2011

Información en riesgo

.Seguridad

Defensa Digital I Número 10 I Mayo 2011 I
ISSN en trámite I REVISTA BIMESTRAL

EN ESTE NÚMERO

Editorial

Con la intención de mejorar, la Revista .Seguridad emprende una nueva etapa, en la que te ofrecemos un contenido versátil y diverso. Ahora, podrás encontrar varios temas actuales de seguridad informática, el objetivo es brindarte información de primera línea y hacer una lectura enriquecedora.

En esta ocasión, presentamos los temas: Ingeniería social, Cifrado web, El caso de Aaron Barr y el grupo hacktivista Anonymous, Sistemas de intrusión, La ley mexicana de Protección de la Información y nuestra acostumbrada sección de consejos sobre medidas preventivas para respaldar la información.

¡Bienvenido! Esperamos que esta edición renovada sea de tu agrado.

Galvy Ilvey Cruz Valencia
Subdirección de Seguridad de la Información

Aaron Barr y el caso Anonymous: Por qué es crucial cuidar nuestra información, y cómo lograrlo

Por Sergio A. Becerril*

La información, como nos estresan repetidamente los expertos en seguridad, es el recurso más valioso que poseemos. Personalmente o representando a una organización, nuestros datos son lo más importante, la razón de ser de la seguridad informática.

Como en otros temas de seguridad, por supuesto, esto se dice mucho más de lo que se practica. Después de todo, si estamos cubiertos por medidas de seguridad a nuestro alrededor, nuestra responsabilidad personal se limita con decir "los sistemas se encargan". Y ciertamente, el área de tecnologías, informática, o seguridad, tiene una gran responsabilidad al respecto. Sin embargo, los usuarios también somos parte crucial del proceso. Si no guardamos buenas prácticas en el manejo de nuestra información, dejamos la puerta, o mejor dicho, muchas puertas abiertas a posibles fugas.

Y... *¿para qué querría alguien mi información?* La siguiente historia responde, de manera explícita y particularmente dolorosa para los involucrados, a esta pregunta.

Conociendo a los involucrados

Hace apenas 4 meses, Aaron Barr contaba con un currículum impresionante, y un futuro brillante. El entonces Director General (o CEO, en inglés) de HBGary Federal, una joven compañía de seguridad informática con un enfoque a servicios para el gobierno estadounidense, había entrado a este puesto hacía poco más de un año, con la reputación de ser un "jugador estrella" en el negocio de la seguridad.

Para Octubre de 2010, HBGary Federal contaba con importantes problemas financieros, aunque tenía en el horizonte una posible salvación: un contrato con un consorcio de instituciones legales y financieras de los Estados Unidos a quienes ofrecía "una solución completa de inteligencia". Este consorcio solicitó una muestra del trabajo de la compañía, como prueba preliminar – ayudaría a controlar al grupo de Wilikeaks.

Wikileaks se había ganado la preocupación y descontento de las principales organizaciones norteamericanas de manera definitiva por dedicarse a publicar documentos filtrados en cualquier medio, con el

---

* Profesionista informático, entusiasta de la computación en general y en particular de la seguridad en tecnologías de la información. Ha colaborado en múltiples proyectos de la Universidad Nacional Autónoma de México, impartido cursos de diversas áreas de la computación, y actualmente se encuentra trabajando en el área de Atención a Incidentes de Seguridad Informática del UNAM-CERT.

objetivo de preservar la libertad de información en su máxima expresión. El gobierno estadounidense, instituciones bancarias, y grupos conservadores lo acechaban; particularmente después de la publicación de documentos que detallaban actividades cuestionables (y en algunos casos, ilegales) del ejército de los E.U.

Barr y su equipo se pusieron a trabajar. Más de 100 diferentes estrategias fueron diseñadas por HBGary Federal y otro par de organizaciones de seguridad en conjunto, incluyendo la desacreditación de aquellos que apoyaban a Wikileaks. Al respecto, Barr se enfocó en uno de los principales y más potentes aliados de Wikileaks: Anonymous.

Imagen cortesía de Scott Beale/Laughing Squid

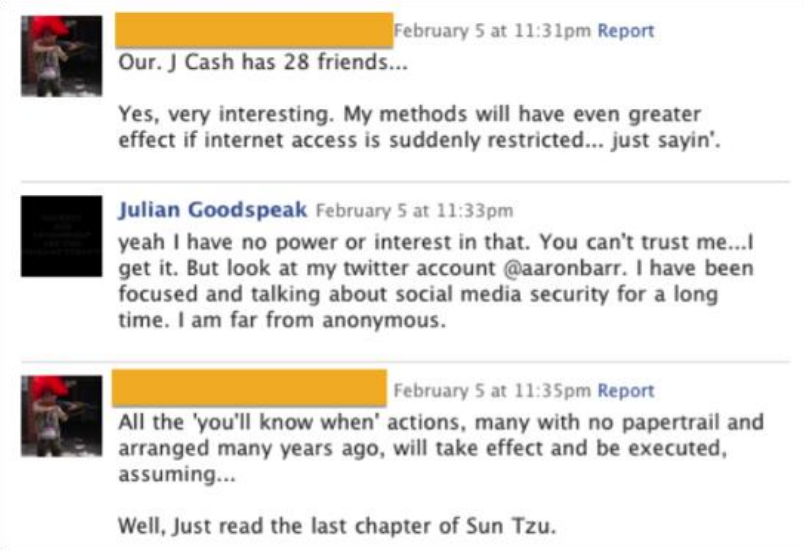
El grupo Anonymous es una mezcla heterogénea: sus miembros suponen un contingente de al menos varios cientos de activistas, intrusos informáticos, expertos en computación, y curiosos. Por años, han personificado la amenaza humana más importante en Internet, manifestándose en persona, protestando ante organizaciones como la Iglesia de la Cienciología, interrumpiendo actividades en sitios y servicios web (MasterCard, por ejemplo) y en general causando interferencia a quien se interponga con sus intereses, creencias y valores. Algunos sectores los consideran guardianes de valores intrínsecos a Internet; otros, meros criminales. De cualquier forma, sus integrantes se han mostrado increíblemente difíciles de rastrear. Anon (como ellos lo abrevian) no cuenta con un liderazgo definido, sus integrantes utilizan diversas técnicas para mantenerse encubiertos digitalmente: servidores proxy, cifrado de datos, etc.

Barr sabía esto, pero aún así determinó que era posible obtener suficiente información de miembros clave como para desmantelar al grupo. Su objetivo principal fueron las redes sociales: después de todo, aún los activistas más avocados a su causa utilizan Facebook, ¿cierto? Barr teorizó que la información divulgada en redes sociales, en particular las uniones entre ciertas personas, podrían revelar quiénes se encontraban involucrados en movimientos de este estilo, así en enero de 2011, comenzó su investigación.

Resultados inesperados

No era la primera vez que Barr se encontraba con este tipo de recolección de información: meses atrás, había realizado algo similar para demostrar su capacidad de recolección de inteligencia a clientes potenciales y obtuvo resultados impresionantes. En esa ocasión, y después de casi un mes de investigación, Barr creía haber obtenido la identidad de los principales miembros de Anon. Tan seguro se encontraba de sus hallazgos, que decidió utilizarlos como base para una futura plática acerca de los riesgos de las redes sociales; además, reservó una cita con el FBI para discutir estos resultados, y decidió – como cortesía profesional – compartir la existencia de dicha información con quien había estimado e identificado en el chat, como una de las 3 principales personas en Anon, CommanderX.

A pesar de que Barr esperaba una reacción poco amigable ante esta revelación, la respuesta de Anon fue sorprendentemente rápida y furiosa. CommanderX puso en claro dos cosas: que Barr no tendría oportunidad de compartir esa información con nadie más, y que Anon entraría en acción rápidamente. Ese mismo día ejecutaron un ataque de DDoS (Distributed Denial of Service -ataque distribuido de denegación de servicio-, una forma común de deshabilitar servidores) contra la página web de HBGary Federal; a la par comenzaron de inmediato el reclutamiento de miembros para coordinar un ataque contra todos los blancos posibles relacionados con HGBary Federal.



Barr se descubre ante Anon (via Ars Technica)

Después de explotar vulnerabilidades en el sitio web de HBGary Federal, Anon obtuvo una lista de contraseñashasheadas*; con esto, y debido a que un par de usuarios - entre ellos, Aaron Barr - utilizaron contraseñas sencillas (letras minúsculas y números únicamente), obtuvieron accesos al

servidor web. Un par de pruebas confirmaron que existía un segundo servidor al que podrían acceder; sorprendentemente, las mismas contraseñas les permitieron ingresar a este equipo. Y es aquí donde encontraron la mina de oro.

Un **hash es una función de cifrado de un solo sentido; esto significa que es imposible obtener el original a partir del hash. Se utiliza ampliamente al almacenar contraseñas; sin embargo, puede vulnerarse mediante el uso **de tablas arcoíris**, que almacenan todas las posibles combinaciones de contraseñas y sus respectivos hashes.*

Cuando encontraron que Barr utilizaba la misma contraseña para estos dos servidores, supusieron que podría utilizarla también para otros servicios. Al probar la contraseña de Barr en Google Apps, obtuvieron también acceso al correo electrónico de todas las personas en la compañía – incluyendo Greg Hoglund, quien es un respetado experto en seguridad informática, su sitiohttp://rootkit.org es una importante fuente de información sobre software malicioso.

Utilizando el acceso a su correo, lograron obtener acceso a este sitio, aplicando un ataque de ingeniería social al administrador del mismo (utilizando el correo de Hoglund, fingiendo ser él). Con privilegios administrativos del mismo, lo deshabilitaron y sacaron fuera de línea.

Finalmente, Anon publicó el resto de los correos electrónicos de todos los empleados de HBGary.

