Magazcitum

El magazine para los profesionales de la seguridad de TI

¡Allí está el detalle!

Aplicaciones seguras contra todos

Mejorando el desarrollo de aplicaciones con el apoyo de FUZZERS

La Seguridad está en todos lados

Una casa sin Planos

AÑO 2, NÚMERO 2
ABR.-JUN. 2011
EJEMPLAR GRATUITO

Secure your network assets.

Every day, Fortinet protects many of the largest financial services organizations in the world, including nine of the Fortune 10 commercial and retail banks. We accelerate your business with extremely high firewall throughput and exceptionally low latency. Our consolidated security platforms deliver complete content protection that keeps your applications secure and detects hidden threats.

Healthcare

Government & Defense

Education

Financial Services

Retail

Utilities

Service Providers

Visit us at www.fortinet.com for more information or call 1-866-868-3678 to find out how you can secure your network assets today.

FORTINET®

Real Time Network Protection

© 2010 Fortinet, Inc. All Rights Reserved. Fortinet and the Fortinet logo are trademarks of Fortinet, Inc.

www.fortinet.com

FTNT NASDAQ LISTED

Magazcitum

AÑO 2, NÚMERO 2. ABRIL - JUNIO 2011

Dirección General
Ulises Castillo

Editores
Héctor Acevedo
Gerardo Fernández

Consejo Editorial
Ulises Castillo
Antonio Fájer
Priscila Balcázar
Héctor Acevedo
Gerardo Fernández
Dinorah Valladares

Marketing
Dinorah Valladares

Colaboradores
Héctor Acevedo
José Ramírez Agüero
Priscila Balcázar Hernández
Jorge Alberto Barroso Andrade
David Gutiérrez
Osvaldo Hernández
Raúl Alejandro Jalomo
Rubí Jaramillo Islas
Marcos Polanco
Eduardo Patricio Sánchez
Esteban San Román
Spencer James Scott
Dinorah Valladares

Correctora de estilo
Adriana Gómez López

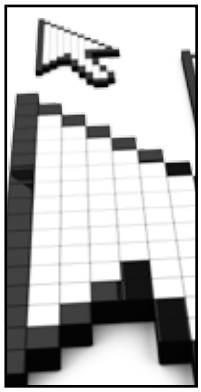
Diseño
Silverio Ortega

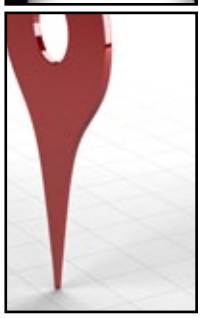
Magazcitum, revista trimestral de Servicios Especializados Scitum S.A. de C.V. Año 2, número 2, abril-junio de 2011. Editor responsable: Héctor Acevedo. Número de Certificado de Reserva otorgado por el Instituto de Derechos de Autor: 04-2010-071512010500-102. Número de certificado de Licitud de Título y Contenido: 14900, Exp.: CCPRI/3/TC/10/18827. Domicilio de la Publicación: Av. Paseo de la Reforma 373 piso 7, Col. Cuauhtémoc, delegación Cuauhtémoc, México DF 06500. Impreso en : Rouge & 21 S.A. de C.V. Av. Rómulo O'Farril # 520 int 5 Col. Olivar de los Padres México DF. Distribuida por Editorial Mexicana de Impresos y Revistas S.A. de C.V: Oaxaca 86-402 Col. Roma México DF. Magazcitum, revista especializada en temas de seguridad de la información para los profesionales del medio. Circula de manera controlada y gratuita entre los profesionales de la seguridad de la información. Tiene un tiraje de 5,000 ejemplares trimestrales.
El diseño gráfico y el contenido propietario de Magazcitum son derechos reservados por Servicios Especializados Scitum S.A. de C.V. y queda prohibida la reproducción total o parcial por cualquier medio, sin la autorización por escrito de Servicios Especializados Scitum S.A. de C.V. Fotografías e ilustraciones son propiedad de Photos.com, bajo licencia, salvo donde esté indicado. Marcas registradas, logotipos y servicios mencionados son propiedad de sus respectivos dueños. La opinión de los columnistas, colaboradores y articulistas, no necesariamente refleja el punto de vista de los editores.
Para cualquier asunto relacionado con esta publicación, favor de dirigirse a **contacto@magazcitum.com.mx**

contenido

» editorial

» opinión





» conexiones

» tips

La seguridad está en todos lados

Héctor Acevedo
CISSP, CISA, CGEIT, ITIL y MCSE
hacevedoj@scitum.com.mx

Cuando se habla de seguridad informática, la conversación suele girar alrededor de cuestiones de infraestructura, tanto la de TI (servidores, centros de datos, etcétera), como la propia infraestructura de seguridad (*firewalls*, IPS, etcétera). Pero a veces olvidamos que el último eslabón de la cadena son dispositivos de usuario final y aplicaciones, a través de los cuales la gente accede a los servicios de TI que necesita para el desarrollo de sus labores diarias y para cuestiones personales.

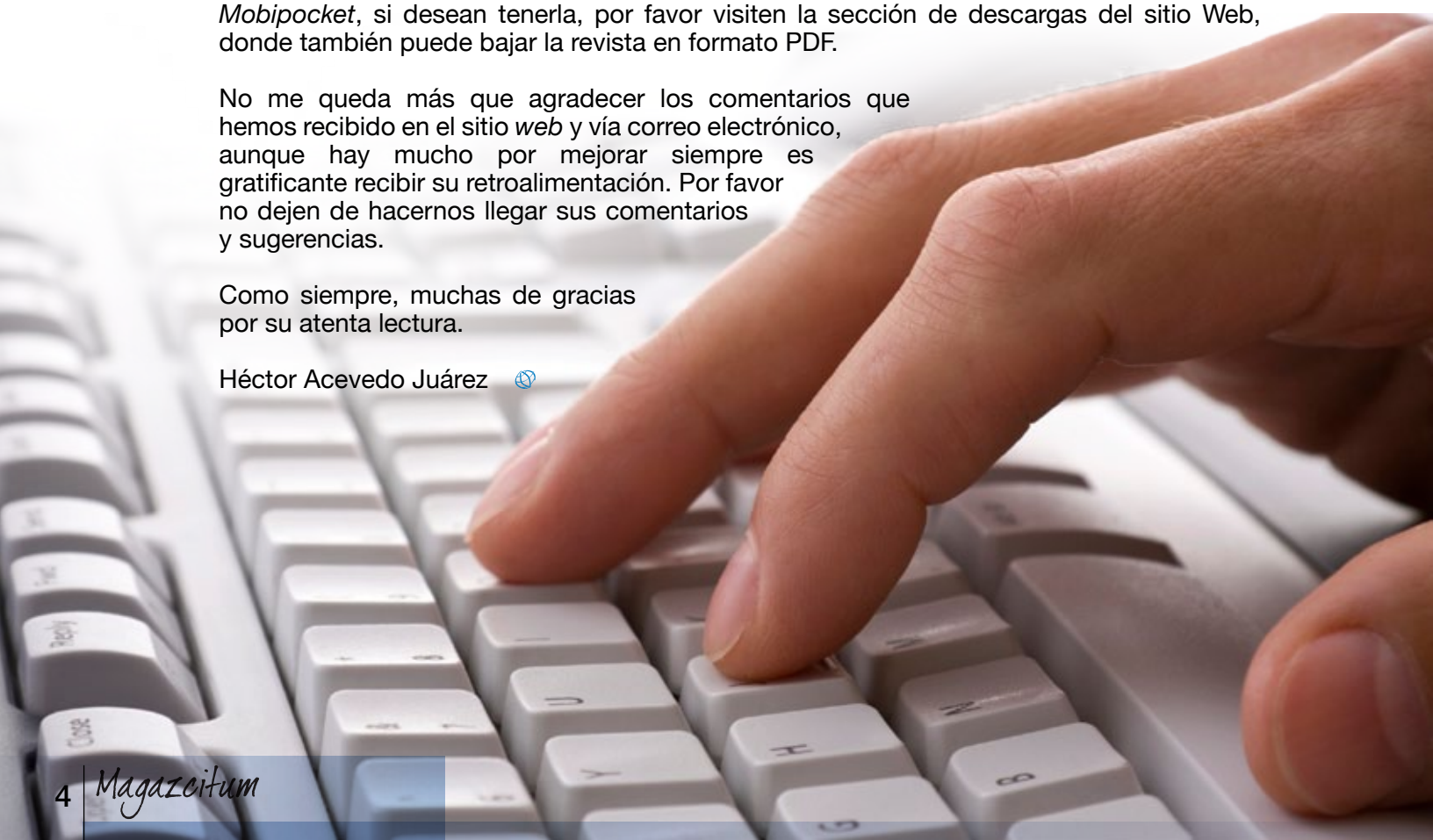
Es por lo anterior que en esta edición de **Magazcitum** decidimos tocar algunos temas que tienen que ver precisamente con los dispositivos de usuario y las aplicaciones. Queda claro que hay un largo trecho por recorrer para lograr que la seguridad informática esté en el diseño mismo de ambas cosas, normalmente los diseñadores tienen una larga lista de requisitos y exigencias que cumplir pero la seguridad no siempre es uno de ellos. Urge que los temas de seguridad sean considerados desde el diseño pues muchas veces lo que el personal de seguridad informática hace es simple y sencillamente estar instalando infraestructura y estableciendo procesos que mitiguen, en la medida de lo posible, los riesgos derivados de las vulnerabilidades en los dispositivos de usuario y en las aplicaciones. Vulnerabilidades que frecuentemente se deben a que la seguridad no fue un requisito de diseño. Esperamos que los temas elegidos por nuestros colaboradores sean de su agrado e interés.

Cambiando de tema, hacemos de su conocimiento que estamos liberando la versión simplificada de Magazcitum para el lector *Kindle* o cualquier otro lector compatible con el formato de *Mobipocket*, si desean tenerla, por favor visiten la sección de descargas del sitio Web, donde también puede bajar la revista en formato PDF.

No me queda más que agradecer los comentarios que hemos recibido en el sitio *web* y vía correo electrónico, aunque hay mucho por mejorar siempre es gratificante recibir su retroalimentación. Por favor no dejen de hacernos llegar sus comentarios y sugerencias.

Como siempre, muchas de gracias por su atenta lectura.

Héctor Acevedo Juárez



Gana Scitum premio como Proveedor Estrella 2010 otorgado por PROSA

Dinorah Valladares
dvalladares@scitum.com.mx

Cd. de México, México. – El pasado 23 de marzo, PROSA (Promoción y Operación S.A. de C. V.) llevó a cabo la 12ª entrega de premios otorgados a sus proveedores más destacados, teniendo como sede el Hotel Camino Real de la Ciudad de México. En esta oportunidad Scitum fue reconocido como "Proveedor Estrella 2010" en la categoría de "Continuidad", por los servicios de soporte técnico e implementación a la infraestructura de seguridad perimetral de dicha empresa, incorporando la utilización de tecnología de vanguardia.

El reconocimiento como Proveedor Estrella 2010 fue recibido por el Ing. Jorge Rodríguez, Director de la Dirección de Servicios Administrados de Scitum, de manos de José Molina, Director General de PROSA, quien expresó las siguientes palabras durante la entrega de reconocimientos:

> *"Nuestro selecto grupo de proveedores representa una importante fuente de conocimiento para que el modelo continúe consolidándose y con esto nos lleve a generar cadenas de valor en todo el proceso con un solo objetivo: la satisfacción integral de nuestros clientes".*

Este galardón forma parte del esfuerzo que desde hace más de una década, PROSA realiza para subrayar la importancia que tiene para ellos el contar con proveedores comprometidos con ofrecer la máxima calidad en los servicios que les proporcionan y que tiene como base un modelo de Desarrollo y Evaluación de Proveedores, que le permite fortalecer la relación entre ellos y sus proveedores que, como Scitum, compartan una visión "ganar- ganar" entre ambas partes.

Más información: www.scitum.com.mx

Cabe mencionar que empresas de la talla de Telmex, Dell, HP -entre otras- han recibido este reconocimiento en otras categorías y oportunidades.

