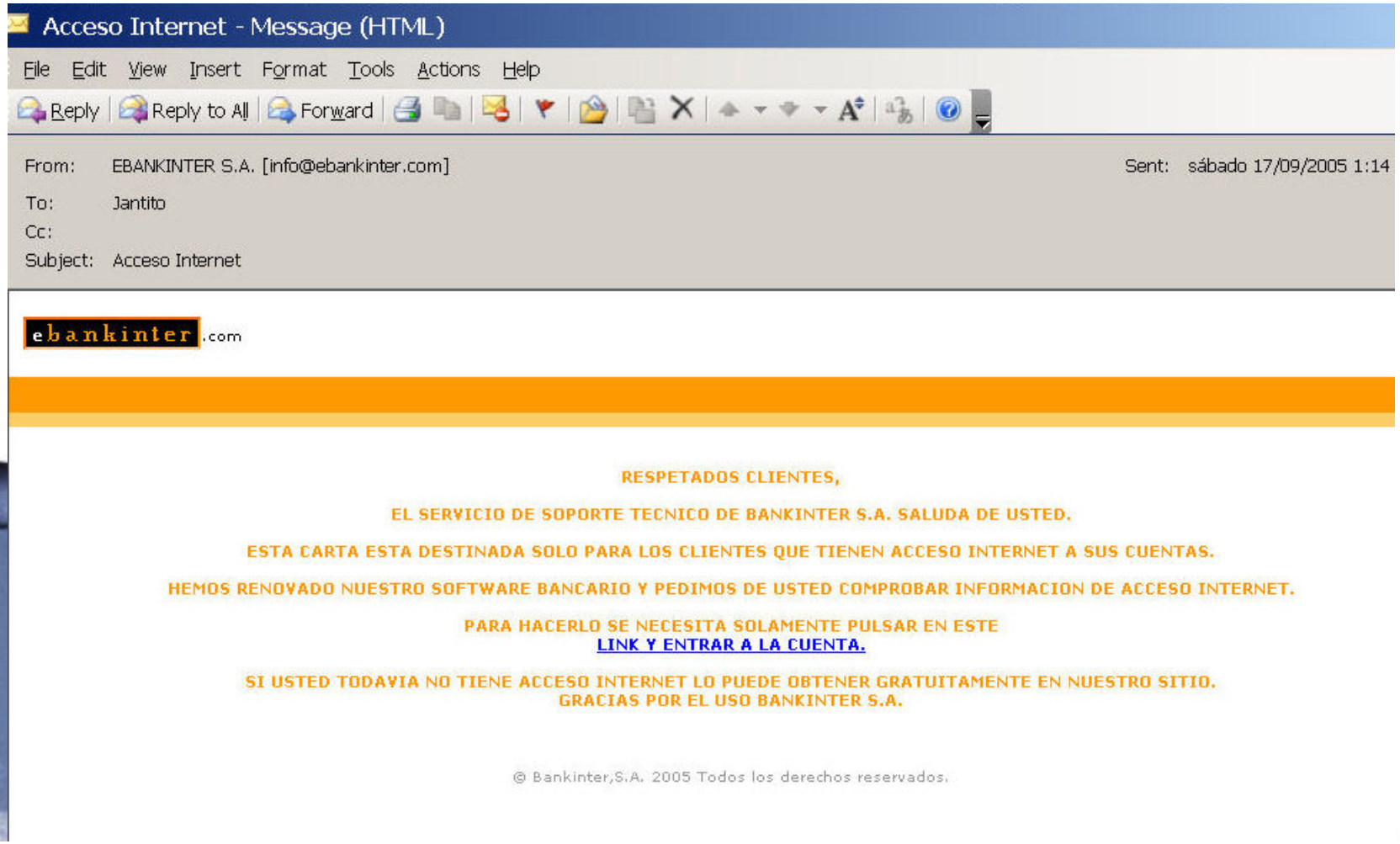
Otros ataques de este tipo son:

- Farming
- SPAM
- Pishing
- Cajeros automáticos
- ETC.

