No.17 / marzo-abril 2013 ISSN: 1251478, 1251477

.Seguridad

Cultura de prevención para TI

17

Herramientas en seguridad

Optimización corporativa y personal

Criptografía | Volcado de memoria | WAF II | Politicas de seguridad II | Consejos de Seguridad | Trolls cibernéticos

Contenido

.Seguridad
Cultura de prevención para TI

Universidad Nacional Autónoma de México. Dirección General de Cómputo y Tecnologías de Información y Comunicación. Subdirección de Seguridad de la Información/UNAM-CERT. Revista .Seguridad Cultura de prevención para TI M.R., revista especializada en temas de seguridad del UNAM-CERT.

Editorial

Herraminetas en seguridad
Optimización corporativa y personal

Tanto a nivel corporativo, como en el aspecto personal, optimizar nuestra seguridad digital requiere tomar en cuenta aspectos muy diversos, además, la gran cantidad de actividades alternas con las que contamos todos los días, muchas veces, nos llevan dejar la seguridad en un terrible tercer plano.

La gestión de la seguridad se llena de tantos puntos que atender y con directrices tan distintas, que muchas veces quisiéramos tener miles de ojos y manos por todos lados, y así, sentir que realmente estamos protegidos.

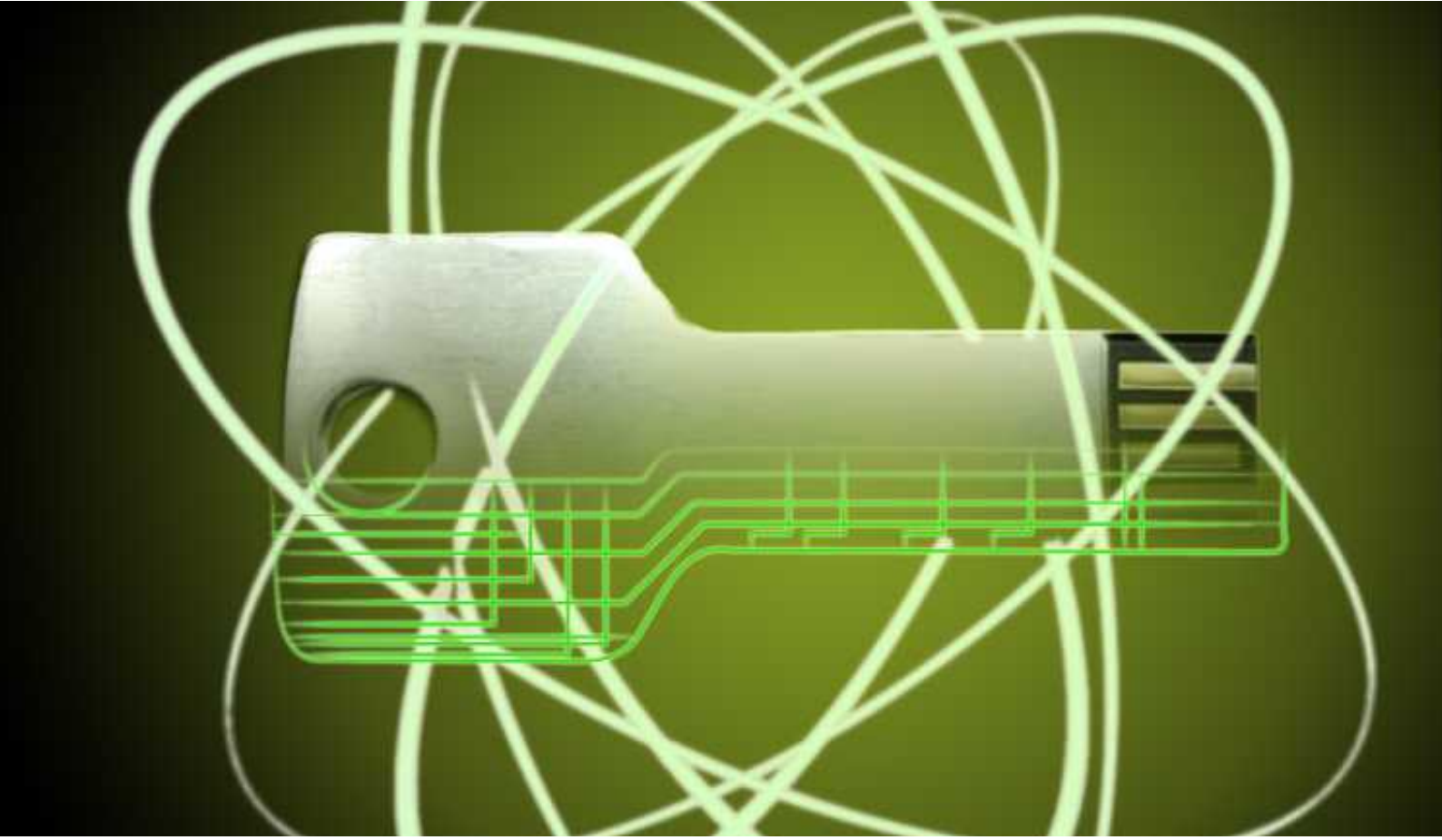
Aunque parece que estamos solos, realmente no es así. Contamos con un gran abanico de herramientas que trabajan para el cuidado de nuestra seguridad informática, apoyo que nos permite dar soporte a la pesada carga de llevar a flote nuestra propia seguridad.

En esta edición, queremos ofrecerte una selección de temas que te servirán como instrumentos para manejar tu seguridad, conocerlos y aplicarlos, significará un gran refuerzo a tu presencia digital en la vida laboral y cotidiana.

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

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 17 / marzo - abril 2013 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829



Criptografía y criptoanálisis: la dialéctica de la seguridad

Jesús Alberto Itzcoatl Salazar Monroy

I Introducción

La criptografía estudia las técnicas para hacer que la información en un mensaje sea más fácil de entender para el destinatario que tiene una clave secreta para el uso y acceso de ella. Por su parte, el criptoanálisis busca recuperar dicha información sin necesidad de un código o clave. El resultado es, que siempre que avanza una, su contraparte necesita ser revisada. Una vez que se logró romper una técnica criptográfica, ésta necesitará aumentar su complejidad.

A principios del siglo IX, Al-kindi (un sabio árabe de Bagdad) escribió un libro titulado *"Sobre el desciframiento de mensajes criptográficos"* en el que se aplicaba una técnica de criptoanálisis al sistema de cifrado dominante en esa época, que se basaba en la sustitución de caracteres. Para romper el sistema, simplemente utilizó un análisis de frecuencias: se sustituyen, con las letras más recurrentes de una lengua, los símbolos que más se repiten en el mensaje cifrado, logrando, desde el primer intento un texto bastante semejante al texto original [2].

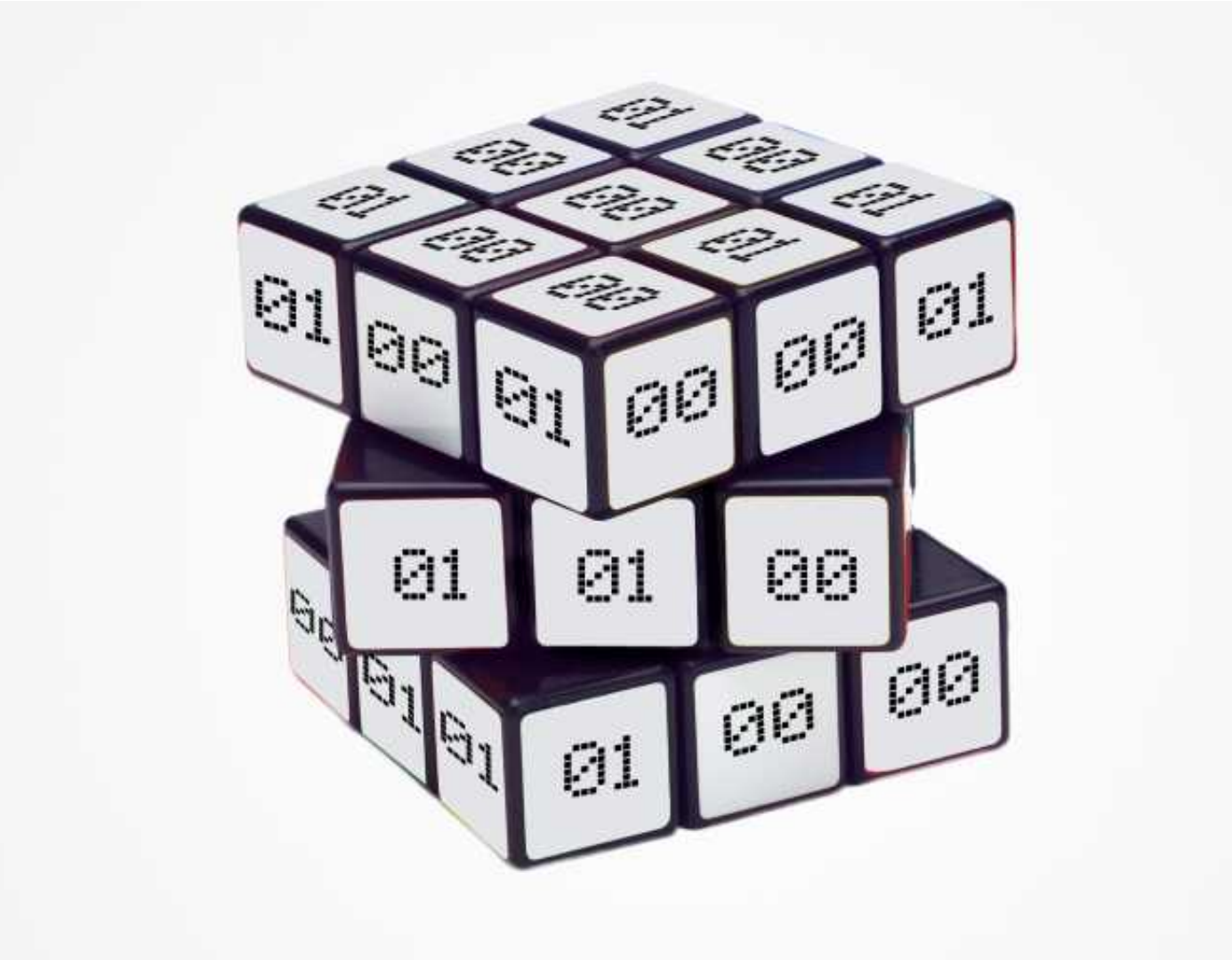
La criptografía europea, que se desarrolló durante el Renacimiento (inicios del siglo XIII), partía de la vulnerabilidad del algoritmo de sustitución simple (quiere decir que había mayor facilidad para acceder a la información), así que las técnicas criptográficas debían ser reformuladas. El resultado fue la aplicación de los homófonos y las nulas. Es decir, destinar dos símbolos diferentes para las letras más frecuentes e introducir más símbolos que el número de letras del alfabeto en el que se escribe. Un siglo después, se comenzó a utilizar la criptografía de dos alfabetos.