Cómo protegerse

Los resultados son innegables: la pérdida de reputación de un experto en seguridad, la anulación de un posible contrato (que llevó directamente a la quiebra de HBGary Federal), la publicación de miles de correos confidenciales, e incluso la vulneración y deshabilitación del servidor de un tercero, apenas involucrado en la situación.

¿Cómo pudo evitarse este problema? Además de la obvia recomendación (no ataques a intrusos informáticos), unas cuantas simples medidas pudieron haber limitado tremendamente el alcance de este ataque:

- Utilizar contraseñas seguras.
- Evitar reutilizar contraseñas en diferentes servicios.
- Cifrar correos electrónicos.

Todas son recomendaciones usuales, y bastante sencillas. Este caso brinda una importante lección, la diferencia entre haber sufrido un simple ataque de denegación de servicio y ver todos los secretos corporativos regados por el Internet, la habría hecho seguir estas buenas prácticas.

Después de todo, los únicos que podemos perder, somos nosotros mismos.

El Cifrado Web (SSL/TLS)

Por Dante Odín Ramírez y Carmina Cecilia Espinosa Madrigal*

¿Qué es SSL/TLS?

SSL (Secure Sockets Layer) traducido al español significa Capa de Conexiones Seguras. Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet. Recientemente ha sido sustituido por TLS (Transport Layer Security) el cual está basado en SSL y son totalmente compatibles.

Te permite confiar información personal a sitios web, ya que tus datos se ocultan a través de métodos criptográficos mientras navegas en sitios seguros.

Es utilizado ampliamente en bancos, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas. No todos los sitios web usan SSL, por eso debes ser cuidadoso.

¿Cómo funciona?

Antes de entender cómo funciona esta tecnología, es necesario abordar algunos conceptos importantes y que forman parte del funcionamiento interno de SSL/TLS.

Cifrado, no Encriptado

El cifrado es el proceso que transforma tu información de manera que no cualquier usuario pueda entenderla, se realiza con base a un elemento único conocido como llave, así nadie, excepto el poseedor puede leerla. El procedimiento inverso al cifrado es el descifrado.

La palabra correcta para describir el proceso de ocultamiento de información es cifrado, usualmente encontrarás literatura con el término encriptado, el cual es incorrecto.

Llave pública y llave privada

Son un par de "llaves" digitales asociadas a una persona o entidad y generadas mediante métodos criptográficos. La llave pública es usada para cifrar la información, haciendo una analogía, es como la llave utilizada para cerrar una puerta y mantener fuera a cualquier persona

* **Dante Odín Ramírez.** Egresado de la Licenciatura en Informática de la Facultad de Contaduría y Administración. Actualmente labora como Operador de Bases de Datos en el Departamento de Seguridad en Sistemas de la Subdirección de Seguridad de la Información/UNAM-CERT. Recientemente ha implementando tecnologías de bloqueo de intrusos mediante firewall de aplicaciones opensource. **Carmina Cecilia Espinosa.** Ingeniera en Computación por la Facultad de Ingeniería, UNAM. Laboró en el Departamento de Seguridad en Sistemas de la Subdirección de Seguridad de la Información/UNAM-CERT como responsable de seguridad de base de datos. Posteriormente, se incorporó al Departamento de Auditoría y Nuevas Tecnologías, en la que se desempeña hasta la fecha como analista de vulnerabilidades. Actualmente, colabora en el análisis de riesgos de la misma subdirección.

mientras que la llave privada se usa para descifrar, es decir, la llave que abre la puerta y sólo la posee la persona autorizada, por lo tanto ésta debe mantenerse en secreto.

Firma digital

Del mismo modo que tu firma autógrafa, es un elemento que te identifica y distingue de las demás personas y que al firmar con ella adquieres derechos y obligaciones. La firma digital se genera con base a la llave privada de quien firma y por lo tanto es única.

Autoridad Certificadora (AC)

Una Autoridad Certificadora (AC, en inglés CA) es una entidad confiable que se encarga de garantizar que el poseedor de un certificado digital sea quien dice ser, bridando confianza a ambas partes de una comunicación segura SSL/TLS.

Certificado Digital SSL/TLS

Es un documento digital único que garantiza la vinculación entre una persona o entidad con su llave pública.

Contiene información de su propietario como nombre, dirección, correo electrónico, organización a la que pertenece y su llave pública, así como información propia del certificado por mencionar: periodo de validez, número de serie único, nombre de la AC que emitió, firma digital de la AC cifrada con su llave privada y otros datos más que indican cómo puede usarse ese certificado.

HTTPS

Simplemente es una combinación del protocolo HTTP (usado en cada transacción web) con el protocolo SSL/TLS usada para establecer comunicaciones cifradas en sitios web.

Funcionamiento

SSL/TLS es una tecnología compleja, pero una vez entendidos los conceptos anteriores comprenderás el funcionamiento de este protocolo de forma general. Usemos un ejemplo con el cual posiblemente estés familiarizado.

Supongamos que intentas acceder al sitio de Facebook de forma segura, es decir, usando “https” en la dirección web. Inmediatamente, aparecerá la página en pantalla y en alguna parte de tu navegador observarás un “candado”, dependiendo del navegador que uses (Imagen 1). Si no viste ningún mensaje de advertencia (generalmente en tonos rojos), el protocolo SSL/TLS ha hecho su trabajo.

Imagen 1. Uso de protocolo HTTPS

SSL/TLS funciona de forma transparente para ti, lo que en realidad ocurre cuando intentas acceder a un sitio seguro se asemeja al siguiente diagrama.

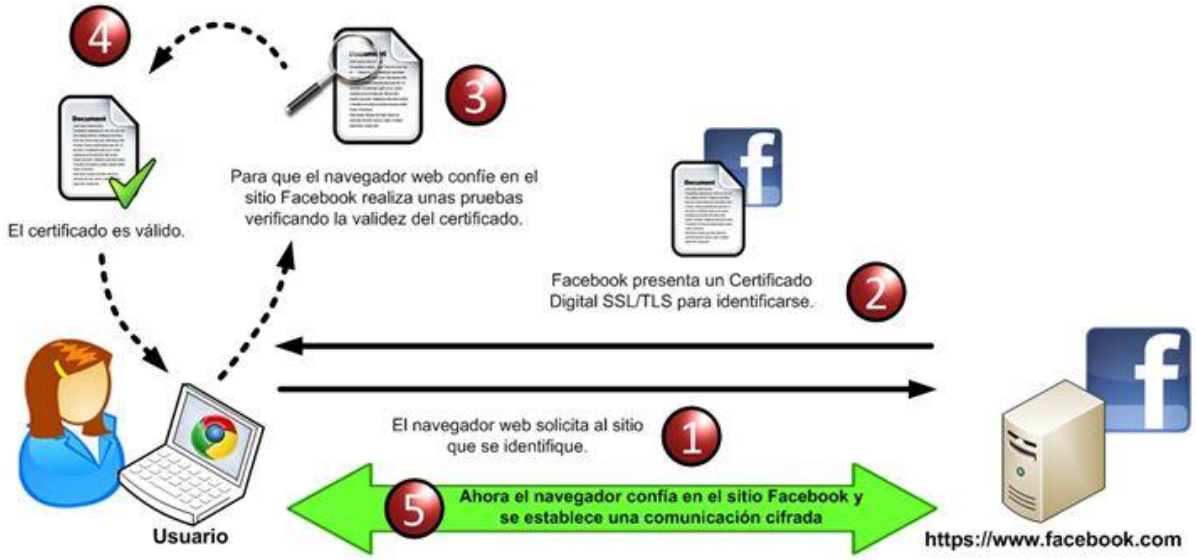


Diagrama 1. Funcionamiento general de SSL/TLS

Iniciando comunicación segura

En el punto dos del Diagrama 1, cuando el navegador hace una petición al sitio seguro de Facebook, éste envía un mensaje donde indica que quiere establecer una conexión segura y envía datos sobre la versión del protocolo SSL/TLS que soporta y otros parámetros necesarios para la conexión.

En base a esta información enviada por el navegador, el servidor web de Facebook responde con un mensaje informando que está de acuerdo en establecer la conexión segura con los datos de SSL/TLS proporcionados.

Una vez que ambos conocen los parámetros de conexión, el sitio de Facebook presenta su certificado digital al navegador web para identificarse como un sitio confiable.

Verificación de validez del certificado

Una vez que el navegador tiene el certificado del sitio web de Facebook, realiza algunas verificaciones antes de confiar en el sitio:

Integridad del certificado: Verifica que el certificado se encuentre íntegro, esto lo hace descifrando la firma digital incluida en él mediante la llave pública de la AC y comparándola con una firma del certificado generada en ese momento, si ambas son iguales entonces el certificado es válido.

Vigencia del certificado: Revisa el periodo de validez del certificado, es decir, la fecha de emisión y la fecha de expiración incluidos en él.

Verifica emisor del certificado: Hace uso de una lista de Certificados Raíz almacenados en tu computadora y que contienen las llaves públicas de las ACs conocidas y de confianza (Imagen 2). Puedes acceder a esta lista desde las opciones avanzadas de tu navegador web (en este caso usamos Google Chrome).

Con base a esta lista, el navegador revisa que la AC del certificado sea de confianza, de no serlo, el navegador mostrará una advertencia indicando que el certificado fue emitido por una entidad en la cual no confía.

