No.15 / Noviembre-Diciembre 2012 ISSN: 1251478, 1251477

.Seguridad

Cultura de prevención para TI

15

Seguridad Preventiva

Distintos enfoques de monitoreo y prevención

Web Semántica | Honeynet Project | Día de Limpieza | WIPS | Riesgo Tecnológico Parte II | Guía de contraseñas

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Seguridad Preventiva: Distintos enfoques de monitoreo y prevención

En honor a nuestro nombre, Cultura de prevención para TI, decidimos lanzar un número enfocado a fortalecer la seguridad de todos nuestros lectores desde el momento mismo en que surge nuestra actividad con la tecnología.

Queremos ofrecer una perspectiva distinta de seguridad que se anticipe a las mentes malintencionadas. Proponemos lanzar el compromiso de seguridad a quienes operamos con la tecnología, no a la tecnología en sí; a quienes manipulamos nuestra información y la de otros para no dejar la seguridad confiada en las aplicaciones con las que se manipula esa información. Es decir, la seguridad reforzada en los usuarios y no en los sistemas.

En .Seguridad creemos que la fortaleza de la seguridad radica en lograr evitar que un ataque suceda y no en cómo defenderse ante éstos. En este número queremos ofrecer un enfoque distinto al conocido paradigma de seguridad. Proponemos en esta edición,que el pilar más importante y por lo tanto el más fuerte de la seguridad seamos los propios humanos, usuarios de la tecnología.
Generar una consciencia de prevención, en materia de seguridad de la información es vital hoy en día. Si mitigamos en la medida de lo posible el origen de cualquier riesgo, lograremos un camino más seguro para transitar en la era digital.

Conocer los riesgos a los que estamos expuestos nos ayudará a prevenirlas. Si identificamos las amenazas, no solo tendremos parte de la solución, sino que también fortaleceremos la consciencia de cómo evitarlas antes de quelogren tocar nuestra puerta.

L.C.S Jazmín López Sánchez
Editora
Subdirección de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad, Cultura de prevención TI / Número 14 / Julio-Agosto 2012 / ISSN No. 1251478, 1251477 / Revista Bimestral

El efecto Blancanieves de la búsqueda de información en Internet y su impacto en entornos educativos virtuales

Por Galvy Ilvey Cruz Valencia

¿Qué es el efecto Blancanieves de la búsqueda de información en Internet?

Todos conocemos el cuento de Blancanieves, en el que una inocente manzana envenenada, dada por la malvada reina hechicera, logra afectar casi hasta la muerte a la bella princesa. Con base en la idea clímax de este cuento, hago la analogía de lo que ocurre con una de las principales tareas a las que nos enfrentamos los usuarios de entornos virtuales: la búsqueda de información.

En este supuesto, los buscadores representan a la manzana, los cuales mediante ciertas técnicas, usualmente scripts de PHP, pueden ser 'envenenados', afectando sus resultados, al igual las computadoras de los usuarios (Blancanieves). Siguiendo con la metáfora, la reina hechicera son personas maliciosas que implementan esas técnicas para alterar, a su conveniencia, los resultados.

Así, el motor de búsqueda envenenado "es el término genérico dado a ciertos trucos y técnicas que se usan para elevar la posición de una URL específica en los resultados enlistados de los motores de búsqueda. Cuando tienen éxito, los motores de búsqueda envenenados pueden tener un efecto significativo en el volumen de tráfico a un sitio" (Howard & Komili, 2010, p.2).

En ocasiones el sitio súper posicionado puede resultar ser uno dedicado a la publicidad de diferentes productos o servicios; pero también es posible que dirija a sitios relacionados con información falsa, pornografía e incluso

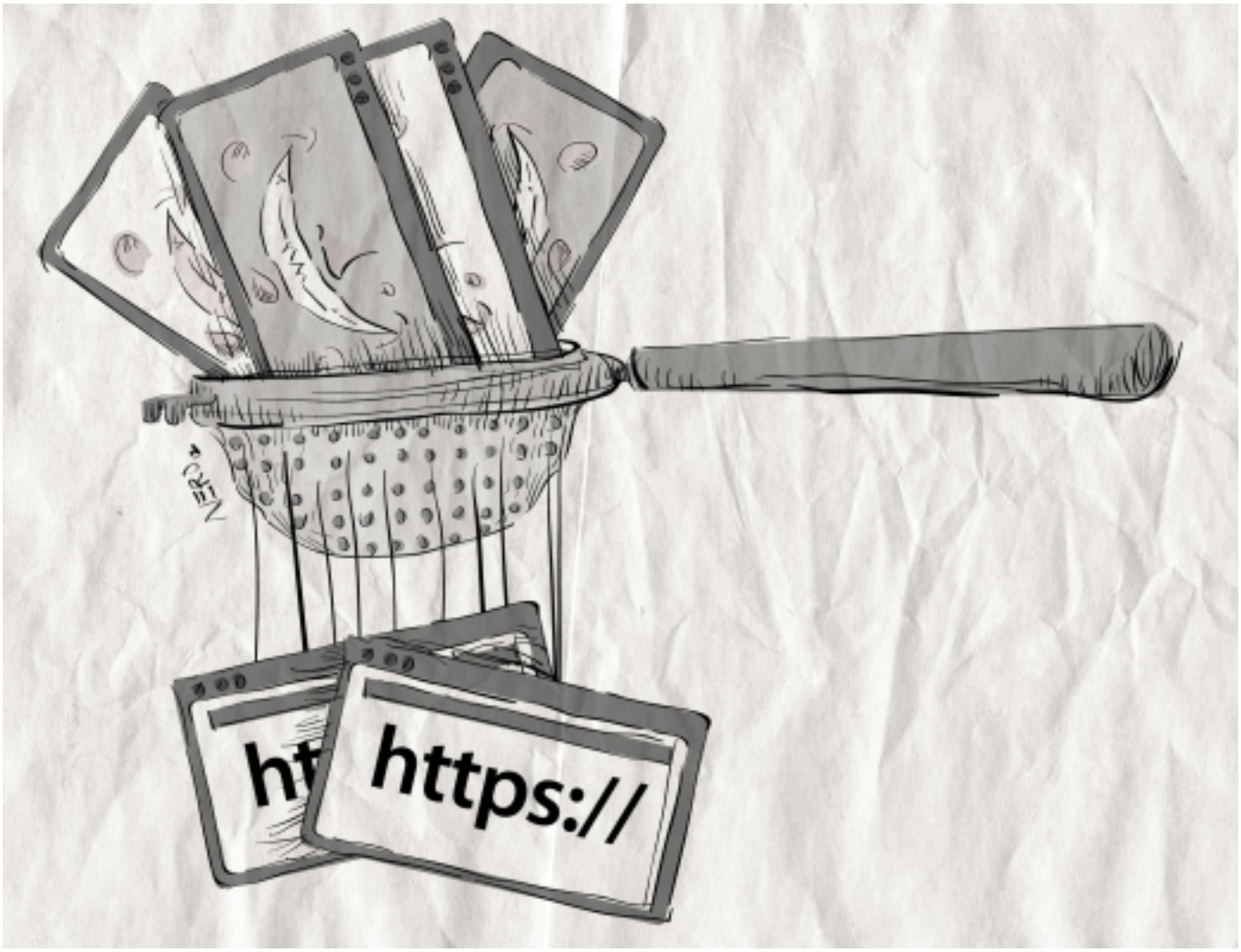
almacenadores de software malicioso (por ejemplo, troyanos de falsos antivirus conocidos como scareware).

Como lo indicó en 2011 la empresa de seguridad informática Imperva, “el abuso de un sitio web puede provocar no solo la pérdida de reputación de una institución, el robo de la base de datos de los clientes o el redireccionamiento, sino tener un impacto claramente negativo en la accesibilidad a un sitio legítimo” (Help Net Security, 2011).

Web Semántica, ¿una verdadera respuesta a las necesidades información legítima?

En el mismo cuento de Blancanieves, cuando llegan los siete enanos a su casa después de una larga jornada de trabajo, empiezan a descubrir a través de pistas que alguien había entrado a su casa. Usando un principio similar, los expertos en búsquedas en Internet proponen el método de Web Semántica como paliativo para detectar sitios con información legítima y útil.

La Web Semántica se define como “una web



Estos datos nos llevan a vislumbrar superficialmente el problema que representa el efecto Blancanieves. Comúnmente, los académicos y expertos en temas en línea evalúan los riesgos; por lo que en respuesta elaboran procesos que ayuden a enfrentarlos, como la Web Semántica, aunque pocas veces tocan el tema de motores envenenados.

extendida, dotada de mayor significado, en la que cualquier usuario en Internet podrá encontrar respuestas a sus preguntas de forma más rápida y sencilla gracias a una información mejor definida […]. Con base en el significado, se apoya en lenguajes universales que resuelven los problemas ocasionados por una Web carente de semántica en la que, en ocasiones, el acceso a la información se convierte en una tarea difícil y frustrante” (Leguízamo & García, 2011, p. 84).

Nótese que la tarea primordial expresada por Leguízamo y García (2011) se centra únicamente en la expresión de accesibilidad, no de seguridad de la búsqueda de información.
Para sustentar esta idea veamos cómo funciona, cada una de estas técnicas.

Funcionamiento de la Web Semántica

Revisemos cómo opera la Web Semántica. Inicialmente requiere que el usuario ubique un identificador único para cualquier recurso presente en la web, es decir, un registro irrepetible; indican Leguízamo y García (2011) que para ello es necesario localizar las Uniform Resource Identifier URI's (Identificador Uniforme de Recurso y su subconjunto conocido como Uniform Resource Locator URL's (Localizador de Recursos Uniforme).

De este modo, los recursos contenidos en la Web Semántica se basan en convertir las expresiones de los recursos de búsqueda en un orden semántico concreto, similar a un enunciado (sujeto, predicado y objeto). Los autores señalan a éste como 'triplete'; donde el sujeto se representa como todo aquello descrito, el predicado es la propiedad de relación que tiene con los recursos y finalmente el objeto es el valor que los relaciona. Su eficacia se basa en esta asociación y en la incorporación de metadatos (definidos como información de la información).
Como detalla el párrafo anterior, nos enfrentamos a un primer predicamento de la Web Semántica para responder a las necesidades prácticas de optimización de búsquedas: la elaboración misma de los documentos, lo que complica su eficacia y deducción.

Al respecto, Leguízamo y García (2011) integran el uso de ontología en la Web Semántica, es decir, que cada uno de los datos posea una significancia propia en tanto sea dato. Así se realizan las clasificaciones pertinentes para que cada uno de ellos exista de manera independiente dentro de un programa de estudios diverso.

Al final el postulado queda aún demasiado hipotético, incluso otros autores afirman que "la 'Web semántica, como un todo para Internet, no es aún una realidad" (Uribe, 2010, p.1), ni tampoco lo más efectivo.

¿Cómo funcionan los ataques de motores de búsqueda?

En primera instancia "los buscadores son herramientas especializadas en localizar datos distribuidos en toda Internet […] contienen una base de datos organizada que sirve para encontrar direcciones electrónicas de otros sitios" (Bassi 2001, p.3). Esa base de datos se conoce como SEO (Search Engine Optimization o Motor de Búsqueda Optimizado).