Preocupaciones y riesgos actuales

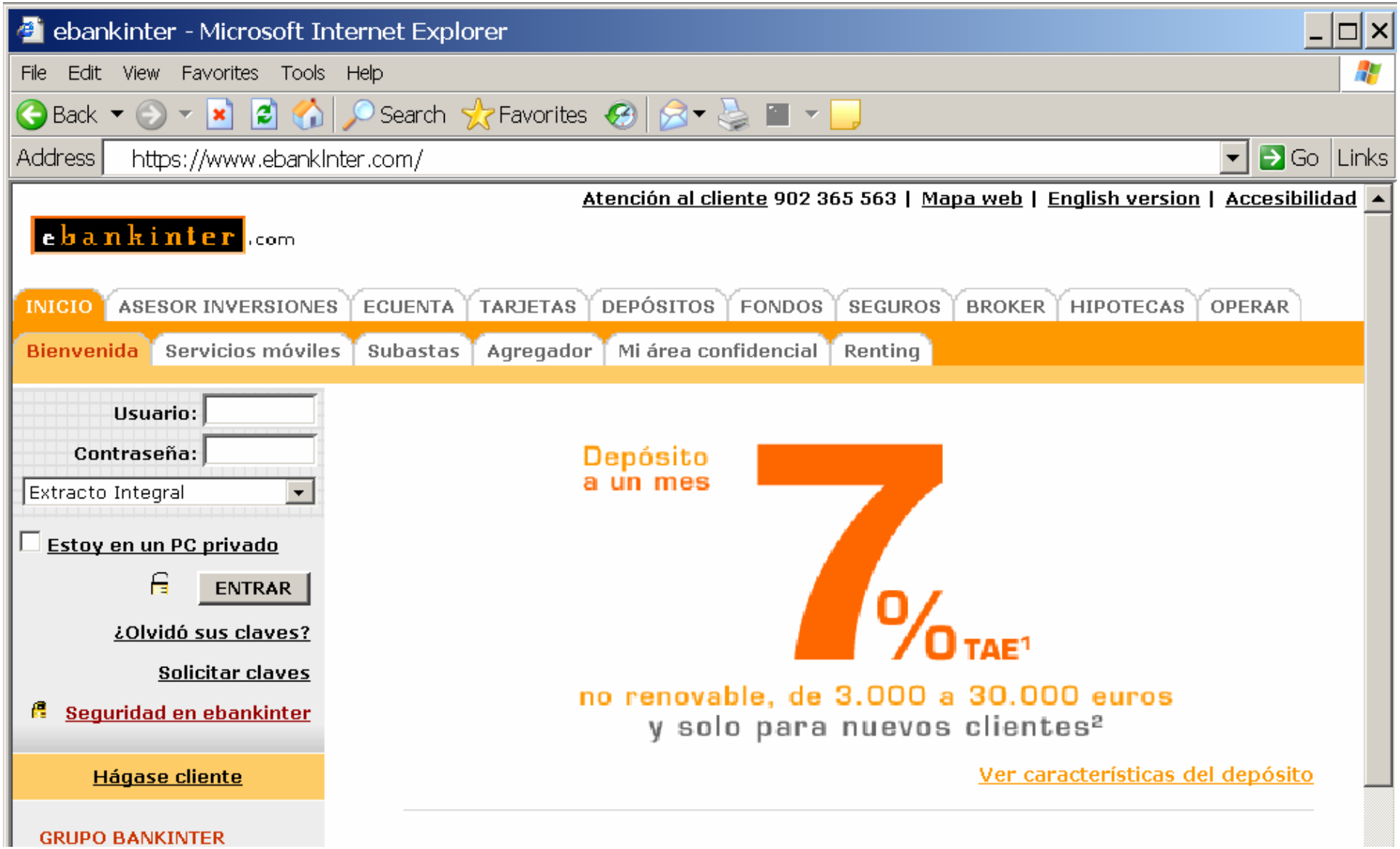
Tipos de ataques actuales: **Ingeniería social**

El ataque que más preocupa hoy en día a las grandes organizaciones, sobre todo en el sector de banca online es, con diferencia, el “PISHING”:



Preocupaciones y riesgos actuales

Ejemplo de Pishing…



Preocupaciones y riesgos actuales

¿Qué preocupa y qué no en un proyecto de seguridad?