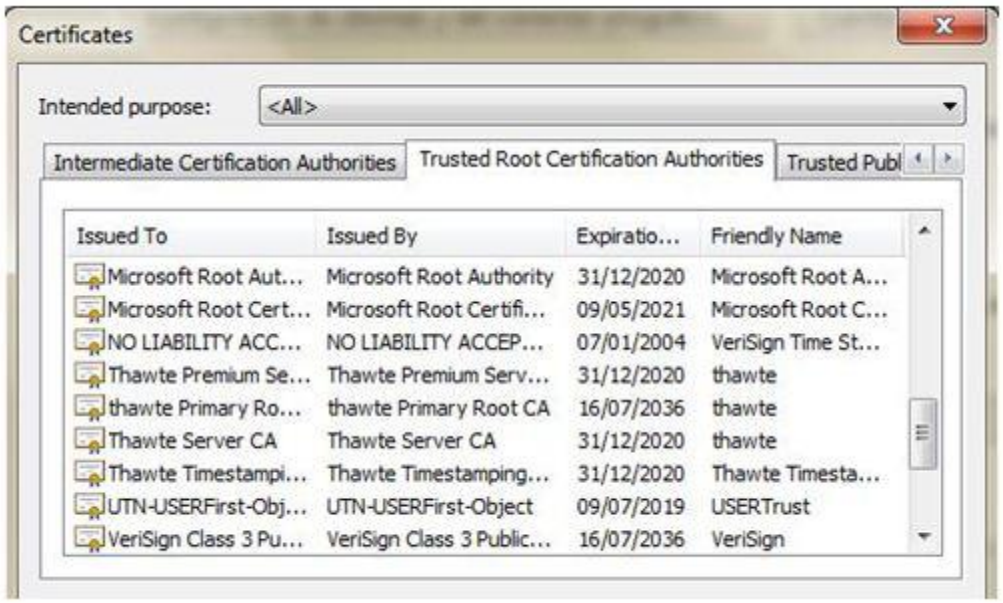


Imagen 2. Certificados raíz

Estableciendo la conexión segura

¡Listo!, una vez que el certificado cumplió con todas las pruebas del navegador, se establece la conexión segura al sitio de Facebook, lo cual se traduce en seguridad para tus valiosos datos personales.

Punto débil de la tecnología SSL/TLS

Es importante que estés consciente que pese acceder sólo a sitios seguros, la tecnología SSL/TLS no garantiza al 100% que tu información esté segura; considera que, como toda creación humana, tiene fallos. Los atacantes se han vuelto muy hábiles e ingeniosos para burlar estos mecanismos de seguridad.

Por ello, debes tomar algunas medidas preventivas antes de realizar transacciones en línea que puedan poner en riesgo tu información.

Caso real

Un caso real que ejemplifica el mal uso de esta tecnología fue publicado en el artículo *'Troyano bancario secuestra conexiones SSL', el cual puedes consultar en:*
http://www.seguridad.unam.mx/noticias/?noti=4419.
En este artículo se detalla un troyano (*Trojan.Tatanarg*) capaz de secuestrar

conexiones SSL/TLS al momento de realizar transacciones bancarias en línea. A grandes rasgos lo que hace este troyano es:

Supongamos que deseas realizar una operación bancaria en línea. Al ingresar a la página web de tu banco, durante el proceso de conexión SSL/TLS, el banco envía a tu navegador su certificado y su llave pública firmados, elementos que utilizará para cifrar la información a transmitir. El troyano se interpone entre el servidor del banco y tu navegador tomando la llave pública y la información del certificado para cifrar su propio canal de comunicación, mientras tanto, del lado del navegador el troyano inserta su certificado auto-firmado (certificado falso) de tal manera que el "*candadito de seguridad*" siempre está visible durante la conexión y así la presencia del troyano resulta imperceptible. (Imagen 3).

Cuando envías tu información al banco, ésta es cifrada utilizando el certificado falso e interceptada por el mismo troyano, quien la manipula y transfiere al banco para que éste la procese.

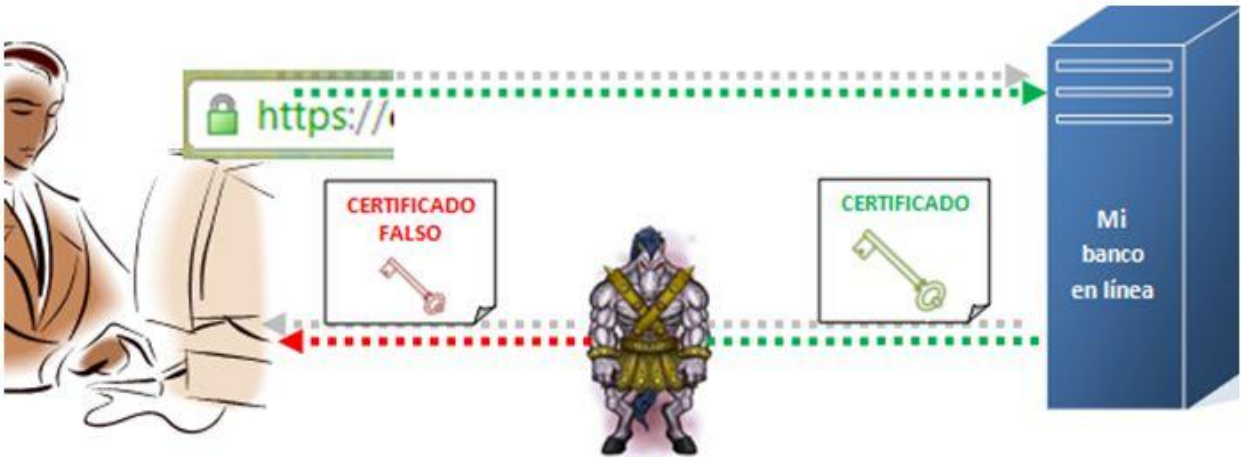


Imagen 3. Ataque de troyano "Trojan.Tatanarg"

Empleando el certificado falso, el troyano es capaz de descifrar y leer la información que compartas con el banco, posiblemente reenviándola a un atacante para que éste haga mal uso de ella, por ejemplo robando tu identidad.

Recomendaciones

- Evita hacer uso de computadoras y redes públicas, sobre todo si vas a utilizar el servicio de banca en línea, realizar cualquier tipo de compra o transferir información valiosa para ti.

- Instala un antivirus y procura mantenerlo actualizado. Al final de este artículo se listan algunas soluciones gratuitas que pueden ayudarte.

- Es importante mantener actualizado tu navegador, ya que si no lo haces, eres más susceptible a ataques. Consulta el sitio web oficial del navegador que elijas y obtén la versión más reciente.

- Cuando utilices HTTPS, verifica la vigencia del certificado, esto lo puedes hacer observando en el periodo de validez del mismo (Imagen 4).

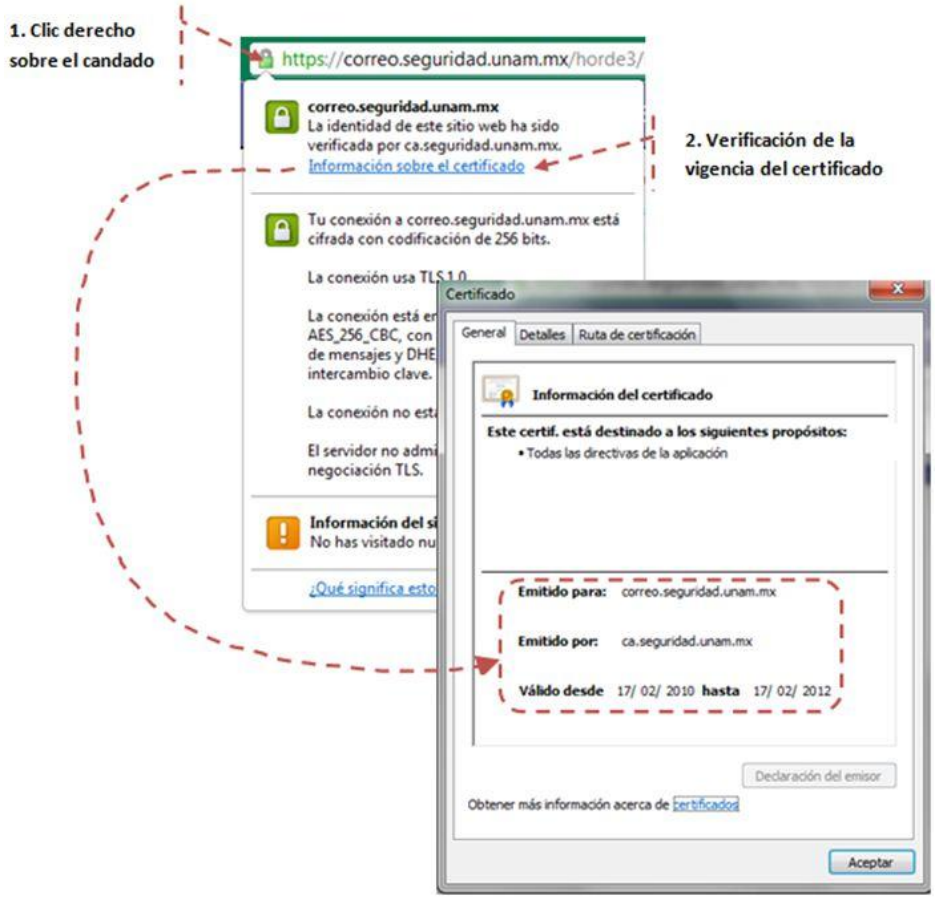


Imagen 4. Verificando vigencia del certificado

Soluciones antivirus:

- AVG free [http://www.freeavg.com]
- avast! Free [http://www.avast.com/es-ww/free-antivirus-download]
- Avira AntiVir Personal - Free Antivirus [http://www.avira.com/es/avira-free-antivirus]

Navegadores web:

- Mozilla Firefox [http://www.mozilla-europe.org/es]
- Internet Explorer [http://windows.microsoft.com/es-ES/internet-explorer/products/ie/home]
- Google Chrome [http://www.google.com/chrome]
- Safari [http://www.apple.com/es/safari]
- Opera [http://www.opera.com]

Referencias:

- http://www.symantec.com/connect/blogs/banking-proxy-trojantatanarg
- http://h71028.www7.hp.com/PublicSector/cache/107893-0-0-140-470.html
- http://curso-src.net/2_4.html
- http://es.wikipedia.org/wiki/Criptografía
- http://www.nxtgenug.net/Article.aspx?ArticleID=42
- http://hubpages.com/hub/SSL-For-Dummies-Understanding-What-it-all-Means
- http://blog.securism.com/2009/01/summarizing-pki-certificate-validation/

Evolución de los sistemas de detección, prevención y análisis de incidentes

Por Javier Ulises Santillán Arenas*

El desarrollo y el incremento de las redes de datos alrededor del mundo han impulsado la creación de mecanismos para compartir, transferir o distribuir información por medios digitales. La facilidad, eficiencia y conveniencia de utilizar medios electrónicos implica, hasta cierto punto, exponer dicha información a determinadas amenazas que existen en ese mundo digital.

