Empresa Asociada: **Mambo Technology**
Usuario/Cliente: Grupo Marsans
Fecha de Publicación: Abril de 2009

GRUPO MARSANS: VIAJANDO POR EL UNIVERSO DE LA PREVENCIÓN DE INTRUSIONES.

INTRODUCCION

GRUPO MARSANS está en mejora continua de sus Sistemas de Información y su Seguridad. Alineado con esta política decidió el año pasado abordar un proyecto de implantación de Sistemas de Prevención de Intrusiones. A lo largo del 2008 se evaluaron varios fabricantes. Los mejores resultados los proporcionó la tecnología de TippingPoint así que se optó por su definitiva implantación en la red de 800 oficinas de Marsans..

PRINCIPALES SOCIOS TECNOLÓGICOS

-TippingPoint se crea en 2001 con el propósito de fabricar un dispositivo que diera respuesta a los requerimientos descritos: Implantar un dispositivo en línea y en modo bloqueo que clasifica el tráfico y aplica políticas en tiempo real, basándose en una inspección exhaustiva, a nivel de aplicación. Y bloquear ataques conocidos y de día cero, sin intervención humana, sin falsos positivos y sin latencia.
En esos años las soluciones de IDS (Intrusion Detection System) estaban ampliamente extendidas. Los fabricantes de dichas soluciones aún siguen disuadiendo de instalar en línea ya que sus soluciones no estaban y aún no están preparadas para comportarse como IPS. Hoy en día la pregunta no es ¿IDS o IPS? a no ser que se dispongan de presupuestos ingentes para contratar personal cualificado para explotar plataformas de IDS que requerirán acciones correctivas por parte del administrador. La Prevención de Intrusiones permite automatizar el proceso. El 100% de la base instalada de TippingPoint, unos 3.400 clientes con 10,000 IPS, están en línea en modo bloqueo con al menos 1,400 filtros del "modo recomendado".

-Mambo Technology
Mambo Technology, compañía encuadrada dentro del Grupo Distrilogie, es mayorista de seguridad informática especializado en la selección e introducción en el mercado español de soluciones punteras en el sector TI. Desde el año de su creación en 2003, el equipo de Mambo Technology busca y selecciona en mercados internacionales los productos de su catálogo, tomando en cuenta la innovación tecnológica, las pruebas de rendimiento, los informes de consultoras, las valoraciones de la prensa especializada, el ROI, el capital invertido, la experiencia en mercados similares, las referencias en cuanto a implantaciones y el perfil de todos los profesionales que participan a la eclosión de estas nuevas tecnologías.
A finales de 2008, la compañía se integró dentro de Grupo DCC, a través de Distrilogie Group.

PROBLEMÁTICA A RESOLVER

Vivimos en una era en la que asistimos a una creciente diversidad de medios de acceso a la red, número de dispositivos conectados a la red, aplicaciones IP, número de nuevas vulnerabilidades, número de ataques y atacantes, tipo y sofisticación de los ataques. Por el contrario disminuyen: los recursos de IT para hacer frente a los mismos, así como el tiempo para parchear nuestros sistemas. GRUPO MARSANS deseaba tener un mayor control sobre los intentos de ataque recibidos desde Internet. Además, buscaba una solución que le permitiera controlar de forma adecuada posibles amenazas provenientes de las redes a las que se encuentra interconectado.

DETALLE DE LA SOLUCION:

Un IPS (Intrusion Prevention System) es un dispositivo en línea y en modo bloqueo que clasifica el tráfico y aplica políticas en tiempo real, basándose en una inspección exhaustiva, a nivel de aplicación. El IPS bloquea ataques conocidos y de día cero, sin intervención humana, sin falsos positivos y sin latencia. Estos requerimientos son los que hacen que muchas tecnologías de IPS se mantengan fuera de línea. ¿Por qué?
- Para bloquear en tiempo real el IPS debe ir en línea, lo que requiere un diseño específico para evitar caídas de la red. Los días en los que los IPS se desplegaban en el perímetro de la WAN con unos pocos filtros basados en firmas en modo bloqueo, han pasado.
La naturaleza de los ataques actuales requiere que los IPS se desplieguen en los puntos críticos de la red interna, es decir a velocidades multigigabit y con latencias inapreciables para no afectar al correcto funcionamiento de dispositivos y aplicaciones.
- Para proteger su red frente al creciente número de amenazas el IPS debe ofrecer una amplia y profunda cobertura, es decir, debe proteger frente a : gusanos, virus, Troyanos, ataques de denegación de servicio, aplicaciones P2P, Spyware, Phising, cross site scripting, SQL injections, PHP file include, ataques a la VoIP entre otros. No basta con cubrir unos pocos y bien conocidos ataques con firmas básicas, sino que se deben cubrir las vulnerabilidades de los sistemas operativos y aplicaciones de forma regular y a tiempo, lo que requiere un equipo de profesionales dedicados y del máximo nivel.

- El filtrado de flujos multigigabit exige que la precisión se trate con prioridad absoluta. De no ser así el administrador de la red se vería abrumado con infinidad de alertas, muchas de las cuales serían falsos positivos, con la consecuente Interrupción del servicio

CONCLUSIONES

-Prevención en tiempo real de amenazas internas y externas.
-Capacidad de respuesta ante los riesgos de seguridad.
-Incremento de la capacidad de respuesta ante posibles intrusiones.
-Minimización de los riesgos de seguridad en todos los sistemas y redes del cliente.

DECLARACIONES DEL CIO /Resp. TIC

En un mundo actual donde aumentan cada vez más los ataques a redes, las amenazas de seguridad son la principal preocupación de los Departamentos de IT", dijo Jaime Rodado, Rble de Informática de Marsans "Tipping Point permite que la seguridad de red sea real y más sencilla para nosotros"

Acerca de...

Mambo Techology (www.mambonet.com):

MAMBO TECHNOLOGY, compañia de Distrilogie Group, es un mayorista de seguridad informática y comunicaciones, está especializado en la selección y oferta de NUEVAS SOLUCIONES como alternativa a los productos ya existentes en el mercado. Mambo Technology busca y selecciona en mercados internacionales los productos de su catálogo, sometiendo previamente los mismos a rigurosos controles de calidad..

La Asociación @asLAN. www.aslan.es

@asLAN, la Asociación de proveedores de sistemas de red, internet y telecomunicaciones, desde su constitución en el año 1989 ha tenido como misión la promoción y difusión de las tecnologías de redes y telecomunicaciones en España en el ámbito empresarial. Actualmente la Asociación @asLAN, agrupa más de 100 empresas, entre las que se encuentran los principales fabricantes de red, integradores, distribuidores y operadores de telecomunicaciones. @asLAN organiza y colabora en iniciativas dirigidas al desarrollo del Sector TIC y difusión de nuevas tecnologías en diversos sectores: Industria, AAPP, Banca, Educación, etc...Entre sus principales actividades se encuentra la organización de SITI/@asLAN, el evento profesional y especializado en Soluciones Tecnológicas para la Administración Pública, Gran Cuenta y Pyme.