El trabajo de Leon Battista Alberti fue la criptografía poli-alfabética, que dio las bases de la criptografía de los siglos que siguieron (sobre todo el concepto de "palabra clave" que hoy conocemos como "llave") [3].

En el siglo XX se registraron ataques a criptosistemas que dejaron su huella en la historia del mundo. Tal es el caso de la Primera Guerra Mundial, en la cual el Telegrama Zimmermann fue conocido por haber influenciado la decisión de Estados Unidos para participar en el conflicto bélico. En la Segunda Guerra Mundial se utilizó por primera vez la automatización de ataques cripto-analíticos por medio de modelos matemáticos, los cifrados de la Alemania Nazi con la máquina enigma y el código Lorenz [4].

Durante la década de los setenta se alcanzan servicios de confidencialidad por medio del estándar de cifrado conocido como DES, hasta que finalmente fue roto en los noventas [1]. Por esa época, algunas funciones *hash* fueron blanco de ataques cripto-analíticos: el sistema de cifrado MD4 fue roto seis años después de su publicación y recientemente se demostró que MD5 puede colisionar[1] [5].

Por otra parte, a finales de 2012, el algoritmo KECCAK fue seleccionado para la nueva función conocida como SHA3, en una competencia organizada por la NIST, a pesar de que SHA2 permanece seguro, por lo menos hasta el día de hoy [6].



El avance tecnológico: La era cuántica

¿Qué hay del día de mañana? Sabemos que los avances tecnológicos ponen a nuestra disposición herramientas más capaces. Al contar con éstas, el cripto-análisis se torna aún más poderoso y, como consecuencia, la criptografía también tiene que evolucionar.

Hoy en día, podríamos estar acercándonos a

una era que marcaría una gran línea en la historia de la humanidad: La era del cómputo cuántico. En términos generales, ¿a qué se refiere el cómputo cuántico? Para empezar, el principio de incertidumbre nos dice que hay un límite en la precisión con la cual podemos determinar la información de una partícula, también llamado estado cuántico o simplemente qubit. [7]

Los qubits son estados cuánticos que representan simultáneamente ceros y unos (del código binario). Antes de que se considere que el número de resultados computados es siempre igual a las combinaciones posibles que se pueden hacer con los qubits (256 para 8 bits), se sabe que esto no es así. La máquina cuántica posee un elevado paralelismo capaz de romper los cripto-sistemas más usados hoy en día; es decir, la capacidad de una computadora cuántica es mayor que aquella que se basa en las leyes clásicas de la física.

El cómputo cuántico y los criptosistemas actuales

Supongamos que hoy existieran las computadoras cuánticas. En primer lugar, sucedería que algunos de los cripto-sistemas actuales se volverían inseguros. La capacidad de la máquina cuántica es tal, que rompería cualquier sistema criptográfico cuya seguridad provenga de álgebra modular (pues ya existe un algoritmo cuántico que rompería la misma), como el esquema de RSA, uno de los más usados hoy en día. Esto representa, a nivel mundial, un peligro potencial y habría consecuencias tanto económicas como científicas.

Podría ser que un algoritmo matemático resista un ataque cuántico durante su tiempo de vida promedio (5 a 25 años). Incluso se podrían asumir medidas simples, como duplicar el tamaño de la llave, entonces los algoritmos clásicos podrían seguir resistiendo un ataque cuántico como sucede hoy entre los cripto-sistemas matemáticos y los ataques no cuánticos.

Aunque hablamos de que la computación cuántica ya tiene su algoritmo para descifrar los sistemas basados en álgebra modular, también es importante mencionar que los esquemas que no se basan en este tipo de álgebra quedan exentos del algoritmo que termina con la seguridad en el álgebra modular, aunque no de la capacidad de procesamiento de la computadora cuántica.

De hecho, no se sabe si otros esquemas, diferentes a los del álgebra modular (como los de redes y los basados en código), se rompan ante un ataque cuántico. Estos alcanzan la complejidad necesaria para resistir el cómputo cuántico al duplicar el tamaño de sus llaves.

Es una realidad que el cómputo cuántico aumenta el poder de procesamiento. Sin embargo (empleado en criptoanálisis), no garantiza la vulnerabilidad de los otros criptosistemas (los no modulares), la razón: aún no hay algoritmo cuántico (más simple que la fuerza bruta) contra estos modelos, pero tengamos presente que la falta de este algoritmo ha sido siempre la problemática, en la esfera del cómputo cuántico o fuera de ella.

Referencias

[1] ELI BIHAM y Adi Shamir, "Differential cryptanalysis of the full 16-round des", en Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, editorial Proceedings, Santa Barbara, California, EUA, volumen 740 of Lecture Notes in Computer Science, August 16- 20, 1992, pp. 487–496.

[2] FERNÁNDEZ, SANTIAGO. "La criptografía clásica", en SIGMA, Euskadi, abril, 2004, pp. 119-142.

[3] RUSSO, BETINA, Criptografía en el aula de matemáticas, artículo disponible en la página: http://www.soarem.org.ar/Documentos/26%20Russo.pdf.

[4] VITINI, FAUSTO MONTOYA, "Testimonio de medio siglo: de la perlustracion al cifrado cuántico", en RECSI, 2012, artículo disponible en la siguiente liga: http://recsi2012.mondragon.edu/es/programa/Fausto_paper.pdf:

[5] SOTIROV, ALEXANDER y Jacob Appelbaum, et al, "Md5 considered harmful today, creating a rogue ca certificate", 25th Annual Chaos Communication Congress el artículo se recupera en la liga: http://www.win.tue.nl/hashclash/rogue-ca/

[6] NIST Computer Security Division, Sha-3 selection announcement. Technical report, NIST, 2012.

[7] HIDAYATH ANSARI y Luv Kumar, "Quantum cryptography and quantum computation" en Network Security Course Project Report. Disponible en la liga: http://www-cs-students.stanford.edu/~adityagp/acads/netsec-writeup.pdf.

AARONSON, SCOTT, "Shor, i'll do it" en Criptograph blog, 2007, disponible en la siguiente liga: http://www.scottaaronson.com/blog/?p=208.

CHAO-YANG LU, y Daniel E. Browne, et al, "Demonstration of shor's quantum factoring algorithm using photonic qubits", en Technical report, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, 2007.