Amenazas potenciales como virus, gusanos, ataques dirigidos, negación de servicio (DoS), escaneos, botnets, spam, etc., no son conceptos nuevos, durante los últimos años han ido evolucionando y adaptándose a los nuevos mecanismos de comunicación digital y en general al desarrollo de Internet. Tomando esto en cuenta, es entendible suponer la necesidad de poder identificar el origen de dichas amenazas con la finalidad de aplicar algún mecanismo de mitigación.

La importancia de poder identificar y detectar el tráfico malicioso se justifica en el hecho de que este tipo de tráfico es el que puede alterar el funcionamiento de una red o, en el peor de los casos, causar tal impacto que interrumpa por completo la actividad general del entorno.

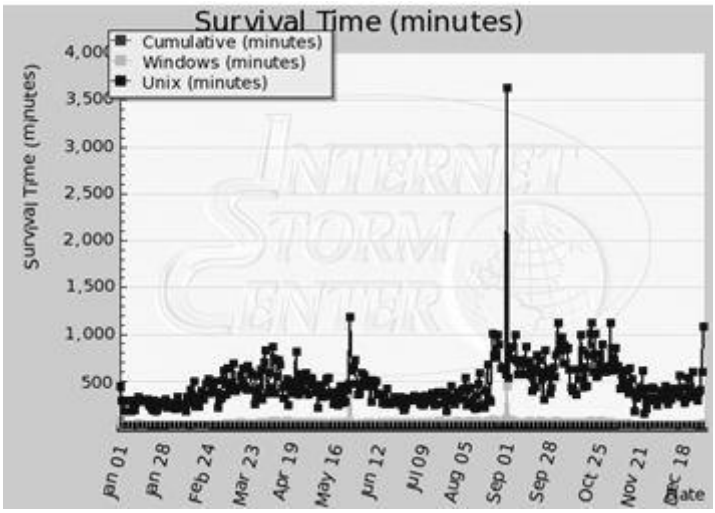
Por ejemplo, un usuario común que utiliza algún procesador de texto, crea presentaciones electrónicas, navega en Internet buscando noticias o algún artículo de interés, etc. de pronto ve interrumpida su tarea por alguna causa extraña. Su computadora despliega mensajes de error, cada minuto que pasa se complica navegar en Internet y controlar el equipo debido a la lentitud de respuesta hasta que finalmente, llega al extremo de un reinicio desesperado, cuya probabilidad de pérdida de información es alta.

El usuario está exasperado y asustado, no sabe qué pasa pero por alguna razón no puede continuar trabajando. Al reiniciar el equipo e intentar reanudar sus actividades, advierte que su información está incompleta y que la lentitud para trabajar es ahora recurrente. Lo primero que le viene

* Ingeniero en Computación por la Facultad de Ingeniería de la UNAM en el módulo terminal de Redes y Seguridad. Labora desde 2008 en la Subdirección de Seguridad de la Información/UNAM-CERT como líder del proyecto Honeynet-UNAM realizando diversas actividades enfocadas al desarrollo e investigación de tecnologías de detección, análisis y procesamiento de tráfico de red malicioso. Tiene la certificación GIAC Certified Intrusion Analysts (GCIA) y ha tomado cursos relacionados con análisis de tráfico de red en el SANS Institute.

a la mente: “es un virus, mi máquina está infectada”. Esto en parte demostraría la creencia de que todo lo malicioso que ocurre en una computadora se debe a “un virus”, sin embargo podría tratarse de algo mucho más complejo. Identificar la causa real del problema o algún indicio certero, puede no sólo corregir el problema, sino también evitarlo en el futuro.

Con el fin de atender esta tarea, el SANS Institute[1], a través del *Internet Storm Center* (ISC), cuenta con un cálculo denominado “Survival Time”[2], el cual consiste en medir el tiempo promedio que tarda un equipo de cómputo en ser atacado o alcanzado por algún tipo de malware en propagación, considerando que se expone a una red pública sin restricciones. En caso de que el equipo no contara con los parches adecuados, entonces esta medición significaría el tiempo en que el equipo sería infectado o vulnerado. En la siguiente figura se aprecia como las últimas mediciones indican que el “survival time” de un equipo Unix es de aproximadamente 3700 minutos, mientras que el de un equipo Windows es casi de 450 minutos. Esto nos da una muestra del verdadero problema con el tráfico de red malicioso.



SANS ISC-Survival time (enero 2005 - agosto de 2010)

¿Cómo saber si determinado tráfico es anormal? ó ¿cómo definir si el tráfico monitoreado es malicioso? Este tipo de cuestiones pueden responderse a través de distintos puntos de vista. Por un lado, se tiene la definición de políticas de una organización en las cuales se puede establecer lo que se considera como anormal y por otro el comportamiento general de determinadas amenazas que definen muy bien a un evento como un incidente de seguridad.

Algunos métodos para detectar "tráfico anormal" se basan en la comparación y análisis del comportamiento "esperado" de cierto tipo de protocolos de comunicación o aplicaciones. Es decir, si se tiene bien identificada la estructura, forma y comportamiento del tráfico según su naturaleza, entonces cualquier patrón fuera de ella representa un factor para poder identificarlo como anormal. Algunos mecanismos para poder lograr dicha identificación y detección son las técnicas basadas en análisis de patrones, las herramientas especializadas y el análisis de bitácoras.

IDS, alternativa pasiva para detección de tráfico malicioso

Los sistemas de detección de intrusos tienen en realidad sus orígenes en el concepto de auditorías. Desde los años 50's, cuando se realizaban diversos tipos de revisiones, se comenzaron a definir técnicas para identificar posibles anomalías. Fue en la década de los 80's, cuando surgieron los primeros sistemas para identificar y detectar en tiempo real posibles patrones en los sistemas de aquellos tiempos.

Actualmente, los sistemas de detección de intrusos (IDS) son dispositivos físicos o lógicos que permiten analizar el tráfico de red para identificar posibles paquetes maliciosos o anómalos. Son un mecanismo pasivo de detección, ya que su tarea fundamental es alertar pero no actuar.

Estos sistemas pueden proveer de información muy específica sobre la actividad detectada debido a que su análisis sobre los paquetes de red es más específico que el que realizado por otros mecanismos de seguridad, como los firewalls. Esto convierte a los IDS en herramientas muy poderosas para conocer el panorama de la actividad en la red.

El funcionamiento general de los IDS se basa en detectar tráfico malicioso mediante firmas o anomalías.

La detección por firmas consiste en la definición de un patrón con características específicas, las cuales comúnmente se basan en patrones de amenazas conocidas. Contienen características como tipo de tráfico, dirección de flujo, protocolo, direcciones IP, puertos o incluso el contenido de datos en el paquete. Cuando un paquete de red coincida con este patrón, entonces se levantará la alerta proporcionando la información relacionada. Los desarrolladores de IDS comúnmente liberan nuevas firmas para poder detectar amenazas recientes.

Por otro lado, la detección basada en anomalías funciona definiendo ciertos criterios base o *baselines,* que suponen un funcionamiento normal

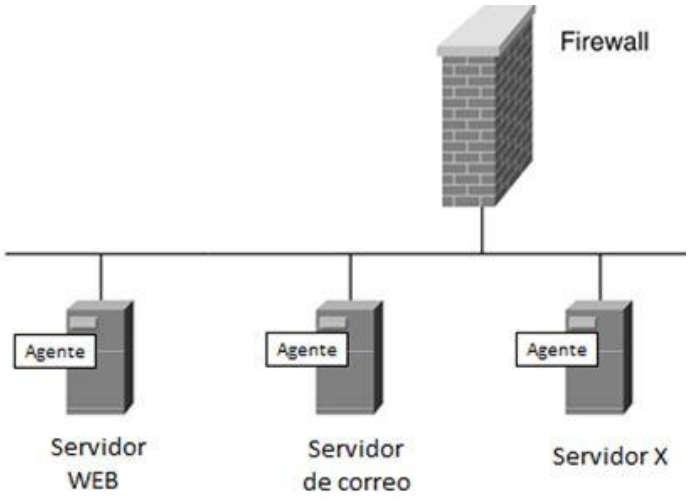
del sistema o de la red. Cuando se detecta cierta actividad que no corresponde con el*baseline* en un cierto rango, entonces el IDS lo puede interpretar como una anomalía, y en su caso, identificarlo como tráfico malicioso.

Con los IDS existen dos problemas principales: los falsos positivos y los falsos negativos. Los primeros se refieren a todos los eventos levantados como alertas pero que en realidad no se trataban de tráfico malicioso. Esto puede deberse a varios motivos, por ejemplo que alguna situación o aplicación llevó a generar el paquete con las características de la firma, un aspecto a tomar en cuenta es que mientras más general se defina la regla, más falsos positivos se pueden tener. Los falsos negativos consisten en todos los eventos que a pesar de presentarse en la red no son alertados por el IDS. En realidad, este tipo de omisiones puede implicar un mayor riesgo pues, desde cierto punto de vista, es más conveniente detectar algo que no existe, que no detectar algo que en verdad existe y que es malicioso, aunque debe tenerse presente que también contar con un número significativo de falsos positivos puede llegar a ser contraproducente.