Por consiguiente, los ataques de envenenamiento se dirigen a la SEO y dicha acción es relativamente simple:
"los atacantes usan paquetes de datos especialmente diseñados para crear páginas web orientadas con palabras y frases clave de algún tópico que saben, por experiencia y/o análisis de tráfico, serán buscadas por los usuarios. Entonces, cuando un visitante consulte por alguna palabra clave el resultado que ellos deseen siempre quedará en la primera posición. Al dar clic sobre el enlace, expondrá al usuario a sitios malintencionados o a infectar su equipo con un malware" (Howard & Komili, 2010, p.3)
Hasta este punto, se pensaría que es fácil detectar: si el sitio se encuentra en primera posición, y si no es de una página que se reconozca como legítima, pues no seleccionarla. Bien, pues los ataques van más allá.

Los paquetes, o kits black hat para SEO, pueden aprovechar las vulnerabilidades de páginas legítimas para comprometerlas y de esta manera lograr un mayor éxito en el ataque.
Un caso concreto que la empresa de seguridad en Internet Sophos ha analizado minuciosamente, es la distribución de falsos antivirus. "De hecho, una vez que un sitio es comprometido, se le puede abusar de muchas maneras: desde hospedar un sitio phishing, hasta proveer una plataforma desde la cual se generen otros ataques" (Howard & Komili, 2010, p.3)
En la siguiente imagen se muestra un ejemplo de motor de búsqueda envenenado, en el se pretende dirigir a los usuarios a sitios maliciosos a través de resultados de búsqueda sobre la Copa Mundial de Fútbol: (Figura 1)

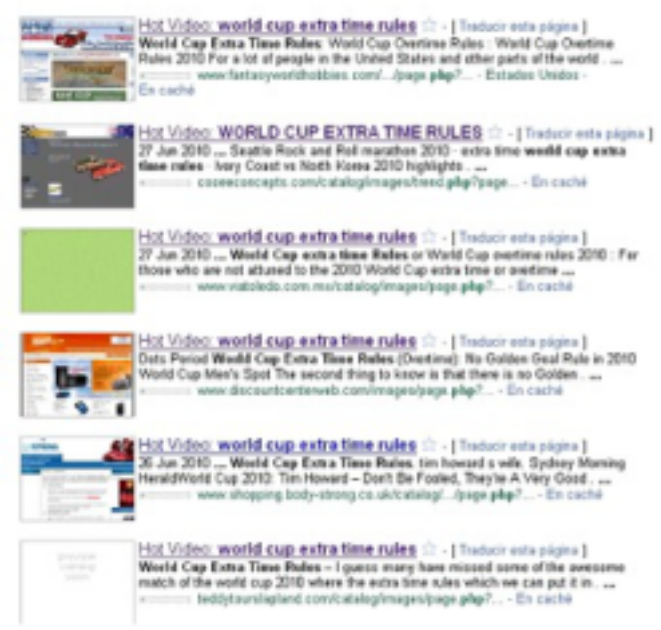


Fig. 1. Ejemplo gráfico de un motor de búsqueda envenenado (Corrons, 2010)Fig.

Hasta aquí, se puede destacar que: tanto la Web Semántica como los ataques al SEO implican una elaboración previa, los URL como identificadores únicos, uno es más activo que el otro y que, finalmente, ambos son producto de palabras o frases concretas enarboladas por los usuarios.

El impacto del efecto Blancanieves en entornos educativos virtuales pese al uso de la Web Semántica

"Aprender a buscar y seleccionar en Internet" (Monereo, 2005, p.1), tres competencias formativas que los alumnos de educación a distancia debemos desarrollar irrenunciablemente, pero se nos advierte: ¡Cuidado, Internet es un espacio de todos y anónimo!
El autor Monereo (2005) enlista riesgos de Internet. Recuperó para propósitos de este ensayo, 3 de ellos:

• Falta de control de automatización y control de la información.
• Información enmascarada.
• Problemas de garantía, procedencia y confiabilidad de la información.

El efecto Blancanieves, como hemos revisado con antelación, encajaría perfectamente en estos tres riesgos, veamos por qué:

A) El usuario promedio no tiene control sobre la SEO del buscador, mucho menos capacidad para automatizar la acotación de sus resultados.
B) Al ocultarse el ataque de motores de búsqueda SEP(Search Engine Poisoningo, envenenamiento de motores de búsqueda bajo un URL de sitios legítimos) hace que pensemos, de una u otra manera, en el riesgo de la información enmascarada.
C) Aunque creamos conocer a los emisores de ciertos datos en Internet, debemos considerar siempre los problemas de garantía señalados.

La Web Semántica apoyada en los tripletes, mencionaba la secuencia hilada de URL; pero con lo que hemos deducido hasta ahora, éstas son sensibles al SEP, por lo que resultaría la falla más sensible de la técnica.

En el ejemplo expuesto por Leguízamo y García (2011):

Fig. 3. Modelo Sujeto-Predicado-Objeto (Leguízamo & García, 2011, p. 85)

Se denota que una de las URL proviene de un enlace de terceros, esto es que el sitio 'noesis' aloja dos de los contenidos y el tercero está en LinkedIn . Según Sophos, muchos de los ataques de SEP se deben a referencias de terceros y no propiamente a deficiencias en los sitios legítimos. Esto comprueba, en cierta medida, la respuesta efectiva avalada de información legítima de la Web Semántica.

Otra de las confrontaciones de SEP y Web Semántica resulta en el uso de 'ontologías', que la segunda rescata para confirmar la unidad de un recurso en la red; describe Leguízamo y García (2011) "la ontología es la manera más habitual para añadir significado semántico a la web. Para lograr esto, la ontología debe estar conformada por una taxonomía y un conjunto de

reglas de inferencia" (Leguízamo & García, 2011, p. 90).

Sin embargo, hay que tener en cuenta que el éxito del SEP radica precisamente en la no ruptura semántica entre la búsqueda y el resultado; es decir, si nos enfrentamos a un motor de búsqueda envenenado, entre más añadamos componentes semánticos, mayor será el riesgo de ser redirigidos a un sitio envenenado.
Y es que, como señala Imperva, "esta técnica es particularmente efectiva en tanto el criminal no irrumpa o corte, cualquier servidor involucrado para ejecutar el ataque. Sino más bien, encuentre sitios vulnerables en él para inyectar su código y después cambiar los resultados de búsqueda para propagar su malware". (Help Net Securty, 2010)

Finalmente, el tercer punto de Monereo (2005): la carencia de garantías. En este sentido, la Web Semántica se vislumbra como un potente recurso, apunta Leguízamo y García (2011), en un periodo de 5 años podría apuntalar y perfeccionar las búsquedas en Internet; durante ese periodo es probable que también se presenten mejoras en la seguridad de los buscadores para evitar el SEP y sus ataques, lo que representaría un cambio totalmente revolucionario para los estudiantes de entornos virtuales.

Consejos para enfrentar el efecto Blancanieves

En el cuento, el antídoto para librar a Blancanieves del efecto de envenenamiento es el beso de amor verdadero. En nuestro caso, se requiere una documentación previa para que los consejos que a continuación se enumeran tengan eco entre los usuarios.
Es importante dejar en claro que los tips aquí presentados son ante todo preventivos y no activos. Algunos estudiantes más ávidos, podrían recurrir a una participación más activa, aunque para efectos de este ensayo, me limitaré a los primeros.

1) Revise la URL

Tal y como lo retoma la Web Semántica, las URL son identificadores únicos de un recurso en la red. No existe una URL igual a otra, aunque sí unas muy parecidas; una letra puede hacer la diferencia, por lo que es necesario ser minuciosos al digitar una URL. SEP puede provocar que una URL escrita perfectamente entregue malware, así que se requiere atender el siguiente consejo.

2) Mantenga una solución antivirus actualizada

Dada la incertidumbre que genera el encontrar una URL comprometida durante una búsqueda, se requiere ir un paso adelante. Por ello, el usuario debe contar con una solución antivirus vigente. De lo contrario, se expone casi por defecto a una inminente infección. Algunos antivirus ofrecen protección preventiva sobre ciertos sitios. Por ejemplo, al buscar el tema 'la ética educativa', el proveedor de antivirus AVG advierte con marcas

Fig. 3. Sistema de seguridad Web de la solución antivirus AVG 2012 (Google, 2012)

la seguridad de un sitio:

3) Actualice el navegador regularmente

Si bien muchos de los ataques se efectúan desde el código para inyectar HTML maliciosos, el no tener al día el navegador web es otra posibilidad que potencializa los ataques SEP, por lo que nunca está demás instalar las actualizaciones del navegador (ni tampoco las que solicite el

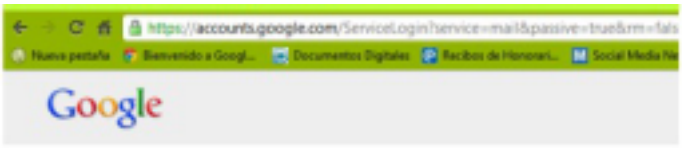


Fig. 4. Sistema de seguridad Web de la solución antivirus AVG 2012 (Google, 2012)

sistema operativo que administre, no importa si es Windows o OS X).

4) Prefiera búsquedas seguras

Por búsqueda segura se entiende a aquellos procesos cuyos resultados requieren ingresar datos de sesión y cuentan con protocolo HTTPS. A estos resultados se les identifica a través de un icono de candado en la línea de entrada de URL; es decir, ese campo de texto donde se ingresan las direcciones electrónicas. En ocasiones, se sobresaltan en color verde. Ya que los ataques SEP, se dirigen en su mayoría a sitios populares. Empresas como Google, Facebook y Twitter, hacen uso de esta tecnología.

5) Deshabilite aplicaciones web que no ocupe o sean innecesarias

Cada aplicación instalada es una oportunidad para ataques. Recuerde: muchos ataques SEP se producen a través de sitios de terceros. Por ello, se debe ser selectivo con lo instalado para evitar abrir oportunidades.

6) El reto de superar la infoxificación

La infoxificación categorizada por Monereo (2005), es una confrontación inmediata. A través de funciones booleanas podemos sortear su persistencia. Sin embargo, como se ha revisado, no basta ser selectivos con los sitios elegidos, sino también precavidos con los resultados sugeridos por el buscador para no caer en sitios indexados por ataques SEP.

Estos consejos son básicos, pero lo suficientes para iniciar una concientización sobre lo que implica una búsqueda en Internet. El propósito no es atemorizar a los usuarios para que se abstengan de hacer búsquedas, sino abrir todos los panoramas, de modo que se tengan las herramientas para actuar de manera rápida y eficaz ante esta realidad.

Referencias

Bassi, R. (2001). Manual: Cómo buscar información en Internet. Recuperado el 4 de mayo de 2012, de http://www.links.org.ar/weblinks/buscar.pdf

Corrons, L. (2010, Julio 16). Dissecting a BlackHat SEO attack. Recuperado el 12 de junio de 2012, de http://pandalabs.pandasecurity.com/dissecting-a-blackhat-seo-attack/

WikiDisney. (2009, Mayo 29). La manzana envenenada. Recuperado el 17 de junio de 2012, de http://es.disney.wikia.com/wiki/La_Manzana_Envenenada

Gándara, M. (2008). Telesesión 6 Búsqueda eficiente en Internet (I) de “Uso de Tecnología de Información y Comunicación” MCyTE-CECTE-ILCE, México.

Gándara, M. (2008). Telesesión 7 Búsqueda eficiente en Internet (II) de “Uso de Tecnología de Información y Comunicación” MCyTE-CECTE-ILCE, México.

Gándara, M. (2008). Telesesión 10 Cómo navegar en Internet sin naufragar en el intento II. Programas auxiliares (plug-ins) de “Uso de Tecnología de Información y Comunicación” MCyTE-CECTE-ILCE, México.

