Comprender la Defensa en profundidad

Publicado: Junio 11, 2008

Revisión por Ing. Miguel Morales

Comprender los negocios riesgosos

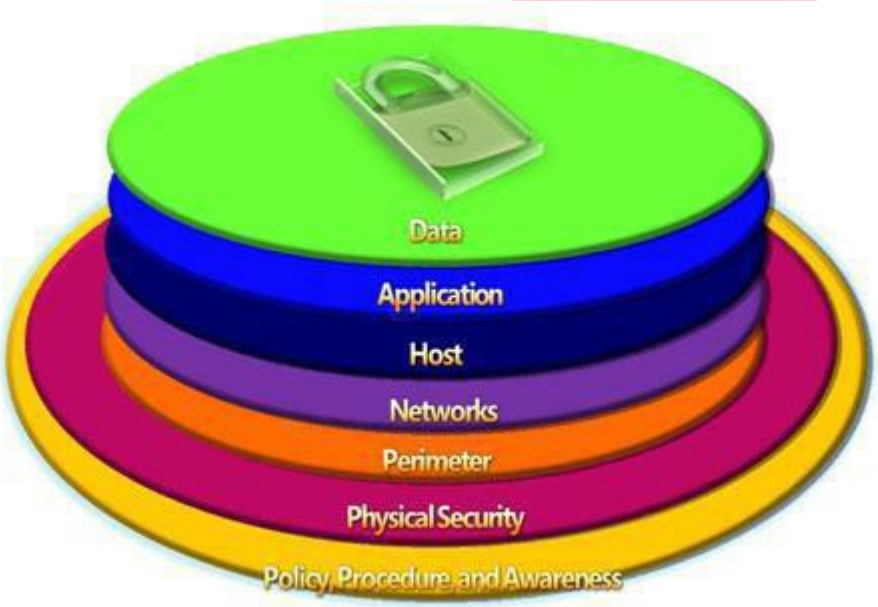
Paso gran parte del tiempo volando alrededor del mundo y conversando con empresarios y profesionales de TI acerca de la seguridad de la información. Jamás dejo de asombrarme cuando escucho que algunos "expertos en seguridad", que cobran más de lo que deberían, pasan horas detallando cuán compleja es la seguridad. No lo es. La seguridad puede resumirse en dos palabras simples: **Gestión de riesgos**.

No se trata de la eliminación de riesgos, se trata de la mitigación de riesgos.

Antes de que saltemos con un montón de jerga de seguridad, deseo que piensen realmente acerca de este concepto.

Si no comprenden el riesgo, no comprenderán lo que es la seguridad y si no comprenden lo que es la seguridad, entonces el concepto de Defensa de profundidad no tendrá sentido para ustedes. El riesgo es la idea global.

Existen muchas metodologías para evaluar el riesgo. En materia de seguridad es demasiado pedir que se comprendan cosas como la valorización de activos, la expectativa de pérdida anual, el retorno de la inversión, etc. pero realmente debemos comprender los riesgos antes de avanzar.



Capa 1: Políticas, Procedimientos y Conciencia (perro que ladra no muerde)

Mientras tenemos en cuenta el modelo del Gráfico 1, me gustaría que piensen acerca de la importancia de la Defensa en profundidad.

Todos recordamos la maravillosa trilogía del Señor de los anillos, cuando los chicos malos atacaban el castillo. Los defensores pudieron utilizar un modelo de defensa en profundidad para mantener alejados a los atacantes.

Los atacantes irrumpían a través de una pared y los defensores se aislaban detrás de otra. ¡Aquí pasa lo mismo! La primera y mejor inversión que pueden hacer es alrededor de la Capa 1: Políticas, Procedimientos y Conciencia.

Hablo de establecer algunas políticas y prácticas escritas de seguridad, como una Política de uso aceptable de una compañía. Aun más importante, se trata en realidad de poner en práctica las políticas que desarrollan.

Los usuarios se dan cuenta rápidamente si en materia de políticas ustedes son perro que ladra no muerde. Obtengan soporte ejecutivo para su política y esto les ayudará con cualquier problema de cumplimiento. Si tienen políticas que no están siendo implementadas...deséchenlas. No valen ni el papel en el que están impresas.