Tipos de IDS

IDS basados en host

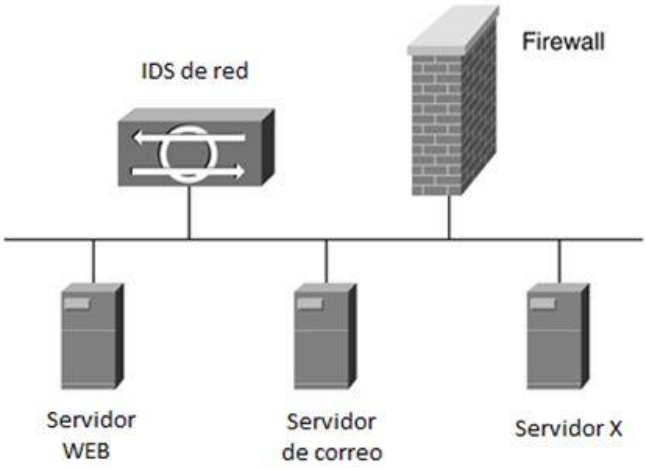
Funciona monitoreando la actividad de un sistema local. Por su esquema de funcionamiento, analiza el tráfico de red que entra y sale de dicho equipo, así como los cambios en el sistema de archivo y actividad del sistema en general.



Esquema de un IDS de host

IDS basados en red

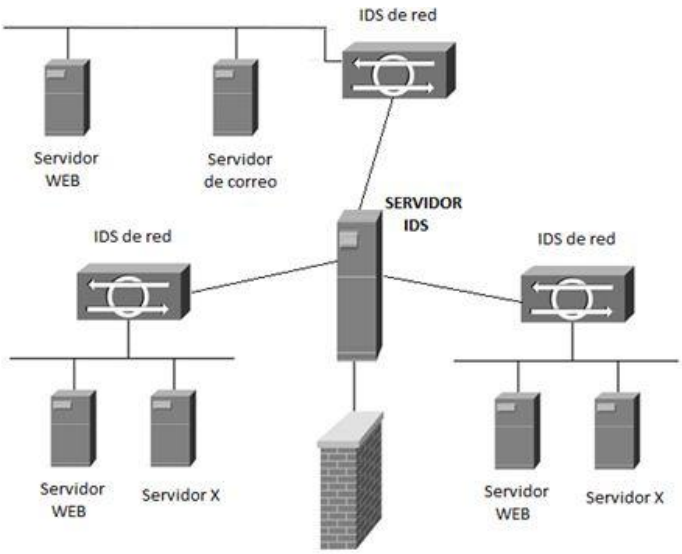
Analiza el tráfico de un equipo o red. Puede instalarse en un equipo analizando sólo el tráfico que fluye a través de él, sin embargo para que funcione plenamente, debe implementarse un esquema en donde reciba el tráfico de todos los equipos conectados a la red (comúnmente llamado "*port mirror*"). Generalmente, se instala en el perímetro de la red o subred para poder monitorear el tráfico de entrada y salida de la misma. El éxito en su funcionamiento depende de su correcta ubicación.



Esquema de un IDS de red

IDS distribuidos

Es un esquema de varios IDS desplegados a lo largo de una red, los cuales centralizan la información. Este tipo de esquemas puede ser útil en redes de gran tamaño, sin embargo debido a la gran cantidad de información que implica, necesita un monitoreo y mantenimiento constante.



Esquema de un IDS distribuido

Los factores clave para el buen funcionamiento de los IDS son entonces: ubicación, buenas firmas, *baselines*, criterios, mantenimiento, etcétera.

IDS e IPS

Los sistemas de prevención de intrusos o IPS son también mecanismos físicos o lógicos para la detección de tráfico malicioso basándose en firmas o anomalías. La principal diferencia con los IDS es que los IPS son dispositivos activos que tienen la característica de actuar bajo demanda según las alertas detectadas, a esto se le conoce como "inline". Esto significa que, a partir de que un evento es detectado, el sistema puede aplicar automáticamente una medida de mitigación. lo cual implica que los IPS tengan capacidades de firewall. Por estas características, a este tipo de dispositivos también se les conoce como IDP o sistemas de detección y prevención de intrusos.

Con este esquema podría pensarse que los IPS son mejores que los IDS, o incluso que podrían sustituir a los firewalls. Desde hace algunos años, firmas internacionales de seguridad y otras organizaciones de desarrollo e investigación, han abierto un gran debate sobre si los IDS han quedado obsoletos o representan una tecnología que será sustituida por los IPS.

Gartner, organización conocida mundialmente por dedicarse a la tecnología y los negocios, publicó en 2003 una declaración donde afirmaba "*Intrusion Detection Systems a Market Failure*"[3], mientras otras opiniones expresaban lo contrario. El argumento era que los IPS no podrían

aún representar la nueva generación de dispositivos de detección debido a que aún eran inmaduros. Lo que evidente es que aún existen consideraciones que deben tomarse en cuenta para la implementación de un IPS.

Primeramente está el problema de los falsos positivos. Con los IDS, este problema implica solamente realizar un proceso de discriminación de alertas, el cual en el peor de los casos representa un trabajo adicional y excesivo para el administrador de la red. En cambio, con un IPS un falso positivo podría representar una auto-negación de servicio o problema general con la red, pues de manera automática, aplicaría las reglas en su firewall interno para poder mitigar "el ataque". Es por eso que las firmas de detección deben definirse con el criterio más acertado posible para minimizar el número de falsos positivos.

En conclusión, las características de los IDS han evolucionado como respuesta al desarrollo de amenazas en Internet. Si bien es cierto que son un mecanismo para detección, debe tomarse también en cuenta que algunas características que los llevan de pasivos a activos como la capacidad de mitigación y el análisis de patrones, han abierto nuevas líneas de desarrollo e investigación para nuevos sistemas de detección adaptados a las necesidades de las nuevas tecnologías y de la industria.

Referencias

- http://www.sans.org/security-resources/idfaq/
- http://www.sans.org/reading_room/whitepapers/detection/
- http://www.google.com/url?sa=t&source=web&cd=12&ved=0CB4QFjABOAo&url=http%3A%2F%2Fftp.iingen.unam.mx%2Fpub%2FSeguridad%2FIDS%2FIDS_v1.0.pdf&rct=j&q=historia%20de%20los%20sistemas%20de%20deteccion%20de%20intrusos&ei=GsyaTfztFc6y0QHu_dnCBg&usg=AFQjCNFFtFiXXEe4Zg4gr2G-weIYGF1IdA&cad=rja
- http://www.google.com/url?sa=t&source=web&cd=7&ved=0CEMQFjAG&url=http%3A%2F%2Fbiblioteca.utec.edu.sv%2Fsiab%2Fvirtual%2Farticulos_soft_libre%2Fintrusos.pdf&rct=j&q=historia%20de%20los%20sistemas%20de%20deteccion%20de%20intrusos&ei=7MuaTYXgGPCQ0QH03LXcBg&usg=AFQjCNGEhkHJFV1kkrUYYFaYhYCHHC7Lew&cad=rja

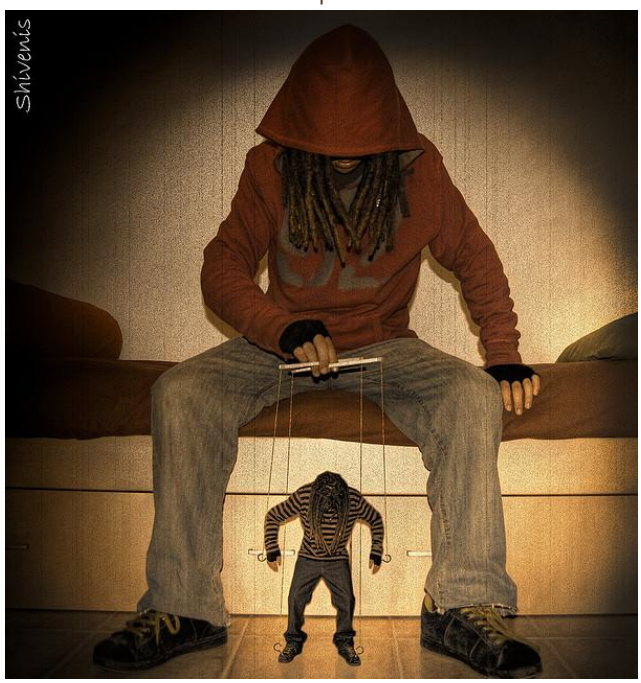
[1] Organización internacional dedicada a la investigación, capacitación y publicación de recursos relacionados con seguridad en cómputo.
[2] http://isc.sans.edu/survivaltime.html
[3] Gartner Information Security Hype Cycle Declares Intrusion Detection Systems a Market Failure.http://www.gartner.com/5_about/press_releases/pr11june2003c.jsp

Ingeniería Social: Corrompiendo la mente humana

Por Edgar Jair Sandoval Castellanos*

Introducción

Hoy en día, uno de los activos más valiosos para las organizaciones es la información. Compartir información con otras entidades, sugiere la mayoría de las veces una invasión de la privacidad.



Img 1. Cortesía Flickr

Por ello, las instituciones (gubernamentales, educativas, financieras, etc.) buscan la manera de implementar controles de seguridad para proteger su información, como circuitos de cámaras, cajas fuertes, firewalls, etc., medidas que además resultan costosas.

Sin embargo, hay un recurso inseguro que almacena información muy sensible: la mente humana. Ya sea por olvido o por el reto que implica asegurar la información dentro de las cabezas de sus empleados, las organizaciones no le prestan mucha atención a este aspecto.