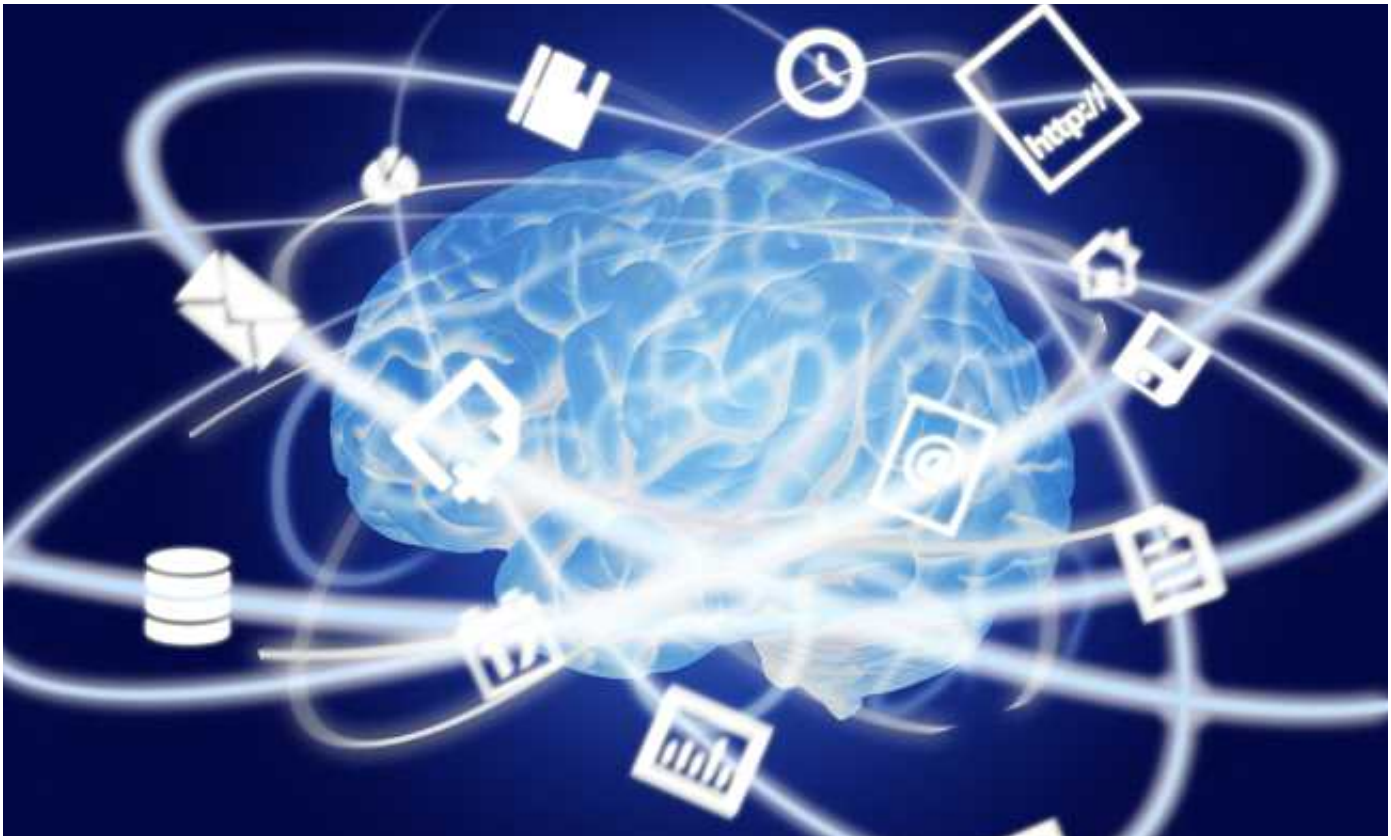
La importancia del análisis de volcado de memoria en investigaciones forenses computacionales

David Bernal Michelena

Los atacantes informáticos mejoran sus técnicas día con día para lograr penetrar, incluso en los sistemas informáticos mejor protegidos, los cuales son custodiados fuertemente por una gran cantidad de controles administrativos, técnicos y por un equipo de administradores especialistas en respuesta y análisis de incidentes informáticos. En esta carrera, solo triunfarán aquellos con la capacidad para dominar los métodos, técnicas y herramientas más avanzadas para superar a los adversarios.

Algunas de las armas más poderosas de los atacantes son los rootkits, que son malware que permite ocultar los procesos maliciosos, puertas traseras y archivos que se utilizan para tomar control de los sistemas comprometidos. Según Hoglund y Butler[1], los rootkits consisten en uno o más programas y código que permiten mantener acceso permanente e indetectable en una computadora. Jesse D. Kornblum[2], uno de los pioneros del análisis forense computacional, indica que son programas maliciosos que subvierten silenciosamente un sistema operativo para ocultar procesos, archivos y actividad.

Hay dos tipos de rootkits: los de nivel de usuario y los de nivel de kernel. Algunos investigadores[3] consideran otros tipos adicionales: los que afectan el BIOS (bootkit) y los basados en virtualización. Sin embargo, nos enfocaremos a tratar los dos primeros.



Los rootkits a nivel de usuario tienen como objetivo reemplazar programas del sistema por versiones modificadas que ocultan información relacionada con la actividad maliciosa del intruso informático. Por ejemplo, un rootkit de nivel de usuario puede ser un programa llamado "netstat", especialmente diseñado para ocultar una conexión de red que es utilizada como puerta trasera por el atacante. Este tipo de rootkits son fácilmente detectados por programas como TripWire, que revelan modificaciones en los programas del sistema.

Los rootkits a nivel de kernel alteran estructuras clave ubicadas en el espacio de kernel (como la tabla de llamadas al sistema), así no requieren modificar los programas del sistema para alterar el resultado que éstos muestran al usuario final. Esta característica dificulta que sean detectados por herramientas de seguridad, administradores de sistemas y especialistas en seguridad informática.

¿Cómo detectar estas perversas y poderosas herramientas?

Existen tres opciones: la primera -y más sencilla- es ejecutar programas especializados en la detección de rootkits, como Rootkit Hunter, Chkrootkit (para sistemas basados en UNIX) o rootkitrevealer (para Windows XP y Server de 32 bits). Algunos de estos programas, además de ser capaces de detectar rootkits conocidos, incorporan alguna funcionalidad genérica para detectar nuevas amenazas. Sin embargo, no existe la seguridad de que un nuevo rootkit utilice esas funcionalidades genéricas, por lo tanto, no hay garantía de que estas herramientas logren detectarlos.

Para explicar la segunda opción, es necesario mencionar la forma en la que se ligan los programas, los cuales pueden estar compilados de forma dinámica o estática.

De forma dinámica, los programas usan bibliotecas del sistema, que son porciones de código externas ubicadas en el sistema operativo. Si por el contrario, están compilados estáticamente, los programas contienen en sí mismos todo el código necesario para su funcionamiento.

La forma de compilación más común es la dinámica, pues diferentes programas comparten alguna biblioteca del sistema, y esto permite optimizar el espacio en disco. Sin embargo, si alguna de las bibliotecas compartidas es alterada por malware (incluyendo rootkits), el resultado de ejecutar un programa que haga uso de dicha

biblioteca, también se vería afectado por esta alteración.

Realizar un diagnóstico, utilizando programas de auditoría compilados de forma estática, evitará que el resultado que producen sea alterado por rootkits a nivel de usuario que hayan alterado bibliotecas del sistema. Pero esta técnica no es efectiva contra rootkits a nivel de kernel.

La tercera y última opción, además de ser la que ofrece una mayor posibilidad de detectar rootkits a nivel de kernel, es el análisis del volcado de memoria[4]. Para explicar cómo funciona, recordaremos algunos conceptos de arquitectura de computadoras.

Una computadora tiene dos tipos de memorias, principal y secundaria. La primera es la de mayor velocidad de lectura, intercambia datos constantemente con el procesador y es de menor tamaño que la memoria secundaria. Almacena la información de forma temporal mientras la computadora se encuentra encendida y, en cuanto se apaga, la información se pierde.

Volcar la memoria consiste en copiar el contenido de la memoria principal en un archivo, el cual puede ser analizado posteriormente para obtener información del estado de la computadora en el momento del volcado.

¿Por qué es tan importante incluir el análisis de volcado de memoria en una investigación forense computacional hacia atacantes informáticos de alto perfil? Porque este tipo de intrusos utilizan el cifrado y ofuscación para protegerse. Los más sofisticados, incluso utilizan herramientas que nunca escriben información en memoria secundaria. Sin importar qué tan perfeccionadas sean las técnicas empleadas por los atacantes informáticos, todo programa que se ejecuta en una computadora, en algún momento se almacena en memoria principal. Por esa razón, es muy probable que el volcado de memoria contenga los programas utilizados por los atacantes informáticos o, al menos, rastros de ellos.

Desde hace años, los analistas forenses computacionales han capturado el contenido de la memoria. Su análisis consistía en la extracción de cadenas de texto para luego buscar direcciones IP o URLs que podían dar un gran contexto al investigador forense, pero no se lograba obtener otras estructuras de la memoria.

En 2007 se creó Volatility, una herramienta para interpretar el contenido de la memoria, que va mucho más allá de las técnicas tradicionales de búsqueda de cadenas de texto. Este poderoso programa tiene la capacidad de interpretar las estructuras internas de memoria que almacena, entre otras cosas, la información de los procesos en ejecución y conexiones de red que estaban activas en el momento en que se capturó la memoria. Incluso proporciona información de conexiones de red y procesos ya finalizados para el momento en que se realizó la captura. Los cuales pueden ser indicios claves para resolver un caso.

En sistemas operativos Windows, particularmente, esta herramienta tiene la capacidad de mostrar las sentencias exactas ejecutadas en la terminal de comandos cmd.exe que, en la mayoría de las ocasiones, no es posible obtener con el análisis de memoria secundaria, ya que no se encuentra habilitado de forma predeterminada ninguna bitácora que almacene esta información.

Entre otras herramientas se encuentra Red Line, la cual tiene interfaz gráfica desarrollada por la compañía Mandiant. Ésta se enfoca exclusivamente al análisis de volcados de memoria de sistemas operativos Windows. También está Volatility, que es una herramienta de código abierto con interfaz por línea de comandos desarrollada en el lenguaje Python que permite analizar volcados de memoria de sistemas operativos Windows, GNU/LINUX, Mac OS y Android. Gracias a que esta herramienta es de código abierto, tiene una gran comunidad de desarrolladores que extienden continuamente su capacidad por medio de módulos o plugins .[5]

No cabe duda de que, tanto los atacantes informáticos como los investigadores forenses digitales, tendrán que mejorar sus técnicas, métodos y herramientas constantemente, con el fin de mantener la ventaja en la guerra cibernética, la guerra de la era digital.