Una de las mayores amortizaciones (también conocido como Retorno de la inversión para nuestros amigos de negocios) en el mundo de la seguridad informática es una fuerte campaña creativa de conciencia.

Los usuarios olvidan pronto las lecciones aprendidas durante la "capacitación anual en seguridad"," por lo que la campaña debe ser algo que realmente recuerden. Concursos, pruebas, premios, boletines de noticias, videos divertidos: estas son algunas de las cosas que pueden hacer si tienen un presupuesto ajustado.

¿Los contadores obsesivos los dejaron sin un centavo?
¿Han visto los materiales de Conciencia de la seguridad de Microsoft que pueden obtener en forma gratuita?

Capa 2: Seguridad física (Puertas, guardias y armas)

Seguridad física. Es una capa que nosotros, las personas de TI, solemos pasar por alto. Realmente no tenemos palabras cálidas de bienvenida para cosas como vigilancia por video IP y candados magnéticos y doble puerta de seguridad o "man traps" (es una palabra real…búsquenla en el diccionario).

Sin embargo, esto no hace que esta capa sea menos importante. Todo aquello como PKI, IPSec, tecnologías de autenticación de factores múltiples no significan nada si yo puedo tomar su controlador de dominio y ponerlo en mi camión.

¿Cuántas veces han robado una computadora portátil en sus empresas? ¿Sabían que todos los años, en la convención del gran hacker en Las Vegas, DEFCON, el concurso de cerraduras de seguridad es uno de los más conocidos? ¿Por qué?

Como la seguridad física y la tecnología comienzan a estar más integradas, es importante comprender cómo trabaja cada una.

Este debate de "convergencia" está muy de moda. Los muchachos de seguridad física ejecutan la vigilancia por video IP y estos bits ahora se atraviesan en la red. Lo mismo pasa con los registros de acceso a edificios que se almacenan en sus servidores.

El concepto de seguridad física es uno que debemos concientizar más en nuestros roles. Pasen algún tiempo hablando con las personas que trabajan en esta área. Busquen una oficina local de American Society for Industrial Security (ASIS) y vayan a una reunión.

En ningún otro lugar encontrarán más experiencia sobre este tema que en este lugar. Beneficio: Microsoft y ASIS firmaron recientemente un acuerdo de sociedad ya que sabemos lo importante que es para ustedes tener una buena comprensión de la seguridad física.

Capa 3: Seguridad del perímetro (vivir al límite)

No voy a entrar en la presentación de ventas de Microsoft acerca de la belleza de las tecnologías como Intelligent Application Gateway (IAG) 2007 e Internet Security and Acceleration Server 2006. Ya saben cómo funcionan y son críticas en la protección del perímetro.

Quiero que piensen más allá por un momento y que consideren, ¿qué pasaría si simplemente nos sacamos de encima el perímetro completo? ¿Y si pudiéramos prescindir de cosas como VPN (que reduce la efectividad del firewall al abrir los puertos) y las conexiones RAS?

Esta idea está recibiendo mucho interés, especialmente de los grupos como Jericho Project. Observen con seriedad cómo Microsoft comienza a avanzar hacia esta nueva idea de Acceso a cualquier lugar.

Con la adopción de nuevas tecnologías como IPv6, donde podemos tener una dirección de IP simple por cada dispositivo en el mundo, habrá un día en el cual sus políticas corporativas serán implementadas sin importar en dónde se encuentre esa computadora portátil corporativa, ya que siempre estará conectada al dominio, no sólo cuando el usuario remoto necesite acceder al servidor del archivo.

¿Un mundo en donde los administradores de TI pueden controlar todos los activos corporativos siempre y cuando estén encendidos y conectados a Internet?

Es tan hermoso que se asoma una lágrima.

Capa 4: Seguridad de la red (proteger su casa)

Fue un gran día en el mundo de la seguridad informática el día que alguien conectó dos computadoras mediante un cable.

Por supuesto, aumentó la productividad pero también aumentaron los riesgos. Una forma de asegurar la red es restringiendo quién puede hablar con quién.