Scitum agradece esta distinción y refrenda nuestro compromiso de continuar ofreciendo servicios innovadores y de excelencia, que permitan apoyar a nuestros clientes a lograr sus objetivos de negocio, poniendo a su servicio nuestra amplia experiencia y tecnología de punta para alcanzar este fin.

Mejorando el desarrollo de aplicaciones con el apoyo de fuzzers

Esteban San Román
CISSP, CISA y CEH
esanroman@scitum.com.mx

Para considerar que una aplicación es segura se tiene que construir con una metodología que involucre, desde su concepción, la seguridad o bien incorporarle herramientas que busquen exhaustivamente defectos para su inmediata corrección.

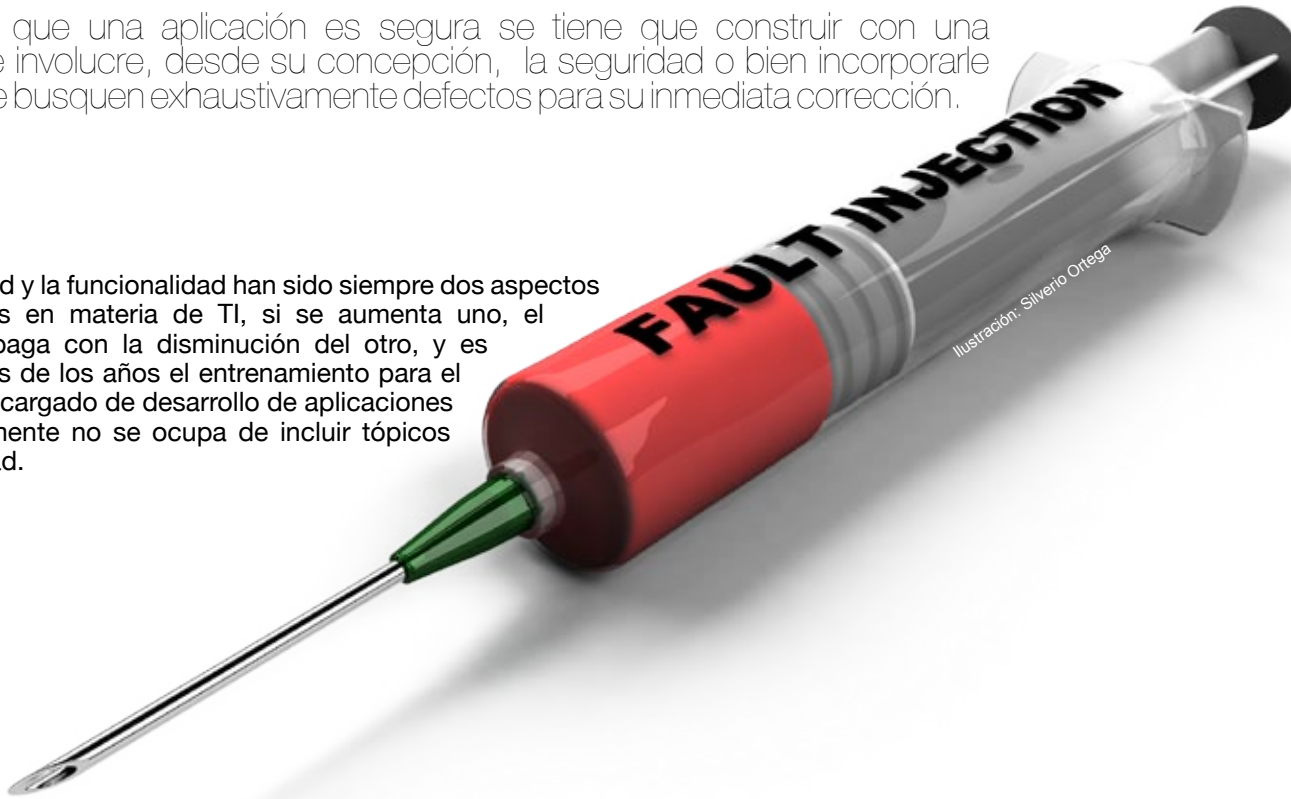


Ilustración: Silverio Ortega

La seguridad y la funcionalidad han sido siempre dos aspectos encontrados en materia de TI, si se aumenta uno, el precio se paga con la disminución del otro, y es que a través de los años el entrenamiento para el personal encargado de desarrollo de aplicaciones tradicionalmente no se ocupa de incluir tópicos de seguridad.

Desarrollo seguro de aplicaciones

Ante la cada vez más común aparición de ataques de día cero, se tiene mayor probabilidad de que una vulnerabilidad en el código de una aplicación sea explotada durante un tiempo considerable antes de que se desarrolle el ajuste (parche) para el código; como es de suponerse, cualquier retraso se traduce en un impacto económico para la organización.

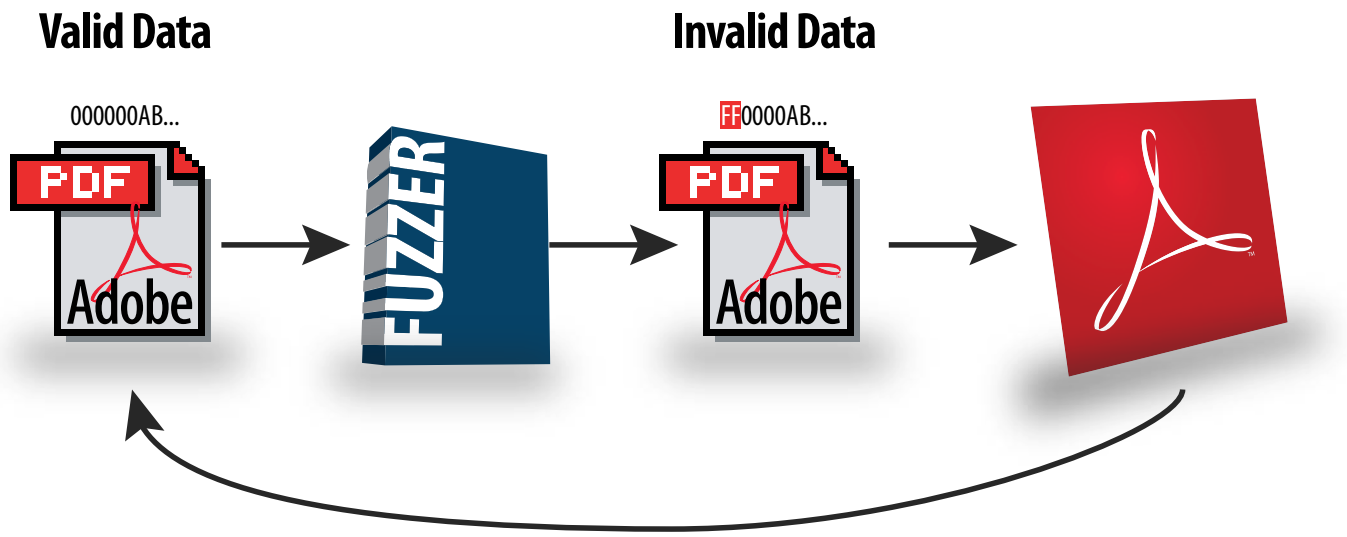
Así pues, una alternativa de primera mano es hacer un drástico cambio en la cultura de los desarrolladores de código para que desde la concepción de un proyecto y a lo largo de las diferentes etapas que comprende el desarrollo de software se considere la seguridad. Los siguientes son algunos de los aspectos que comprenden esta visión:

- Manejar controles precisos que restrinjan el tipo de valores que se dan a las variables de entrada a una aplicación (*inputs*).
- Incorporar mecanismos robustos de autenticación (contraseñas, *tokens*, biometría o bien la combinación de varios de ellos).
- Realizar una definición y gestión adecuadas de los perfiles para proteger quién tiene acceso a un recurso y lo que puede hacer con él (autorización).
- Definir mecanismos para la salida de la aplicación que controlen lo que se pretende obtener después de la ejecución de un proceso (entregables de la aplicación y mensajes de error).
- Incluir mecanismos adecuados para detectar proactivamente cualquier anomalía (bitácoras de actividades).

El uso de fuzzers para garantizar la calidad del código

No existe, como habría de suponerse por la diversidad de aplicaciones y lenguajes de programación utilizados en TI, una fórmula única para contrarrestar las anomalías que se puedan dar en el código de una aplicación dada, sin embargo, existen herramientas que colaboran en entornos de prueba con el fin de aumentar el nivel de confiabilidad de las aplicaciones que se liberan para producción.

Entre estos mecanismos existen los *fuzzers*, herramientas que permiten hacer un primer nivel de pruebas al código introduciendo datos aleatorios e inválidos a un programa, de manera que si éste falla (cerrando la aplicación o provocando errores en ciertos módulos del programa) se agiliza la labor de localizar y corregir tempranamente defectos en el código.



Este enfoque de calidad de código nos permite probar si éste es robusto o si soporta fallas de sintaxis o pruebas negativas (es decir, entradas inaceptables como el uso de letras cuando se esperan solamente dígitos del 0 al 9 para el campo de “Edad” de una persona en una aplicación).

Para un *fuzzer* los blancos más comunes son los formatos de archivos, los protocolos de red, las variables de ambiente, o ciertas secuencias de teclas e inclusive movimientos del ratón. Para fines de hallazgos, que el fuzzer arroje resultados sobre una parte privilegiada de un sistema tiene más impacto que lo que se pueda encontrar entre interfaces hacia los usuarios de las mismas.

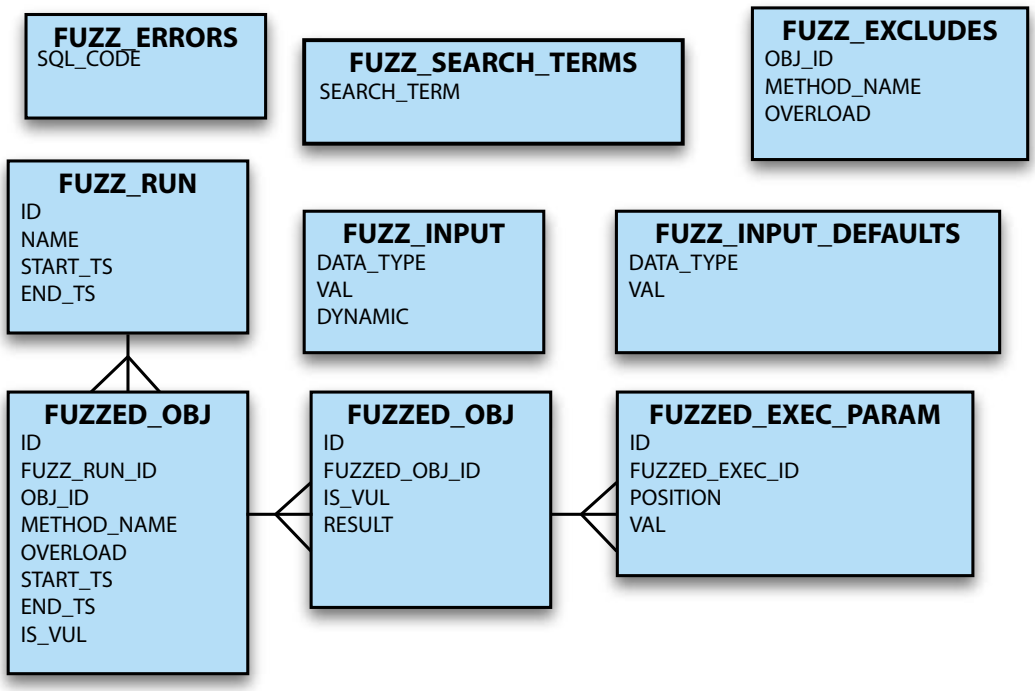
Cabe aclarar que las pruebas con *fuzzers* no pretenden sustituir los métodos formales exhaustivos, lo que entregarán es un primer panorama de cómo está la aplicación, y lo mejor que podríamos esperar es que nos den una idea de si la aplicación puede manejar excepciones (aseguramiento), mas no una certeza absoluta de que el código se comporte correctamente ante cualquier evento (localización de errores).