Existe un problema subyacente en la mente de TODOS los Directores de informática de las grandes compañías que nunca debemos olvidar si queremos tener éxito en la implantación de un sistema de seguridad:

"La compañía puede vivir sin seguridad pero no sin comunicaciones"

Si un sistema de seguridad, por muy maravilloso que sea, destinado a evitar problemas que pueden no haberse producido aun puede generar problemas Nuevos, ese sistema NO SERA ACEPTADO.

Preocupaciones y riesgos actuales

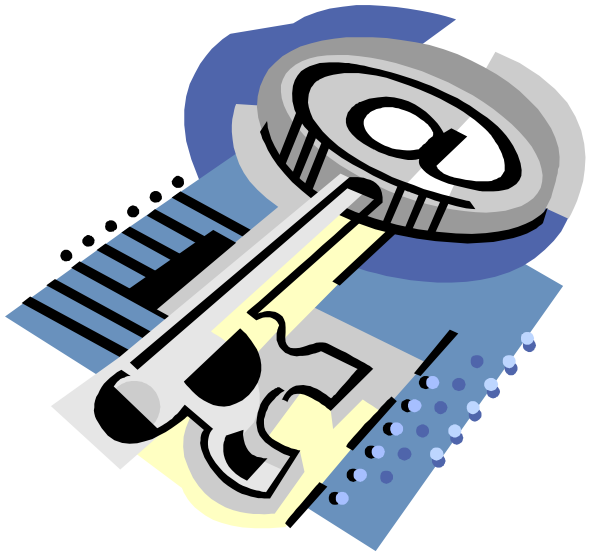
¿Donde queda la criptografía en todo esto?

Los estándares actuales de cifrado de la información (AES, DES, RSA, MD5, etc., etc.) son globalmente aceptados como buenos y suficientes en la mayoría de los casos, quedando su estudio reducidos a pocos entornos, Universidades, Fuerzas del Orden, Ministerios, etc.

La criptografía capta la atención general pocas veces, pero cuando lo hace suele ser por algo serio, cuando algún protocolo y/o algoritmo es “reventado”. Por ejemplo, WEP, el cifrado que usan las redes WiFi basado en RC4 que puede ser descifrado si se consigue una captura de tráfico suficientemente grande.

Agenda

Costes de la seguridad



El Coste de la seguridad

El esfuerzo tanto económico como humano de los Departamentos de Seguridad debe buscar siempre cuatro objetivos:

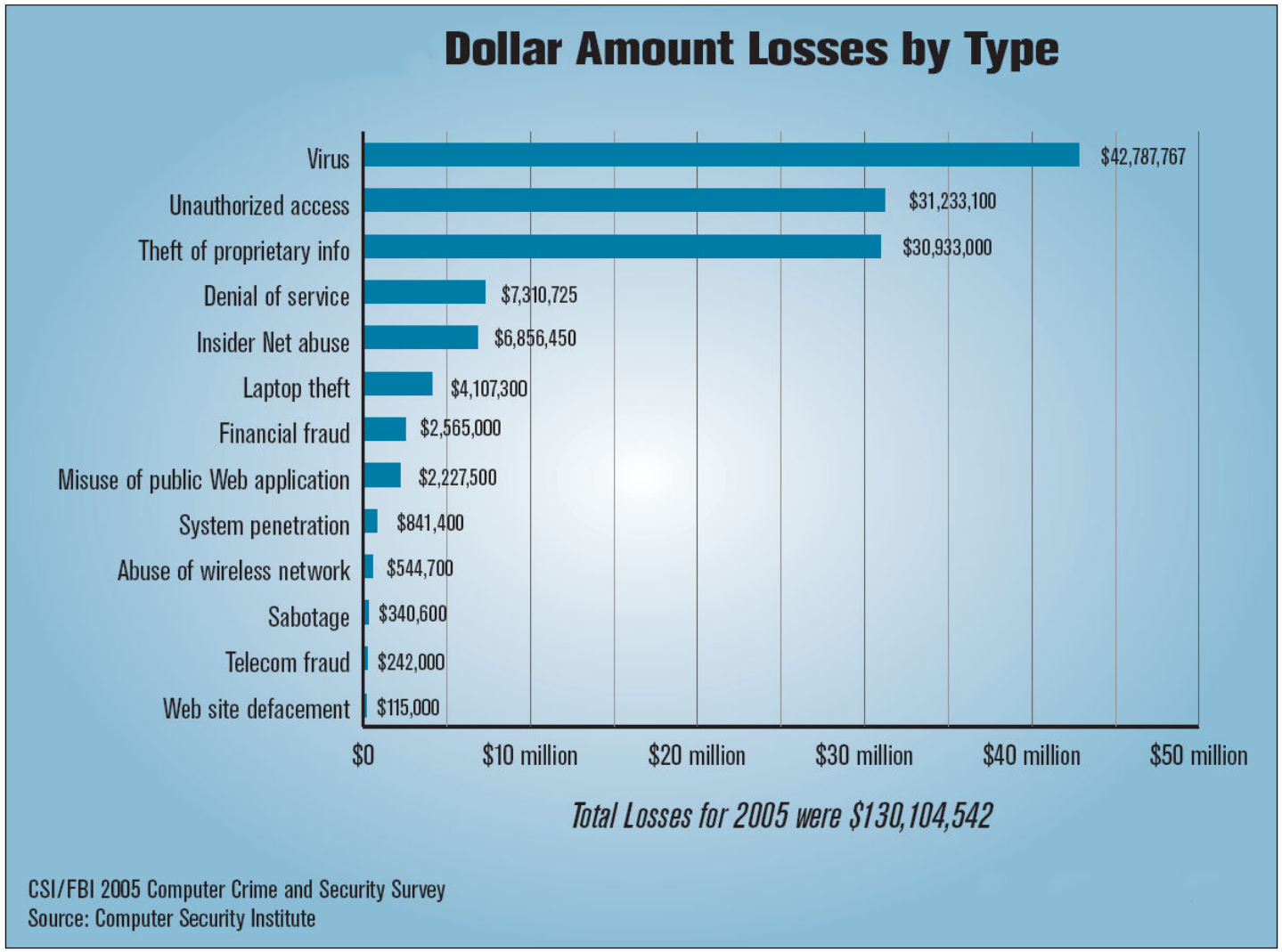
1. Disponibilidad

   Se consideran sistemas aceptables a partir de dos nueves, esto es: disponibles el 99,99% del tiempo. La inversión por cada nueve extra es siempre muy elevada.

2. Confidencialidad: Seguridad “keep the good giys in”
3. Integridad: Seguridad “Keep the bad guys out”
4. Cumplimiento de la legalidad: LOPD, Sarbanes-Oxley, ISO17799

Costes de la Seguridad

El esfuerzo económico en seguridad es imposible de medir pero como éste debe ser siempre proporcional al riesgo de perdidas, que SI ES MEDIBLE, si es posible hacer estimaciones razonables



Costes de la Seguridad

Problemas colaterales de la seguridad en las grandes compañías

1. Costes & ROI (Return of Investment)

1. Costes de personal
    1. Difícil encontrar técnicos cualificados
    2. Muy alta rotación en según que sectores
2. Costes tecnológicos: HW, SW, ROI
3. Costes ocultos (a menudo elevados)
4. Costes de cumplimiento de la legalidad (LOPD, Sarbanes-Oxley, etc)
5. Costes de cumplimiento de políticas y normativas
6. Costes de seguros (aprox. 25% de las compañías)

Preocupaciones y riesgos actuales

Problemas colaterales de la seguridad en las grandes compañías

2. De organización

Lleva mucho tiempo y esfuerzo conocer e integrar cualquier sistema de seguridad cuando hay implicado más de un departamento.