Google. (2012). Recuperado el 12 de junio de 2012, de http://www.google.com.mx/webhp?source=search_app

Help Net Security. (2011, Junio 9). How search engine poisoning works. Recuperado 13 de mayo de 2012, http://www.net-security.org/secworld.php?id=11141

Howard, F & Komili, O. (2010). Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware. SophosLabs, 15pp. Recuperado el 4 de mayo de 2012, de http://www.sophos.com/security/technical-papers/sophos-seo-insights.pdf

Leguízamo, L.V.,& García, C.J. (2011). Semántica de las búsquedas de información en entornos virtuales de formación. Revista TESI. Universidad de Salamanca, 432, 80-97. Recuperado el 17 de abril de 2012, de http://bit.ly/HT9k2A

Monereo, C. (Coord.) (2005). Aprender a buscar y seleccionar en Internet. México: Graó.

Uribe, A. (2010). La Web semántica y sus posibles aplicaciones en las universidades. Recuperado el 10 de junio de 2012, de http://acimed.sld.cu/index.php/acimed/article/view/41/20

1 Para referencias de problemas de seguridad en LinkedIn, véase la nota: http://www.seguridad.unam.mx/noticia/?noti=3851

HoneyNet Project map

Ing. Miguel Raul Bautista Soria

El mapa de visualización Honey Net es un proyecto nacido del Honeynet Project, un esfuerzo de la autoría de Florian Weingarten y Mark Schloesser con el fin de mostrar de forma clara una parte de los ataques que se realizan a computadoras y estaciones de todo el mundo.

Actualmente el proyecto Honeynet Map se encuentra en su fase Alpha, sin embargo, no

todos los sensores o Honeypots se visualizan en la pantalla del Honey Map. El UNAM-CERT se unió a este proyecto aportando las estadísticas de los sensores o Honeypots que se pueden apreciar en la sección de México en el mapa.

El Proyecto Honeynet

Es una organización de seguridad informática de talla internacional y sin fines de lucro. Está dedicada a realizar investigaciones acerca de los más recientes ataques informáticos y a desarrollar herramientas de seguridad de código abierto que ayudan a mejorar la seguridad de Internet.

El proyecto realiza acciones de concientización para involucrar a especialistas en seguridad informática, así como enseñar e informar al público en general, acerca de las amenazas a los sistemas de TI y a la información.

Desde 1999 el proyecto ha contribuido con herramientas de detección de intrusos y ataques maliciosos, incluidas algunas como captura de malware y visualización de ataques. Gracias a estas contribuciones, la organización se ha

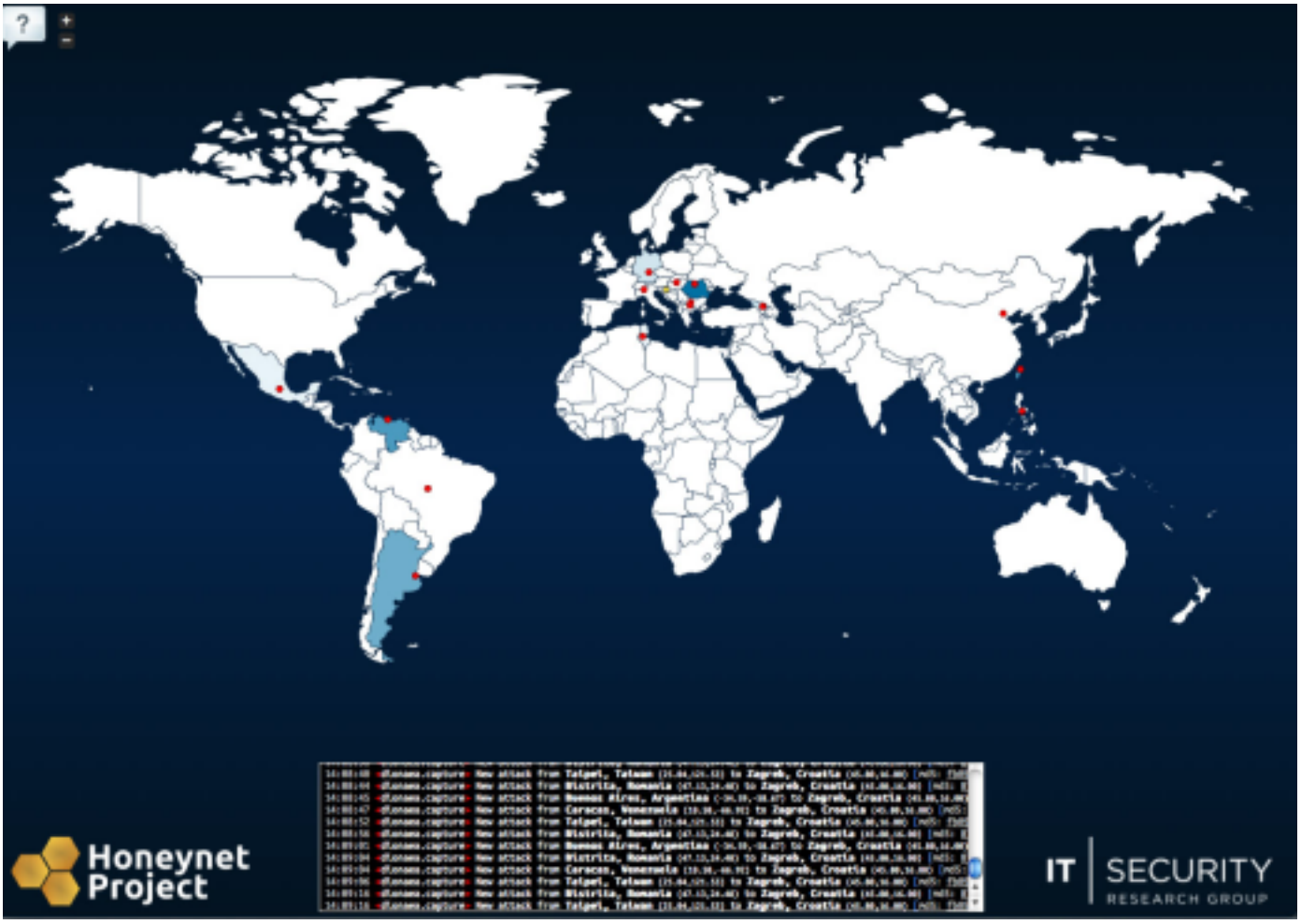


Fig. 1. Honeynet Project map

mantenido a la vanguardia en la seguridad informática en todo el mundo.

Estas herramientas son y se mantienen de uso libre, así como el mapa mismo, puede ser accedido desde cualquier computadora para darle el uso que mejor convenga.

El UNAM-Chapter

En el año 2002, el UNAM-CERT se convierte en miembro del Proyecto Honeynet como UNAM-Chapter. Desde entonces ha tenido acceso a la información, avances y herramientas desarrolladas (y en fase de desarrollo) antes de que éstas sean publicadas, además de compartir experiencias, lo que ha ayudado al UNAM-CERT a aumentar y mejorar sus técnicas y herramientas de detección de intrusos, a lo largo de Red-UNAM.

En el año 2010 la UNAM fue la sede de la reunión anual del proyecto llamada Honeynet Project Annual Workshop. Este evento de carácter mundial fue organizado por UNAM-CERT y el UNAM-Chapter, en el que todos los miembros del proyecto a lo largo del mundo se reúnen para mostrar sus avances, presentar nuevas herramientas desarrolladas, resultados e, incluso, impartir talleres públicos y privados sobre conceptos de seguridad, manejo de herramientas, competencias de seguridad, etc.

La idea del mapa nace a partir del uso e implementación de un servidor centralizado que se utilizará para recolectar la información de ataques que detecten las herramientas desarrolladas por los miembros del proyecto.

Toda la información recolectada en el servidor es compartida entre todos los miembros que tengan acceso al servidor central y ayuda a generar estadísticas y obtener muestras de actividad maliciosa para estudio de las mismas por otros miembros.

PROYECTO honeynet UNAM CHAPTER

La función del mapa es mostrar toda la información que recibe el servidor central en tiempo real, es decir, ataques que están ocurriendo en este momento. Para lograr su objetivo, se realizan una serie de acciones para transformar la información a coordenadas del mundo, mostrando la ubicación en donde se generó el ataque y la ubicación en donde se detectó este ataque.

Los Honeypots que reportan al mapa son de ataques web, ataques SSH y los resultados de captura del malware. Este mapa muestra a los usuarios una visión más clara de ataques reales que están sucediendo a lo largo del mundo.

El mapa consta de tres partes a destacar.

• Los puntos amarillos indican la ubicación geográfica de la herramienta que detectó el ataque.
• Los puntos rojos indican la ubicación geográfica en donde se originó el ataque.
• Un recuadro en la parte superior en el cual se indica la hora y la herramienta que detectó el ataque seguidos de la ciudad, país y coordenadas atacantes; posteriormente la ciudad, país y coordenadas en donde se detectó el ataque.

El UNAM-Chapter participa en este mapa por medio de la implementación de las herramientas de detección desarrolladas por los miembros del proyecto y su correcta configuración de envío al servidor de recolección centralizado. Esto posiciona al UNAM-CERT dentro de la colaboración con el proyecto y su interés por mejorar sus capacidades de detección y así mantener informada a la comunidad.

Firmas o identificadores de malware, tendencias de ataques.
Generar una base de datos completa de Honeynet.
Ser los primeros del país en aparecer en el mapa.

La iniciativa de haber implementado un mapa de ésta índole ayuda a la comunidad a tener una visión más acercada a los ataques cibernéticos que ocurren día a día en el mundo.

Día de Limpieza

Lic. Tonatihu Sánchez Neri

Anualmente se celebra el “Sweep Day” o “Día de Limpieza”, un ejercicio internacional, que consiste en la navegación en Internet simultánea en varios países para monitorear de manera aleatoria diversos sitios electrónicos con el fin de verificar si éstos cumplen con lo estipulado en los Lineamientos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la Protección de los Consumidores en el Contexto del Comercio Electrónico y en lo particular, con la Ley Federal de Protección al Consumidor (LFPC). De esta forma se ubican prácticas potencialmente engañosas, injustas o fraudulentas para los consumidores.

Por lo anterior, este día es dedicado a buscar exhaustivamente páginas web con las características mencionadas y así contar con una lista de sitios sospechosos sobre los que se puedan emprender acciones para minimizar el impacto negativo hacia los consumidores.

La Red Internacional de Protección al Consumidor y Aplicación de la Ley (ICPEN, por sus siglas en inglés) es una organización compuesta por las autoridades de protección al consumidor de aproximadamente 40 países. Su objetivo es facilitar las acciones de cooperación internacional para combatir las prácticas de comercio transfronterizo que puedan afectar a los consumidores.

El ICPEN propuso que el Sweep Day de este año, que se realizó en la semana del 17 al 21 de septiembre de 2012, se centre en el tema “¿Qué compré? Identificando la divulgación de información engañosa e inadecuada en los mundos en línea y móvil”.

La Procuraduría Federal del Consumidor (PROFECO), al ser miembro activo de la ICPEN, participa en este ejercicio desde 2003 contando en diversas ocasiones con el apoyo de otras instituciones. Una de ellas es la DGTIC-

UNAM a través de la Subdirección de Seguridad de la Información/UNAM-CERT.

El ejercicio realizado por UNAM-CERT de la DGTIC-UNAM consistió en la búsqueda de mensajes de correo electrónico con temáticas de venta de servicios y productos en línea. La búsqueda se centró en 81,626 correos considerados como spam dirigidos a usuarios del correo unam.mx del 18 al 21 de septiembre del 2012.