Clasificación de los fuzzers

De acuerdo a lo establecido anteriormente, se puede constituir una clasificación de los fuzzers con base en las afectaciones que realiza en los siguientes tipos:

1. **En el sistema de Archivos** – Estas herramientas se encargan de crear archivos en el disco donde radica la aplicación, p. ej. *FileH/FileP, FileFuzz*
2. **Dentro del flujo de tráfico de Red** – Los de esta clasificación insertan paquetes generados aleatoriamente en el flujo de la red, p.ej. *TAOF, Sully, GPF, EFS*
3. **Generales** – Éstos usualmente son interfaces de entrada/salida que se adicionan a la aplicación que se tiene bajo prueba, p.ej. Peach, *SPIKE, Fuzzled, Fuzzware*
4. **Personalizados** – Dentro de esta clasificación se ubican aquellas herramientas que son desarrolladas ex profeso para poner a prueba una aplicación, p.ej *Fuzzers* para LDAP, *Axman, DOM-Hanoi, Hamachi, Mangleme*

Existen diversas opciones en el mercado de *fuzzers* comerciales y de código abierto, por ejemplo "*Mu Security*" (http://www.mudynamics.com/products/Mu-Test-Suite/security-testing.html) que está pensado para aplicación en entornos de Redes, o "*beSTORM*" (http://www.beyondsecurity.com/black-box-testing.html) y "*Codenomicon*" (http://www.codenomicon.com/products/buzz-on-fuzzing.shtml) que están considerados para aplicación general.



Para crear *fuzzers* personalizados hay que tener en cuenta la necesidad de invertir recursos de tiempo y monetarios en su desarrollo, pruebas, entrenamiento de los aplicadores y en el mantenimiento de estas herramientas.

Proceso de aplicación de un fuzzer

Los procesos de pruebas de aplicaciones con *fuzzers* se apegan por lo general a las siguientes etapas:

- **Investigación** – Donde se determina a qué porción de código se aplicará el "*fuzzing*" y se seleccionan las características de la herramienta que se deben explotar y los alcances de la misma.
- **Modelado** – En esta etapa se escogen los atributos que se evaluarán en los datos, las relaciones entre ellos dentro de la ejecución del código y los estados del sistema durante la evaluación; esta etapa suele ser de las más consumidoras de tiempo.
- **Validación** – Se verifica que lo definido en la etapa anterior encaja con la realidad; esto le dará sentido a los resultados que finalmente se generen.
- **Monitoreo** – Esta etapa se encarga de detectar fallas, colectar información y puede implicar ajustes finos así como una configuración más detallada para obtener información realista y de valor para la organización. En el monitoreo se hace la labor de depuración de errores.
- **Corrida** – Trabaja estrechamente con la etapa anterior y es aquí donde se define qué pasa tras la ocurrencia de una falla, ¿continúa el proceso aplicativo?, ¿termina?, ¿se puede ejecutar algo en paralelo?, ¿se invoca otro proceso?, ¿cuántas iteraciones?, etcétera.
- **Resultados** – Es donde finalmente se obtienen los resultados de la prueba, donde se eliminan las duplicidades, se descartan los eventos que no son de interés y se realiza un análisis con profundidad de las fallas para dictaminar la calidad del código evaluado.

Conclusiones

Un argumento que suele esgrimirse es ¿para qué necesitaría un *fuzzer* si hoy existen scanners de vulnerabilidades?, la respuesta es simple: los scanners se basan en la detección de ataques conocidos, de manera que no se puede encontrar una vulnerabilidad específica si ésta aún no es conocida. Cuando la vulnerabilidad se detecta, por lo general ya hay alguien en algún lugar explotándola.

De aquí se desprende la necesidad de contar con herramientas proactivas, como los *fuzzers* a los que hemos dedicado en esta ocasión un espacio de discusión en **Magazcitum**. Las bases de datos de vulnerabilidades arrojan que 80% de las fallas en las aplicaciones se debe a errores de programación y que en este mismo porcentaje se presentarán fallas vía la aplicación de una herramienta de *fuzzing*. Si logramos vencer los actuales paradigmas del desarrollo de *software* lograremos tener cada vez código más robusto, aplicaciones más confiables y mejores niveles de productividad en un entorno cada vez más competido.

Para saber más:

» *Fuzzing for Software Security Testing and Quality Assurance.*
  - o Ari Takanen, Jared DeMott, Charlie Miller.
  - o Artech House Publishers, 1st edition (June 30, 2008).

» *Open Source Fuzzing Tools.*
  - o Noam Rathaus, Gadi Evron.
  - o Syngress (December 28, 2007).

Modelo SAMM aplicado al desarrollo de aplicaciones Web

Rubí Jaramillo Islas
CISM, ITIL e ISO 27001 Lead Auditor
rjaramillo@scitum.com.mx

Las aplicaciones *Web* son programas de *software* que los usuarios pueden utilizar accediendo a ellas a través de un navegador como *Internet Explorer, Firefox, Safari y Chrome*, entre otros. Muchas de estas aplicaciones son desarrolladas "a la medida" y frecuentemente los requerimientos de seguridad no son tomados en cuenta durante el proceso de desarrollo o adquisición de la aplicación, lo cual sí sucede por ejemplo con las características de funcionalidad, diseño visual, y uso.

El *software* inseguro está impactando de manera crítica en muchos sectores (financiero, de salud, defensa, energía, de servicios, etc.) y a medida que la infraestructura digital es cada vez más compleja e interconectada, la dificultad para lograr que una aplicación *Web* sea segura se incrementa en gran medida.

Para muchas organizaciones implementar controles de seguridad en las aplicaciones *Web* parece ser una tarea imposible debido a que en muchas ocasiones se carece de experiencia en esta área, sin embargo en la industria del *software* existen modelos, marcos de trabajo y estándares internacionales tales como CMMi, COBIT ®, OWASP y el estándar ISO/IEC 27001:2005 que pueden ser utilizados como referencia para la puesta en marcha de mejores prácticas en el desarrollo de *software* seguro.

Lograr aplicaciones *Web* seguras solo es posible cuando se utiliza un ciclo de desarrollo de *software* seguro (SDLC, *Software Development Life Cycle*), para lo cual OWASP recomienda que las organizaciones establezcan una base sólida de formación, estándares y herramientas que hagan posible la codificación segura. Por encima de esa base las organizaciones deben integrar la seguridad a su desarrollo, verificación y procesos de mantenimiento que a su vez permitan a la gerencia utilizar los datos generados para gestionar los costos y riesgos asociados a la seguridad en aplicaciones.

En esta ocasión hablaremos del modelo SAMM (*Software Assurance Maturity Model*), el cual es un marco de trabajo abierto que ayuda a definir y estructurar una estrategia de seguridad en el desarrollo de *software* basada en los riesgos específicos que enfrenta cada organización. En este artículo se toma como referencia el modelo SAMM y se proporciona una guía de los controles que se deben implementar en cada una de las prácticas de seguridad del modelo.

Entendiendo el modelo SAMM

El modelo se fundamenta en desarrollar el *software* de acuerdo a las funciones críticas del negocio y cuenta con 3 niveles de madurez definidos a través de 12 prácticas de seguridad, como lo muestra la figura 1. Estas prácticas determinan una variedad de actividades que deben ser implementadas en la organización para reducir los riesgos de seguridad e incrementar el aseguramiento del *software*.

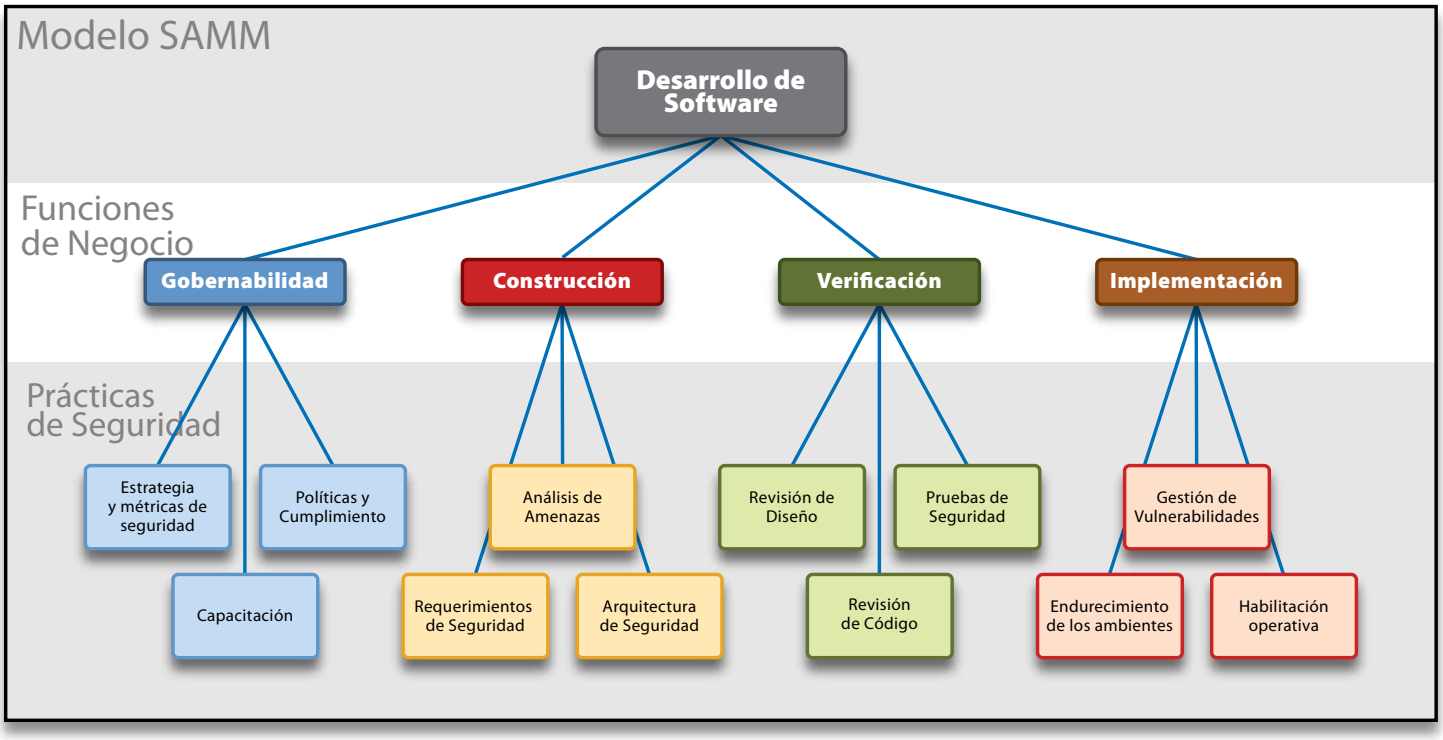


Figura 1. Modelo SAMM

El modelo SAMM fue diseñado para ser flexible, de tal manera que puede ser adoptado por cualquier tamaño de organización y fue construido bajo los siguientes principios:

- **Cambios paulatinos en la organización**.- Un programa de seguridad exitoso deben ser implementado en pequeñas iteraciones, lo cual permitirá producir entregables tangibles y de valor para la organización en el corto plazo, los cuales se pueden ir incrementando para el logro de metas a largo plazo.
- **No existe una receta única que funcione en todas las organizaciones**.- Un marco de trabajo de seguridad de *software* debe ser flexible y permitir poner en marcha los controles necesarios basándose en el nivel de riesgo de la organización.
- **Establecimiento de una directriz de seguridad**.- Las actividades de un programa de aseguramiento deben estar bien definidas, ser prácticas y medibles.

Funciones de negocio

SAMM define cuatro funciones críticas de negocio de alto nivel. Cada función es una categoría de actividades que la organización debe cumplir en el proceso de desarrollo de *software*. Estas funciones son:

I. **Gobernabilidad**. Está centrada en la definición de la estrategia, en los procesos y políticas relacionadas a cómo una organización debe gestionar el SDLC (*Software Development Life Cycle*).