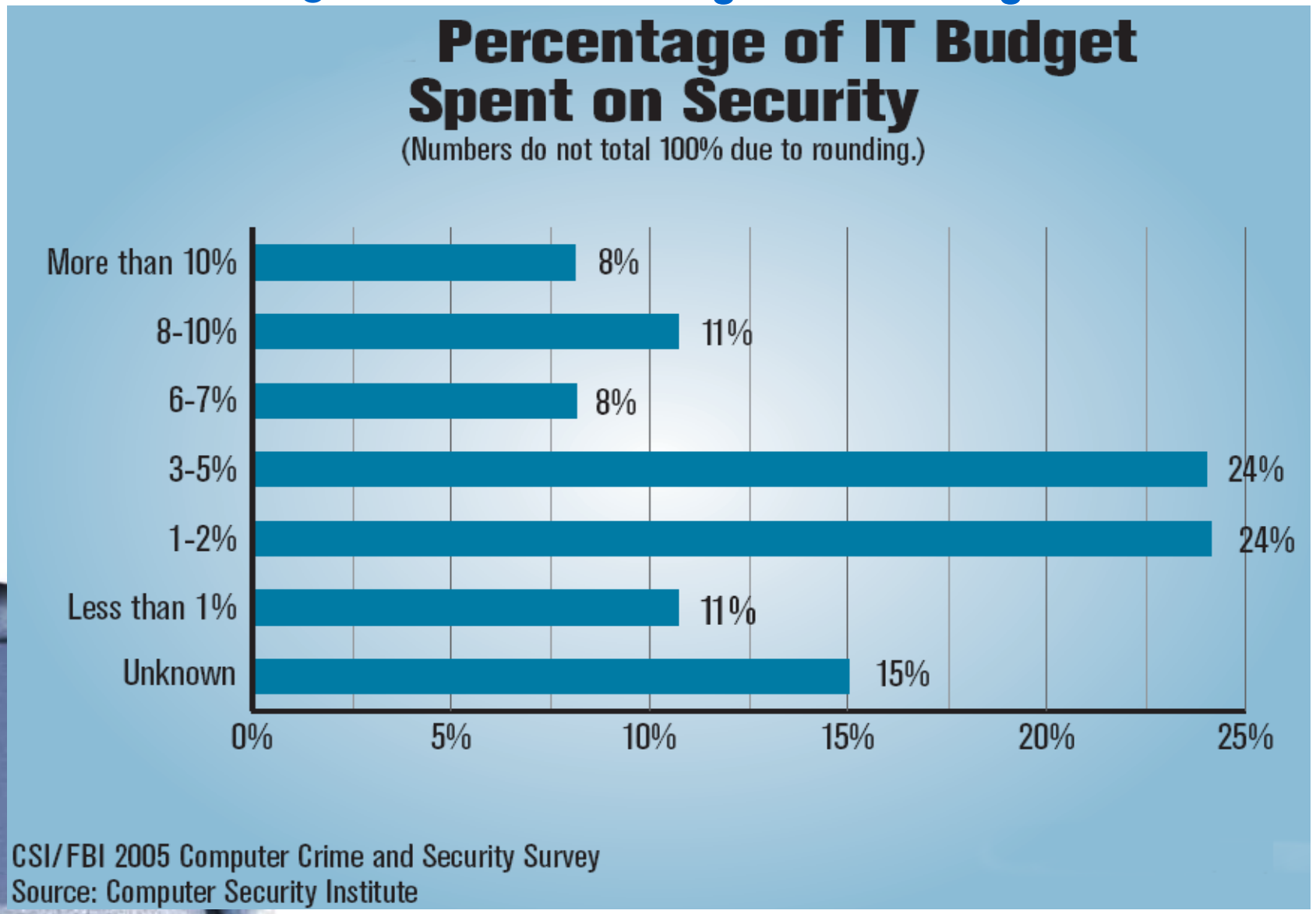
Se estima que 30 minutos de un Hacker pueden suponer una semana de trabajo de un ingeniero con experiencia para reparar lo dañado y prevenir nuevos incidentes