A continuación se numeran los pasos realizados:

1. Se realizó un conteo del número de mensajes en los que aparecía cada “asunto” (subject) de correo y se generó una lista ordenada descendentemente conforme a la cantidad de mensajes.
2. De la lista anterior se seleccionaron los asuntos relacionados con ofertas, venta de productos o servicios y publicidad en general.
3. Se hizo una revisión de un mensaje por cada asunto seleccionado en el punto anterior y se realizó una nueva lista con los que contenían publicidad engañosa.
4. Tomando en cuenta estos últimos, en el cuerpo del mensaje se buscaron enlaces a sitios de venta de productos y servicios que representaran un riesgo para el usuario.
5. En los enlaces obtenidos en el punto anterior se hizo un conteo de los dominios más comunes.
6. Finalmente, se realizó una estadística de los países de donde provenían los mensajes analizados.

Resultados

La siguiente tabla muestra un extracto de los asuntos seleccionados en el punto 2 del desarrollo: (Figura 1)

Se muestra un extracto de los asuntos seleccionados en el punto 3 del desarrollo en la siguiente tabla: (Figura 2)
Por cada asunto se revisó el cuerpo del mensaje, identificando aquellos que contenían enlaces a sitios con publicidad engañosa.

#mensajes	Asunto
2799	'Check our prices'
1937	'Lady Gaga y Evanescence en concierto 2012'
1408	'Important notice'
724	'Salidas Grupales Royal Decameron - Nvo Vallarta'
697	'Estudie un Magister Online en Chile desde cualquier parte del mundo'
658	'SUPER PACK DIDACTICO INFANTIL'
610	'Curso: Prevencion de Demandas Laborales'
504	'Tecnicas Super Efectivas de Cobranza'
503	'Certificacion Oficial de Subastas Electronicas Compranet 5.0 Plus'
486	'Celebra las fiestas patrias en tu destino favorito'
478	'Secretos para Vender por Telefono'
413	'Este Otoño vive la experiencia Paradisus Playa del Carmen'
395	'Licitaciones Electronicas Compranet 5.0'
270	'Sistema COMPROBADO para Incrementar Ventas.'
258	'2012 Chevy and Ford Clearance Event'
175	'Combustivel Gratis | Louis Vuitton 179 | Galaxy S3| UltraBook 799 | Iphone 4S 599 | Kipling 149'
166	'SUPER PACK VIDA SANA '
144	'News_1.00_a Day Buys 500,000 of Life Insurance'
133	'Tenemos Nuevos CLIENTES para ti . . .'
123	'Curso de Nominas 2012'
113	'Have you had a mesh implant?'
112	'Rebates 2012 Finder cars n trucks'
101	'Lowered Rates,__Relaxed Requirements__'
101	'Millonaria de Verano'
100	'Adquiere tu propia Tienda Virtual'
95	'Esta Primavera, disfrutala junto a EstiloSpa.com · PROMOCIONES EXCLUSIVAS'
95	'Puede ser su pasaporte a una vida de millonario'
80	'Galaxy S3|Prada | Louis Vuitton | Chanel | D&G | Gucci | Fendi | Dior | Nike| Iphone-5 Slim'
80	'Nuevas ThinkPad. Preventa exclusiva a un precio excepcional.'
76	'Football is Here!!_DISH_Over 900 channels__'

Fig. 1. Lista asuntos relacionados con ofertas, venta de productos o servicios y publicidad en general

Tomando en cuenta los sitios a los que se dirigía

#mensajes	Asunto
2799	'Check our prices'
1408	'Important notice'
258	'2012 Chevy and Ford Clearance Event'
144	'News_1.00_a Day Buys 500,000 of Life Insurance'
113	'Have you had a mesh implant?'
112	'Rebates 2012 Finder cars n trucks'
101	'Lowered Rates,__Relaxed Requirements__'
101	'Millonaria de Verano'
100	'Adquiere tu propia Tienda Virtual'

Fig. 2. Lista de sitios con publicidad engañosa

al usuario en los mensajes con publicidad engañosa, se presenta a continuación un listado de los dominios más numerosos:

Cabe destacar que la mayoría de sitios visitados resultaron ser sobre venta de medicamentos en línea, además de sitios que dirigen a los usuarios a encuestas con la promesa de que el usuario podrá "ganar" productos de moda.
Con los datos anteriores obtenemos el

# de Mensajes	Dominio
355	doctoranim.ru
320	insurequestertech.us
304	matterresolverspius.us
300	doctorwind.ru
269	doctorpenc.ru
267	doctorinst.ru
262	doctorbrai.ru
252	systemschartingpress.us
243	doctorsout.ru
229	doctorgeor.ru
228	rebatescentredrives.us
228	entrygrantedhere.us
228	instacarswappers.us
215	doctorchef.ru
209	doctorwash.ru
202	doctorfarm.ru
201	medickanga.ru
200	liveresultsfastest.us
197	doctorvoya.ru
193	doctorrang.ru
190	doctoriron.ru
188	doctorshov.ru
187	medicarchi.ru
186	doctortank.ru
184	doctorspan.ru
184	medicspain.ru
182	doctorempi.ru
180	requestlifeqoutes.us
171	doctorforc.ru
171	medicalgeb.ru
164	doctorperi.ru
162	mediccub.ru
161	doctorcoas.ru
156	doctoroyst.ru
155	doctormacr.ru
153	iranmedic.ru
150	doctorrand.ru
139	doctorphil.ru
137	doctortoma.ru
132	doctortort.ru
126	doctortarg.ru
117	managefixerstake.us
117	lifehelpinglines.us
108	dealsfordriverplus.us
104	doctoracto.ru
99	medicnoteb.ru
93	medicvisit.ru
91	doctorbage.ru
91	medicblade.ru
75	entryselectionspass.us
67	medicshear.ru
51	clearnacerackdrives.us
41	doctornurs.ru
39	drivercouponshere.us
6	medilifecompares.us

Gráfico 1. Listado de dominios con publicidad engañosa

porcentaje de mensajes que se identificaron como engañosos para los usuarios, como lo muestra el siguiente gráfico:

Gráfico 1. Porcentaje de mensajes de publicidad válida y publicidad engañosa

Respecto al origen de los mensajes, el gráfico siguiente muestra los 10 países de los que provienen más mensajes:

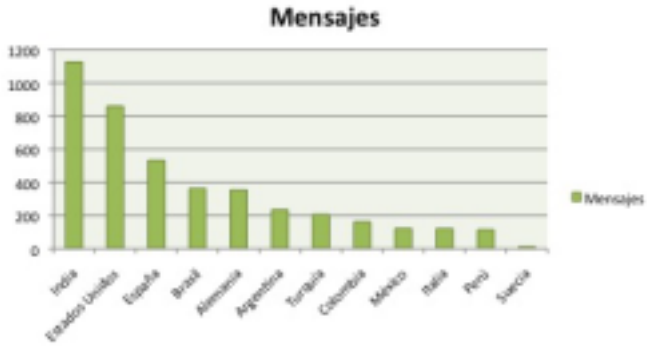


Gráfico 2. Países donde se originan más mensajes de publicidad engañosa

Los resultados del gráfico anterior son interesantes ya que, aunque era de esperarse que India y Estados Unidos aparecieran entre los primeros lugares, sorprende la aparición de países como España y Alemania.

En un ejercicio de limpieza como el descrito en este artículo, se buscan identificar sitios en Internet que representen la posibilidad de que el consumidor sea defraudado, ya sea porque las condiciones de venta no sean muy claras o los

productos ofrecidos, aunque pretendan ser de marca, sean de mala calidad al ser falsificaciones.

Este tipo de análisis nos permite observar que el spam juega un rol primordial para llegar a los posibles consumidores, a pesar de caracterizarse por ser “no deseado”, el éxito de los spammers proviene del hecho de que las personas ceden a la tentación de comprar a precio rebajado productos como Viagra, un Rolex falso o en general productos con descuento que no podrían permitirse de otra manera. Respecto al producto recibido, éste puede funcionar o no, pero la mayoría de las veces corresponde al producto mostrado en el correo o en el sitio web. El spam se vuelve así un punto al cual poner atención para combatir las prácticas engañosas del comercio en línea.

Referencias:

https://icpen.org/

http://www.seguridad.unam.mx/noticia/?noti=300

http://www.seguridad.unam.mx/noticia/?noti=391

El nuevo paradigma de seguridad en redes inalámbricas

Ing. Erika Gladys De León Guerrero

El incremento en el uso de tecnologías móviles ha creado un aumento en el interés en protocolos de redes inalámbricas, atención que también se ha manifestado en el desarrollo de nuevos ataques y en el descubrimiento de vulnerabilidades. Con el aumento de la tecnología inalámbrica, crece también el atractivo ante individuos malintencionados que buscan obtener información sin autorización para modificar el buen funcionamiento de los dispositivos.

El objetivo de este artículo, es informar al lector sobre la protección de la información transmitida mediante estas tecnologías inalámbricas y su disponibilidad, buscando también un acercamiento a la explicación de diversas técnicas de explotación complementarias al artículo divulgado en la edición 11 de esta revista ,en donde se habla de la obtención de credenciales mediante ataques sobre los protocolos de cifrado WPA/WPA2 o WEP.

Dado que la tecnología inalámbrica sobrepasa los límites físicos, en ocasiones, resulta difícil cumplir por completo con la triada de seguridad (confidencialidad, integridad y disponibilidad). Independientemente de una buena configuración, como lo podría ser WPA-Enterprise con el servidor RADIUS, existen riesgos inherentes a la tecnología; por mencionar algunos, ataques de denegación o degradación de servicio a Access Points (AP) o clientes, o la existencia de Rogue Access Points (AP falsos) que podrían tener como consecuencia el robo de credenciales y certificados para posteriormente ingresar de manera no autorizada a la red.

La inadecuada configuración y el cifrado vulnerable son comúnmente relacionados con problemas de seguridad de tecnologías inalámbricas, con los que frecuentemente se adquieren los servicios de Internet inalámbrico. Sin embargo, no todos los problemas de seguridad se solucionan con una configuración adecuada.

La problemática
Rogue Access Point o Evil Twin

Se define como un Access Point (AP) no autorizado que puede estar conectado a la red cableada de una institución , denominándolo **Rogue Access Point interno**, siendo administrado por alguien ajeno al rol autorizado. Tiene la característica de no cumplir con las políticas organizacionales y por lo general permiten el acceso a cualquier usuario sin credenciales.

Existe otro tipo, **Rogue Access Point externo**, que no está conectado a la red cableada de la organización, sin embargo, emula un dispositivo auténtico. Este ataque es muy simple, ya que basta con configurar un Access Point con las mismas características del dispositivo genuino, incluyendo ESSID (Extended Service Set IDentifier o nombre de la red) y características de cifrado. Uniendo a esto un incremento de la intensidad de la señal, se provocaría que los clientes soliciten autenticación al dispositivo falso haciendo posible ejecutar otros ataques que incluyen la obtención de credenciales, monitoreo no autorizado de la red, robo de cookies entre otros. Este problema es ocasionado debido a fallas en el protocolo de autenticación Access Point - cliente, ya que se presenta en usa sola vía, es decir, el AP autentica al cliente, pero el cliente no verifica la autenticidad del AP.

Tenable Security define los siguientes tipos de Rogue Access Point :

1. Wireless router conectado vía una interfaz trusted: el Access Point es conectado en algún lugar confiable de la red interna, generalmente habilitando DHCP, acción que puede causar conflicto con el DHCP interno. Por lo general, este tipo cuenta con todos los servicios habilitados (HTTP, SNMP, etc.) y es más peligroso ya que el intruso puede tener acceso en un rango más amplio.