El análisis de volcado de memoria será cada vez más importante para resolver con éxito los casos de intrusiones informáticas avanzadas.

1 Hoglund y James Butler, "Rootkits, Subverting the Windows Kernel", Addison-Wesley, 2009.
2 Kornblum, Exploiting the Rootkit Paradox with Windows Memory Analysis http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE2FC4D-0B11-BC08-AD2958256F5E68F1.pdf
3 Pär Österberg Medina, Detecting Rootkits in Memory Dumps, http://www.terena.org/activities/tf-csirt/meeting27/oesterberg-rootkits.pdf4
4 Kornblum, Jesse, Ibidem.
5 http://code.google.com/p/volatility/wiki/Plugins Volatility Project

Referencias

GREG HOGLUND y James Butler, "Rootkits, Subverting the Windows Kernel", Addison-Wesley, 2009, ISBN 0-321-294319-9.

KORNBLUM, JESSE, Exploiting the Rootkit Paradox with Windows Memory Analysis , en: http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE2FC4D-0B11-BC08-AD2958256F5E68F1.pdf

PÄR ÖSTERBERG MEDINA, Detecting Rootkits in Memory Dumps, en: http://www.terena.org/activities/tf-csirt/meeting27/oesterberg-rootkits.pdf

http://code.google.com/p/volatility/

http://code.google.com/p/volatility/wiki/Plugins

http://code.google.com/p/volatility/wiki/VolatilityIntroduction

Firewall de Aplicación Web - Parte II

Sayonara Díaz Sarahí Méndez, Dante Odín Ramírez López

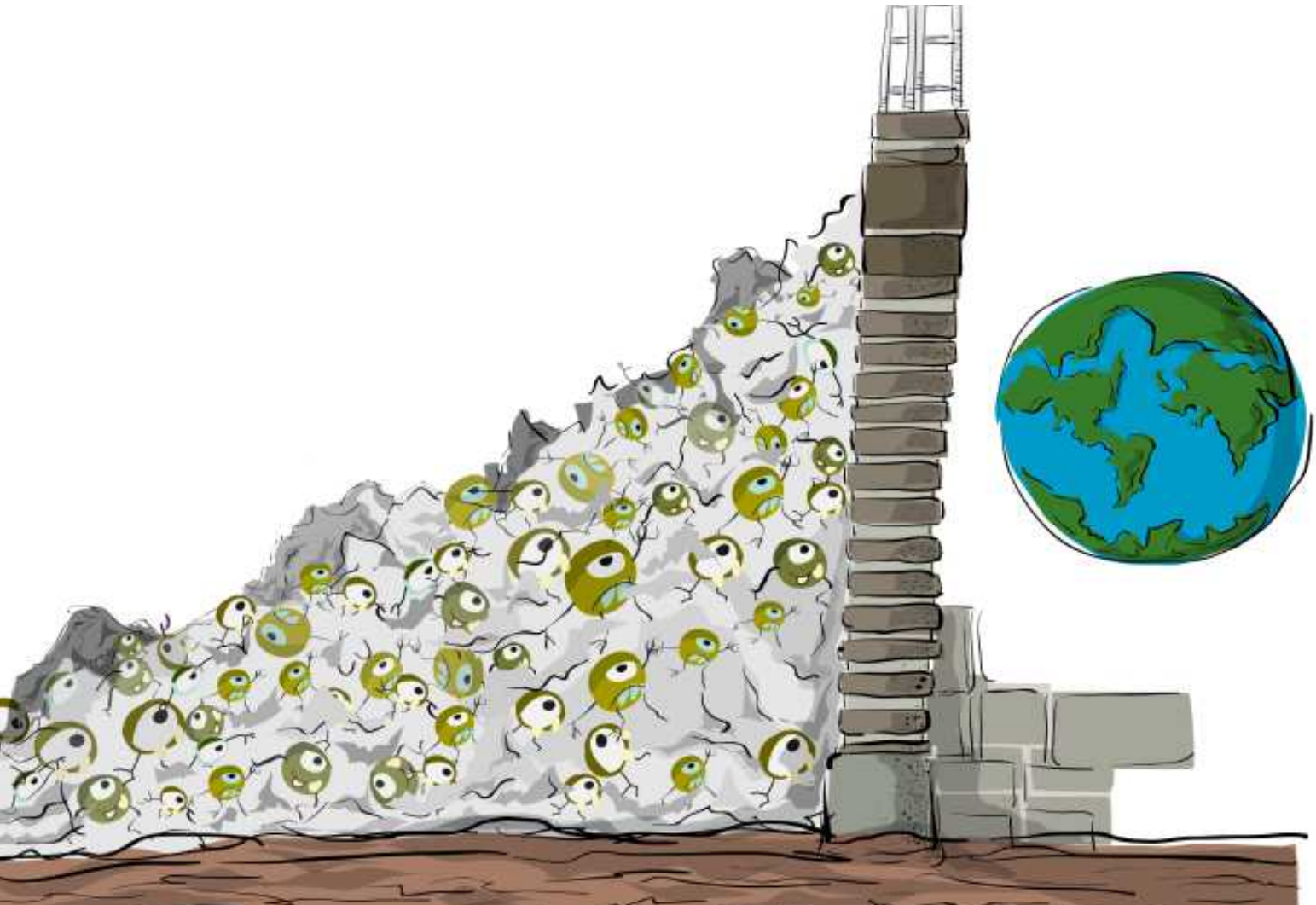
Este artículo es la segunda parte de nuestra entrega sobre los Firewalls de Aplicación Web (WAF por sus siglas en inglés), publicada en la edición anterior de esta revista. Para esta edición prometimos prepararte una sección con los manuales de implementación de un WAF open source paso a paso, pero antes de que los revises, es muy importante dejar claro cómo funciona un Firewall de Aplicaciones Web.

A continuación, te explicamos cómo es que un WAF lleva a cabo su tarea y, después de saber cómo funciona, podrás proseguir con la implementación de tu propio WAF.

Funcionamiento de un WAF

Un WAF trabaja como intermediario entre usuarios externos (ej. usuarios de Internet) y las aplicaciones web. Esto quiere decir que las peticiones y respuestas HTTP son analizadas por el WAF antes de que éstas lleguen a las aplicaciones web o a los usuarios de las aplicaciones.

Para la revisión del tráfico HTTP, el WAF aplica un conjunto de reglas (definidas con anterioridad) para llevar a cabo la detección de peticiones HTTP malformadas, ataques web como Cross Site Scripting, SQL Injection, ataques de DoS y DDoS, e incluso la detección de fuga de información proveniente de la aplicación web. Cuando el WAF detecta un ataque, intento de intrusión o fuga de información, entonces bloquea el tráfico web descartando la petición o respuesta HTTP evitando que los ataques afecten a la aplicación web o que información sensible sea enviada como respuesta a potenciales usuarios maliciosos.



De no detectarse peticiones web maliciosas o alguna anomalía, entonces las peticiones y respuestas HTTP fluyen con normalidad. Todo el proceso de análisis y protección ocurre de forma transparente para los usuarios, evitando así, interferir con las operaciones normales de las aplicaciones web.

Modos de implementación

Puedes implementar un WAF de diferentes modos. El modo de implementación depende de la topología de red con la que cuentes y de

las necesidades de seguridad que requieras para tus aplicaciones web. A continuación se listan los modos de implementación más usados para un WAF.

WAF en modo Puente Transparente (Bridge):

Funge como un equipo que interconecta dos segmentos de red de forma transparente (sus interfaces de red no tienen dirección IP), de modo que no se requiere alterar la configuración de direcciones IP de los servidores web, ya que son estos mismos los que responden las peticiones web. No requiere de la reconfiguración de los registros DNS y permite proteger múltiples servidores de aplicaciones web, siempre y cuando estos se accedan mediante el canal que protege el WAF.

WAF en modo Proxy Inverso:

Funge como un equipo que interconecta dos o más segmentos de red, pero éste si cuenta con dirección IP propia. Concentra, gestiona y analiza las peticiones y respuestas HTTP que circulan entre los usuarios y aplicaciones web. En pocas palabras, el WAF en modo de proxy inverso responde las peticiones web como si éste fuera el servidor web mismo, por lo tanto es de utilidad para ocultar a los servidores de aplicaciones web de la red exterior. Permite proteger múltiples servidores de aplicaciones web. Su implementación requiere modificar los registros DNS que ahora deben dirigirse a la dirección IP del WAF en modo proxy inverso en vez de a los servidores web.