II. **Construcción**. Se refiere a los procesos y actividades que la organización debe seguir para el desarrollo de la aplicación, lo cual incluye la administración del producto, recolección de requerimientos, especificaciones de la arquitectura a alto nivel, definición del diseño detallado e implementación de la aplicación.

III. **Verificación**. Se enfoca a los procesos relacionados a la revisión y pruebas de los artefactos producidos durante el desarrollo del *software*; incluye aseguramiento de calidad y diferentes tipos de pruebas.

IV. **Implementación**. Se refiere a las actividades relacionadas a la liberación de la aplicación.

SAMM precisa 3 prácticas de seguridad por cada función de negocio. Cada una de ellas es un grupo de actividades relacionadas con la seguridad. En total hay 12 prácticas de seguridad que soportan las funciones de negocio, las cuales son:

I. Prácticas de seguridad de la función de gobernabilidad

1. **Estrategia y métricas de seguridad**. Consiste en la definición de una estrategia del programa de aseguramiento de software y la definición de los procesos y actividades para la recolección de métricas de seguridad.

2. **Políticas y cumplimiento**. Involucra el establecimiento de lo que está permitido hacer por la aplicación y los usuarios de la aplicación. Identificar y trabajar dentro del ámbito de las políticas de seguridad mientras se diseña la aplicación, asegura un correcto despliegue y el cumplimiento de requerimientos regulatorios.

3. **Capacitación y entrenamiento**. Se refiere a incrementar el conocimiento de seguridad del personal involucrado en el SDLC a través de un plan de capacitación y concientización de acuerdo a las funciones de los diferentes actores. Algunos de los tópicos a incluir son: manejo de errores, administración de bitácoras, autenticación, autorización, entre otros.

El cumplimiento en tiempo real genera confianza en tiempo real cuando las TI y el control trabajan como uno.

Cada segundo de cada día hay miles de eventos a través de la red. Las soluciones de Administración del Cumplimiento de Novell® monitorean continuamente esta actividad en búsqueda de inconsistencias, generarando una vista holística en tiempo real de quién está accediendo qué y si están autorizados—todo mientras se integra con la infraestructura actual de tecnología. Así que en vez de documentar los riesgos después del suceso, puede confiar que el cumplimiento está activo, que la información está segura y que los costos de administración son reducidos. Obtenga cumplimiento en tiempo real y permita que Novell haga que las TI trabajen como una para su empresa.

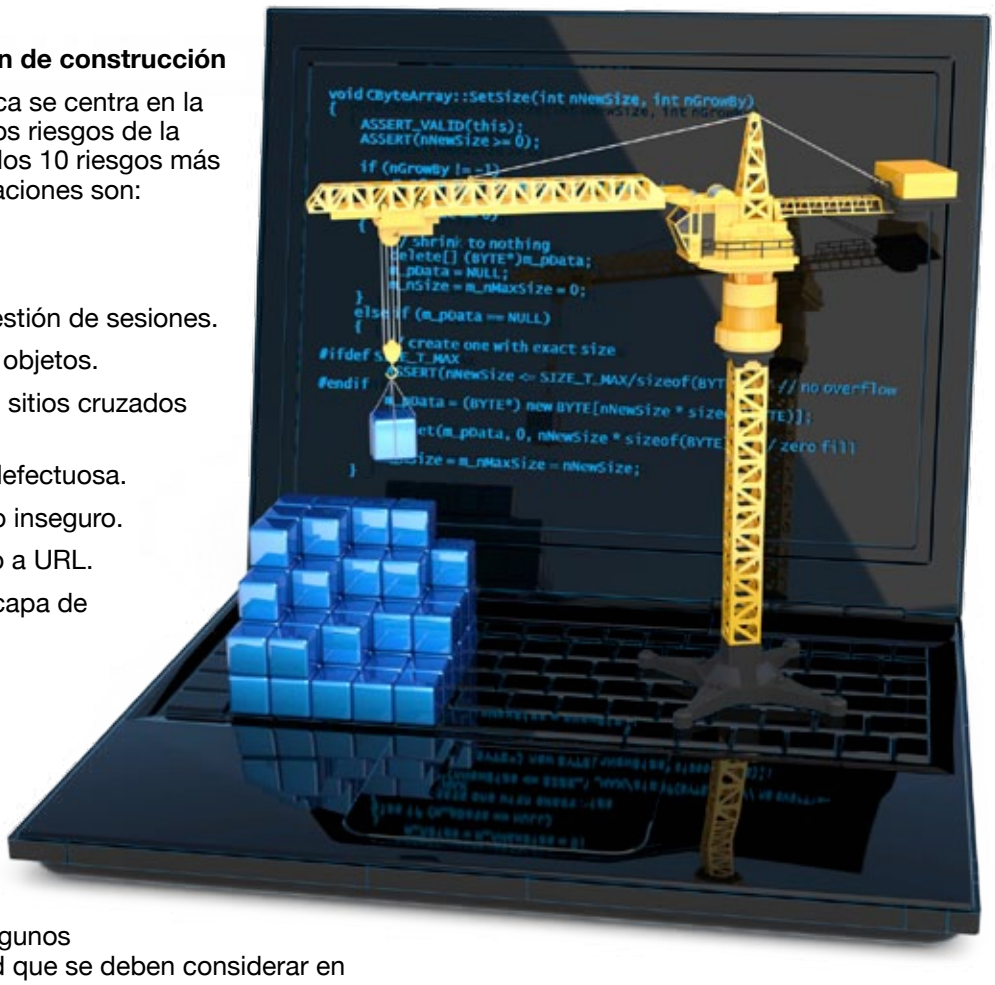
Para mayor información contáctenos al (55) 5284 2700
o visite www.novell.com/compliance

Novell®
Making IT Work As One™

Copyright © 2010 Novell, Inc. All rights reserved. Novell and the Novell logo are registered trademarks and Making IT Work As One is a trademark of Novell, Inc. in the United States and other countries.

II. Prácticas de seguridad de la función de construcción

1. **Análisis de amenazas**. Esta práctica se centra en la identificación y entendimiento de los riesgos de la aplicación. De acuerdo al OWASP los 10 riesgos más importantes de seguridad en aplicaciones son:
    a. Inyección de código.
    b. *Cross site scripting* (XSS).
    c. Pérdida de autenticación y gestión de sesiones.
    d. Referencia directa insegura a objetos.
    e. Falsificación de peticiones en sitios cruzados (CSRF).
    f. Configuración de seguridad defectuosa.
    g. Almacenamiento criptográfico inseguro.
    h. Falla de restricción de acceso a URL.
    i. Protección insuficiente en la capa de transporte.
    j. Redirecciones y reenvíos no validados.

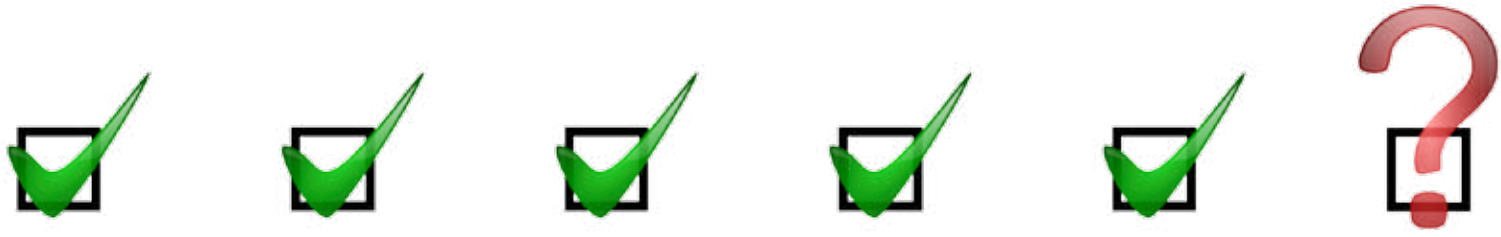


2. **Requerimientos de seguridad**. Se refiere a las expectativas de la aplicación respecto a la seguridad; los requerimientos de seguridad deben estar basados en las necesidades del negocio. Algunos de los requerimientos de seguridad que se deben considerar en aplicaciones *Web* son:
    a. Autenticación de usuarios.
    b. Autorización de usuarios.
    c. Prevención de manipulación de parámetros.
    d. Protección de datos sensibles.
    e. Prevención de hacking de sesión.
    f. Validación de datos de entrada.
    g. Auditoría y registro de actividades y transacciones.
    h. Cifrado y *hashing* de datos confidenciales.

3. **Arquitectura de seguridad**. Se refiere a introducir la seguridad en las aplicaciones *web* desde el diseño

III. Prácticas de seguridad de la función de verificación

1. **Revisión de diseño**. Se enfoca a la evaluación del diseño del *software* y problemas relacionados a la arquitectura, lo cual permite detectar problemas de manera temprana en el proceso de desarrollo de la aplicación, antes de que sea liberada.



2. **Revisión de código**. Se refiere al proceso de revisar manualmente el código fuente de la aplicación para detectar huecos de seguridad. Existen numerosos problemas de seguridad de aplicación *Web*, como los errores de inyección, que son mucho más fáciles de encontrar a través de revisión de código, que mediante pruebas externas. La revisión de código se debe realizar contra una lista de verificación que incluya:

   a. Requerimientos del negocio acerca de la disponibilidad, integridad y confidencialidad.

   b. Revisión del "Top 10 de OWASP".

   c. Requerimientos específicos de la industria tales como Sarbanes-Oxley, ISO 17799, HIPAA, PCI, entre otros.

   d. Algunas herramientas para la revisión de código como *CodeCrawler*, Orion y O2.

3. **Pruebas de seguridad**. Involucra pruebas de seguridad para descubrir vulnerabilidades y establecer un estándar mínimo para la liberación del *software*. Así como la revisión de código tiene sus puntos fuertes, también los tienen las pruebas de seguridad. Es muy convincente cuando se puede demostrar que una aplicación es insegura demostrando su explotabilidad. También hay muchos problemas de seguridad, en particular la seguridad proporcionada por la infraestructura de las aplicaciones, que simplemente no pueden ser detectados por una revisión del código, ya que no es la aplicación la que está proporcionando la seguridad. Una herramienta para llevar a cabo pruebas de seguridad a aplicaciones *Web* es *WebScarab*, la cual ayuda a la identificación de vulnerabilidades XXS, de autenticación y de control de acceso.

IV. Prácticas de seguridad de la función de implementación

1. **Administración de vulnerabilidades**. Involucra el establecimiento de procesos para manejo de vulnerabilidades e incidentes de seguridad, así como la recolección de métricas e información detallada que permita un análisis de la causa raíz del incidente para tomar acciones de mitigación.

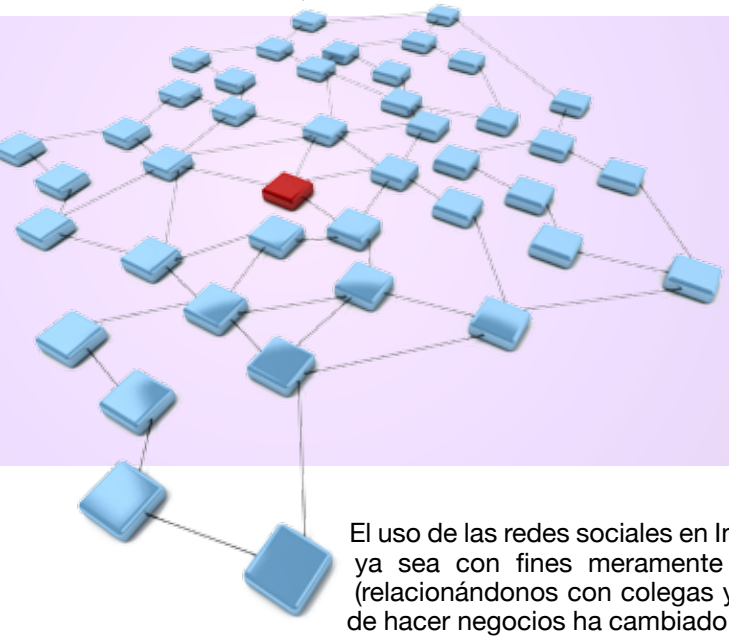
2. **Endurecimiento de los ambientes**. La práctica se centra en el aseguramiento de la infraestructura que soporta a la aplicación *Web*, tales como: sistemas operativos, *firewalls* y manejadores de bases de datos.