3. De garantía de disponibilidad

4. De garantía de ajuste a normativa y legalidad

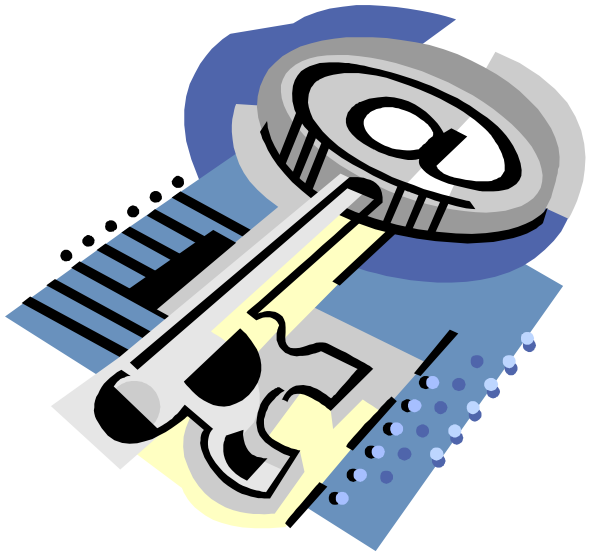
Costes de la Seguridad

Entonces ¿Cuánto se suele gastar en seguridad?



Agenda

Tecnologías



¿Qué tecnologías existen y cuál es su estado actual?

Desde el punto de vista empresarial existen dos posibles enfoques para clasificar los sistemas de seguridad:

1. Según coste:

1. Software libre: Linux, Snort, Nessus, Ethereal, etc.

   Suele ser difícil implantar este tipo de sistemas salvo que haya verdaderos problemas presupuestarios.

2. Sistemas propietarios: Microsoft, Sun, IBM, Symantec, ISS, Checkpoint, Trend, etc.

   Gran calidad debida a la competencia

Tecnologías

¿Qué tecnologías existen y cuál es su estado actual?

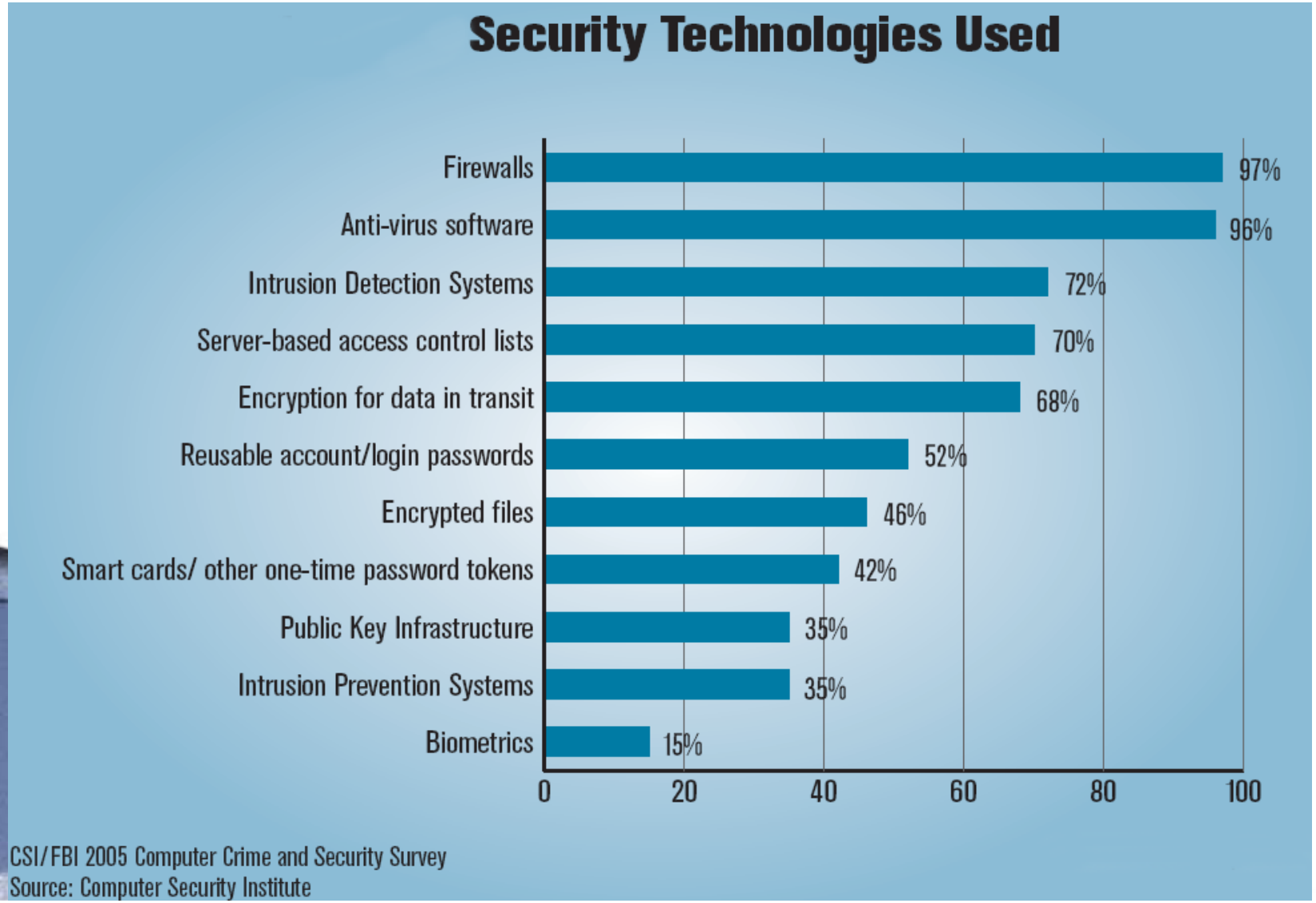
Desde el punto de vista empresarial existen dos posibles enfoques para clasificar los sistemas de seguridad:

2. Desde el punto de vista de su utilidad:

1. “Keep the good guys in”: VPN, PKI, RAS, Radius, Tacacs+, Single Sing On, etc.
2. “Keep the bad guys out”: AntiVirus, FW, IPS, IDS, ADS, etc.

Tecnologías

¿Qué grado de implantación tiene cada una?



Tecnologías

¿ Cuáles son las tendencias actuales ?

Firewalls

Todas las compañías montan sistemas de filtrado de paquetes, bien mediante FireWalls, bien mediante listas de control de acceso en routers.

Existen FW personales cuya utilidad suele cuestionarse (a favor de los IPS personales)

Antivirus

Se montan siempre a dos niveles: a nivel de red (para filtrar correo electrónico principalmente) y a nivel de puesto de trabajo.

Tecnologías

¿ Cuáles son las tendencias actuales ?

IDS

Los sistemas de detección de intrusos han estado ayudando a detectar problemas en las redes durante años pero su incapacidad de detener los ataques que ellos mismos detectaban y la gran cantidad de alarmas que generaban (imposibles de perseguir) han dado paso a los IPSs

IPS

Están en pleno auge. Son capaces de detectar y detener tanto ataques conocidos como desconocidos, detectar y detener virus, troyanos, aislar hackers cuando se les detecta y hasta proteger a los otros elementos de seguridad de la red, por ejemplo a los Firewalls.

ADS

Sistemas de detección de anomalias. Son totalmente novedosos y aún es pronto para hablar de sus resultados reales.

Tecnologías

¿ Cuáles son las tendencias actuales ?

Single Sign-on

Han sido, son y seguirán siendo de gran utilidad, máxime en las grandes empresas donde la gran variedad de sistemas y claves a memorizar convierten los post-it junto a los monitores en algo común.

Control de acceso a red

Microsoft y Cisco están en plena pugna por “llevarse el gato al agua” en lo que a control de acceso a red se refiere y aunque recientemente anunciaron su intención de colaborar, lo cierto es que cada uno sigue por su lado, NAP, NAC... el tiempo dirá...

Tecnologías

¿ Cuáles son las tendencias actuales ?

VPN + PKI

Durante años el binomio VPN + PKI han dominado el mundo de los accesos remotos seguros pero la necesidad de instalar un cliente de VPN en el PC los ha hecho incómodos. Están dejando paso a marchas forzadas a las VPN + SSL.

VPN + SSL

Sin más complejidad para el cliente que conectarse a una página web segura de la compañía para poder entrar en ella vía VPN. Sencillas, cómodas y ligeras. Existen ya sistemas basados en appliances de red.

¡ GRACIAS !

Ruegos y preguntas