Sin importar cuántos candados físicos o lógicos haya para proteger un activo, al dar acceso a una persona, siempre existirá un riesgo humano presente, y por tanto, vulnerable a ingeniería social.

¿Qué es la Ingeniería Social?

La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de

---

* Se desempeñó como pentester en el Departamento de Auditoría y Nuevas Tecnologías de la SSI/UNAM-CERT hasta mayo de 2011. Ha sido instructor en la Facultad de Ingeniería impartiendo cursos de Redes de Datos y Administración de Sistemas Operativos, y de Técnicas de Intrusión en el Congreso de Seguridad 2010.

información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo.

La Ingeniería Social se sustenta en un sencillo principio: "el usuario es el eslabón más débil". Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla[1].

La Ingeniería Social es un arte que pocos desarrollan debido a que no todas las personas tienen "habilidades sociales". Aún así, hay individuos que desde pequeños han demostrado tener la aptitud y con un poco de entrenamiento convertirla en el camino ideal para realizar acciones maliciosas. Por ejemplo, hay *crackers* que en vez de perder horas rompiendo una contraseña, prefieren conseguirla preguntando por teléfono a un empleado de soporte técnico.

Formas de ataque

Las formas de ataque son muy variadas y dependen de la imaginación del atacante y sus intereses. En general, los ataques de Ingeniería Social actúan en dos niveles: el físico y el psicosocial. El primero describe los recursos y medios a través de los cuales se llevará a cabo el ataque, y el segundo es el método con el que se engañará a la víctima.

Las formas usadas a nivel físico son:

- **Ataque por teléfono.** Es la forma más persistente de Ingeniería Social. En ésta el perpetrador realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, como un técnico de soporte o un empleado de la misma organización. Es un modo muy efectivo, pues las expresiones del rostro no son reveladas y lo único que se requiere es un teléfono.

Img. 2 Cortesía Flickr

- **Ataque vía Internet.** Desde que Internet se volvió uno de los medios de comunicación más importantes, la variedad de ataques en red se incrementaron tanto como la gran cantidad de servicios que existen en él. Los ataques más comunes son vía correo electrónico (obteniendo información a través de un phishing o infectando el equipo de la víctima con malware), web (haciendo llenar a la persona objetivo un formulario falso) o inclusive conversando con personas específicas en salas de chat, servicios de mensajería o foros.

- ***Dumpster Diving* o *Trashing*** (zambullida en la basura). Consiste en buscar información relevante en la basura, como: agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD's, USB's, etc.), entre muchas otras cosas.

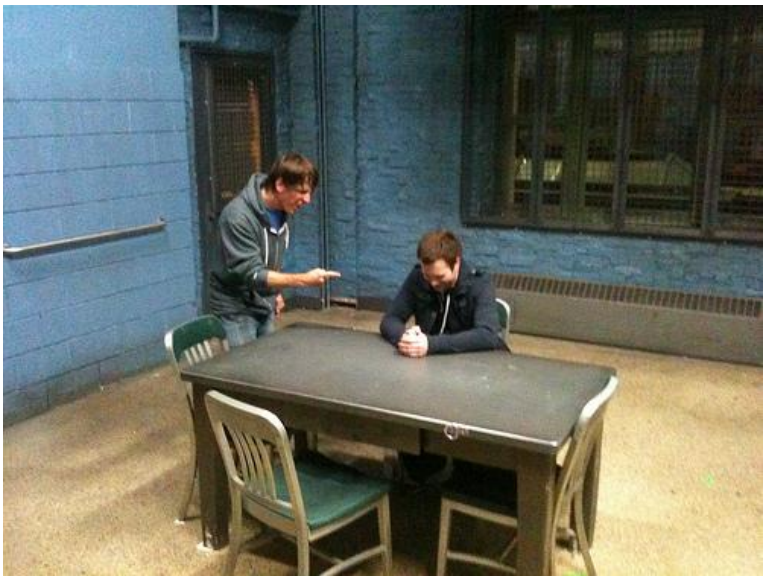
Img. 3 Cortesía Flickr

- **Ataque vía *SMS*.** Ataque que aprovecha las aplicaciones de los celulares. El intruso envía un mensaje *SMS* a la víctima haciéndola creer que el mensaje es parte de una promoción o un servicio, luego, si la persona lo responde puede revelar información personal, ser víctima de robo o dar pié a una estafa más elaborada.
- **Ataque vía correo postal.** Uno de los ataques en el que la víctima se siente más segura, principalmente por la fiabilidad del correo postal. El perpetrador envía correo falso a la víctima, tomando como patrón alguna suscripción de una revista, cupones de descuento, etc. Una vez que diseña la propuesta para hacerla atractiva, se envía a la víctima, quien si todo sale bien, responderá al apartado postal del atacante con todos sus datos.
- **Ataque cara a cara.** El método más eficiente, pero a la vez el más difícil de realizar. El perpetrador requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que se le presente. Las personas más susceptibles suelen ser las más "inocentes", por lo que

no es un gran reto para el atacante cumplir su objetivo si elige bien a su víctima.

Por otro lado, existen entornos psicológicos y sociales que pueden influir en que un ataque de ingeniería social sea exitoso. Algunos de ellos, son:

- **"*Exploit* de familiaridad".** Táctica en que el atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por cualquiera de ellos. Un ejemplo claro de esto ocurre cuando un conocido llega a una fiesta con uno de sus amigos. En una situación normal nadie dudaría de que ese individuo pudiera no ser de confianza. Pero ¿de verdad es de fiar alguien a quien jamás hemos tratado?
- **Crear una situación hostil**. El ser humano siempre procura alejarse de aquellos que parecen estar locos o enojados, o en todo caso, salir de su camino lo antes posible. Crear una situación hostil justo antes de un punto de control en el que hay vigilantes, provoca el suficiente estrés para no revisar al intruso o responder sus preguntas.



Img. 4 Cortesía Flickr

Conseguir empleo en el mismo lugar. Cuando la recompensa lo amerita, estar cerca de la víctima puede ser una buena estrategia para obtener toda la información necesaria. Muchas pequeñas y medianas empresas no realizan una revisión meticulosa de los antecedentes de un nuevo solicitante, por lo que obtener un empleo donde la víctima labora puede resultar fácil.

Leer el lenguaje corporal. Un ingeniero social experimentado puede hacer uso y responder al lenguaje corporal. El lenguaje corporal puede generar, con pequeños, detalles una mejor conexión con la otra persona. Respirar al mismo tiempo, corresponder sonrisas, ser amigable, son algunas de las acciones más efectivas. Si la víctima parece nerviosa, es bueno reconfortarla. Si está reconfortada, ¡al ataque!

- Explotar la sexualidad. Técnica casi infalible. Las mujeres que juegan con los deseos sexuales de los hombres, poseen una gran capacidad de manipulación, ya que el hombre baja sus defensas y su percepción. Probablemente suene asombroso, pero es aprovechar la biología a favor.

¿Cómo defenderse contra la Ingeniería Social?

La mejor manera de enfrentar el problema, es concientizar a las personas al respecto. Educarles sobre seguridad y fomentar la adopción de medidas preventivas. Otros mecanismos sugeridos son:

- Nunca divulgar información sensible con desconocidos o en lugares públicos (como redes sociales, anuncios, páginas web, etc.).
- Si se sospecha que alguien intenta realizar un engaño, hay que exigir se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del sospechoso.
- Implementar un conjunto de políticas de seguridad en la organización que minimice las acciones de riesgo.
- Efectuar controles de seguridad física para reducir el peligro inherente a las personas.
- Realizar rutinariamente auditorías y *pentest* usando Ingeniería Social para detectar huecos de seguridad de esta naturaleza.
- Llevar a cabo programas de concientización sobre la seguridad de la información.

Conclusiones

La seguridad de la información no sólo debe entenderse como un conjunto de elementos técnicos y físicos, sino como un proceso cultural de personas y organizaciones. Si el usuario es el eslabón más débil, deben existir controles que ayuden a disminuir el riesgo que éste pueda representar.

Kevin Mitnick, el hacker más reconocido a nivel mundial y experto en Ingeniería Social, concluye: “Puedes gastar una fortuna en tecnología y servicios... y como sea, tu infraestructura de red podría estar vulnerable a la forma más vieja de manipulación”.

Ahora que conoces más sobre la ingeniería social y la seguridad de la información, la próxima vez que sientas que tu información está completamente segura, recuerda que no todas las intrusiones son siempre tan obvias como esta:

Img. 5 Cortesía Flickr

Referencias

- GRANGER, Sarah; **Social Engineering Fudamentals, Part I: Hacker Tactics**;
- HEARY, Jamey; **Top 5 Social Engineering Exploit Techniques**;
- DOLAN, Aaron; **Social Engineering**; http://www.sans.org/reading_room/whitepapers/engineering/social-engineering_1365
- RAMÍREZ, Jorge; **Ingeniería Social, una amenaza informática** http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica
- **Ingeniería Social (seguridad informática)**;http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)
- **The Official Social Engineering Portal**

---

[1] MOLIST, Mercè; Ingeniería Social: Mentiras en la Red; http://ww2.grn.es/merce/2002/is.html

Ley Federal de Protección de Datos Personales en Posesión de Particulares

Por Juan Carlos Carrillo D'Herrera*

El pasado mes de julio de 2010 se publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Este tipo de ley no es nueva en el mundo, pues tanto en Europa como en Estados Unidos existen leyes parecidas a la nuestra desde hace varios años. En México tenemos la ventaja de que la ley integra conceptos que no contemplan las leyes de otros países, ya que la innovación tecnológica de los últimos diez años hace que el tratamiento de datos personales sea completamente distinto.

El objetivo de la ley es **proteger los datos** personales en posesión de las empresas, así como **regular** que dichos datos sean usados únicamente para la finalidad que fueron entregados, que se tenga un control de quién y para qué los tiene y que el titular o dueño de los datos siempre esté informado del trato de dichos datos, buscando con lo anterior garantizar la privacidad y el **derecho a la autodeterminación** informativa de los individuos.