Una de las mejores maneras de hacer esto es utilizar una tecnología que ya mencioné indirectamente antes: Seguridad IP, más conocida como IPSec. IPSec es simplemente un mecanismo que permite al sistema operativo una seguridad mediante un canal cifrado. Básicamente, IPSec tiene dos modos:
Modo transporte, utilizado para conexiones de extremo a extremo y Modo túnel, utilizado para conexiones portal a portal. IPSec está incorporado a IPv6 y es opcional para IPv4. Al utilizar IPSec, podemos garantizar que sólo computadoras específicas, que utilicen la misma clave de cifrado, puedan conectarse entre sí.

También podemos garantizar que las computadoras que no tengan estas claves no puedan conectarse a equipos que cuenten con ellas. Esto nos permite aislar computadoras de miembros de dominio confiable de aquellos dispositivos no confiables a nivel de red.

También permite a los miembros de dominio confiable restringir el acceso de entrada a la red para un grupo específico de computadoras de miembro de dominio. Lo bueno de esto es que ya está disponible. ¿Lo están utilizando? ¿Por qué no?

Capa 5: Seguridad del host (Salven a la caja, salven a la red)

Estarían locos si no protegen los servidores que ejecutan las aplicaciones comerciales críticas. No voy a dar un sermón aquí. Sin embargo, permítanme contarles acerca de una cosita que me preocupa de esta área.

Es el concepto de seguridad virtualizada. Existe mucha presión hoy en día en cuanto al despliegue de algunas soluciones de virtualización en un esfuerzo por consolidar los servidores. Una idea genial.

No podemos pasar por alto la importancia y necesidad de asegurar los equipos virtuales (Virtual machines, VM) y los equipos host en los que se alojan. He oído una gran cantidad de conjeturas incorrectas como

"Si el host es seguro, VM es seguro" y otros cuentos de hadas similares. Con relación a la seguridad, deben tratar a estos equipos virtuales como servidores físicos, lo que significa ejecutar un antivirus dentro de VM.

Esto significa utilizar ACL para restringir los movimientos de quienes pueden modificar los archivos de configuración.
Esto significa estar concientes del panorama amenazante con respecto a la virtualización.

Capa 6: Seguridad de las aplicaciones (Si se construye…sólidamente, no vendrán)

En caso de que no se hayan enterado, cada vez es más difícil que los ataques sean exitosos frente a los sistemas operativos y software de uso comercial.

La cuestión es que las metodologías para desarrollar códigos seguros, como nuestro Ciclo de vida de desarrollo de seguridad (SDLC) valen la pena y cada vez más vendedores están comenzando a implementar está técnica u otras similares.

¿Qué harán los atacantes? Simple. Comienzan a apuntar a las aplicaciones internas personalizadas que fueron desarrolladas por su Equipo de desarrolladores con una seguridad como ocurrencia tardía, o peor, con una función de "nombre de usuario y contraseña" antes de la implementación de la nueva aplicación en toda la compañía.

Si su equipo de desarrolladores no implementa alguna clase de metodología de código seguro dentro de su empresa, no es cuestión de tener brechas, sino una cuestión de tiempo.

Capa 7: Seguridad de los datos (si su Terabyte cae en el medio de la jungla del Directorio activo…)

Estamos llegando al final de un viaje asombroso, pero este último paso probablemente sea el más crítico. Nuestra misión clave es la Protección de los datos. Entonces, ¿qué medidas están tomando para asegurar los datos?

Una de las cosas más fáciles que pueden hacer es implementar algún tipo de estrategia de cifrado para sus datos.

El uso de tecnologías como BitLocker para los controladores de dominios y viajeros es tan obvio que hasta dudo en mencionarlo...hasta que leí acerca de otra compañía más que sufrió una brecha de seguridad...y que no había cifrado. ¿Sabían que algunas leyes estatales acerca de las brechas de seguridad realmente limitan la exposición de sus compañías si cifraron los datos en forma adecuada?

Díganle esto al CEO y apuesto a que tiene algún tipo de pasión por el cifrado.

cifrado es simplemente demasiado fácil de implementar como para ignorarlo, dadas las diversas amenazas y ataques que existen; tiene sentido.

Conclusión

Defensa en profundidad es un modelo crucial para implementar seguridad de la información efectiva.

Más información de nuestra empresa:

Acerca de nosotros
Casos de éxito
10 razones para contratarnos
Partners certificados de Microsoft

Visítenos en: www.mmssa.co.cr