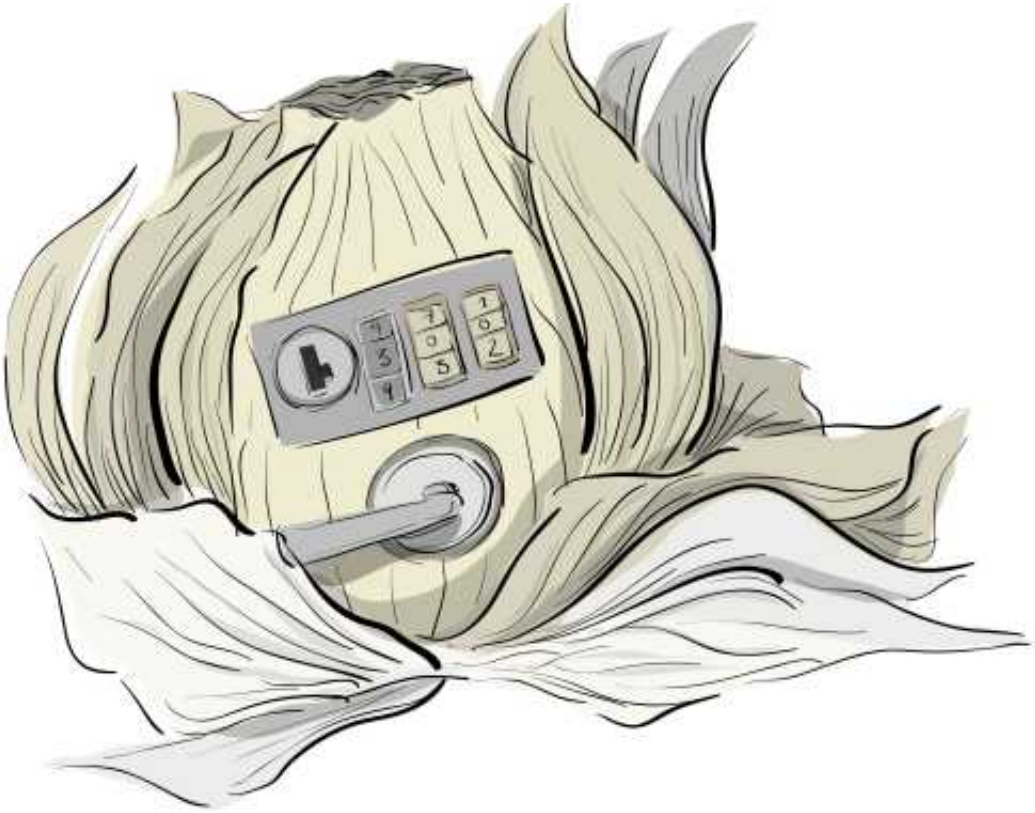
WAF en modo embebido o plugin:

El WAF se instala como un software de complemento o plugin en el servidor web a proteger. Para su operación hace uso de los recursos de hardware (procesador, RAM, disco duro) y software del servidor donde se ha instalado. Su instalación depende totalmente del tipo de servidor web y del sistema operativo subyacente. Afortunadamente existen WAFs para los entornos Windows, GNU/Linux y Unix, así como para los distintos servidores web más populares. Este modo de operación es el más sencillo pues no requiere configuraciones adicionales en la red.

Algunos WAF soportan características como:

• Normalización del tráfico web: Usualmente los usuarios maliciosos usan técnicas para ocultar sus ataques web mediante codificación o cifrado. El WAF debe ser capaz de decodificar o descifrar el tráfico web para poder aplicar sus reglas de seguridad.

• Aceleración SSL: Algunos WAF comerciales cuentan con hardware especializado para poder atender las peticiones web seguras (HTTPS) de forma rápida, pues el uso de cifrado en las transacciones web implica el uso adicional de



procesador y memoria RAM de los servidores web. Emplear aceleradores SSL permite quitar carga de procesamiento a los servidores.

Variedad de soluciones WAF

En el mercado existen varias opciones de WAF a elegir que nos pueden ayudar a aumentar la seguridad sobre nuestros servidores de aplicaciones web de forma considerable. Entre las dos opciones open source más populares, encontramos las siguientes:

ModSecurity
Desarrollado por: Trustwave

ModSecurity funciona como un complemento que se instala en el servidor web. Actualmente soporta los servidores web Apache HTTPD, Microsoft IIS y NGinx. Provee protección contra las principales amenazas del Top 10 de OWASP mediante su conjunto de reglas especializadas en detección y bloqueo de ataques. Es un proyecto con madurez de desarrollo y cuenta con una creciente comunidad de usuarios que lo han implementado.

IronBee
Desarrollado por: Qualys

IronBee es un WAF desarrollado y mantenido por el equipo que diseñó y desarrolló a ModSecurity en sus inicios. Este proyecto apunta a producir un WAF que sea aún más seguro, de alto rendimiento, portable y libremente disponible, incluso para el uso comercial. El enfoque de este WAF va dirigido a perfilar el comportamiento de la aplicación web y sus usuarios, de esta forma se pueden establecer controles de seguridad basados en la forma de uso de las aplicaciones web, así como los convencionales contra ataques web comunes.

¿WAFs en el código de las aplicaciones web?

Dentro de la amplia gama de herramientas de seguridad para aplicaciones web, existen otro tipo de opciones que están muy ligadas con las acciones que realiza un WAF. Estas herramientas también pueden ser de utilidad cuando se quiere proporcionar seguridad adicional a las aplicaciones web a nivel de código.
Este conjunto de herramientas se implementan directamente en el código de la aplicación, para hacer uso de ellas, tendrás que tener acceso directo al código fuente de tu aplicación web, lo

que implica conocer el lenguaje de programación en que se desarrolló y, con base en ello, puedas comenzar con la modificación del código y acoplarlo según tus necesidades.

En muchos casos no se tiene acceso al código fuente de la aplicación web debido a que la aplicación misma podría ser solo un archivo ejecutable. Es ahí cuando el uso de este tipo de herramientas se tiene que descartar. Si este no es el caso, podrás hacer uso de herramientas como las siguientes:

ESAPI WAF (Enterprise Security API Web Application Firewall):

Son bibliotecas que se incluyen directamente en el código y, una vez que se implementan en tu aplicación web, proporcionarán seguridad de una forma más directa mediante la validación de los datos de entrada, permitiendo así filtrar ataques web. El equipo de desarrollo debe implementar las bibliotecas de esta API sobre el código de las aplicaciones web que se deseen asegurar.

PHPIDS Web Application Security 2.0 (PHP-Intrusion Detection System)

Es un software utilizado para reforzar la seguridad en la capa de aplicación a nivel web (directamente en tu aplicación). Al igual que los WAF convencionales, se basa en el análisis de transacciones HTTP mediante un conjunto de reglas que se encargan de filtrar anomalías y ataques web. Su modo de operación se lleva a cabo mediante puntajes, donde a un ataque o anomalía se le asigna un puntaje numérico mediante el cual se decide qué tipo de acción defensiva debe seguirse.

Conclusión

Existen varias alternativas que ayudan a complementar la seguridad de tu aplicación web, haz uso de ellas. Indaga sobre las que más te interesen, ya que solo de esta manera podrás descartar algunas o bien, acoplarlas según tus necesidades.

Recuerda que la seguridad de un sistema es tan fuerte como lo sea su eslabón más débil. No olvides que hoy en día la seguridad web es un punto crítico que no puede echarse en saco roto, pues las afectaciones por ataques exitosos, intrusiones y fugas de información sensitiva, pueden traer repercusiones sociales (pérdida de reputación), monetarias e incluso legales. A veces, una simple entrada de datos no asegurada puede acarrearnos grandes problemas.

Los WAF son herramientas que han evolucionado y han demostrado su efectividad a tal grado que dentro de poco tiempo serán considerados como una capa de seguridad obligatoria en cualquier entorno de aplicaciones web seguro.

Implementación de tu propio WAF

Las guías de instalación contemplan la implementación del WAF ModSecurity en un servidor web apache en modo embebido. Ten en cuenta que la instalación de un WAF puede resultar sencilla, pero el proceso de aprendizaje para su administración y afinación de políticas requiere de entendimiento en su forma de operación y en las configuraciones específicas.

Nota: Una regla importante para todos los WAF en general, es que siempre se deben de implementar en modo de solo monitoreo por un periodo de tiempo. Esto con la finalidad de que observes las alertas que muestran al analizar el tráfico web dirigido a tu aplicación web y así puedas determinar si hay reglas del WAF que puedan interferir con el funcionamiento de la misma. Recuerda que como otras tecnologías de monitoreo es susceptible a falsos positivos.

Referencias

http://www.modsecurity.org/documentation/ModSecurity2_Rule_Language.pdf

http://revista.seguridad.unam.mx/numero-10/evoluci%C3%B3n-de-los-sistemas-de-detecci%C3%B3n-prevenci%C3%B3n-y-an%C3%A1lisis-de-incidente

https://www.owasp.org/index.php/Virtual_Patching_Best_Practices
http://www.blogtecnico.net/web-application-firewall-waf/
https://phpids.org/
http://www.cert.org.mx/index.html
http://www.modsecurity.org/
https://www.owasp.org/
http://www.fromdev.com/2011/07/opensource-web-application-firewall-waf.html
https://www.owasp.org/index.php/Virtual_Patching_Best_Practices

Normatividad en las organizaciones: Políticas de seguridad de la información- Parte II

Miguel Ángel Mendoza López, Pablo Antonio Lorenzana Gutiérrez
Coautores: Sandra Atonal Jiménez, Rubén Aquino Luna

En el artículo anterior se revisaron las características que pueden poseer las políticas y sus objetivos dentro de una organización. Se definió que aquellos que conocen y operan los procesos críticos de la empresa, deben tener los roles encargados de escribir, revisar, aprobar, difundir y actualizar los documentos, por medio de un comité estratégico que permita el cumplimiento de las políticas en todos los niveles de la estructura jerárquica de la organización.