2. Wireless router conectado vía una interfaz untrusted: Se encuentra del lado untrusted o externo del firewall o del router. Por lo general cuenta con pocos servicios por lo que hace difícil su detección en la red.

3. Instalación de una tarjeta inalámbrica en un dispositivo conectado en la trusted LAN: Aunque se requiere acceso físico, se podría instalar una tarjeta inalámbrica y configurarla como Access Point. La mayoría de los chipsets, dispositivos y sistemas operativos actuales permiten realizar esta función.

4. Activación inalámbrica en un dispositivo ya existente conectado en la trusted LAN: Es el mismo caso que el anterior, con la diferencia de que aquí se emplea la infraestructura inalámbrica ya existente en el dispositivo, lo que facilita el ejercicio. Un ejemplo para la ejecución de este tipo de técnica de explotación es la herramienta airbase-ng combinada con karmetasploit (Figura 1 y 2).

Karmetasploit es un plugin de metasploit, que usado junto con airbase-ng, permite crear una red falsa y abierta para incitar a la conexión de los clientes que quieren obtener Internet gratis. Tras conectarse, ejecuta una serie de técnicas que podrían robar las cookies, obtener contraseñas de distintas aplicaciones y, si el sistema operativo tiene alguna vulnerabilidad, trata de explotarla y obtener un shell.

-P El AP falso responde todas las pruebas sin importar el ESSID especificado
-C 30 Enviará beacons de prueba durante 30 segundos.
-e "test" Se especifica el nombre de la red
-v modo verbose
mon0 interfaz inalámbrica en modo monitor

En la Figura 1 únicamente se está creando el AP falso abierto.

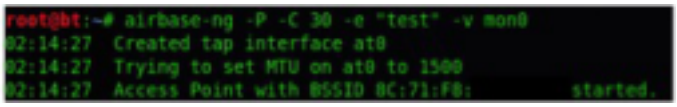


Figura 1. AP falso

En la figura 2, se muestra la ejecución de karmetasploit, que realiza la captura de información y ejecuta las técnicas de explotación hacia los clientes conectados. Lo único que resta es esperar la conexión de un cliente para almacenar su información.

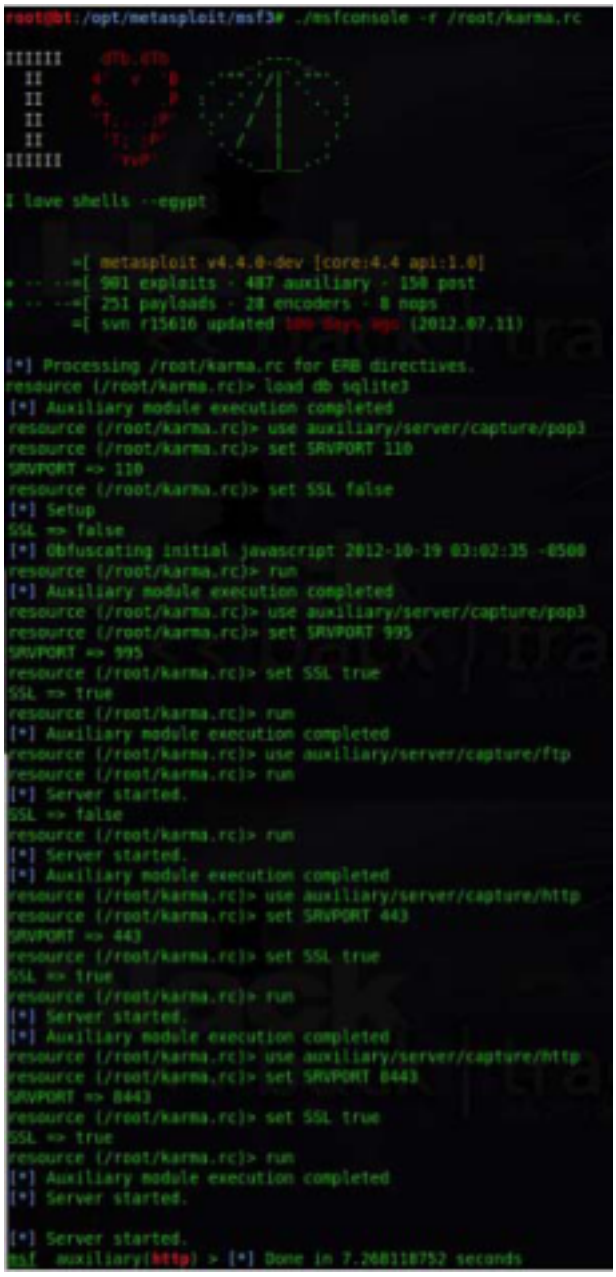


Figura 2. Karmetasploit

MAC address spoofing

Un Access Point podría ser configurado para permitir el acceso solamente a las direcciones MAC almacenadas en una lista, sin embargo, un atacante podría modificar esta dirección con la intención de obtener acceso, es posible realizar este tipo de técnicas con herramientas como Win 7 MAC Address Changer. (Figura 3)

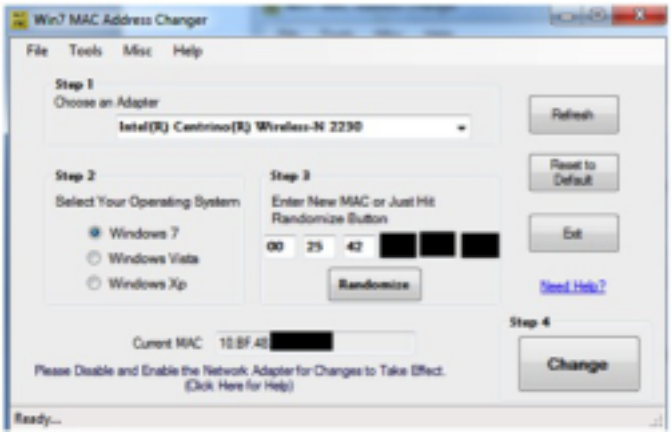


Figura 3. MAC Address Change

Denegación de Servicio (DoS)

Un ataque de denegación de servicio ocurre cuando un Access Point no puede brindar servicio a clientes autorizados, debido a una inundación de peticiones de clientes no autorizados. Existen distintas variantes:

Jamming: generar señales aleatorias en frecuencias específicas.

Inundación con asociaciones: El AP tiene una tabla de asociaciones que cuenta con un número limitado de entradas, si se llena esta tabla, el dispositivo no puede atender más solicitudes de asociación.

Disociación provocada: El atacante envía tramas de disociación falsas con direcciones MAC modificadas, el cliente puede enviar tramas de autenticación y regresar al estado anterior, pero el atacante puede continuar enviando tramas de disociación por un periodo, evitando la re-asociación.

De-autenticación provocada: Este ataque es similar al anterior, pero enviando tramas de de-

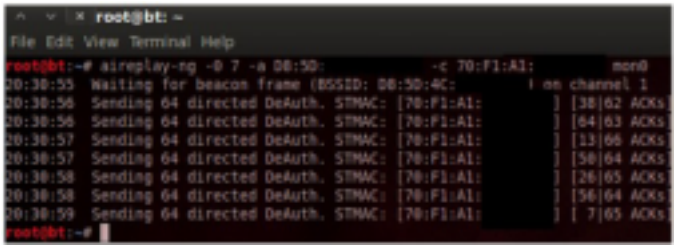


Figura 4. DoS De-autenticación

autenticación (Figura 4). El ataque puede ir dirigido a un cliente en específico o a todos los clientes asociados al AP.

En la imagen se muestra el uso de aireplay-ng para enviar tramas de de-autenticación donde:

-0: enviar tramas de de-autenticación.
-a: dirección MAC del AP
-c: dirección MAC del cliente asociado
mon0: interfaz

La solución

Una vez analizado el problema, es fácil comprender la naturaleza de la solución, que sí bien puede disminuir el riesgo la aplicación de buenas prácticas de seguridad, no lo elimina por completo.

Existen soluciones especificas para redes inalámbricas que permiten la detección y corrección de algunos de los problemas antes mencionados, son nombrados Wireless Intrusion Prevention System (WIPS), trabajan de manera similar a in IPS (Intrusion Prevention System) tradicional, solo que enfocado a redes inalámbricas.

Hay que saber distinguir entre WIDS (Wireless Intrusion Detection System) y WIPS, así como ocurre con los dispositivos tradicionales, un WIDS solamente realiza la detección de problemas de seguridad mientras que un WIPS realiza la detección y mitiga al mismo tiempo, es decir, toma acciones con respecto a políticas previamente creadas.

La arquitectura típica de un WIPS tiene los siguientes elementos:

Sensores: Monitorean y realizan la captura de la actividad.
Servidores de administración: Analizan la información enviada por los sensores.
Servidor de base de datos: Almacena los eventos generados por el servidor de administración.
Consola: Es la interfaz para la administración del sistema.

Los sensores se deben distribuir con base en el tiempo para monitorear los distintos canales por un determinado periodo, por lo que sería necesario el uso de múltiples sensores o bien, de sensores especiales para realizar el monitoreo permanente de todos los canales.

Probablemente, lo primero que llega a la mente cuando se habla de este tipo de tecnologías es el factor económico, sin embargo, existen soluciones de software libre que podrían ayudar a resolver los mismos problemas.

Por parte de las opciones de software libre, existe openwips-ng creado por el autor de la suite aircrack-ng (Thomas d´Otreppe de Bouvette, quien expuso su proyecto en el Congreso de Seguridad en Cómputo 2011), es un sistema de detección y mitigación segmentado en módulos (sensor, servidor e interfaz), actualmente está en construcción, sin embargo, ya hay una versión beta disponible. Para mayor información se puede recurrir a http://openwips-ng.org/.

Como parte de las ponencias del Congreso de Seguridad en Computo 2011, se expuso con mayor detalle el desarrollo y funcionamiento de un WIPS de creación propia , desarrollado con apoyo de la suite airckrack-ng, el cual se basa en el monitoreo y análisis de tramas con la intención de encontrar comportamientos maliciosos, el cual toma acciones con respecto al tipo de ataque detectado.

De acuerdo al cuadrante de Gartner de soluciones comerciales WIPS, se tienen las siguientes opciones marcadas como líderes en orden alfabético:

- AirTight Networks
- Aruba Networks
- Cisco
- Fluke Networks
- Motorola

Los criterios de evaluación principales fueron los siguientes:

Experiencia del cliente: Simplicidad, flexibilidad, capacidades de operación y soporte.

Viabilidad integral: Financiera, estratégica, organizacional, de negocio.

Producto/servicio: Amplitud de características, capacidades de detección y prevención, integración, monitoreo, reporte.

Las capacidades generales de este tipo de dispositivos son las siguientes:

- Identificación de tráfico malicioso en el aire
- Detección de Rogue Access Point
- Identificación física de dispositivos WiFi vulnerables
- Protección de ataques de fragmentación
- Detección de ataques de de-autenticación
- Detección y bloqueo de clientes no autorizados
- Detección y bloqueo de conexión de clientes confiables a redes externas
- Detección y bloqueo de conexión sin autorización de dispositivos móviles
- Adaptación a políticas organizacionales
- Detección de configuración inadecuada de la red
- Detección de patrones de uso inusual
- Detección de escaneo activo de redes inalámbricas
- Detección y bloqueo de ataques de de-negación de servicios
- Detección y bloqueo de ataques de hombre en medio (MitM)

El uso de redes inalámbricas implica riesgos inherentes a la tecnología que no son solucionados con la aplicación de buenas prácticas de seguridad, por lo que surge la necesidad de dispositivos WIPS que ayudan a disminuir el riesgo y a eliminarlo en algunos casos. A pesar de que no existe una amplia gama de dispositivos de este tipo, hay buenas opciones a las que es posible recurrir.