3. **Habilitación operativa**. La práctica se centra en la recopilación de información crítica por parte del equipo de desarrollo de la aplicación y la distribución de la misma a los usuarios y operadores. Abarca la documentación operativa y funcional de la aplicación.

Conclusiones

Las aplicaciones *Web* pueden ser complejas cuando interactúan con múltiples sistemas, y para la mayoría de las organizaciones la tarea de producir una aplicación segura o corregir una ya existente puede ser difícil, pero la seguridad en las aplicaciones no es opcional ya sea por el incremento de ataques o por cumplimiento regulatorio, por lo cual se deben establecer prácticas para el aseguramiento de sus aplicaciones *Web*. Se recomienda instituir un programa holístico que incluya a diferentes actores en la organización tales como los departamentos de seguridad y auditoría, desarrollo de *software* y la alta dirección del negocio. Es importante centrarse en las actividades que realmente ayuden a reducir el riesgo en las aplicaciones y en la organización de la manera más rentable.

Referencias:
[1] Software Assurance Maturity Model v1.0, 2009, www.opensamm.org
[2] The Open Web Application Security Project, OWASP Top 10 -2010, www.owasp.org
[3] Open Web application Security Project, OWASP Testing Guide 3.0



Seguridad y redes sociales ¿Agua y aceite?

Dinorah Valladares
dvalladares@scitum.com.mx

El uso de las redes sociales en Internet ha marcado un parteaguas en el modo en que interactuamos, ya sea con fines meramente personales (haciendo y reencontrando amigos) o profesionales (relacionándonos con colegas y grupos de trabajo e investigación con intereses afines). La forma de hacer negocios ha cambiado de manera radical comparándola con la que existía antes de que su uso se volviera masivo. Hoy en día es común que las empresas tengan presencia en las redes sociales y a través de éstas compartan información de interés para sus clientes. Las empresas que no incorporen esta nueva forma de comunicación estarán en grave riesgo de quedar rezagadas frente a sus competidores.

Las ventajas que ofrece el uso de las redes sociales saltan a la vista: nos proporcionan un medio para tener mayor alcance global, pudiendo llegar a mercados y audiencias a las que de otro modo difícilmente podríamos acceder; nos permiten posicionar nuestra marca y generar demanda, por mencionar algunas. Sin embargo debemos reflexionar en que participar de este nuevo modelo también implica afrontar riesgos, algunos conocidos y otros nuevos, y debemos estar alerta para detectarlos y evitarlos. Algunos de los que podemos identificar en primera instancia van desde fuga de información e ingreso de *malware* a nuestros sistemas, hasta atraer la atención de *hackers* y grupos delictivos con fines de lucro.

¿Qué se puede hacer?

Desde el punto de vista de negocios, una política sería la de prohibir el uso de las redes sociales en el trabajo; sin embargo esto evitaría obtener los beneficios que un buen uso de estas opciones puede significar y las cuales ya hemos mencionado.

Existen compañías que desarrollan herramientas diseñadas específicamente para brindar seguridad a quienes usan redes sociales y desde luego son una alternativa pero, como cualquier tecnología, no será suficiente si no va acompañada de nuevas prácticas de trabajo y colaboración, basadas en el diseño e implementación de políticas de cumplimiento y mejores prácticas que deben ser seguidas por los usuarios.

En octubre de 2007, la ENISA (*European Network and Information Security Agency*) agrupó en 4 categorías los 15 principales riesgos para los usuarios de las redes sociales. Los grupos y sus contenidos son:

1. Riesgos asociados a privacidad.
   - Creación de repositorios de datos personales por parte de terceros no autorizados.
   - Recolección de datos complementarios a los del perfil, como duración promedio de las conexiones, perfiles de otros usuarios con los que se tenga contacto, mensajes enviados, etcétera.
   - Reconocimiento de rostros. Sabemos que las fotografías son muy populares dentro de las redes sociales pero se puede hacer un mal uso de éstas así como facilitar conocer los detalles del círculo en el que nos movemos.
   - CBIR (*Content-Based Image Retrival*). CBIR (*Content-Based Image Retrival*). Es una tecnología emergente que permite el manejo de imágenes en un cierto contexto que tiene por objetivo incrementar la posibilidad de ubicar a algún usuario si esto fuera necesario. Por ejemplo, si en las fotos que se publican hay algún elemento del ambiente que la compone o algún patrón que se pueda identificar, esto facilitaría determinar la posible ubicación de dicho usuario.
   - Posibilidad de hacer ligas entre imágenes y metadatos mediante el etiquetado (*tagging*) de la información en las redes sociales, lo que facilita el tener ligas no deseadas a datos personales.
   - Dificultad para eliminar completamente una cuenta.

2. Variantes de los riesgos de seguridad en redes comunes.

- *Spam*
- Virus, gusanos y scripting en sitios cruzados. Las redes sociales son vulnerables a ataques XSS debido a dispositivos frágiles o no probados al 100%.
- Portales de acceso a múltiples redes sociales. El tener un portal desde el cual se accede a varias redes resultaría peligroso ya que vulnerando una sola contraseña, sobre todo si ésta es débil, se daría acceso a varios perfiles de usuario en una sola vez.

3. Riesgos de identidad.

- Hacer "*phishing*" altamente focalizado y dirigido a individuos con cierto perfil.
- Infiltración en la red social que termina en fuga de información. En la medida en que se supone que solo "mis amigos" pueden ver cierta información, pero en realidad es fácil lograr que alguien nos acepte como amigos sin conocernos. Esto dará acceso a terceros a información personal sensible.
- Suplantación del perfil y difamación por medio del robo de identidad.

4. Riesgos Sociales

- *Stalking*. Es la práctica de acosar a una persona por distintos medios (correo electrónico, Messenger, etcétera).
- *Bullying*. Lamentablemente una práctica muy común hoy en día, sobre todo entre jóvenes en edad escolar, mediante la cual humillan, lastiman y acechan a algún individuo, divulgando secretos, o inventando información que lo dañe.
- Espionaje corporativo.

Por otra parte debemos cuidar diversos factores que se desprenden del uso de las redes sociales y que pueden repercutir de manera negativa en la operación del negocio, como por ejemplo el uso del ancho de banda que se dedique a este fin o vigilar y monitorear la información que se publica, pues no hay que olvidar que lo que va a las redes sociales será público y no debemos poner en riesgo nuestra reputación y credibilidad como empresa.

Conclusiones

Es claro que si pensamos en el uso de las redes sociales como herramientas que nos permiten llegar a un mayor número de personas, podríamos suponer –equivocadamente- que el diseñar e implementar políticas de seguridad que normen su uso podría afectar nuestra audiencia. Falso. No caigamos en esta falsa creencia.

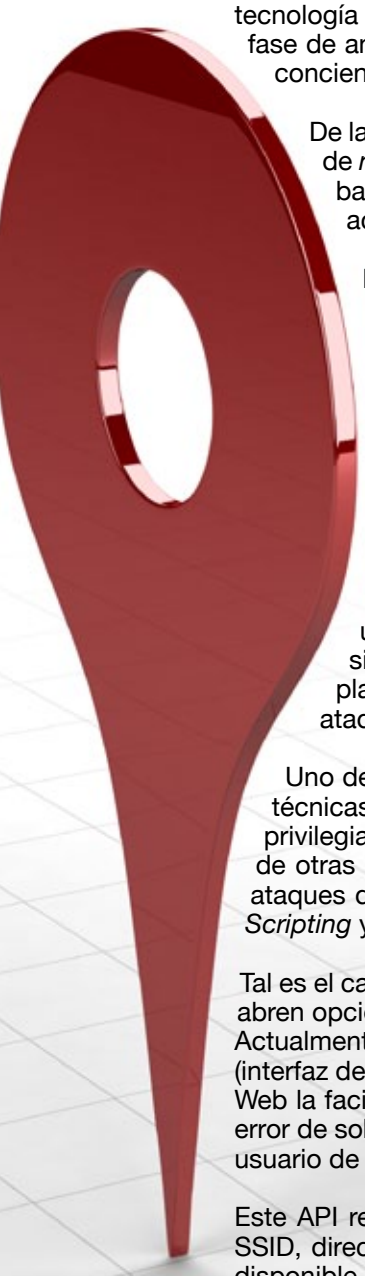
Por otra parte, debemos seguir normas básicas de seguridad y entre ellas se encuentran mantener actualizado el *software* de los dispositivos desde donde accedemos, verificar las políticas de seguridad de las redes en las que vayamos a participar, mantener las configuraciones de nuestros perfiles de usuario de acuerdo con las políticas de seguridad definidas en nuestra empresa, etcétera.

Tengamos siempre en mente que las redes sociales son un recurso público y en ellas debemos colocar solo información que nos haga sentir cómodos y no nos coloque en una situación vulnerable.

Para más información:
http://www.us-cert.gov/cas/tips/ST06-003.html
http://www.us-cert.gov/reading_room/safe_social_networking.pdf
http://www.enisa.europa.eu/act/it/oar/social-networks/security-issues-and-recommendations-for-online-social-networks

Geolocalización en Web 2.0
¿mejora la experiencia del usuario o expone su privacidad?

Raúl Alejandro Jalomo
MCTI, CISA, SSCP e ITIL
rjalomo@scitum.com.mx



Es de esperarse que en este 2011 las organizaciones tomen precauciones ante a las amenazas que la tecnología *Web* 2.0 trae consigo y éstas sean consideradas dentro de su programa de seguridad desde la fase de análisis de riesgos, así mismo, que estos temas sean tratados en su programa de capacitación de concientización en seguridad.

De la misma manera y siendo más específicos, hoy en día uno de los principales medios de introducción de *malware* a las empresas, son las redes sociales y el uso de redes *peer-to-peer*. Teniendo esto como base, cada vez más organizaciones incorporan a sus políticas sobre uso de Internet restricciones de acceso a redes sociales, apoyándose en controles tecnológicos para reforzar dichas políticas.

La *Web* 2.0, junto con nuestra tendencia a acceder y compartir información desde cualquier lugar, ha comenzado a exponer datos que en primera instancia no parecieran ser importantes, pero que al final del día la extracción de éstos, en conjunto con la extracción de otros, pudiera llegar a ser de gran relevancia para una organización. La confidencialidad de la información puede verse amenazada, a partir de que algunas personas compartan información sensible inadvertidamente cuando usan este tipo de aplicaciones, información que pudiera ser útil para competidores, ya que puede tratarse de situaciones relacionadas con nuestros clientes o bien detalles de nuevos proyectos.

Una de las premisas de los *hackers* es atacar donde están las masas, y en los últimos años hemos visto incrementarse el número de usuarios de redes sociales, la proliferación de "*Apps*" (aplicaciones de *software*) y la incorporación de funcionalidades para mejorar la interacción de los usuarios de Internet, por lo que ahora los criminales apuestan a desarrollar *malware* para la *Web* 2.0, siendo su motivo principal el robo de información. Esto les reporta una ventaja por tratarse de una plataforma popular a la cual las personas responderán de manera rápida, obteniendo como resultado ataques altamente efectivos.

Uno de los principales ataques en redes sociales es el *clickjacking*, el cual hace uso de un sinnúmero de técnicas de ingeniería social para llamar la atención de la víctima con la intención de robo de información privilegiada, como por ejemplo datos de tarjetas de crédito o datos personales que se pueden capitalizar de otras maneras. Ya sea desde un *Smartphone* o desde una *laptop* estamos cada vez más expuestos a ataques que hacen uso de aplicaciones más sofisticadas con contenido malicioso, ataques de *Cross Site Scripting* y ataques desde *botnets*.

