

Seguridad Gerenciada

Monitoreo Perimetral

Ing. Pablo A. Masoero
pam@baicom.com
Presidente
BAICOM networks S.A.

13 de Septiembre de 2005

BAICOM
networks

La Seguridad Informática en el Mundo

- Durante los años noventa, la tecnología tuvo el salto mas grande, y fue el período en el cual las empresas mas invirtieron en tecnología
- El concepto de seguridad informática no estaba instalado
- Las empresas fueron volcando sus procesos de core sobre distintas tecnologías
- Pasando la segunda mitad de los años noventa se comenzaron a descubrir vulnerabilidades sobre los sistemas instalados ...

En Argentina...

- La recesión y la debacle del 2001 hizo que entre 1998 y el 2003 no se invirtiera en Seguridad Informática
- Esto produjo una brecha que expuso demasiado los procesos de cada negocio

Situación Actual

El 52 % de las empresas reconocen haber sufrido interrupciones inesperadas o no programadas de sus sistemas críticos de negocio.

- Se producen aproximadamente 200 incidentes diarios de gravedad en el mundo
- El 90% de las empresas del mundo son víctimas de ataques informáticos contra sus redes
- El 70% de los ataques provienen desde Internet
- Se detectaron 1220 nuevas vulnerabilidades en lo que va del año
- Aparece el concepto de “Managed Security”
- Aparecen los SSP (Security Service Provider)

“En 2004 los ataques provocaron pérdidas de entre 40.000 y 50.000 M de dólares”

Evolución de incidentes publicados

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

Total incidents reported (1988-2003): **319,992**

Fuente: CERT

Evolución de vulnerabilidades

1995-1999

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

2000-2005

Year	2000	2001	2002	2003	2004	1Q-2Q,2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	2,874

Total vulnerabilities reported (1995-2Q,2005): **19,600**

Fuente: CERT

Seguridad

Hoy en día, las empresas recurren a dos modelos para protegerse:

- ✓ Seguridad Interna: provista por personal propio
- ✓ Seguridad Gerenciada: provistas por terceros

Seguridad Interna

Desventajas que presenta la Seguridad In - House

- ✓ Necesidad de personal cada vez más capacitado y/o certificado
- ✓ IDS/IPS quien controla/maneja los logs?
- ✓ Tienen tiempo para todo?

Seguridad Gerenciada

Ventajas de tercerizar la Seguridad

- ✓ Expertise en diversas áreas
- ✓ Auditorías periódicas (de Código, Perimetrales, Internas)
- ✓ Penetration Tests
- ✓ Servicios
- ✓ NDA - Confidencialidad

Monitoreo Perimetral

- ✓ Se refiere a controlar los activos que se encuentran expuestos a ser objetivos de ataques malintencionados desde una red pública
- ✓ Complementa otros sistemas de seguridad
- ✓ Detecta posibles ataques
- ✓ Protege servidores y estaciones de trabajo

IDS basados en red (NIDS)

Monitorean el tráfico de red que afecta a múltiples hosts.

Ventajas:

- ✓ Un IDS bien localizado puede monitorear una red grande
- ✓ Tiene un impacto pequeño en la red

Inconvenientes:

- ✓ Problemas en redes con tráfico elevado (soluciones hardware)
- ✓ No analizan información encriptada
- ✓ No saben si el ataque ha tenido éxito o no
- ✓ Problemas con paquetes fragmentados

IDS basados en host (HIDS)

Operan sobre los logs del sistema.

Ventajas:

- ✓ Detectan ataques que no pueden ser vistos por un NIDS
- ✓ Pueden operar en entornos con tráfico encriptado

Inconvenientes:

- ✓ Más costosos de administrar que los NIDS
- ✓ Puede ser deshabilitado si el ataque logra tener éxito (penetración o DoS)
- ✓ No son adecuados para detectar ataques en toda una red
- ✓ Disminuyen el rendimiento del sistema monitoreado

Tipos de Análisis

Detección de abusos o firmas

Buscan eventos que coincidan con un patrón predefinido o firma que describe un ataque conocido.

Ventajas:

- ✓ Son efectivos sin generar muchas falsas alarmas
- ✓ Diagnostica rápidamente el uso de un ataque específico

Inconvenientes:

- ✓ Deben de ser actualizados continuamente
- ✓ Firmas ajustadas les privan de detectar variantes comunes

Tipo de Análisis

Detección de anomalías

Se centra en identificar comportamientos inusuales en un host en una red.

Ventajas:

- ✓ Capacidad de detectar ataques para los cuales no tiene conocimiento específico
- ✓ La información que producen puede ser utilizada para definir firmas en la detección de abusos

Inconvenientes:

- ✓ Gran número de falsas alarmas
- ✓ Requieren conjuntos de entrenamiento muy grandes

Tipo de Respuesta

Activa:

- ✓ Al detectar un ataque se toman acciones de forma automática:
- ✓ Recogida de información adicional.
- ✓ Cambio del entorno

Pasiva:

- ✓ El IDS avisa al analista, al administrador del sistema atacado

Consultas y Preguntas

Ing. Pablo A. Masoero

pam@baicom.com

Muchas Gracias