Referencias

•Katrin Hoeper and Lily Chen. NIST Special Publication 800-120. Recommendation for EAP Methods Used in Wireless Network Access Authentication. 2009.

•sitio Openwips-ng http://openwips-ng.org/

•Karen Scarfone, Peter Mell, NIST 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), Feb 2007

•Ken Hutchiunson, Wireless Intrusion Detection Systems, SANS Institute, October 2004.

1http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Seguridad_Num_11_0.pdf

2 Fuente airtight networks http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf

3 Teneable Security es considerada una compañía líder en materia de seguridad creadora de Nessus Vulnerability scanner, una de las herramientas más importantes para escaneo de vulnerabilidades. http://blog.tenablesecurity.com/2009/08/using-nessus-to-discover-rogue-access-points.html

4 http://www.metasploit.com/dev/trac/wiki/Karmetasploit

5http://congreso.seguridad.unam.mx/2011/memorias/files/s_ThomasdOtreppe.pdf

6http://congreso.seguridad.unam.mx/2011/memorias/ponencias.dsc

Riesgo tecnológico y su impacto para las organizaciones parte II Gobierno de TI y riesgos

Ing. Alexandra Ramírez Castrol

Palabras clave:
COBIT, gestión de riesgos, gobierno de TI, métricas para riesgos.

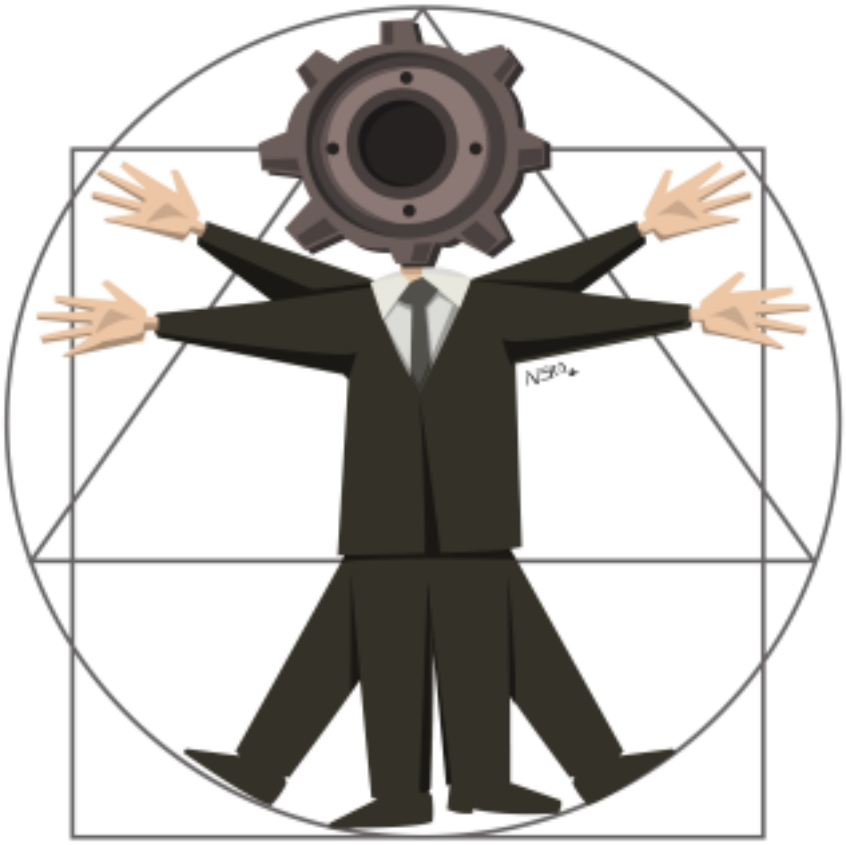
En el artículo anterior, se habló del origen del riesgo tecnológico, de cómo afecta a las organizaciones y las medidas que pueden ser tomadas para mitigarlo; además de tratar algunos casos reales sobre cómo el riesgo tecnológico es fuente de otro tipo de riesgos.

En la presente entrega, se abarca el riesgo tecnológico dentro del gobierno de TI, haciendo referencia al marco COBIT para indicar la importancia de su trato como riesgo fuera del ámbito estricto del riesgo operativo.

Papel dentro del gobierno de TI

Cuando se habla de tecnología y de mantener la seguridad sobre ésta, fácilmente se piensa en términos de protección física, lógica y protección sobre los sistemas y equipos. Solo al final se trata lo referente a medidas técnicas. Sin embargo, esta seguridad es limitada y debe ser respaldada por una gestión y procedimientos adecuados; de aquí la importancia de alinear estas medidas con las estrategias del negocio.

A partir de esto, aparece el concepto de gobernanza de TI o gobierno de TI (GTI), que busca la alineación de las tecnologías de la información y las comunicaciones con las estrategias del negocio. De esta forma, se aplican las mejores prácticas de administración con el fin de ayudar en la toma de decisiones, mientras se proporciona el mejor uso de la tecnología.



Por ello, el gobierno de TI tiene como objetivo entender la importancia estratégica de TI para mantener las operaciones e implementar las actividades que se requieran a futuro.

Este gobierno integra procesos y recursos de TI con la información de las estrategias y objetivos de la organización, la finalidad es alcanzar estos objetivos añadiendo valor al negocio con el debido equilibrio sobre los riesgos y el retorno de inversión sobre TI y sus procesos.

En el año 1996, la asociación ISACA (Information Systems Audit and Contol Association, Asociación de Auditoría y Control en Sistemas de Información) teniendo en cuenta que el gobierno de TI requería un marco de referencia para lograr los fines expuestos, lanzó COBIT (Control Objetives for Information and Related Technologies, Control de Objetivos para Información y Tecnologías Relacionadas) que ofrecía principios para gestionar la tecnología dentro del gobierno de TI.

El marco de trabajo de COBIT, en su versión 4.1, brinda buenas prácticas a través del manejo de dominios y procesos, con el cual se plantean los objetivos de control para la información y tecnología relacionada que permita a las organizaciones mantener vigilancia respecto a los requerimientos del negocio y gestionar los recursos de tecnología. De esta forma, se busca alinear las metas organizacionales con las metas de TI.

Así, dentro del dominio, planeación y organización, el proceso PO9 hace referencia a la evaluación y administración de los riesgos de TI, donde se busca documentar en un nivel común y acordado, estrategias de mitigación y riesgos residuales de acuerdo a los límites definidos por las directivas. La idea es identificar, analizar y evaluar impactos potenciales sobre las metas de la organización. Al aplicar esto, se logra garantizar que la administración de riesgos se incluye dentro de todos los procesos administrativos y se establecen planes de acción para la mitigación, teniendo en cuenta las recomendaciones de todos los niveles organizacionales y la divulgación sobre los mismos.

Para la última versión de COBIT 5, generada este año, se toma la gestión de riesgos como un objetivo de gobernanza para la creación de valor, buscando la optimización de riesgos, haciendo el mapeo de estos junto a la optimización de

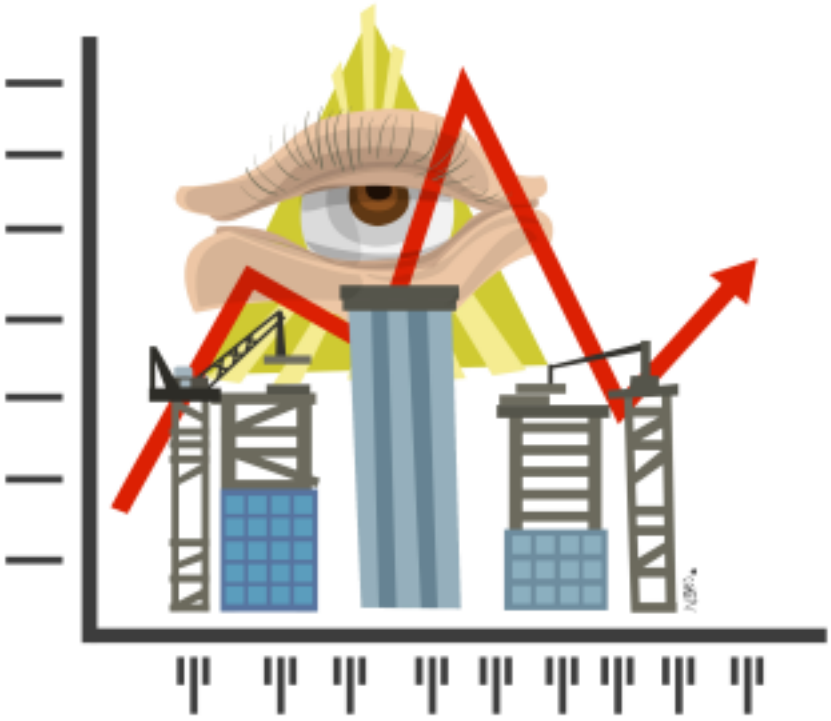
recursos y el realce de beneficios a las metas organizacionales de información y tecnología. La finalidad es cumplir con procesos, capacidad en servicios, habilidades, competencias, principios y políticas, información, estructura organizacional, además del ambiente ético y cultural requerido .

Esta versión de COBIT dentro del dominio APO (alineación, planeación y organización), contiene un proceso de riesgos APO12 (gestión del riesgo), en el cual se integra la gestión de riesgos empresariales relacionados con tecnología, con la evaluación, dirección y monitoreo (EDM) de la organización. Además tiene un enfoque en los riesgos de los terceros.

Para lograr esta gestión, se requiere contar con los planes estratégicos y tácticos de TI, junto al portafolio de servicios, los planes de riesgos a nivel de proyecto, riesgos asociados a los proveedores, resultados de pruebas de contingencia e histórico de riesgos. Con esto, lo que se busca es la definición de planes de acciones correctivas para riesgos de TI y la definición de directrices de administración que puedan surgir de la evaluación de riesgos. El objetivo es llegar a una administración de nivel óptimo en donde se ve la implantación de la gestión de riesgos en toda la organización, bajo una buena administración. Con todas las medidas de buenas prácticas, procesos automatizados y la debida revisión y mejora continua por parte de las directivas.

Es importante definir algunas premisas cuando se gestionan riesgos, sin importar si son de tipo tecnológico u otros y cuando se habla de implementar medidas de seguridad dentro de las organizaciones. Dentro de estas están:

• Apoyo y aval de la alta gerencia o administración. Sin esto no tiene sentido el proyecto de seguridad.
• Definición de los responsables del desarrollo, implantación y gestión de las medidas acordadas.
• Alineación de las medidas definidas con los objetivos y la cultura organizacional. Al igual que con las definiciones de procesos de seguridad y gestión de riesgos a otros niveles, se realiza con el fin de encontrar un marco general e integral que dicte los principios y normas de la gestión para toda la organización.
• Procesos de comunicación y retroalimentación bien definidos que permitan el flujo adecuado para realizar la gestión.
• Mantenimiento y mejora continua de la gestión para realizar ajustes y cambios pertinentes en los momentos idóneos. Esta gestión debe realizarse mediante la medición, dado que es la única forma de confirmar el funcionamiento e



implantar medidas para mejorar. Por lo anterior, el uso de métricas es relevante. La idea es recolectar, analizar y reportar datos de desempeño relevantes.