Tal es el caso de aplicaciones *Web* 2.0 cuyo objetivo es facilitar la interacción con sus usuarios, y que a la vez abren opciones para que los criminales vulneren nuestra seguridad.
Actualmente un ejemplo real es la Geolocalización *WIFI* que desde 2008 Google ofrece a través de un API (interfaz de aplicación) de localización de dispositivos móviles a cualquier entidad que desee incluir en su sitio Web la facilidad de conocer de manera automática la localización geográfica de un visitante (con margen de error de solo algunos metros), con lo cual se ofrece la funcionalidad de desplegar contenido de interés para el usuario de acuerdo al lugar donde se encuentre.

Este API recaba información referente a los *access points Wi-Fi* cercanos, así como la fuerza de su señal, SSID, dirección MAC y dirección IP. El cliente del API viene ya incluido en *Chrome, Android, Firefox*, y está disponible como un Add-In para *Internet Explorer y Safari*, inclusive existe una especificación W3C para su implementación. La forma en que Google cierra el círculo entre la información de nuestra conexión y la localización geográfica, está basada en el mapeo de *access points Wi-Fi* y las coordenadas GPS que obtuvieron al circular por las calles del mundo para generar el contenido de *Street View* y cuya base de datos consulta el servicio de geolocalización.

Ilustración: Silverio Ortega

Su integración a un sitio *Web* es tan simple como una llamada a un método *JavaScript* y en implementaciones estándares la solicitud de autorización se lleva a cabo mediante un diálogo *JavaScript* o bien como opción en el menú del explorador para habilitar/deshabilitar.

Si bien esta funcionalidad trae algunos beneficios al usuario como ahorro de tiempo en búsquedas, resultados más precisos, así como ventajas a los comercios mejorando la exactitud de descubrimiento de *targets* de mercadotecnia, esto trae consigo una vía para divulgar información que en un momento dado o a ciertas personas no les queremos revelar. Así mismo es una oportunidad para que *hackers* o inclusive *script kiddies* obtengan información sobre nuestra última ubicación, nuestra posición actual, los lugares que frecuentamos, basándose en los lugares en que nos conectamos. Haciendo uso del cliente del API de geolocalización, -el cual se distribuye en el paquete Google *Gears* y que cada vez más frecuentemente lo encontramos ya embebido en más versiones de navegadores- en conjunto con la utilización de técnicas como *Cross-Site Scripting*, un atacante puede obtener fácilmente nuestra latitud y longitud, almacenar la información, compartirla o simplemente utilizarla para extorsión u otro tipo de ataque.

Si bien, la política de privacidad de Google indica que no almacenan información sobre la localización de los usuarios, advierte que sitios terceros podrían hacerlo. Así mismo, Google establece que el uso o lectura de información del usuario se llevará a cabo a reserva de la autorización del usuario, pero sabemos que un hacker no pedirá permiso para obtenerla.

La recomendación que haré puede parecer irrelevante, partiendo de la idea de que a la mayoría de la gente le gusta publicar en las redes sociales dónde está y a dónde irá. Sin embargo para las personas que no deseamos revelar nuestra ubicación y nos ocupamos de preservar nuestra privacidad, podemos asegurarnos de no habilitar la autorización de lectura de información que solicitan los sitios *Web* que hacen uso de Google *Gears*. Esto lo realizamosr seleccionando "*Deny*" en el diálogo de advertencia que nos presenta. Un ejemplo de esta solicitud se muestra en la figura 1.

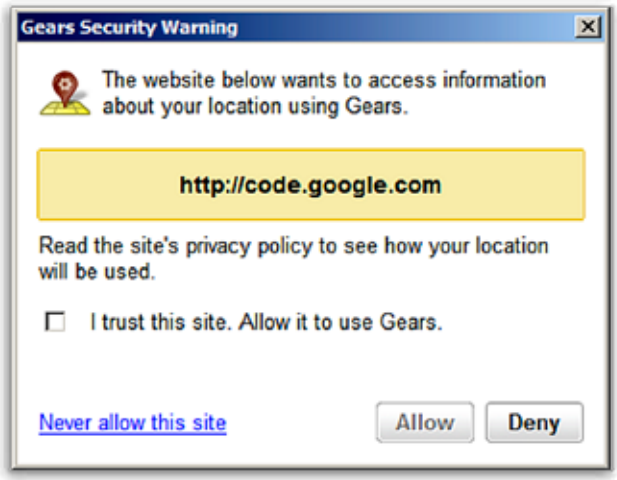
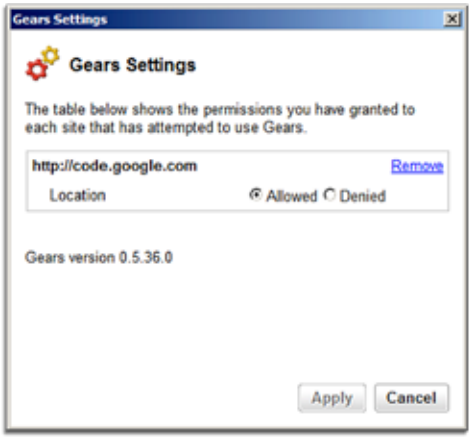


Figura 1. Solicitud de autorización de lectura de información para geolocalización.

De la misma manera, en el navegador o cliente que ya incluya el paquete Google *Gears*, podemos administrar la autorización a los sitios a los que hemos otorgado permisos de lectura de nuestra información de ubicación. Un ejemplo, accediendo desde el menú Herramientas > *Gears Settings* en *Internet Explorer*, es el siguiente:



Para el caso en que los *hackers* obtengan la información sobre nuestra localización, esperaría que en los siguientes meses las compañías de Antivirus y *Firewalls* estuvieran liberando actualizaciones con firmas que bloqueen a nivel aplicativo el envío de información de direcciones MAC y SSIDs por medio del protocolo HTTP.

En la parte legislativa, algunos países europeos han solicitado a Google dejar de recabar información de redes inalámbricas *Wi-Fi* a través de los automóviles de *Street View*, como una medida de protección a la privacidad de sus ciudadanos.

A continuación se describen algunas recomendaciones para implementar dirigidas hacia empresas que deseen reforzar sus políticas de seguridad para preservar la confidencialidad de su información, uno de sus activos más importantes.

- Detectar y remover código malicioso en *scripts* de páginas Web.
- Soluciones de filtrado *Web*, a un nivel de *Gateway*, que ayuden a detectar *malware* que esté siendo descargado.
- Información sensitiva y de negocio debe mantenerse cifrada en la medida de lo posible.
- Implementación de una solución *Data Loss Prevention* para detectar cuando la información es movida o extraída de su sitio designado, esto produce protección ante ataques externos, así como ante ataques (intencionales o no) de los propios empleados.

Una casa sin planos

Priscila Balcázar Hernández
CISA, CISSP y CGEIT
pbalcazarh@scitum.com.mx

Hoy, yo no podría hacer una rutina en C++ que al compilar funcione a la primera, porque ya olvidé las instrucciones: creo acordarme de lo más genérico de un lenguaje como: *go to, if …then, repeat…until, end*; pero lo que no olvidaré nunca es lo que dijo nuestro profesor de C++: lo más importante en la programación es la documentación ¿Se pueden imaginar a los chamacos que estábamos tan felices frente a la computadora maravillados con todo lo que podíamos hacer?, desde gráficos hasta juegos y sistemas muy complejos, ¡la cara que habremos puesto cuando nos habló sobre la documentación!

¿Se acuerdan cómo documentábamos en *BASIC*?:

```
REM Este programa calcula la masa corporal de una persona
REM La variable n es el nombre del cliente hasta 255 caracteres
```

Hasta que di clases y revisaba los programas de mis alumnos para ayudarles a que "*jalara*", y no tenían comentarios comprendí lo que decía el profesor; les cuento las sorpresas que me llevaba con los anidados, las llamadas recurrentes, y sobre todo con la lógica personal de cada quien para construir un algoritmo. Lo que decidí hacer el segundo semestre fue que la calificación del código pesaba lo mismo que la documentación, es decir, cada rutina tenía que decir para qué servía, a quién llamaba, un diagrama del flujo, un diccionario de variables, y también el "*release notes*", y un manual del usuario (por cierto también premiaba la rutina más corta, para impulsar temas de desempeño). Por supuesto me alucinaron.

Pero cuando realmente cobró sentido para mí fue cuando empecé a auditar, ya en mi trabajo, al realizar pruebas sustantivas donde me tocaba revisar código, buscando controles, evidencias, e información útil para determinar hallazgos, incumplimiento, riesgos, etcétera. El 90% de los códigos no estaba documentado, así que la interpretación estuvo sujeta a mis corridas de escritorio y un trace manual para entender los flujos. Esto me restaba precisión en las conclusiones porque tenía que suponer ciertos criterios que había tomado el programador, además de todo el tiempo que implicaba. Cuando se aproximaba el año 2000, el mundo informático preveía que muchos sistemas podrían "*tronar*" primordialmente por haber usado sólo dos dígitos para los años, y que al cambiar de 99 a 00 los programas se volverían locos. Fue la época mejor pagada para los programadores de Cobol y de varios otros lenguajes que tuvieron su auge en los años 70 y 80, y que no habían documentado sus sistemas. ¡Eran los únicos que sabían por dónde moverle al código!

Imaginemos una casa sin planos. Sería muy difícil de remodelar, correríamos riesgos al decidir modificar un muro, construir otro piso, agregar servicios; también sería muy difícil encontrar las causas de goteras, fugas, cuarteaduras. Un banco no podría calcular una valuación; un perito no querría emitir un juicio sobre la salud de la construcción; un posible comprador cuestionaría la falta de los planos; un notario no la escrituraría.

En la actualidad, una de las enormes aportaciones a la industria informática ha sido el *open source*; entre sus bondades se encuentra la disponibilidad gratuita del código fuente para hacer mejoras y adaptaciones, y el hecho de que está documentado y cuenta tras bambalinas con una entusiasta comunidad de desarrolladores y usuarios que continuamente revisan y documentan el código. El código abierto nos permite conocer la calidad del producto en sus entrañas y también garantiza que no hay en su interior ningún "caballo de Troya" que comprometa su seguridad.

De acuerdo con Gary McGraw, en su libro "*Software Security – Building Security In*", los siete puntos para (re-) construir aplicaciones seguras son, en orden de efectividad:

1. Revisión de código
2. Análisis de riesgos de la arquitectura
3. Pruebas de penetración
4. Pruebas de seguridad basadas en riesgos
5. Casos de abuso
6. Requerimientos de seguridad
7. Operaciones de seguridad

Prácticamente en los siete aspectos la documentación existente es un aspecto muy relevante que no sólo ahorraría tiempo en un proyecto de auditoría de seguridad aplicativa o en la detección de fallas, sino que aportaría información notable sobre cómo está construido el sistema, cuáles son los servicios de una clase, los límites de transaccionalidad debidos a tamaños de variables, las propiedades de objetos que heredan a otros objetos, los datos que se pasan por valor o por referencia, lo que significa una variable, los criterios que se definieron para declarar una variable, la exposición de un campo a recibir cualquier tipo de input que permita una ejecución de comandos de SQL (provocando inyecciones de SQL, *buffer overflows*, etcétera).

En fin, creo que no tenemos que convencernos de la importancia de la documentación, sino asegurar que se lleve a cabo para obtener grandes beneficios como:

- Agilizar las actualizaciones.
- Entender el flujo del sistema.
- Prolongar la vida del sistema.
- Detectar huecos de seguridad del código.
- Facilitar los procesos de solución de fallas.
- Buscar la universalidad y compatibilidad.
- Identificar riesgos de la aplicación.

En la contraparte, el código bien documentado de un sistema crítico o sensible es un arma de dos filos que podría proporcionar información útil para ataques y fraudes. Por ello, es importantísimo implementar a su vez controles de seguridad al código para protegerlo, como cifrado, DLP, firmas digitales, bloqueo de puertos USB, acuerdos de confidencialidad con programadores, entre otros.