Así mismo, se hizo énfasis en el enfoque de la redacción de los enunciados permisivos (todo lo que no está expresamente prohibido está permitido) y prohibitivos (todo lo que no está explícitamente permitido está prohibido). Sin embargo, se recomendó evitar la escritura en sentido negativo. También se mencionó que la redacción debe estar orientada al tipo de lectores (audiencias), donde se determinará el sentido de los enunciados.

Por último se mencionaron técnicas para la difusión entre las audiencias. En caso de que las políticas no sean documentadas, publicadas, difundidas y aceptadas por los miembros de la organización, la normatividad no será efectiva.

Este último artículo aborda la estructura que puede tener una política, así como los elementos de importancia considerados para el éxito en

implantar y aplicar políticas de seguridad de la información en una organización.

Como todo documento, una política se conforma de varias secciones que proporcionan información relevante para la audiencia y permiten tener un contexto amplio de la misma. Las secciones que pueden ser consideradas en el desarrollo se describen a continuación:

• **Introducción**. Esta sección debe proporcionar una breve descripción de la política, nombre y ubicación dentro de la jerarquía de políticas de la organización.
• **Propósito.** Indica los objetivos principales de la política y su razón de ser. Permite a las audiencias entender la manera de utilizarla. Puede incluir declaraciones sobre un requerimiento o legislación a la cual se debe adherir.
• **Alcance.** Indica el ámbito de aplicación de la política, que puede relacionarse con la infraestructura, aplicaciones, información, personas u otro activo de la organización que se desee proteger.
• **Enunciados de la política.** Son las declaraciones que deben cumplirse en la organización, es decir, todos los enunciados que deben ser acatados por los miembros de la organización.
• **Sanciones.** Detalla el incumplimiento de la política, considerado como una violación. Define la manera en la que debe ser reportada y las acciones a considerar cuando se presente un evento de esta naturaleza. También se debe incluir información detallada acerca de las acciones correctivas que se aplicarán como resultado de una falta.
• **Glosario.** Define cualquier término que sea desconocido para el lector. Aunque se recomienda no emplear términos técnicos en la redacción de los enunciados, en ocasiones se puede hacer uso de acrónimos, siglas, anglicismos y otro tipo de argot que pueden ser definidos en esta sección.
• **Histórico de revisiones, actualizaciones y aprobaciones.** Este apartado define al responsable de realizar las actualizaciones, revisiones y aprobaciones de la política, así como la frecuencia para ejecutar estas tareas. Es útil para determinar la obsolescencia o vigencia de la política.
• **Fecha de publicación y entrada en vigor.** Esta parte permite erradicar ambigüedades en relación a la vigencia y aplicación de las políticas.
• **Versión del documento.** Permite conocer el estado de las actualizaciones y revisiones del escrito, así como los cambios que se han presentado en la política.
• **Referencias.** En esta sección se coloca la lista de documentos asociados a la política (políticas, guías, procedimientos o formatos).

Por otro lado, las guías y procedimientos que soportan las políticas, también contienen secciones que proporcionan información relevante para el lector. Este tipo de documentos están dirigidos a una audiencia generalmente operativa, por lo que el lenguaje suele ser totalmente técnico. Las secciones que pueden incluir son:

• **Introducción.** Debe proporcionar un panorama general del documento, nombre y ubicación dentro de la jerarquía de documentos de la organización.
• **Propósito.** Indica los propósitos principales del escrito y su justificación. También permite a los lectores entender la manera de utilizarlo.
• **Alcance.** Indica el ámbito de aplicación del documento, que puede ser infraestructura, aplicaciones, información y/o personas.

• **Desarrollo.** Establece las actividades que deben realizarse, así como los roles y responsabilidades encargados de ejecutar tales labores. La guía propone actividades que pueden ser consideradas (son de carácter opcional), mientras que el procedimiento debe tener un apego total.
• **Diagrama de flujo**. Esquema que permite ver de manera gráfica las actividades descritas en el desarrollo. Puede incluir al personal responsable de ejecutarlas, herramientas e información necesarios para llevar a cabo las tareas.

Las políticas de seguridad de la información tienen diferentes ámbitos de aplicación, los cuales deben ser seleccionados por cada área de acuerdo a sus necesidades y características propias. Una referencia para la elección pueden ser los objetivos de control y controles de estándares o marcos de referencia (frameworks).

ISO 27001:2005 es un estándar internacional auditable para la seguridad de la información ampliamente utilizado. Define los requisitos para un sistema de gestión de seguridad de la información (SGSI) y los controles enfocados a proteger la información necesaria para la

• **Glosario.** Define los términos que el lector pudiera desconocer.
• **Histórico de revisiones y actualizaciones.** Define al responsable de realizar las actualizaciones y revisiones del documento, así como la frecuencia para ejecutar estas tareas. Este apartado permite determinar su obsolescencia o vigencia.
• **Fecha de aprobación, publicación y entrada en vigor.** Esta sección posibilita erradicar ambigüedades en relación a la vigencia y aplicación del documento.
• **Versión del documento.** Da a conocer el estado de las actualizaciones y revisiones del documento, así como de los cambios que se han presentado en el mismo.
• **Referencias.** En esta sección se coloca la lista de documentos asociados (políticas, guías, procedimientos o formatos).

operación y permanencia de las organizaciones. Algunos ámbitos que incluye son:

• Responsabilidades relacionadas con la seguridad de la información.
• Ética y conducta.
• Recursos humanos/administración.
• Seguridad física.
• Clasificación, manejo, respaldo y eliminación de información.
• Uso adecuado de activos, inmobiliario e infraestructura.
• Protección de hardware/software.
•Uso de correo electrónico, Internet y mensajería instantánea.
• Accesos remotos y conexiones de red.
• Administración de cuentas de usuarios y contraseñas.
• Autenticación y control de acceso.

• Aplicaciones y desarrollo de aplicaciones.
• Dispositivos periféricos, de seguridad o móviles.
• Criptografía (cifrado y manejo de llaves).
• Monitoreo.
• Auditoría.
• Detección y respuesta a incidentes.
• Recuperación de desastres y continuidad del negocio.
• Administración de cambios.
• Administración de proveedores de servicios/terceras partes.
• Cumplimiento contractual y legal.

En este sentido, el estándar puede ser la base para el desarrollo de las políticas organizacionales de seguridad de la información. Sin embargo, ésto no limita la inclusión de temas de interés para la organización y sus miembros, así como asuntos de relativa actualidad, como el uso de dispositivos móviles o cómputo en la nube (temas que, por su importancia, se han considerado integrar en la actualización del marco de referencia ISO 27001 en su versión 2013[1] , el cual se espera sea publicado el segundo semestre del presente año).

Una vez que se hayan desarrollado las políticas de seguridad alineadas a algún estándar o framework, es necesario considerar elementos de importancia para el éxito y funcionalidad durante la implantación de políticas de seguridad de la información. Por ejemplo, la resistencia al cambio por parte de los miembros de la organización, quienes con la entrada en vigor de las políticas, deberán realizar sus actividades bajo la normatividad establecida en los documentos y modificar algunos hábitos.

En el caso de las personas que se integran a la empresa, es importante informarles y darles a conocer en el momento que inicia la relación laboral con la organización. La capacitación es un elemento necesario durante el proceso de implantación.

La aceptación y cumplimiento de las políticas se pueden facilitar a través de la concientización de los miembros de la organización. Se comprende la importancia de la seguridad de la información al explicar las medidas de protección de los activos por parte de los dueños, custodios y usuarios al sensibilizar sobre amenazas y riesgos.

Por otro lado, resulta necesario definir objetivamente sanciones de las que serán acreedoras aquéllas personas que de forma deliberada, intencional o por desconocimiento, infrinjan alguna política de seguridad de la información. Estas sanciones serán aplicadas para que se cuente con un marco sólido de estricto apego.

Finalmente, las políticas junto con los procedimientos y guías (controles administrativos) deben estar integrados con un conjunto de controles físicos y técnicos que permitan la interacción entre lo descrito en los enunciados y la implementación tecnológica.

1 Revisión ISO/IEC 27001 por parte de "The British Standards Institution" http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/

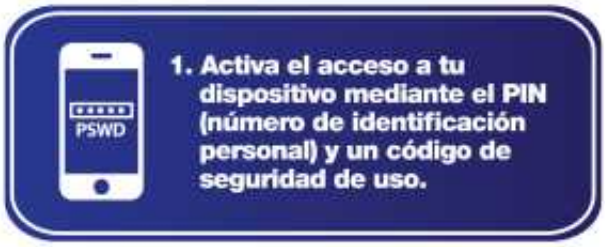
Referencias

•International Organization for Standardization. ISO/IEC 27001:2005.
•SANS Institute. Information Security Policy - A Development Guide for Large and Small Companies.
•SANS Institute. Security Policy Roadmap - Process for Creating Security Policies.
•SANS Istitute. A Short Primer for Developing Security Policies.

10 consejos para mantener nuestra seguridad en el celular

Miguel Zúniga

Ahora que el Banco Mundial reporta más teléfonos celulares que personas en el mundo, la gente se ha acostumbrado a confiar mucha información personal en los dispositivos móviles. En un celular se encuentran contactos de familiares y amigos, entradas directas a redes sociales y multitud de aplicaciones con información personal, bancaria, agendas y documentos laborales. Al descuidar éste tipo de información es relativamente sencillo comprometer la seguridad del equipo y de sus propietarios. En este artículo se listan 10 consejos para proteger nuestra información y flanquear los peligros más comunes.