Por ejemplo, pueden usarse factores como el porcentaje de riesgos mitigados de una auditoría a la anterior, número de unidades de negocio en las cuales se han identificado riesgos, controles definidos por unidad, asignación de recursos por unidad de negocio proporcionales a la ganancia o riesgo, entre otras; y con ello definir acciones de mejora y acciones correctivas. De igual forma, las métricas definidas pueden definirse en tres tipos: métricas de impacto, métricas de efectividad o eficiencia y métricas para medir la implantación de medidas . Para verificar o comparar la efectividad de la gestión de riesgos y seguridad puede tomarse como referencia el modelo de madurez de COBIT , a través del proceso de certificación en ISO 27000 y revisando la norma ISO 27004, que trata sobre métricas y medidas.

Concluyendo, la gestión de riesgos tecnológicos en la actualidad, dada la masificación de la tecnología en las sociedades y todo lo referente a la sociedad de la información, nos implica brindar mayor atención a los riesgos tecnológicos. Más allá de las medidas técnicas que se tomen para su mitigación, hacerlo desde la gestión misma a nivel directivo, con la finalidad de no hacer de ésta, un simple medio o una barrera para lograr niveles óptimos de seguridad.

Para información adicional sobre el riesgo tecnológico y su actuar en las sociedades consultar:

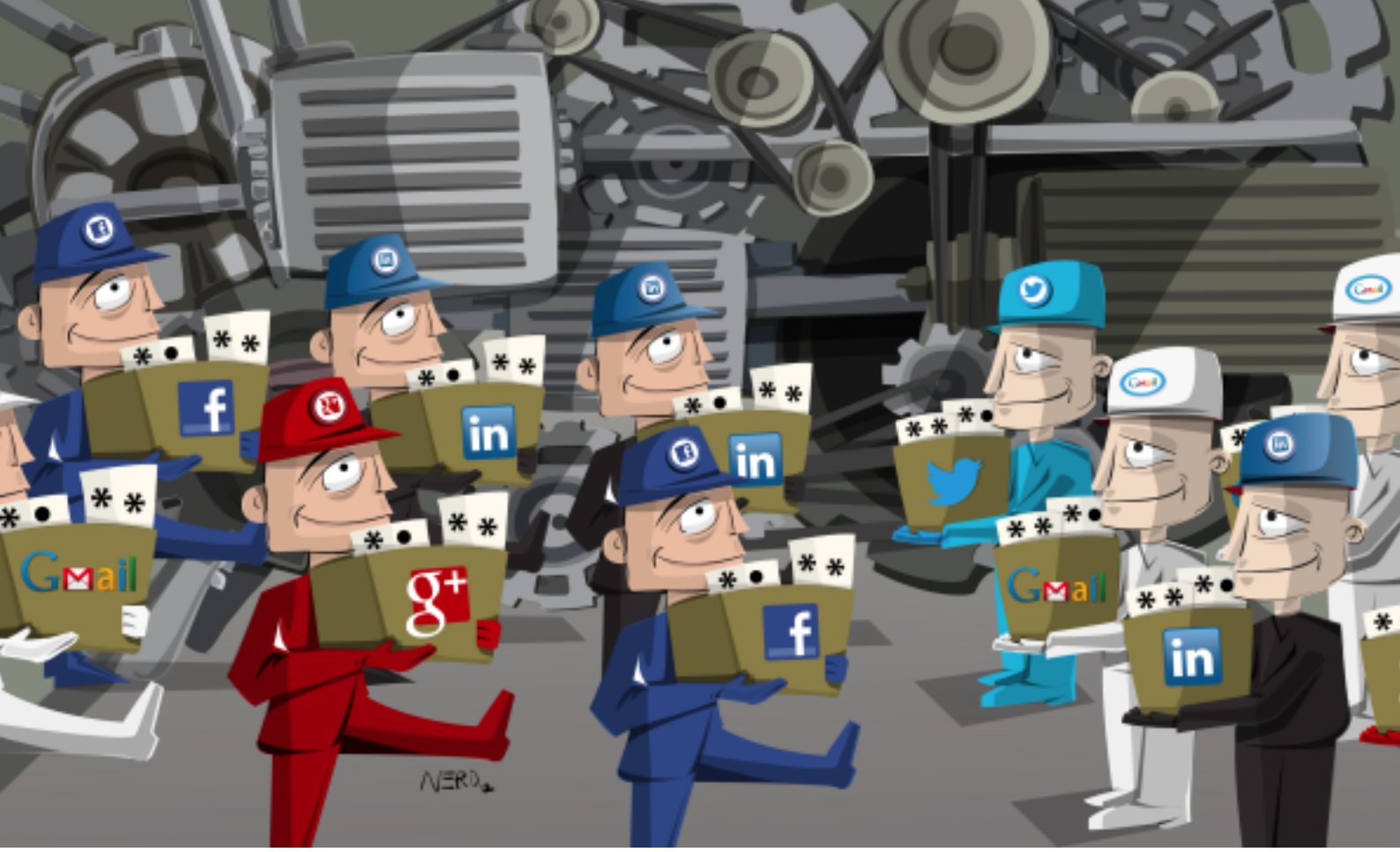
• Filosofía de la tecnología y Riesgo Tecnológico. Una confrontación con los riesgos y las tecnologías:http://ecotropicos.saber.ula.ve/db/ssaber/Edocs/pubelectronicas/agoratrujillo/Agora8/ivan_mateos.pdf

•Riesgos de Origen Tecnológico: apuntes conceptuales para una definición, caracterización y reconocimiento de las perspectivas de estudio del riesgo tecnológico: http://200.21.104.25/lunazul/downloads/Lunazul29_9.pdf
•World Economic Forum, Global Risks 2012: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

Referencias

[1] Instituto de Gobierno de TI. COBIT 4.1., Marco de Trabajo - Objetivos de control – Directrices Generales – Modelos de Madurez, 2007.
[2] Instituto de Gobierno de TI. COBIT 5. A Business Framework for the governance and management of enterprise IT, 2012.
[3] ISO (International Standard Organization). Estándar de Seguridad ISO/IEC 27002. Tecnología de la Información – código de prácticas para la gestión de la seguridad de la información, 2005
[3] HARRIS, Shon, CISSP Certification Exam Guide, Tercera edición, McGraw-Hill, 2005.

1 El valor al negocio puede interpretarse desde diferentes perspectivas: es aquello que le puede retribuir algún tipo de beneficio o ganancia a la organización; puede ser en términos económicos, capital intelectual, imagen, entre otros.
2 Para mayor información sobre el nuevo marco de COBIT http://www.isaca.org/COBIT/Pages/default.aspx y http://www.slideshare.net/CarlosFrancavilla/cobit-5-comparacion-con-cobit-41
3 Para mayor información sobre el proceso de desarrollo de métricas consultar NIST SP-800-55
4 Plantea 6 niveles de madurez (de 0 a 5) desde no existente a optimizado.
5 Requerimientos para implantación de un sistema de seguridad de la información ISO 27001 y buenas prácticas para implantación de controles ISO 27002.



Password-fu: Guía fácil para contraseñas realmente seguras

Sergio A. Becerril

"Debes utilizar contraseñas seguras" Viejo mantra de seguridad

¿Cuántas veces hemos escuchado esta recomendación? Si has asistido a un curso, leído artículos (incluso los de esta revista) o tal vez escuchado un poco del tema de la seguridad informática, es casi seguro que has recibido este consejo más de una vez. Es una receta clásica que como los consejos de la abuelita, son más sencillos de decir que de seguir.

Pues bien, no te preocupes más. La siguiente es una sencilla guía de 3 pasos para que tus contraseñas sean (y se mantengan) siempre seguras. Explicaré un poco la razón detrás de estas recomendaciones, algunos puntos adicionales a considerar y cómo, tomados en conjunto, te ayudarán a resistir la mayoría de los embates contra tu seguridad.

1. Nunca utilices datos personales para crear tu contraseña

Recordemos que el propósito de las contraseñas es evitar accesos indeseados, no queremos que cualquiera pueda leer nuestro correo, por ejemplo. Si utilizas información personal para crear tu contraseña (tu calle y número o tu fecha de nacimiento), estás aumentando la probabilidad de que alguien la adivine, ya que esta información es 1) fácil de obtener, pero sobre todo 2) muy comúnmente utilizada en contraseñas.

2. Una frase es mucho mejor que una 'contraseña'

- Pero (me dirán), ¿voy a tener que utilizar algo como 'b&kqAp5H' de contraseña? ¡Nadie se acuerda de esas cosas!- (con cierta razón).

Las supuestas contraseñas “seguras” son un ejemplo de buenas intenciones y pésimos métodos, porque los humanos no somos máquinas. Una persona recuerda algo mucho mejor si ese algo tiene sentido, una relación con su vida, etc. Después de todo, así funcionan nuestros cerebros.

Lo que es más, esa contraseña no es tan segura como parece. Además del (muy real y muy común) riesgo de ser apuntada en un post-it (algo así como dejar las llaves de la casa colgadas afuera de la entrada) un atacante con los medios apropiados la descubrirá en un santiamén. Específicamente, en 12 horas o menos .

¿Cuál es la solución entonces? Mi sugerencia: una frase de contraseña.

Consideremos la siguiente frase:

“Todos los días, gimnasio a las 8”

Tal vez es parte de tu rutina diaria o es un propósito de año nuevo. Como sea, una buena parte de ustedes se habrán identificado con esta frase. Y eso buscamos para no olvidarla. Ahora, ¿cómo utilizamos esto como contraseña? Muy sencillo. Quita acentos, espacios y escribe:

Todoslosdias,gimnasioalas8

Sorprendentemente, esta contraseña es ***un millón de cuatrillones de veces más segura*** que la que escribí al principio de esta sección -algo así como comparar una caja fuerte con una cajita de papel-. El mismo atacante que vulneró nuestra contraseña anterior en 12 horas tardaría miles, millones de años en encontrarla.
Tiene suficiente relación con nuestra vida como para recordarla fácilmente, pero no lo suficiente para que alguien la adivine.

Cada quien tendrá su propia fuente de inspiración para sus frases. Algunos utilizan frases de libros; otros, refranes populares. Conviene evitar una frase muy famosa; busca algo memorable únicamente para ti. La clave es la longitud: mientras más larga, mejor. Con 5 o 6 palabras usualmente basta. Esto lo discutimos a mayor detalle al final de este artículo, en la sección “el tamaño sí importa”.

Lamentablemente, habrá sitios que no te permitirán contraseñas tan grandes

(Outlook.com, anteriormente conocido como Hotmail, es uno de los principales culpables). Mi recomendación: abandona el servicio, o quéjate. Si es imprescindible que utilices el servicio utiliza una contraseña tan grande como te permita el sistema (en el caso de Outlook, el límite son 16 caracteres), pero considera al servicio como trascendentalmente inseguro.

3. Acomoda, rota y anota

¡Muy bien! Ya tenemos una guía para crear contraseñas seguras, que además son fáciles de recordar. Sin embargo, nos falta atender el resto de las recomendaciones comunes:

"Nunca utilices la misma contraseña en diferentes sitios"
"Debes cambiar tus contraseñas periódicamente (e.g. cada año)"
"Jamás apuntes tus contraseñas, mejor memorízalas"

Muchos expertos de seguridad me odiarán por lo que diré a continuación, pero la realidad es que puedes ignorar estas recomendaciones bajo ciertas circunstancias. Para ello, hay que entender qué se pretende con cada una y cómo podemos resolver cada problema con un enfoque diferente.

La razón por la cual se sugiere utilizar siempre una contraseña diferente es que, si un atacante logra obtener acceso a un servicio, podrá obtener acceso a otros sin mayor esfuerzo. En ocasiones, ¡no importa si tu contraseña es segura! Esto es porque a veces los atacantes logran vulnerar la seguridad de los proveedores y obtener acceso a todas las contraseñas. Un ejemplo es el reciente ataque a LinkedIn (junio 2012), donde las contraseñas de más de seis millones de usuarios de la red social fueron publicadas en Internet.