La ley define a los datos personales como cualquier información que haga a una persona identificada o identificable, y a su vez menciona que, son datos personales sensibles aquellos datos que afecten a la esfera más íntima de su titular, como podrían ser estado de salud, preferencias religiosas o sexuales.

La ley les otorga a los titulares de datos personales, léase que esta ley no sólo aplica a los mexicanos, sino a cualquier persona que entregue datos personales, cuatro derechos fáciles de recordar, pero que serán un dolor de cabeza para las empresas. Dichos derechos son: (1) acceso a sus datos; (2) rectificación de datos erróneos o incompletos, así como la responsabilidad de que las empresas notifiquen a sus terceros dichas rectificaciones; (3) Cancelación de los datos, que puede involucrar el que sean bloqueados por un periodo o su total borrado, y (4) Oposición, por la cual, el titular puede solicitar la exclusión de los datos de cualquier tipo de tratamiento.

---

*Director de Desarrollo de Negocios de SM4RT Security Services. Anteriormente, se desempeñó como líder en venta de soluciones de seguridad para el sector financiero en IBM. Fue gerente de Infraestructura en Grupo Bursátil Mexicano y Merrill Lynch, encargado de soporte a transacciones B2B en GE Ddemesis y gerente de tecnología en Boston Consulting Group. Egresado de la Universidad del Valle de México, campus Lomas Verdes, posee una maestría en finanzas por la EGADE del Tecnológico de Monterrey, campus Santa Fe. Juan Carlos tiene más de 15 años de experiencia dando charlas, conferencias y diplomados en diversos ámbitos de la información.

Uno de los temas más importantes de la ley es el reparto de responsabilidades. Ahora, la autoridad responsable tiene el poder de realizar verificaciones de oficio o a petición de parte, poner penas de hasta 10 años de prisión o multas de hasta 76 millones de pesos, y por último, publicar los resultados y resoluciones de forma pública, lo que implica un riesgo altísimo a la reputación.

Durante los últimos meses he impartido distintas conferencias sobre la Ley de Protección de Datos; en la gran mayoría de los casos, las personas no conocen la ley, ni sus derechos, y aún peor, las empresas están realizando esfuerzos mínimos para proteger a los titulares. ¿Por qué ocurre esta situación? Hay dos aspectos básicos:

1. Dado que se trata de una ley, quienes la están leyendo-entendiendo son únicamente las áreas legales, dejando de lado las áreas de sistemas, recursos humanos, operaciones, finanzas, riesgos, etcétera.

2. En nuestro país tenemos una escasa cultura sobre seguridad informática, por lo que nos parece que una ley como ésta es letra muerta, y que las autoridades no cumplirán ni con las penas ni con las multas que la ley prescriba.

¿Qué debemos hacer? Existen tres visiones distintas, las cuales quiero contemplar:

- **Como titulares de datos personales**, debemos exigir a los responsables del tratamiento de nuestros datos personales, que antes de julio de este año, nos hagan llegar nuestro aviso de privacidad y así poder leerlo a conciencia. Tenemos derecho a que nos expliquen detalladamente aquello que no nos quede claro.

- **Como empleados de una empresa responsable de protección de datos personales**, es necesario estar conscientes de nuestra responsabilidad en la protección de los datos de mi empleador, ya que la inobservancia de esto podría significarle a una persona hasta 10 años de cárcel (Artículo 67,68 y 69). Por otro lado, es imperativo exigir a nuestro empleador que nos comunique el tratamiento de nuestros datos personales (aviso de privacidad) a la mayor brevedad.

- **Las empresas responsables de protección de datos** Requieren tomar en cuenta que estamos a menos de tres meses para que todos los obligados por la ley entreguen a los titulares sus avisos de

privacidad y designen al responsable de protección de datos. La mayoría de los responsables no han enviado, publicado o presentado sus avisos de privacidad. En general, existe un desconocimiento al respecto, en algunos casos no saben que lo tienen que hacer, en otros no están al tanto de qué datos personales tienen de los titulares (sus clientes) y, en el peor de los escenarios, creen que sus áreas legales lo pueden hacer en unas semanas antes de la fecha límite (5 de julio del 2011).

Es necesario comprender que no todo el mundo necesita proteger los datos de la misma manera; es imposible pedir el mismo nivel de seguridad a los pequeños comercios que manejan pocos o ningún dato personal, comparado con las grandes compañías internacionales que utilizan millones de datos personales de los clientes.

La visión de los riesgos financieros, operativos o tecnológicos se ha centrado en establecer calificaciones subjetivas para los diferentes factores que influyen en dichos riesgos. Las valoraciones son subjetivas, hay una tendencia para atribuir valores a los riesgos que no reflejan completamente la realidad, atribuyéndose comúnmente esta tarea a la experiencia previa del consultor o de la empresa que lo realiza.

¿Cuál es la solución? Hay que administrar los riesgos relacionados con los datos personales en tres niveles:

- **Riesgo Accidental**: Históricamente, las áreas de TI entienden muy bien este riesgo y elaboran sus planes de recuperación ante desastres, o bien la empresa crea sus procedimientos de continuidad de negocio. Para el tratamiento de este riesgo debemos medir el mejor esfuerzo, donde únicamente una fuente de poder, puerto, enlace o servidor funcione adecuadamente para mitigar este riesgo. La forma en que solventamos los riesgos accidentales es aplicando controles de disponibilidad de los datos y la información.

- **Riesgo oportunista**: La mayor parte de los datos personales está amenazada por este tipo de riesgo; aquí tenemos que aumentar la altura y grosor de nuestras "paredes", ya sean internas o externas. Una analogía de esta propuesta es la siguiente: hay dos automóviles iguales en diferentes situaciones; el primero tiene alarma, bastón para el volante, las ventanillas cerradas y se encuentra en un estacionamiento que cuenta con seguridad y video-grabación continua; el segundo está estacionado en una calle sin luz y con las ventanillas mal cerradas. Si un ladrón roba cualquiera de los dos vehículos, obtiene el mismo beneficio

económico, pero si roba el segundo su oportunidad de hacerlo requiere un esfuerzo menor y su riesgo está atenuado por el entorno. El riesgo oportunista es mitigado colocando "la reja más alta de la calle", es decir, no requerimos tener los controles más estrictos, sino únicamente mejores controles que los que tiene nuestra competencia, el estándar o la industria. "No hay que correr más rápido que el dragón, únicamente, más rápido que el hobbit". Este riesgo se minimiza implementando la mayor cantidad de controles (entre más mejor) y manteniendo buenas prácticas.

- **Riesgo intencional**: Este riesgo es atendido mediante controles de privacidad y de integridad. Cualquier error en un control podría significar la pérdida de datos.
  Si no entendemos esta categoría diferente, no podemos evolucionar en la gestión de riesgos. El riesgo de un presidente de ser asaltado, secuestrado o atacado es tan alto, que los niveles de seguridad que requiere, deben ser los más rigurosos en todo momento. Sus atacantes no lo agredirán por accidente, ni porque exista la oportunidad, lo harán con una intención directa, tendrán tiempo de planear el ataque y por lo mismo los controles deben ser máximos, ya que una sola falla en el sistema de protección provocaría que todo el esquema de seguridad se afectara.

Una vez analizados estos tres tipos de riesgo, y ante la inminente entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, debemos tener claro que en la protección de datos, el mayor riesgo es que no exista la administración de riesgos.

Como un método rápido y sencillo de lo qué las empresas deben hacer, sugiero tres pasos muy simples, pero efectivos:

1. Concientización de los empleados sobre el trato que dan a la información de sus clientes, proveedores y su mismo personal.

2. Realizar un análisis del impacto de privacidad, en dónde se encuentren las diferencias del estado actual versus el estado de cumplimiento y desarrollar un plan para subsanar dichas deficiencias.

3. Crear procesos que mantengan al día la protección de datos personales.

Por nuestra parte, en tanto titulares de datos personales, lo más importante es estar informados y conocer nuestros derechos y

obligaciones, la mejor forma de lograrlo es leer, entender y ejercer nuestros derechos.

Los lectores pueden consultar, la publicación de esta ley en el sitio: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010, si al leerla la encuentra complicada, el IFAI (http://www.ifai.org.mx) ha creado información sencilla y entendible para aquellas personas que quieran una referencia rápida del tema.

Medidas preventivas para resguardar la información

Por César Iván Lozano Aguilar*

El respaldo de información consiste en realizar un duplicado de ésta, llamado también copia de seguridad o *backup*. Estas copias pueden realizarse de forma manual, en las que el usuario determina la información y periodicidad para llevar a cabo el respaldo, o bien establecerlo automáticamente mediante herramientas de *software*[1].

¿Cuál es la importancia o ventaja de realizar respaldos? Los respaldos permiten cierta protección contra errores humanos, borrado accidental, uso negligente, virus[2], etc. Cualquier persona que utilice una computadora, sea ésta personal o de oficina, debe preguntarse si su información está realmente a salvo, pues los imprevistos están a la orden del día.

¿Qué sucedería si por ejemplo, un día prendemos nuestra computadora y nos damos cuenta que ya no enciende correctamente? Lo primero que se nos vendría a la mente es "¡mis archivos!". Ésta y varias situaciones pueden suceder, por ello es indispensable realizar un respaldo a fin de aminorar estos problemas.

Selección de medios de almacenamiento

A medida que pasa el tiempo, los medios de almacenamiento evolucionan, ahora cuentan con mayor capacidad, son más pequeños y versátiles, pero susceptibles a fallas, por esa razón no es bueno confiar al 100% en ellos.