1. Activa el acceso a tu dispositivo mediante el PIN (número de identificación personal) y un código de seguridad de uso.

El número de identificación personal (PIN, por sus siglas en inglés Personal Identification Number) está registrado en el «chip» o tarjeta SIM (Suscriber Identity Module, módulo de identidad del suscriptor) como medida para proteger los datos si se reinicia el equipo o cuando se cambia el chip del dispositivo. Cuando esto sucede, se activa un menú para ingresar el PIN. Si se opta por este método, es importante guardar en un lugar seguro la tarjeta plástica que acompañaba a la SIM en el momento de su compra, pues allí también está el código PUK (PIN Unlocked Key, clave para desbloquear el PIN) en caso de que el equipo se bloqueé.

Además del PIN, puede activarse un mecanismo de seguridad para usar el equipo. De acuerdo con cada fabricante, puede ser un número, una secuencia de movimientos, un tono de voz o una palabra clave. Esto será una barrera adicional y sencilla para proteger los datos ante cualquiera que tome el teléfono.

2. Realiza una copia de seguridad de los datos del dispositivo.

Respaldar es extremadamente importante, porque permite guardar la información del móvil en caso de falla, pérdida de datos o borrados accidentales. Hay varias formas para hacer respaldos. Una opción rápida es la copia a la tarjeta de expansión o mediante el software de sincronización del fabricante, que también puede respaldar datos como favoritos o las contraseñas Wi-Fi. Dicho software de sincronización hace copias de seguridad periódicas con los datos y ajustes en aplicaciones, mensajes, diccionarios del teclado, entre otras configuraciones. Al conectar el equipo para recargarlo a la PC se puede realizar el respaldo.

Otra alternativa son los servicios en la nube para respaldar en Internet fotos o archivos conforme

se generan, éstos pueden ser aplicaciones en línea que guardan datos, agendas y contactos. Lo importante es tener un esquema de respaldo disponible por cualquier imprevisto.

3. Activa las conexiones por Bluetooth, infrarrojos y WiFi solo cuando vayas a utilizarlas.

Las ventajas de comunicación mediante los puertos Bluetooth, infrarrojo o Wi-Fi son evidentes: facilitan usar un manos libres en el auto, conectarse con impresoras, otros móviles y enviar texto o imágenes a otras personas, entre otras. Pero tenerlas encendidas todo el tiempo tiene dos consecuencias: en poco tiempo acaban con la batería del teléfono y propician la fuga de datos.

Al estar abierta alguna señal del teléfono, usuarios malintencionados pueden aprovecharse para transmitir virus o conectarse al dispositivo y obtener contraseñas o contactos, dependiendo el modelo y sistema del equipo. Al conectarse a redes WiFi públicas o inseguras, se puede interceptar con relativa facilidad la información que viaja desde nuestro teléfono. Otra práctica común es el bluejacking (la recepción de mensajes o archivos indeseados): cualquier persona que vea nuestro dispositivo con los puertos Bluetooth o infrarrojo habilitados puede, desde gastar una broma o iniciar conversaciones aparentemente inocentes,

hasta emplear ingeniería social para cometer posteriormente un robo. Como buena práctica, es mejor evitar que sepan que se posee un buen equipo móvil.

4. Asegúrate de que la información transmitida o recibida esté libre de malware.

Según el sistema operativo de cada teléfono, existe una variedad de malware que puede afectar su funcionalidad. Para combatirlo, instala un paquete antivirus y utiliza los antivirus de tus aplicaciones en línea para comprobar los archivos que se transmiten. Asimismo, cuida los archivos que se instalan o se usen en el teléfono. Un análisis del antivirus nunca está de más cuando se reciben archivos de otras personas.

5. Descarga aplicaciones solo de sitios de confianza.

La seguridad de datos en tu teléfono es el blanco preferido de programas que sustraen tus preferencias y configuraciones. Existe una cantidad enorme de aplicaciones con funciones ocultas para crear desperfectos en un teléfono o para enviar hábitos de consumo y preferencias a agentes publicitarios. La recomendación es solo instalar una aplicación cuando se corrobore la confiabilidad de su procedencia y se esté seguro de que se utilizará.

Las tiendas de aplicaciones del fabricante de tu equipo o del sistema operativo de éste, son ideales para instalar aplicaciones. Para llegar a ellas solo debes registrarte, la mayoría de las descargas son gratuitas. También hay sitios (como foros y blogs) que hablan sobre aplicaciones móviles que desarrollan gente y

empresas entusiastas que tienen buenas opciones para tu equipo. Es cuestión de buscar referencias adicionales en Internet y obtenerlas de su sitio oficial.

Descargar aplicaciones crackeadas (liberadas del mecanismo que comprueba si fueron adquiridas legalmente) puede tener consecuencias, como descargar software defectuoso o programas espía. Además, hay que vigilar los permisos de las aplicaciones que se instalan: aunque vengan de una fuente de fiar, pueden solicitar más permisos de los necesarios.

De igual manera, nunca hay que abrir enlaces facilitados a través de mensajes SMS/MMS no solicitados que impliquen la descarga de contenidos en el equipo. Ésta es una forma popular para propagar aplicaciones que dañan dispositivos móviles como parte de una cadena por Internet. Por mucho que digan que vienen de parte de tu operador de telefonía, es mejor desconfiar.

6. Cierra todas las sesiones iniciadas al terminar de usarlas.

Nunca se sabe cuándo se puede perder el teléfono o cuándo pueda caer en manos equivocadas, aunque sea solo por unos minutos. Una persona que utiliza tu teléfono después de ti, tiene la facilidad de acceder a las páginas que hayas visitado y a la información personal que dejes abierta. Emplea contraseñas seguras y nunca las facilites a terceros.

7. Mantén el software del dispositivo siempre actualizado.

Al mantener actualizado el software del equipo se evitan fallos de seguridad y se agregan y optimizan características ante problemas potenciales que los fabricantes encuentran. Las actualizaciones menores van enfocadas a resolver fallos y mejorar la seguridad, por lo tanto siempre es buena idea instalarlas. En cambio, las actualizaciones mayores suponen modificaciones relevantes en el software, las cuales pueden requerir mejores prestacionesde hardware, por lo que es importante verificar en las notas de actualización y en foros que el equipo mantendrá su rendimiento después de incorporar nuevas funciones y utilidades.

Evita modificaciones de software extraoficiales para garantizar que, cuando se actualice el equipo, siga funcionando correctamente a buena velocidad y con el esquema de seguridad que proporciona el fabricante. Una actualización homebrew puede ser divertida o provechosa de momento, pero puede representar un hueco de seguridad a futuro o vacío al agregar nuevas aplicaciones.

8. Instala una aplicación de borrado de datos remoto.

Instalar una aplicación para borrar los datos remotamente es una buena idea en el caso de extraviar el celular. Con alguna de estas aplicaciones se puede activar el celular mediante un mensaje de texto antes o después del robo o extravío y, de esa manera, se borra la información

privada. Entre las características adicionales, según el paquete que se instale, se puede: localizar el móvil incluso si el GPS está desactivado, producir fuertes alarmas (aunque el equipo esté en modo silencioso), obtener una copia de seguridad y bloquear el dispositivo al conectarse desde cualquier navegador web después del incidente.

9. Guarda el número IMEI.

Una forma para ayudar a detener el robo de equipos celulares es mediante el código IMEI. La Identidad Internacional de Equipo Móvil (IMEI por sus siglas en inglés) es un código pregrabado en los teléfonos móviles que identifica unívocamente a nivel mundial a cada equipo. Éste se transmite por el aparato a la red cuando se conecta con su operador de telefonía.

Busca el IMEI en la parte posterior del teléfono, debajo de la pila o tecleando *#06# si está encendido. Es un número de 15 a 18 dígitos y se asocia por las siglas IMEI. Anótalo y guárdalo con la factura y su caja: te será de gran utilidad a futuro. Desde el 1 de septiembre de 2012, entró en vigor un convenio por América Móvil (Telcel), Iusacell, Nextel y Telefónica Movistar para compartir los IMEI que hayan sido robados o extraviados, para evitar que se utilicen en otras compañías. Si confirmas que tu número ha sido robado o extraviado, ve a un centro de atención de tu compañía y rinde informe del hecho. Solicita el bloqueo total de la línea, del chip y del IMEI, para que no se pueda reactivar ni desbloquear el proveedor de telefonía (así se evita que el celular acepte chips de otras compañías) , o reutilizar en posibles actos delictivos. Al bloquear el equipo telefónico mediante el IMEI, el aparato queda inservible.

10. Cuida a quién le prestas tu celular.

Por último, cuida a quién le prestes tu teléfono celular, aunque sea por unos instantes. En la escuela, en la calle, un lugar público o una reunión privada, una inocente llamada puede significar el robo de tu información, un secuestro virtual o la pérdida de tu teléfono, en el caso de que la supuesta persona solicitante de ayuda corra repentinamente con el celular en mano.

