Seguridad Informática -- 10 + Medidas preventivas en un ambiente de TI.

Como administradores de redes, una de nuestras obligaciones es la seguridad, o al menos eso creen nuestros jefes. Si este es nuestro caso, lo mejor es permanecer cerca del mundillo underground, para mantener la forma.

1. No tendremos activos servicios innecesarios en nuestros sistemas. Cualquier día nos llevamos un disgusto por una brecha de seguridad en un servicio que jamás hemos utilizado, pero que teníamos activo.

2. Intentaremos que todos nuestros equipos dispongan de las últimas actualizaciones en seguridad. Si esto no es posible por motivos de presupuesto, será mejor que obtengamos por escrito la negativa por parte del responsable de dotación presupuestaria. No suelen negarse cuando les solicitas una respuesta escrita y les explicas las posibles consecuencias de no actualizar.

3. Otra de nuestras funciones será analizar cuidadosamente el diseño de red, ver las partes sensibles de esta, y realizar un informe por escrito, ofreciendo una solución preventiva, basada en conmutadores ethernet o firewalls departamentales con encriptación de tráfico, para minimizar el impacto de un posible ataque espía. Nuestra opinión podría no será tomada en consideración en ningún caso, pero podremos rescatar nuestro informe en el futuro, cuando suframos un ataque.

4. Debemos ser serios y hasta duros con nuestros usuarios, y obligarles, de forma automática preferiblemente, al cambio periódico de claves de acceso, y a que dichas claves no sean fáciles de adivinar. Sería lamentable que el usuario "presidente" usara la clave "presidente". Podemos estar seguros que a los primeros que señalarán cuando pase algo, será a nosotros, por no proteger las cuentas de los usuarios.

5. Nunca debemos acceder a nuestros sistemas usando sesiones no encriptadas, al menos si vamos a operar como administradores. Un buen sustituto de Telnet, rlogin y rsh es ssh. Existen clientes para Windows, y las versiones unix son libres y gratuitas.

6. Realizaremos u obligaremos a la realización de copias de seguridad, diariamente o semanales. El período solo depende del riesgo.

7. Evitaremos en lo posible las “relaciones de confianza” entre máquinas, especialmente si no las administramos todas nosotros.

8. Por ningún punto debemos conectar directamente nuestros recursos a Internet o a redes de terceros. Antes de hacerlo, lo primero será instalar un servicio cortafuegos separando nuestras redes interna y externa. Definiremos una política de restricción total, y abriremos paulatinamente a medida que se nos solicite por escrito, y esté correctamente aprobado.

9. No facilitaremos las claves de administrador a nadie que no deba utilizarlas. Si nuestro jefe no sabe administrar los equipos, es mejor no dárselas, pues las apuntará el algún papel.

10. Intentaremos violar la seguridad de nuestros propios sistemas periódicamente. Si en la red hay más de un administrador, es una práctica muy conveniente y provoca un "mayor grado de confianza".

11. Analizaremos o realizaremos herramientas que analicen nuestros ficheros de alarmas e históricos. Localizadas las cuentas mas sensibles y comprobaremos que solo acceden desde las direcciones habituales. Si aparece un acceso desde una posición extraña, hablaremos con el propietario de la cuenta para comprobar la autenticidad del acceso. Este tipo de comprobaciones conciencian a los usuarios de que en el departamento de informática nos tomamos muy en serio nuestro trabajo.

Este documento forma parte de nuestros programas de entrenamiento a manera de ayudarle a establecer un sistema de seguridad y control basado tanto en el soporte tecnológico, como en la <culturización> del recurso humano el cual es pieza clave o fundamental para el éxito de un programa de Seguridad en su Departamento de Tecnología de la información. Hace poco una nota en un medio de Internet decía: ... ""Hay una mentalidad global que tiene que ver con creer que los casos de brechas de seguridad y robo de información sólo suceden en la televisión", afirmó en entrevista el director de Investigación de la estadounidense, Bryan Sartin."" cnnexpansion.com Dic/16/2008. No vea este tópico como un costo, No lo vea como algo ajeno o lejano a sus bienes confidenciales que maneja en su sistema informático; Hoy el cibercriminal ya no es un tipo solitario aislado en algún cuarto en alguna parte del mundo, no Señor; Es crimen organizado cuyo blanco o target ES cualquier sistema conectado, esté donde esté geográficamente hablando.

Un término ahora usado comunmente en el ambiente de seguridad en tecnologías de la Información es: "Out in the wild"; es decir: "Afuera en la Jungla" refiriéndose al espacio global en el cual se mueve Su Información. Precisamente porque ahora es nuestra obligación extender nuestros esquemas de seguridad ya no solo a nuestro mundo real cada día mas inestable socialmente hablando sino a la comunidad mundial que es Internet, en la cual el delincuente puede ser cualquier tipo en cualquier parte del planeta tocando a su puerta .

Mil gracias por su visita!!

La Seguridad no es solo un proceso tecnológico.... es un proceso organizacional!

2da Calle, 2da etapa No. 37 Jardines del Valle, 504- 544-0334 504-9840-1996
www.econsultores.biz **** email: helpdesk@econsultores.biz