aprenderaprogramar.com

Seguridad informática: hacking a los hackers ¿y nuestros datos? (DV00102A)

Sección: Divulgación

Categoría: Tendencias en programación

Fecha última actualización: 2029

Autor: César Krall

Resumen: Este artículo explica en clave de humor aspectos claves de la seguridad informática. Resume y comenta una conferencia impartida por Chema Alonso (ingeniero experto en seguridad informática) en la Escuela de Ingeniería Informática de la Universidad de Sevilla.

LEYES PARA COMPRENDER LA SEGURIDAD INFORMÁTICA

1. Todo es mentira.
2. Las cosas funcionan de casualidad.
3. El mundo es un gran trapicheo.
4. En una empresa toda persona va ascendiendo hasta que llega a su máximo nivel de incompetencia (Principio de Dilbert).

¿QUÉ ES EL HACKING Y QUIÉNES SON LOS HACKERS?

Se llama hacker, que podríamos traducir por "saboteador" a una persona habilidosa con los ordenadores que trata de destruir las barreras de seguridad informática establecidas por empresas y organizaciones.

Un hacker puede tener distintos objetivos: robar datos, solo curiosear, hacer daño (por ejemplo borrando datos), enriquecerse, chantajear, demostrar su capacidad o simplemente hacerse el gracioso. Los hackers muchas veces dan muestra de un gran (y peculiar) sentido del humor. Los hackeos muchas veces parecen "de chiste". Los hackers se basan en herramientas conocidas y de fácil acceso (una muy usada es SQL-injection) en unos casos, y en complejos programas o algoritmos desarrollados tras mucho esfuerzo en otros. Algunos hackers son inofensivos y otros están en el mundo de la delincuencia. Aquí cabe clasificar a los desarrolladores de troyanos bancarios. Un troyano bancario es un programita que nos entra sin darnos cuenta a través de internet. Este programita va a estar pendiente para cuando realicemos una operación con una tarjeta bancaria o accedamos a nuestra cuenta bancaria vía internet, capturar los datos y enviárselos a los amigos de lo ajeno.

A nivel de usuario la mejor defensa o forma de tener seguridad es disponer de un buen antivirus, las copias de seguridad y no realizar descargas ni instalaciones indiscriminadas.

Un experto en seguridad informática puede ser consultado sobre si un sistema o una web pueden ser tan seguras como para llegar a ser no hackeables. La respuesta es que no se puede garantizar la seguridad absoluta de ningún sistema. Seguidamente podemos preguntar: ¿Debemos ser entonces pesimistas respecto a las posibilidades de securizar los sistemas, redes, webs, etc.? La respuesta técnica vamos a omitirla; la respuesta en clave de humor sería la siguiente: "Hombre, no te desanimes. Esto es como ligar, aunque no se consiga, hay que seguir intentándolo."

Si nos ponemos a escala, podemos pensar en una persona como usuaria de un ordenador, en una pequeña, mediana o gran empresa y en multinacionales. Las multinacionales dedican muchos esfuerzos a la seguridad. Aún así, la seguridad sigue siendo una utopía. Oracle es una multinacional que gestiona las bases de datos quizás más seguras del planeta. A día de hoy la última versión de la base de datos Oracle tiene contabilizados más de 150 fallos de seguridad.

©aprenderaprogramar.com, 2006-2029

LOS ATAQUES DE LOS HACKERS: ALGUNOS CASOS MÍTICOS

Debian GNU/Linux es una distribución libre del sistema operativo GNU/Linux. Es mantenida y actualizada gracias al trabajo de muchos usuarios expertos en informática que trabajan con algunos servidores principales. Hace un par de años el servidor principal de Debian fue atacado y "tumbado" (puesto fuera de servicio) por uno o varios hackers. Después del estudio correspondiente, se concluyó que el problema había estado en que el servidor estaba funcionando con un sistema Linux que no tenía mantenimiento, o al menos que no tenía el mantenimiento adecuado. Los administradores del servidor "no se percataron" de que habían salido distintas actualizaciones de seguridad hacía algunos meses y por supuesto no las habían instaurado sobre su sistema. Resultado: vulnerabilidad aprovechada por los amigos de la debilidad.

A la web del Ministerio de la Vivienda español, concebido con el loable propósito de fomentar el acceso de todos los españoles a la vivienda, tuvo acceso un hacker que dejó el siguiente mensaje como respuesta a los usuarios que trataban de acceder a la página web del ministerio: "No vas a tener casa en tu puta vida". ¿Tendría razón? Bueno, eso es cuestión aparte. En lo que a seguridad informática respecta, el fallo se demostró que había sido tener accesibles al público los directorios de administración de la página web.

Ataques de hackers han sufrido muchísimas comunidades e instituciones. Microsoft mismo ha sufrido ataques de hackers con éxito en algunos de sus sitios, siendo esto posible en general debido a fallos de mantenimiento. También han sufrido ataques de hackers famosos comunidades de Ubuntu (una distribución Linux), Oracle (multinacional americana) y cómo no, los famosos sistemas de correo electrónico universal hotmail y gmail entre otros.

Muchos ataques son evitables. Para empezar, es conveniente realizar testing y auditorías de seguridad de los sistemas informáticos y páginas web para detectar sus vulnerabilidades. En la práctica, son pocas empresas quienes mantienen estas prácticas.