Ahora bien, ¿qué es lo que incluye la documentación de un sistema para asegurar que cumple con sus objetivos? Aquí una lista de los componentes principales:

- Los requerimientos del negocio (funcionalidad, regulaciones, volumen y desempeño)
- Los requerimientos de seguridad
- La arquitectura de la aplicación
- La funcionalidad del sistema
- El diccionario de datos
- Los casos de uso
- Mapeo de controles versus casos de abuso
- Diseño específico de los controles de seguridad del sistema
- Las premisas del o de los programadores
- Las especificaciones de la plataforma de desarrollo
- Requerimientos del sistema para que funcione la aplicación
- Los convencionalismos tomados en el código
- Los comentarios dentro del código
- La posibilidad de reuso de objetos, clases, módulos
- La conectividad e interfaces del sistema con otros sistemas
- Las especificaciones de comunicación hacia el sistema (¿cómo podría un externo llamar a este sistema o a algunas de sus partes?, regulado, claro, por los requerimientos de seguridad)
- Los casos de prueba y sus criterios de aceptación
- Limitaciones o errores conocidos del sistema
- Manual del usuario
- Manual de instalación
- Manual del administrador
- Manual de capacitación
- Las políticas de protección del código
- "*Release notes*" para nuevas versiones
- Control de versiones del código
- Responsables del sistema

La invitación es a todos los jóvenes programadores que empiezan su carrera profesional (y a los veteranos también), para que adopten prácticas sanas encaminadas a la seguridad de las aplicaciones, robusteciendo su funcionalidad y agilizando la actualización. Hoy existen muchas herramientas que brindan las comunidades open source las cuales ayudan y facilitan la vida del desarrollador para no reinventar la rueda, incluyendo rutinas y controles de seguridad, técnicas de documentación, errores frecuentes, vulnerabilidades conocidas de los lenguajes, prácticas de codificación, técnicas de optimización, librerías para evitar que se explote alguna vulnerabilidad y un sinfín de material enriquecedor

¡Mucha suerte entonces!

Algunas fuentes que se pueden consultar al respecto:
http://www.galeon.com/neoprogramadores/howdocod.htm
http://mit.ocw.universia.net/6.170/6.170/f01/related-resources/javastyleguide.htm
http://www.swsec.com/resources/touchpoints/
http://www.owasp.org/index.php/Main_Page
http://www.cert.org/secure-coding/
https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/coding.html

Bibliografía:
Building Secure Software
Gary McGraw
Addison-Wesley, 2001

¿Se puede aprovechar la nube sin crear tormentas?

we can

ca technologies

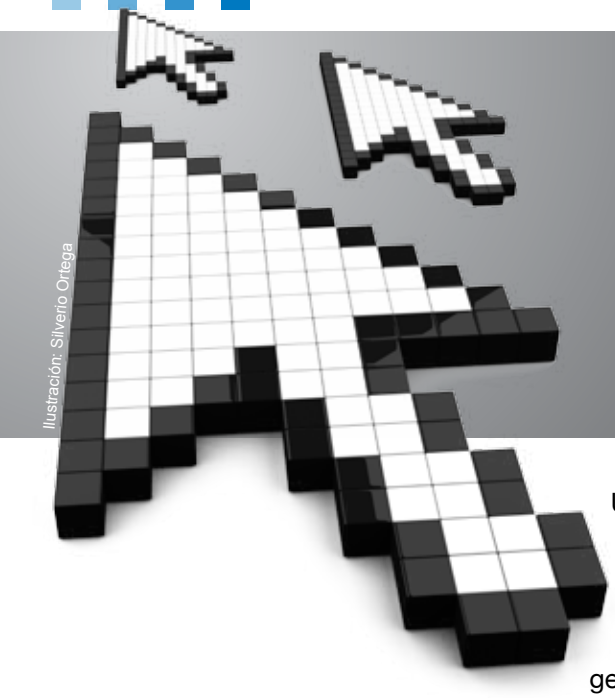


Ilustración: Silverio Ortega

¡Allí está el detalle! Aplicaciones seguras contra todos

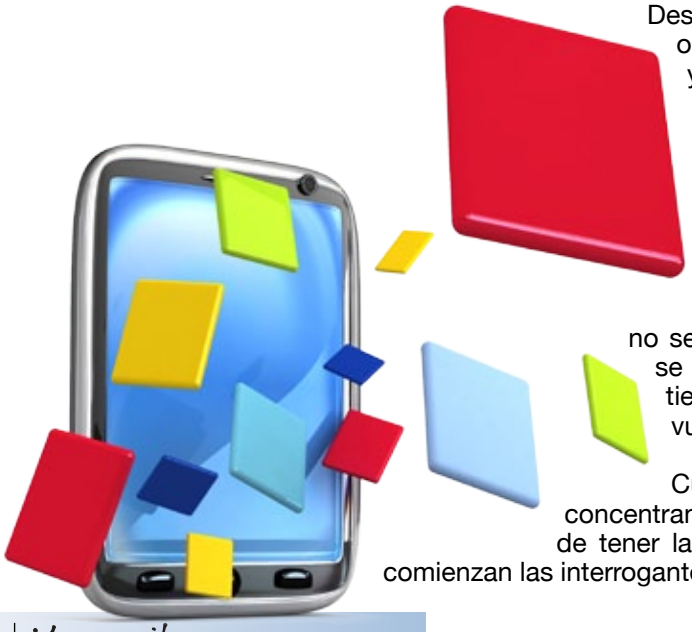
Jorge Alberto Barroso Andrade
jbarroso@scitum.com.mx

Una aplicación es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo. La diferencia radica en la especialidad para la que fue diseñada; las aplicaciones son la parte que interactúa directamente con los usuarios finales, a diferencia de otros programas como los sistemas operativos (control de las computadoras), las utilidades (que realizan tareas de mantenimiento y tienen otros usos en general), y los lenguajes de programación (mediante los cuales se crean los programas).

Las aplicaciones móviles son extensiones informáticas para dispositivos portátiles y son un punto focal para todas las empresas, debido a la gran cantidad de dispositivos de esta índole habilitados para los altos ejecutivos y personal clave (normalmente "*smartphones*"). Para estos dispositivos las aplicaciones pueden ser gratuitas o de pago, y a los propietarios les brindan las más variadas funcionalidades que incluyen tanto el ámbito laboral como el del entretenimiento ya que han evolucionado para permitirnos llevar el registro de gastos, información deportiva, guías de restaurantes, carteleras de cine, reservación de hoteles, procesar textos, así como realizar funciones de hojas de cálculo.

Las nuevas aplicaciones más innovadoras son las llamadas de realidad aumentada que combinan elementos reales y virtuales (tal es el caso de GPS y *Googlemaps*). Una de las aplicaciones que estará en la mira durante este año es *Android* (sistema operativo desarrollado por Google y que podrá alcanzar un gran incremento en su penetración del mercado móvil durante este año) que, si bien como lo mencionamos anteriormente es un sistema operativo, estará disponible en dispositivos móviles por lo que su interacción con usuarios finales será importante.

La automatización es posible en prácticamente cualquier aspecto de la vida: compras, comunicación, cómics, deportes, estilo de vida, finanzas, herramientas, multimedia, noticias, meteorología, ocio, productividad, referencia, salud, sociedad, temas, viajes, demostración, bibliotecas de *software*…y así se puede continuar la lista para resaltar lo impactantes que son en el nuevo estilo de vida, y en efecto, están allí para ayudar a alcanzar nuestros objetivos más fácil, rápida y eficientemente. Pueden ejecutarse en todas las plataformas y dispositivos, la cantidad de aplicaciones hoy no tiene comparación con el pasado (y de eso, hace apenas unos cinco años).

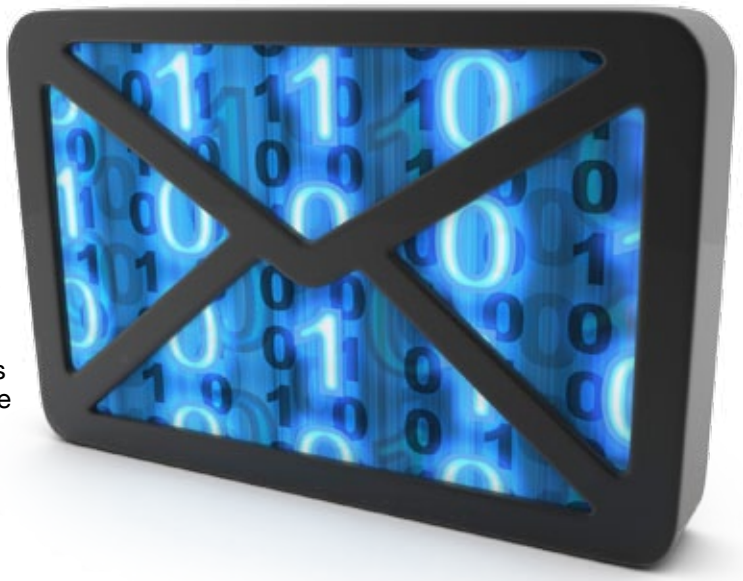


Desde el año 2009 se ha visto un incremento en las aplicaciones orientadas a SaaS (*software as a service*), movilidad, virtualización y portabilidad, redes sociales, *Web* y video, arquitecturas orientadas a servicios *Web* (WOA), debido a tendencias que están dirigidas hacia los sectores que utilizan las redes sociales, dispositivos móviles o cómputo en la nube.

Las aplicaciones pueden ser muy simples o muy complejas en su función; con las herramientas de programación que ahorran a los programadores mucho código, se hacen cada vez más dinámicas y en tiempos más cortos, ya que para desarrollarlas no se requiere de un elevado nivel de conocimiento. En un estudio se menciona que casi 60% de las aplicaciones de todo tipo tienen errores graves en cuanto a la seguridad, lo que hace más vulnerables a las empresas.

Cuando se crea una nueva aplicación los desarrolladores se concentran en la funcionalidad, debido a que siempre existe la urgencia de tener la mejor solución en el menor tiempo, entonces allí es donde comienzan las interrogantes: ¿La aplicación está alineada a los estándares de seguridad?,

¿cumple con las políticas internas de la compañía?, ¿pueden realizarse cambios que no afecten la productividad de la empresa?, ¿se puede extraer o importar información?, ¿la información es compatible entre los diferentes sistemas? y un largo etcétera.



El hacer aplicaciones seguras requiere entonces de considerar los aspectos básicos que permitan la ausencia de errores. Al estar en la capa más cercana al usuario, el diseño debe considerar las necesidades e inclusive las preferencias o sugerencias de los mismos usuarios.

Cuando se realizan aplicaciones seguras no podemos perder de vista los procesos que intervienen en el uso que se da a los datos:

- Entrada u origen.
- Procesamiento (generar resultados).
- Almacenamiento.
- Salida de datos (resultados obtenidos).
- Registro de eventos.

Cada una de estas etapas forman un proceso que puede estar lleno de controles de todo tipo y definidos por diferentes personas con distintos roles como responsables de ejecutar, validar, autorizar y revisar los resultados.

Las aplicaciones actuales permiten entregar controles con la confiabilidad que hoy en día se requiere, siempre que sean implementados en el lugar y tiempo adecuados, de lo contrario no nos sorprenda encontrar aplicaciones que no sean seguras.

¿Qué controles y en dónde?

La pregunta es sencilla de contestar, sin embargo la complejidad y el nivel detallado para su implementación no lo son tanto; lo más que se puede lograr es crear una aplicación que cumpla con la funcionalidad y las mejores prácticas para alcanzar el objetivo deseado.

He aquí tres conceptos a tener en cuenta que ayudan a entender la seguridad aplicativa:

1. Las aplicaciones deben hacer únicamente lo que tienen que hacer, nada más.
2. La seguridad es tan importante como la funcionalidad.
3. Para comprender la funcionalidad y la seguridad de las aplicaciones es necesario entender en dónde ocurren los fallos de seguridad, cuándo son más susceptibles de error y qué es lo que puede ocurrir.

Existen muchos tipos de fallos de seguridad que pueden tener las aplicaciones, por mencionar algunos: las contraseñas por omisión y de configuración débil, que bien pueden ser errores de los usuarios o incluso de los programadores.

