

Mistakes People Make that Lead to Security Breaches

Conductas erróneas que frecuentemente crean brechas de seguridad

Updated September 10, 2005

Actualizado al 10 de Septiembre de 2005

Traducción libre por Santiago Cavanna – 5 Enero de 2007

Fuente: <http://www.sans.org/resources/mistakes.php>

Technological holes account for a great number of the successful break-ins, but people do their share, as well. Here are the SANS Institute's lists of silly things people do that enable attackers to succeed.

Los agujeros o bugs en la tecnología explican una gran cantidad de ataques exitosos (realizados por hackers intencionados o por usuarios no intencionados), pero los mismos usuarios colaboran, también. Esta es una lista creada por SANS Institute de las cosas tontas que la gente hace y que facilita a los atacantes tener éxito.

The Five Worst Security Mistakes End Users Make

Los peores cinco errores de seguridad que cometen los usuarios.

1. Failing to install anti-virus, keep its signatures up to date, and apply it to all files.
 - Fallar en la instalación del antivirus, teniéndolo incorrectamente configurado, mantener sus actualizaciones de firmas actualizadas y escanear todos los archivos.
2. Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.
 - Abrir adjuntos de correos no solicitados sin previa verificación del origen o del contenido, o ejecutar juegos, protectores de pantallas u otras aplicaciones provenientes de fuentes no confiables.
 - Las fuentes no confiables incluyen conocidos que pueden estar cometiendo estos mismos errores
 - Las fuentes no confiables incluyen desarrolladores de software "freware" que podrían estar incluyendo dentro de sus creaciones, código malicioso o spyware.
 - Los adjuntos de correo no solicitado, pueden provenir de usuarios conocidos cuyos equipos estén comprometidos por un hacker o un virus.
 - La ejecución directa de un archivo desde el cliente de correo podría saltar la protección antivirus que se está ejecutando en tiempo real.
 - Presentaciones, video y hasta fotos, pueden estar infectadas por virus
3. Failing to install security patches-especially for Microsoft Office, Microsoft Internet Explorer, Firefox, and Netscape.

- Fallar u omitir actualizaciones de seguridad del Sistema Operativo, las herramientas de oficina y/o los navegadores y clientes de correo.

4. Not making and testing backups.

- No realizar o probar backups.

5. Being connected to more than one network such as wireless and a physical Ethernet or using a modem while connected through a local area network.

- Quedarse conectado a más de una red como Wireless o Red telefónica mientras esta conectado a la red corporativa.

The Seven Worst Security Mistakes Senior Executives Make

Los peores siete errores (respecto a seguridad de la información) que cometen la alta gerencia.

1. Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job.

- Asignar personas sin entrenamiento para mantener la seguridad y no proveerles el tiempo o los recursos para formarse y hacer correctamente su trabajo.

2. Failing to understand the relationship of information security to the business problem- they understand physical security but do not see the consequences of poor information security.

- Fallar en la comprensión de la relación entre su negocio y la seguridad de la información. Entender el problema de la seguridad física, pero no ver las consecuencias de una deficiente seguridad de la información

3. Failing to deal with the operational aspects of security: making a few fixes and then not allowing the follow through necessary to ensure the problems stay fixed

- Fallar en el tratamiento de los aspectos operativos de la seguridad: Realizar algunas correcciones y luego no permitir el correspondiente seguimiento y el resto de las tareas necesarias para mantener el problema corregido.

4. Relying primarily on a firewall.

- Descansar primaria o exclusivamente en la protección de perímetro.

5. Failing to realize how much money their information and organizational reputations are worth.

- Fallar en la estimación del valor o costo de la información o la reputación de la organización.

6. Authorizing reactive, short-term fixes so problems re-emerge rapidly.

- Únicamente autorizar soluciones reactivas, de corto plazo de forma que los problemas vuelven a ocurrir una y otra vez.

7. Pretending the problem will go away if they ignore it.
- Pretender que si el problema es ignorado o desestimado, desaparecerá.

The Ten Worst Security Mistakes Information Technology People Make

Los peores 10 errores de seguridad que cometen la gente de IT.

1. Connecting systems to the Internet before hardening them.
- Conectar los sistemas a Internet antes de Hacerles el Hardening correspondiente.
2. Connecting test systems to the Internet with default accounts/passwords
- Conectar los sistemas de testing a Internet con las credenciales de autenticación que traen configuradas de fabrica.
3. Failing to update systems when security holes are found.
- Fallar en la actualización de los sistemas cuando son informados de huecos en la seguridad del mismo.
4. Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI.
- Usar protocolos de comunicación sin encriptación para la administración de sistemas, Routers, Firewall o PKI.
5. Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
- Otorgar passwords a usuarios a traves de las líneas telefónicas o cambiar el password de un usuario a partir de una llamada telefónica aun cuando no es posible autenticar la solicitud.
6. Failing to maintain and test backups.
- Fallar en la realización o pruebas de Backups
7. Running unnecessary services, especially ftpd, telnetd, finger, rpc, mail, rservices
- Ejecutar servicios innecesarios en los sistemas, especialmente, ftpd, telnetd, finger, rpc, mail, rservices
8. Implementing firewalls with rules that don't stop malicious or dangerous traffic-incoming or outgoing.
- Implementar o configurar defectuosamente los Firewalls, en particular omitir aquellas reglas que permiten detener tráfico entrante o saliente malicioso o peligroso.
9. Failing to implement or update virus detection software

- Fallar en la implementación o actualización de software de detección de virus u otras amenazas.

10. Failing to educate users on what to look for and what to do when they see a potential security problem.

- Fallar en la educación de los usuarios en cuanto a que deben mirar o como deben reaccionar frente a un posible problema de seguridad.

And a bonus, number 11: Allowing untrained, uncertified people to take responsibility for securing important systems.

Bonus, Numero 11: permitir que gente no especializada o certificada tome la responsabilidad por la seguridad de sistemas críticos.

Santiago Cavanna
CISSP - SANS GSEC
Consultor en Seguridad de la Información
Information Security Consultant
Ciudad Autónoma de Buenos Aires - Argentina
www.santiagocavanna.com.ar
www.santiagocavanna.blogspot.com
www.issaarba.org