¿SON HACKEADOS LOS HACKERS?

Zone-h.org es una web digamos que de hackers. Esta misma web ha sido también hackeada, lo que demuestra que no hay nadie libre de sufrir un ataque, ni siquiera los mismos atacantes.

LA SEGURIDAD DE LAS REDES SOCIALES

Otra pregunta podría ser: ¿Son seguras las redes sociales como Facebook o Tuenti? La respuesta en clave de humor sería la siguiente: "Vamos hombre, las redes sociales son un gran invento, ahora la cosa está más fácil para, digámoslo así, intimar cariñosamente con personas del sexo opuesto. ¡Si nuestros abuelos hubieran tenido estas herramientas!" Ya más seriamente, el problema no es que existan las redes sociales, sino que la gente se conciencie de que lo que escribe ahí es algo que tiene visibilidad para otras personas, es público. ¿Público? ¿No estamos protegidos? Obviamente no. ¿Quién tiene los datos? ¿Quién tiene un conocimiento profundo sobre las opciones de configuración de las redes

©aprenderaprogramar.com, 2006-2029

sociales y el funcionamiento de sus bases de datos? Pues digamos que nadie, lo cual hace muy difícil decir que los datos almacenados en esas páginas sean seguros.

De la relevancia de las redes sociales y de su accesibilidad para conocer qué hacen y piensan las personas da idea el hecho de que muchas empresas de recursos humanos, antes de decidir la entrevista o contratación de una persona, realizan rastreos exhaustivos en la red en busca de información sobre ella.

¿QUIÉN ES EL MALO DE LA PELÍCULA?

Si pensamos en *fallos de seguridad*, hemos de pensar en **responsables** de los *fallos de seguridad*. Pensemos un segundo… ¡Ya está! ¡Los informáticos! Si algo falla, está claro que son los informáticos, y si algo funciona está claro que es por casualidad. Podemos comprobarlo en las noticias de los periódicos. Suelen ser de este tipo: "Un error informático deja a miles de usuarios sin acceso al servicio nacional de salud", o "Un error informático provoca el caos en los aeropuertos", "Un error informático…", otro error informático, muchos errores informáticos. ¿Qué es lo que falla cuando falla la seguridad informática? Muchas veces lo que falla es que no hay dinero para seguridad. ¿Pero dónde se ha ido el dinero? ¿Se lo han llevado los políticos corruptos? Quizás sí, quizás no, pero lo que parece claro es que en las empresas e instituciones falta conciencia sobre lo importante que es la seguridad informática… hasta que se produce un fallo importante. De hecho, cuando una empresa se decide desde el principio a pagar por seguridad, ¿qué es lo que ve? Pues ve que no pasa nada, es decir, que las cosas funcionan mejor o peor. Y si las cosas funcionan, ¿para qué nos vamos a gastar un dinero en seguridad informática que nos podríamos ahorrar? Entonces tenemos planteado el dilema: si se gasta dinero en seguridad no pasa nada y nos preguntamos por qué gastarlo, y si no se gasta estamos en peligro ¿Qué hacer?

LA SEGURIDAD INFORMÁTICA EN ESPAÑA

Si hacemos un repaso general a la situación de la seguridad informática en España podremos llegar a conclusiones de este tipo:

a) No se invierte en seguridad informática.
b) Hay una ley nacional de acceso a la administración electrónica para facilitar que todas las gestiones que tienen que realizar los ciudadanos ante las administraciones se puedan hacer vía web. ¿Y si un hacker se da de alta a un hijo virtual para cobrar la ayuda de 2500 euros que se facilita por tener hijos? ¿Y si un hacker empadrona a todos los madrileños en Barcelona? ¿Será esto fácil o difícil?
c) Hay una ley de protección de datos que intenta evitar los fallos de seguridad, el uso de ficheros de datos con fines desleales como el bombardeo publicitario, el acceso de terceros a nuestros datos privados, etc. ¿Se cumple esta ley? Pues más bien no: misión imposible. Un caso curioso fue el de un trabajador de una administración pública que tenía en el disco duro de su ordenador datos de miles de usuarios. Instaló el emule en su ordenador y

©aprenderaprogramar.com, 2006-2029

¡voilá!, quedaron a disposición de todo aquel que quisiera recogerlos. Cometió el pequeño error de poner todos los contenidos de su disco duro "para compartir" con sus amigos.

d) La gente no tiene ni idea de seguridad informática, pero todo el mundo se considera un experto. ¿Cuántas veces hemos oído decir a alguien frases como "la seguridad de Windows es una mierda"? ¿Y qué conocimiento tendrá esa persona sobre el sistema operativo Windows? Esto es como el fútbol: todo el mundo opina sobre qué es lo que falla, pero nadie lo sabe realmente.

REFERENCIAS Y MÁS INFORMACIÓN

Este artículo resume y comenta la conferencia pública impartida por Chema Alonso, ingeniero experto en seguridad informática, en el marco de las "Jornadas Imaginática: La informática del futuro", que tuvieron lugar en la Escuela Técnica Superior de Informática de la Universidad de Sevilla (España) y a las que tuvimos la oportunidad de asistir.

Para más información algunas webs interesantes sobre seguridad informática son la web de Chema Alonso (elladodelmal.com), kriptopolis.org y enriquedans.com.

©aprenderaprogramar.com, 2006-2029