Inicialmente existieron las cintas magnéticas para resguardo de la información, al igual que los diskettes de 3 pulgadas y media, los de 5 pulgadas un cuarto, todos utilizados para resguardar información de bajo volumen. En la actualidad son prácticamente obsoletos.

El sucesor de estas unidades fue el *CD* (disco compacto) con capacidad de hasta 900MB, el equivalente a casi 700 diskettes de 3 y media pulgada, el *CD* es más común para el almacenamiento de música y software autoejecutable, este dispositivo de resguardo requiere para este proceso, un

---

* Egresado de la carrera de Ingeniería en Computación por la UNAM. Se desempeña como desarrollador de soluciones de seguridad en sistemas en la Subdirección de Seguridad de la información UNAM-CERT de la DGTIC. Entre sus líneas de interés se encuentran las buenas prácticas de seguridad de la información y los lenguajes de programación. Actualmente, elabora la tesis "Sistema de autenticación centralizado para los servicios web de la Subdirección de Seguridad de la Información".

software especializado, por ejemplo *Nero Express* y una unidad escritora de discos compactos (quemador).

El *DVD* también es un medio de almacenamiento óptico dentro de la categoría de los discos compactos con capacidades de entre 4.7y 8.5GB. El *DVD* es utilizado en la mayoría de los casos para almacenamiento de audio y video; también para software autoejecutable en el que normalmente el espacio de un *CD* no es suficiente. Para el respaldo de información es necesario contar con una unidad lectora/escritora de DVD junto con software especializado para la grabación ej. *Nero Burnning*.

Entre lo más nuevo, en cuanto a discos compactos ópticos se refiere, se encuentran el HD DVD (de 15GB y 30GB) y el Blue-ray (de 25GB y 50GB), utilizados para almacenar video de alta definición.

En cuanto a dispositivos electrónicos, encontramos memorias *USB* con capacidades de hasta 32GB, en ellas es posible almacenar cualquier tipo de información, ya sean documentos de texto, hojas de cálculo, imágenes, audio, video, etcétera.

Las *SD cards* o tarjetas *SD* con capacidades hasta de 32GB, utilizadas en su mayoría para almacenar fotografías y videos; rara vez se utilizan para almacenar información convencional.

Finalmente, están los discos duros externos con conexión *USB* con capacidades de hasta 2TB (2000GB), muy útiles para el resguardo de grandes volúmenes de información de cualquier tipo.

Buenas prácticas para el respaldo de información

Elige el medio de almacenamiento: Si sólo manejas archivos de texto, hojas de cálculo, presentaciones con diapositivas o documentos PDF, éstos requieren de muy poco espacio, por lo que es mejor utilizar *USB's* o *CD's*; pero si manejas grandes cantidades de información utiliza dispositivos de mayor capacidad, como dice el dicho "de acuerdo al sapo es la pedrada".

Establece tus tiempos de respaldo: Dedica un tiempo para resguardar tu información, si manejas información crítica y de constante actualización, es recomendable que respaldes tu información regular y periódicamente, diario si te es posible, no te distraigas ni dejes la máquina desatendida por largos periodos de tiempo al efectuar tu respaldo. Si hay oportunidad pide a alguien que te ayude en esta tarea.

Selecciona y divide tu información: Separa cuidadosamente la información importante, no la mezcles con información de menor importancia (tal como imágenes, juegos, música, videos), puede suceder que al borrar una carpeta de imágenes que ya no te gusten, accidentalmente borres comprobantes de pago que habías escaneado y los tenias en formato imagen.

Control de los medios de almacenamiento: Sea cual sea el medio de almacenamiento que utilices, etiquétalo de manera adecuada y lleva un control de: etiquetas de los medios, fechas y tipo de información respaldada. Si llevas este control en un documento electrónico ten a la mano una impresión, seguramente te será muy útil a la hora de restaurar.

Utiliza el mayor espacio posible del medio: Es posible que cuando llevemos a cabo el respaldo de nuestra información, éstos no llenen completamente el medio de almacenamiento. Si esto sucede, indica el espacio que quedó disponible en el etiquetado o regístralo en tu control de respaldos, este espacio siempre puede ser utilizado.

Respaldar fotografías, imágenes, música o videos: Es preferible utilizar discos ópticos, ya que esta información no cambia constantemente y puede ser preservada por mucho tiempo (hasta por 100 años) con el debido cuidado.

Las máquinas no son un medio seguro de respaldo: Tener información respaldada en dos o más particiones en el disco duro de la computadora no es seguro, ya que si es infectada por virus todas las particiones lo estarán, al igual que la información contenida en ellas. Igualmente, si el disco duro se daña, la información en las particiones se perderá. Las particiones del disco duro únicamente son útiles para tener respaldos temporales y a corto plazo, la información siempre debe respaldarse en algún medio externo para evitar perderla.

Un solo respaldo no es suficiente: No basta con tener un solo respaldo de la información, si te es posible haz un duplicado de éste, los respaldos también son susceptibles a factores externos o fallas a la hora de la restauración.

Un respaldo total o parcial: Si realizas respaldos totales, asegúrate que sea información que no cambie constantemente, así evitarás redundancia y un alto costo en medios de almacenamiento, se puede llevar a cabo un respaldo total cada semana, junto con respaldos diarios de la información que haya cambiado; de este modo al momento de restaurar bastará con tomar el ultimo respaldo total junto los subsecuentes respaldos parciales.

Comprime tu información: Comprimir la información consiste en utilizar un software de compresión (*Winzip, Winrar, 7Zip,* entre otros), para juntar toda la

información en un solo archivo con opción de ponerle contraseña y utilizar menos espacio en el medio, no está por demás tener unos cuantos mega bytes extras.

Alternativas virtuales[3] **de almacenamiento:** Si necesitamos respaldar inmediatamente información latente y no contamos con un dispositivo de almacenamiento a la mano, pero sí con una conexión a internet, un correo electrónico nos puede sacar del apuro, *Google* ofrece 7.5GB de almacenamiento en correo electrónico con la capacidad de enviar información adjunta que no rebase los 25MB, así mismo existen proveedores de alojamiento de espacio virtual ej. *Dropbox*, muy útiles si queremos que nuestra información esté disponible desde cualquier parte del mundo.

Protege tu información si se encuentra respaldada en la nube: Si utilizas un correo electrónico o un espacio de alojamiento en la Red, comprime tu información y mantenla bajo contraseña, de esta manera evitarás que caiga en manos equivocadas y hagan mal uso de ella.

Verifica tus respaldos cada determinado tiempo: No dejes pasar más de 6 meses, máximo un año, sin revisar que los medios y la información resguardada se encuentran en buenas condiciones, realizando simulacros de restauración para verificar el estado de la información, cualquier sospecha de falla en la lectura del medio será indicador que es tiempo de transferirla a uno nuevo.

Ten presente la compatibilidad y versatilidad de los medios: Utiliza medios que sean compatibles con la mayoría de los equipos de cómputo y que no requieran dispositivos de hardware adicionales para su utilización.

Maneja adecuadamente los medios de almacenamiento: Mantén alejado cualquier medio de almacenamiento de altas temperaturas, polvo, luz solar y humedad. Limpia los discos ópticos con agua y un paño para lentes (sólo en caso de requerirlo), evita manipularlos por la parte de lectura del disco y utiliza estuches para CD's.

Para tarjetas *SD*, memorias USB y discos duros externos, evita golpearlos y retirarlos de la computadora de manera repentina o mientras se encuentren en proceso de transferencia de datos, utiliza siempre la expulsión segura del sistema operativo que manejes.

Mesografía

- *Red Hat Enterprise Linux 4: Introducción a la administración de sistemas*, http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/s1-disaster-backups.html. 22 de marzo de 2011
- Sebastián Beeche, *Cómo respaldar la información del computador* (en)http://www.guioteca.com/tecnologia/como-respaldar-la-informacion-del-computador/. 5 de abril 2011
- Sebastián Beeche, *Discos duros, cuál elegir* (en) http://www.guioteca.com/tecnologia/discos-duros-cual-elegir/. 5 de abril 2011.
- *El disco compacto* (en) http://www.tecnotopia.com.mx/mecatronica/cd.htm. 5 de abril 2011.
- *Alta Definición: Blu-ray y HD DVD* (en) http://www.zonadvd.com/modules.php?name=Sections&op=viewarticle&artid=608. 5 de abril 2011.
- *SD Technology Overview* (en) http://www.sdcard.org/developers/tech/. 5 de abril 2011.
- *Graciela Marker, Cómo conservar los CD y DVD en buenas condiciones* (en) http://www.informatica-hoy.com.ar/electronica-consumo-masivo/Como-conservar-los-CD-y-DVD-en-buenas-condiciones.php. 5 de abril 2011.

---

[1] Software: es toda aplicación y programas de computadora que se visualizan mediante ventanas en el monitor de la misma.

[2] Virus: son programas de computadora diseñados para dañar y corromper la información de los equipos de cómputo y hacer mal funcionamiento del mismo.

[3] Virtual: hace referencia a algo que existe, pero no es posible manipularlo físicamente. Para este caso, es un espacio de almacenamiento que no se encuentra en un dispositivo físico inmediato a nosotros.

Créditos

PUNTO SEGURIDAD, DEFENSA DIGITAL

Galvy Ilvey Cruz Valencia
Edición

Carmina Cecilia Espinosa Madrigal
César Iván Lozano Aguilar
Dante Odín Ramírez López
Edgar Jair Sandoval Castellanos
Javier Ulises Santillán Arenas
Juan Carlos Carrillo D'Herrera
Sergio A. Becerril
Colaboraciones

Ing. Rubén Aquino Luna
Subdirector de Seguridad de la Información
UNAM-CERT

Galvy Ilvey Cruz Valencia
Jesús Mauricio Andrade Guzmán
Revisión de Contenidos

Iván Yossi Santa María González
Diseño y Desarrollo Web