Aunque aquí la culpa yace en el proveedor, como usuarios podemos minimizar el riesgo. Utilizar diferentes contraseñas hace justamente eso, porque garantiza que, aunque un atacante logre tener acceso a uno de tus servicios, no llegará más lejos .

Cambiar periódicamente las contraseñas sirve a un propósito similar: no importa qué tan bueno sea un atacante, si cambias el objetivo (i.e. tu contraseña) regularmente, frustrarás sus intentos por vulnerar tu seguridad.

Finalmente, evitar apuntar las contraseñas es la recomendación más sencilla de entender: evita que alguien (accidentalmente o a propósito) obtenga tus credenciales con mínimo esfuerzo.

¿Cómo le damos la vuelta a esto? El primer paso es ***acomodar***. Debes acomodar todos los servicios que utilices con base a dos preguntas: ***¿Contiene información crítica? ¿Es una puerta para otro servicio?***

La primera solo tú la puedes responder. Cada quien tendrá su definición de información crítica, aunque generalmente te diría que es algo que no puedes arriesgarte a perder (como tus declaraciones de impuestos) o a publicar (como tus correos privados). Recuerda que tu identidad también es muy valiosa. Considera, ¿qué podría lograr un atacante que obtuviera acceso a tu cuenta de Facebook, por ejemplo?

La segunda es más difícil de contestar. En esencia, una "puerta" es aquella cosa que te puede brindar acceso a otro servicio. El ejemplo clásico es tu cuenta de correo electrónico. ¿Por qué? Tu cuenta de correo electrónico se utiliza, entre otras cosas, para la recuperación de

Img. 1 Ilustración representativa

contraseñas de, probablemente, todos los demás servicios. Los atacantes saben esto y por eso consideran tu cuenta de correo uno de los premios más jugosos por obtener. Deberás buscar esas puertas y anotarlas.

Una vez que hayas hecho esto, podrás acomodar tus servicios respecto a su importancia. En mi caso (Imagen 1):

Al centro está mi servicio más preciado: mi cuenta de correo principal. Tiene información crítica y es puerta para el resto de mis servicios. Ligeramente menos importantes son mis accesos a mis redes sociales, mi banco y mi servicio de compras en línea (no son "puertas", pero sí tienen información crítica). Finalmente, mis servicios menos críticos (Netflix, Wordpress y Skype) están en el menor nivel de importancia.

Una vez acomodados tus servicios, puedes ***"rotar"***.

Piensa en cada "nivel" de tus servicios como un mundo en sí mismo. Dentro de ese nivel, no debes repetir contraseñas y debes cambiarlas periódicamente. Pero, en vez de crear nuevas contraseñas cada que quieras cambiar tus servicios, puedes rotarlas. En mi caso, tengo 4 contraseñas diferentes en el segundo nivel. Cuando llega la hora de cambiarlas, simplemente roto: la contraseña de Twitter se convierte en la contraseña de mi banco, la contraseña de eBay en la contraseña de Twitter, etc.

También puedes rotar entre niveles, de arriba hacia abajo. ¿A qué me refiero? Cuando llega la hora de cambiar la contraseña de la cuenta de correo, es evidente que debo ***crear*** una nueva contraseña (después de todo, es mi servicio más sensible – debo ser más cuidadoso). ¿Qué hacer con la contraseña anterior? ¡Puedo rotarla hacia abajo! Digamos, a mi Facebook. Esto causaría que una contraseña de este nivel rotara hacia abajo y así sucesivamente.

De esta manera, mis contraseñas tienen un largo tiempo de vida (¡varios años!), lo que facilita su memorización, sin que esto haga que mis servicios sean más inseguros. Por supuesto, en el momento que descubra que algún servicio ha sido vulnerado, esa contraseña desaparece completamente de la rotación.

Aún así nos queda un reto: recordar qué contraseña le toca a qué servicio. El famoso "post-it de la muerte" puede aquí ser utilizado a nuestro favor. ¿Por qué? Pues porque si utilizas frases de contraseña, puedes ***anotar*** referencias a las frases, en vez de las contraseñas en sí. Por ejemplo, utilizando nuestra frase de contraseña (Todoslosdias,gimnasioalas8) podríamos anotar algo como: correo – gimnasio.

Para un atacante, esto tiene poca utilidad – la sola presencia de la palabra gimnasio no ayuda mucho, porque no es la contraseña en sí. Sin embargo, para ti cumple su propósito – te permite recordar fácilmente que, si quieres ingresar a tu correo, debes utilizar la frase que utiliza gimnasio.

Suena cansado y difícil, pero recuerda que son solo tres fases:

a) ACOMODA tus cuentas en niveles de importancia
b) ROTA las contraseñas dentro de su mismo nivel o hacia abajo
c) ANOTA las referencias entre servicios y contraseñas

Solo para mecanógrafos: ¡desplaza tus manos!

Si eres mecanógrafo (es decir, que puedes escribir sin ver el teclado), este tip es para ti. Es tremendamente sencillo: desplaza tus manos uno o más lugares hacia la izquierda, derecha, arriba o abajo.

Por ejemplo, desplazando mis manos un lugar hacia arriba, puedo lograr que la contraseña que realizamos anteriormente:

Todoslosdias,gimnasioalas8
Se transforme en algo como esto:

%9e9wo9we8qwkt8jhqw89qoqw8

¡Inténtalo con tus propias contraseñas!

Y ahora... ¿qué sigue?

Siguiendo los tips anteriores, podrás memorizar más fácil tus contraseñas sin sacrificar nada en términos de seguridad. Estas ideas me han servido bien por más de 10 años y confío que las encontrarás útiles en el manejo de tus credenciales.

Un último consejo: todo esto es irrelevante si el sitio o sistema que utiliza tu contraseña es inseguro. Desconfía de sitios web que no utilicen https (busca un candadito en tu barra de direcciones; a veces es color verde, pero nunca debe ser color rojo) para procesar tus datos de inicio de sesión. Desconfía más de sitios que te piden contraseñas de tamaño pequeño. Si tienes dudas, utiliza una contraseña "desechable". Sobre todo, ejerce tu sentido común. Es buen consejo para cualquier reto en la vida.

Anexo. El tamaño sí importa

Constantemente nos indican que nuestra contraseña debe contener caracteres especiales (como símbolos), además de letras mayúsculas, minúsculas y números. Esto se conoce como la complejidad de la contraseña y se puede calcular fácilmente.

Pensemos como un atacante. Si queremos adivinar una contraseña por fuerza bruta (probando sucesivamente cada posibilidad de contraseña), primero debemos definir el espacio o el universo de posibilidades. Supongamos que sabemos que las contraseñas requieren letras (mayúsculas y minúsculas), números y caracteres especiales. Por lo tanto, nuestro universo se compone de:

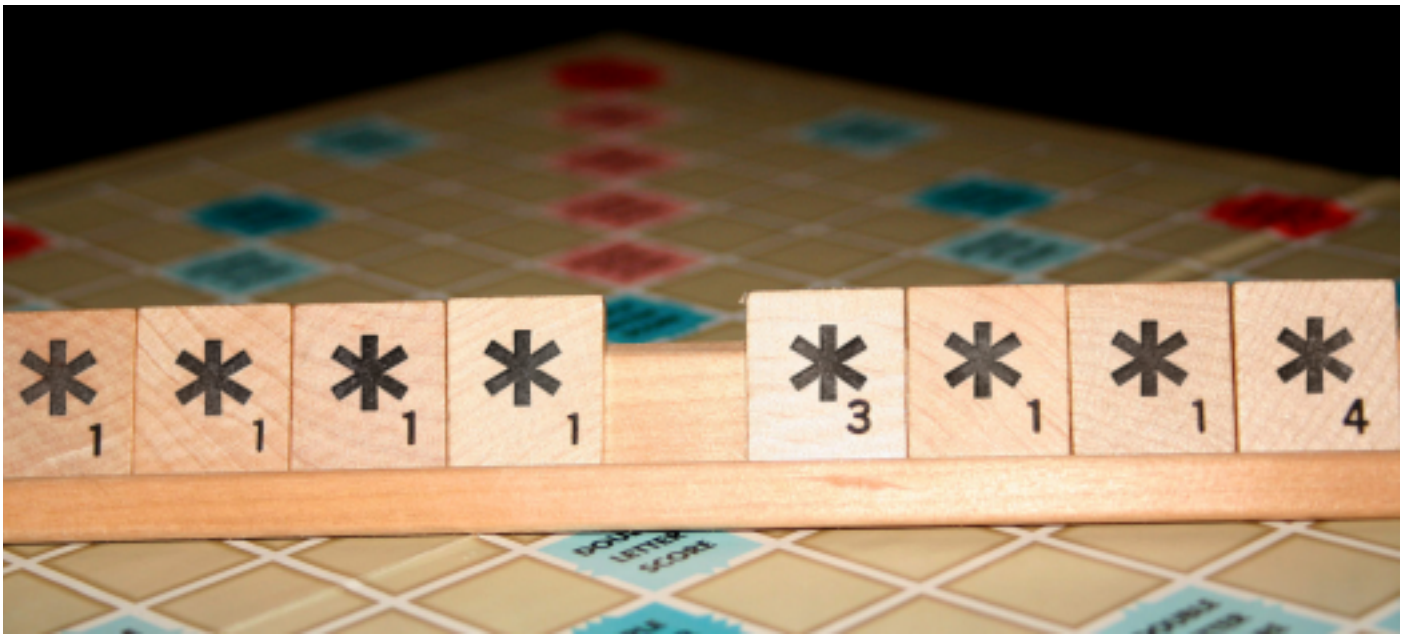
26 (letras minúsculas)
26 (letras mayúsculas)
10 (dígitos)
10 (símbolos – aquí estoy suponiendo, cada quien podrá dar un número diferente).

Entonces, la complejidad de esta contraseña no es más que la suma de estos números: 72.

Asombrosamente, el tamaño (o longitud de la contraseña) es más importante que su complejidad. Si te interesan las matemáticas detrás de esto, te bastará saber que la fórmula de la "fortaleza" de una contraseña se puede definir por la siguiente expresión:

complejidad longitud

Es fácil notar que la longitud es más importante. Consideremos dos ejemplos: una contraseña tradicional, como 'b&kqAp5H' y una frase de contraseña: 'muypequeña'. La fortaleza de la primera es 728 y la de la segunda 2611. A pesar de que nuestra frase de contraseña es muy pequeña (11 caracteres) y que solo contiene letras minúsculas, su fortaleza es 5 veces superior a la contraseña tradicional. Si agregamos una sola letra a la frase, la hacemos



132 veces más fuerte a ataques de fuerza bruta. ¿Dos letras más? 3,435 veces más fuerte.

No estoy argumentado que la complejidad es inútil (después de todo, es la mitad de la fórmula). Además, es probable que al crear tu contraseña te exijan utilizar letras mayúsculas, dígitos y símbolos. Mi recomendación es que no te preocupes por hacer tu contraseña algo muy complejo; como has visto, te conviene más hacerla más grande.

1 Para más información consulta el apartado "El tamaño sí importa" al final de este artículo.
2 Esto no es 100% correcto: sugiero leer sobre el ataque contra el escritor de la revista electrónica Wired, Mat Honan.

UNAM

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM
CERT

Revista .Seguridad Cultura de prevención para TI
No.15 / noviembre-diciembre 2012 ISSN: 1251478, 1251477