Conclusión:

Estos consejos pueden aplicarse a teléfonos tradicionales e inteligentes. Las amenazas de seguridad siempre estarán latentes, pero haciendo conciencia con nosotros mismos y con la gente que nos rodea, se puede reducir enormemente la cantidad de información que pueda comprometerse. Nada es infalible, pero con acciones sencillas se pueden evitar posteriores dolores de cabeza. La protección de nuestros datos debe ser una acción constante, que con el tiempo se vuelve algo natural y cotidiano.

Referencias:

• *Apple Support, Qué es el PIN de la SIM, https://support.apple.com/kb/HT1316?viewlocale=es_ES&locale=es_ES (30 de marzo de 2013).*

• *Cibergeek, Código PUK, http://cibergeek.com/codigo-puk/ (3 de abril de 2013).*

• *HERNÁNDEZ, J, Ventajas y desventajas de Bluetooth, https://junihh.wordpress.com/2007/06/02/ventajas-y-desventajas-de-bluetooth/ (26 de marzo de 2013).*

• *KILLER STARTUPS, Keep yor Mobile Data Secure. (29 de marzo de 2013), http://www.killerstartups.com/mobile/mobical-net-keep-your-mobile-data-secure/ (30 de marzo de 2013).*

• *Más celulares, Virus para teléfonos móviles, http://mascelulares.blogspot.mx/2007/06/virus-para-telfonos-mviles.html (1 de abril de 2013).*
• *Mi próximo móvil, Se unen para crear lista negra de teléfonos robados en América Latina, http://www.miproximomovil.com/2012/07/se-unen-para-crear-lista-negra-de-telefonos-robados-en-america-latina/ (3 de abril de 2013).*
• *ROSEN, R (2012), A World With More Phones Than People, The Atlantic, http://www.theatlantic.com/technology/archive/2012/07/a-world-with-more-phones-than-people/260069/ (2 de abril de 2013).*

Los trolls cibernéticos

César Iván Lozano Aguilar

Los trolls (o en su forma hispanizada, trol) en Internet se han convertido en una verdadera molestia, sus actos y actitudes pueden llegar a convertirse en una confrontación personal o grupal. En ocasiones puede hacerse una mezcla entre trolleo y bullying y, ¿qué diferencia existe entre uno y otro? En breves palabras hacer bullying es molestar y hacer trolleo, también, pero con el toque de desprestigio a los demás, a costa de difamaciones, creando controversia con supuestas pruebas prefabricadas para intentar fundamentar lo que dicen. A lo largo de este artículo trataremos de explicar el fenómeno del troll en Internet, con el fin de crear conciencia entre los usuarios.

Un caso particular, que bien vale la pena mencionar, es el caso de "Bebexito Emoxito", en el que, a pesar de tratarse de un caso de ciberbullying, contiene señales de trolleo. Como bullying, reconocemos el hecho de molestar a la víctima de una manera denigrante y, por el lado del trolleo, se reconoce crear discusión entre la gente que opina a favor o en contra del victimario por desprestigiar a la víctima con fuertes declaraciones, como tacharlo de violador.

El victimario mismo declara en un video, sin el más mínimo remordimiento, el por qué de sus acciones: él dice hacerlo por gusto y porque así llama la atención de la gente.

¿Qué es un troll cibernético?

El término troll proviene del nórdico troll, un ser que se comporta de una manera violenta. En Internet, un troll es un usuario que se sienta frente a una computadora y busca llamar la atención, la cual consigue al publicar (de manera textual o gráfica, es decir con imágenes) temas polémicos, ideas o contenido sensible para otros usuarios.

¿Cuál es el lugar perfecto para que un troll ocasione problemas?

Los trolls se inmiscuyen en foros, comunidades de usuarios y en algunos otros servicios de comunicaciones públicas de Internet y redes sociales, los cuales son los lugares perfectos para provocar e incitar peleas entre los usuarios de esos servicios. Los trolls pueden confrontarse directamente con los usuarios o crear confrontación entre los mismos.

¿Por qué lo hacen?

Según varias investigaciones(1) los trolls tienen sed de atención, ya sea positiva o negativa. Ellos no tienen cargo de conciencia ni remordimientos, no sienten vergüenza al exponer una situación o compasión contra una víctima. Es inútil razonar e interactuar con ellos, pues crean una atmósfera de tensión con ideas negativas, al grado de generar un ambiente totalmente paranoico en el que nuevos usuarios suscritos a estos servicios de comunicaciones pueden obtener respuestas demasiado agresivas al tratar de hacer entrar en razón al troll.

Los trolls más hábiles llegan a suplantar a moderadores de blogs y foros, e inclusive a personas, de los cuales los usuarios troll imitan su manera de escribir o expresarse en las publicaciones y en los mensajes de los foros. Esta táctica es un camuflaje útil que primero detona como una incitación y, después, termina en una discusión entre los usuarios.

¿Tienen un nombre los mensajes que envían los trolls?

Sí, esos mensajes se denominan mensajes Flame. sSon mensajes deliberadamente hostiles o insultantes que se envían en respuesta a un mensaje provocativo.

Por ejemplo, veamos el siguiente intercambio de mensajes:

Mensaje o post inicial por un usuario:

"Me parece que el mejor equipo de la temporada de la liga mexicana de fútbol fueron los Pumas, bien hecho Pumas!! Sigan así!!"

Mensaje flame posteado por un troll:

"Parece ser que no sabes lo que dices y creo que eres poco competente para tratar sobre temas de futbol, a leguas se nota que no sabes nada y además la liga mexicana de futbol es una basura"

El mensaje flame anterior, es un ejemplo de un "mensaje anzuelo". Éste sirve para ver si el usuario cae en el juego del troll, en el que se espera que el usuario que inició el post responda con un mensaje como el que se muestra:

"De seguro haz de ser argentino, todos ustedes son una bola de ..."

El usuario convierte en argentino al troll, aunque sea mexicano, pero el troll solo lo hizo para generar esta controversia. A partir de ahí el troll continúa su juego, en el que usuarios argentinos puedan sentirse ofendidos y desencadenen mensajes ofensivos y agresivos. En este caso, el Troll ganó y cumplió su objetivo al desatar una guerra de mensajes en la publicación. A este tipo de guerra también se le denomina flamewar.

Cada quien es libre de publicar lo que quiera en el momento que quiera

Un punto importante acerca de este tipo de mensajes es la libre expresión. Un troll, al verse censurado por sus comentarios por los administradores del servicio o moderadores de foros, puede incitar a otros usuarios para que se unan a la causa y aboguen por la libre expresión. En este caso, el troll puede argumentar que algunos de sus mensajes están siendo censurados. Al ver esta actitud del troll, los demás usuarios de la comunidad pueden exigir que no se censure a nadie, argumentando la libertad de pensamiento y expresión. Lo que no saben los usuarios, es que los mensajes flame están siendo detectados por los administradores y moderadores de los foros, quienes saben que no deben liberarlos, porque conocen las consecuencias. De esta manera, el troll gana al poner a los usuarios en contra de los administradores, aunque algunos de sus mensajes o publicaciones hayan sido censurados.

¿Qué hago si me encuentro con un troll?

Los trolls son inevitables, invaden cualquier foro, blog, comunidad o red social. La única manera

de tratar con trolls es limitar nuestra reacción y recordar a otros que no se debe responder a sus provocaciones. Cuando tratas de razonar con un troll, él gana. Cuando le gritas a un troll, él gana. Cuando insultas a un troll, él gana. Lo único que un troll no soporta es que lo ignoren.

Puedes tomar en cuenta estas recomendaciones cuando te encuentres frente a un troll:

Notifica a los administradores o moderadores de los servicios que utilices, si has notado o detectado a un troll.

Evita a toda costa publicar de manera deliberada información personal tuya o de gente que conoces, fotos o imágenes en foros o comunidades públicas, en los que tú no poseas el control total sobre lo que estás publicando. Un troll con ingenio puede utilizar esos recursos para ocasionar daño sobre ti o la gente que estimas.

Cuando un troll se siente ignorado, busca con más esmero endurecer sus ataques, tratando de llamar la atención, es lo que le interesa. Ignorarlo constituye el mejor remedio para que se canse y se vaya.

Evita caer en el mismo juego del troll, es decir, no te unas a él defendiéndolo para que siga incomodando o agrediendo a los demás usuarios.

Consuta las normas de comportamiento para una mejor convivencia y un fructífero intercambio de información entre la gente que participa en foros públicos.

http://www.comunidadelectronicos.com/listas/netiquette.htm

Referencias:

"Definición de troll",[en línea],URL: http://definicion.de/troll/, [consulta: 18 de abril de 2013]

SLATTERY, BRENNON, "Internet Trolls: The Psychology Behind the Rants", PCWorld,[en línea], octubre de 2011, URL: http://www.pcworld.com/article/242526/internet_trolls_the_psychology_behind_the_rants.html, [consulta: 18 de abril de 2013]

"Don't flame me, bro", [en línea], noviembre de 2007, New Scientist, URL: http://www.newscientist.com/blog/technology/2007/11/dont-flame-me-bro.html, [consulta: 18 de abril de 2013]

(1) GARDNER, AMANDA, "Troll Psychology: Why People Are So Mean on the Internet", Healt, [en línea], agosto de 2012, URL: http://news.health.com/2012/08/02/troll-psychology-mean-internet/, [consulta: 18 de abril de 2013]

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad Cultura de prevención para TI
No.17 / marzo-abril 2013 ISSN: 1251478, 1251477