Identificar en dónde se encuentran los problemas en el uso de las aplicaciones y los resultados que se quieren obtener es la base para el desarrollo de la “seguridad aplicativa”.

Lo primero es identificar la entrada de datos de manera que cumpla con la lógica que tiene la aplicación: tipo de datos y longitud son puntos críticos para evitar un hueco de seguridad que pueda costarnos más que el no recibir la respuesta a una petición. Aquí lo mejor es discriminar aquellos datos que no son adecuados para realizar las operaciones necesarias, lo que puede evitar un registro de indisponibilidad del servidor o incluso un acceso no autorizado.

Al procesar un dato pudiera establecerse alguna verificación que permitiera conocer que éste es válido para realizar las operaciones y generar una salida válida, es decir, se podría generar una validación antes de llevar a cabo cualquier procesamiento para, de este modo, obtener el resultado esperado de acuerdo a cada instrucción.

La siguiente etapa será mostrar, presentar o almacenar el resultado; aquí se podría comprometer éste al no lograr almacenarlo el tiempo suficiente para que pueda ser consultado, reprocesado y presentado al usuario en un tiempo razonable, es por ello que almacenar los datos requiere de protección de memoria. Simultáneamente es importante validar que los datos procesados sean almacenados de acuerdo con las características esperadas: tipo de dato y validez.

Una vez que el dato ha sido almacenado correctamente la consistencia de su consulta deberá evitar algún riesgo relacionado (falta de encriptación, pérdida de credenciales, acceso no autorizado) que comprometa la integridad, confidencialidad y veracidad de quién lo ha solicitado. Si bien la encriptación de los datos almacenados implica un costo, al realizar un análisis acerca de qué información puede ser cifrada y cuál no, de manera que no tenga un impacto en el desempeño de las operaciones, redituará en grandes beneficios.

Siempre será necesario contar con un registro de las actividades que se han realizado para identificar si la información ha sido modificada, alterada o ha sufrido algún cambio importante. Protegerla de alteraciones no autorizadas es indispensable para mantener su utilidad y confiabilidad.

«Las aplicaciones deben hacer únicamente lo que tienen que hacer, nada más»

Conclusiones

Cuando se trata de aplicaciones nada es “seguro”. La seguridad aplicativa es toda una disciplina que se tiene que considerar cuando se hace un desarrollo o cuando se compra una aplicación para mejorar la productividad y calidad de las operaciones empresariales; mientras más segura sea una aplicación mayor será el costo y aun así no se puede estar totalmente seguro de que la información estará 100% libre de fallos.

Seleccionar la aplicación que cumpla con las mejores prácticas proporciona la certeza de que la probabilidad de ocurrencia de algún fallo de seguridad sea mínima y, en consecuencia, propiciaría el continuar operando cuando nadie más pueda hacerlo, sin embargo hay que considerar los costos (de infraestructura, servicios y humanos).

Recordemos que para avanzar un gran paso se requiere atacar el eslabón más débil y en el caso de las aplicaciones éste se encuentra tanto en el origen como al final, es decir, todo viene y va a los usuarios. Antes de comenzar a sacar la cartera se tendrá que analizar en dónde se puede conseguir el mayor beneficio de una aplicación segura, si el impacto es real y si el personal es el indicado.

La “seguridad aplicativa” comienza con el usuario responsable, que posee el conocimiento y la suficiente consciencia para saber que cualquier aplicación de negocios tiene como objetivo lograr un beneficio específico relacionado con el negocio y *¡allí está el detalle!...*

La seguridad de los teléfonos inteligentes en el ambiente empresarial

Spencer James Scott
sscott@scitum.com.mx
Traducción: Héctor Acevedo Juárez

Somos consumidores de información, vivimos y compartimos nuestras vidas en línea. Habitamos un mundo en el que la demanda de acceso a la información en plataformas móviles crece a un ritmo acelerado: queremos nuestro correo electrónico en cualquier momento, ver el perfil de nuestros amigos en *Facebook*, saber dónde está el café más cercano para poder "*tweetear*" nuestros pensamientos diarios y queremos estar al tanto de lo que ocurre en el mundo. Los teléfonos inteligentes, conocidos en inglés como smartphones, permiten este nivel de conectividad y se han convertido en herramientas esenciales en nuestra vida diaria y en los negocios.

Los *smartphones* están cambiando el ambiente de los negocios, conforme las empresas se mueven hacia operaciones globales se han vuelto indispensables en muchos casos. Los dispositivos móviles ofrecen a las organizaciones la habilidad de mantener conectados a sus empleados a toda hora, permitiéndoles desarrollar sus tareas en cualquier lugar, sin importar si están en casa, en la oficina o viajando.

Cuando una compañía favorece el uso de teléfonos inteligentes por parte de sus empleados, debe afrontar muchas amenazas que son similares a las que enfrenta por el uso de estaciones de trabajo o computadoras portátiles, entre ellas están el *malware*, virus, explotación de vulnerabilidades e intercepción de datos; lo que puede llevar al robo de información sensible para la organización. Así pues, las empresas que opten por el uso de dispositivos móviles tendrán que estar conscientes del riesgo asociado y tomar medidas para minimizarlo.

Descripción de los riesgos

Los teléfonos inteligentes proveen un tipo de conectividad y movilidad que los convierte en plataformas de cómputo móvil con funcionalidad similar a la de una laptop, por lo que se enfrentan a los mismos riesgos. De hecho, los *hackers* están desarrollando *malware* muy sofisticado para dispositivos móviles y buscan constantemente nuevas formas para atacarlos. Estos ataques a menudo son exitosos debido al pequeño tamaño de las pantallas, lo que hace difícil verificar la integridad de las ligas y de los sitios *Web* desplegados, además de que también suele haber poca conciencia de los usuarios acerca de las amenazas y el *malware* que posibilitan las fugas de información vía los teléfonos inteligentes.

Riesgo	Descripción
Fuga de información	Un teléfono robado o extraviado sin protección en la memoria puede permitir que un tercero tenga acceso a los datos almacenados en el dispositivo
Procesos incorrectos para poner un aparato fuera de servicio	Un teléfono descartado o transferido a un tercero sin antes remover la información sensible puede permitir que un tercero tenga acceso a dicha información
Divulgación no intencional de información	La mayoría de las aplicaciones permite configurar el nivel de privacidad, pero muchos usuarios no saben, o no recuerdan, que se transmiten datos y que hay que revisar los controles de privacidad para controlar la transmisión
Phishing	Un atacante puede colectar contraseñas, números de tarjeta de crédito y cosas semejantes mediante aplicaciones o mensajes falsos
Spyware	El *software* espía puede permitir el acceso a información almacenada en el teléfono. Nota: El *spyware* incluye cualquier *software* que solicita y abusa de peticiones de acceso o cambio de privilegios. No incluye *software* específico de vigilancia

Ataques de *network spoofing*	Un atacante puede desplegar puntos de acceso inalámbrico falsos para que los usuarios se conecten a ellos y a partir de eso despliegue otro tipo de ataque
Vigilancia	Es factible espiar y vigilar a un usuario en particular mediante su teléfono
Dialerware	Un atacante puede realizar fraudes mediante malware instalado en un teléfono para hacer uso fraudulento de tarifas SMS y llamadas telefónicas
***Malware* financiero**	*Malware* específicamente diseñado para robar datos de tarjetas de crédito y de cuentas bancarias en línea o para modificar transacciones bancarias o de comercio electrónico
Congestión de redes	Ataques de negación de servicio para evitar que los usuarios hagan uso de la red

El impacto en la seguridad de la red

No importa si son proporcionados por la empresa o de uso personal, los teléfonos son dispositivos que fácilmente se mueven dentro y fuera de la red corporativa, atravesando los *firewalls* internos y externos, y pueden conectarse por *WiFi* o incluso evitar la red mediante conexiones celulares. Esto significa que los usuarios pueden descargar *malware* de sitios Web mediante sus conexiones a redes 3G/4G y luego dispersarlos en la red corporativa al emplear la *WiFi.*

Por otro lado, los teléfonos suelen tener grandes cantidades de memoria que suponen una amenaza de fuga de datos al permitir la transferencia de datos al celular desde una computadora.

Es muy difícil para los departamentos de TI controlar lo que los usuarios hacen con sus teléfonos inteligentes y cómo esos dispositivos exponen información del negocio a las amenazas de seguridad. Aún en los casos en los que los celulares son proporcionados por el propio departamento de TI, cualquier dispositivo que pueda evitar las medidas de seguridad es falible y está sujeto a los mismos riesgos.

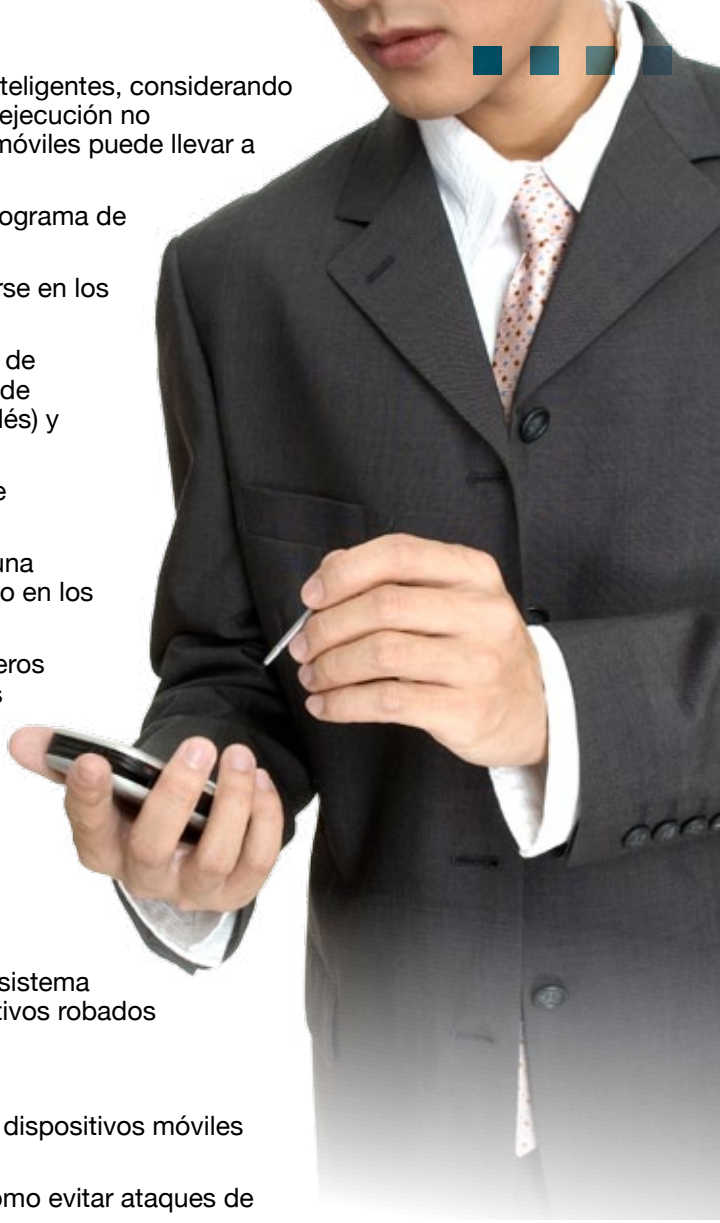
Mejores prácticas para administrar teléfonos inteligentes

En ambientes de alta seguridad, como los bancos o algunas agencias gubernamentales, se exige el uso controlado de teléfonos inteligentes, aunque esto será cada vez más difícil para éstas y otras organizaciones conforme el mercado de consumo siga creciendo y sea un motor para la adopción de estos aparatos: hoy en día en cualquier oficina podemos ver *Blackberrys, iPhones* y teléfonos con *Android*.

Así pues, a continuación listo algunas prácticas a tener en cuenta para administrar teléfonos inteligentes en una organización:

1. Actualice su política de seguridad para incluir el tema de los teléfonos inteligentes y para definir planes de concientización que provean información que ayude a un uso seguro.
2. Defina con claridad qué dispositivos están permitidos, sin importar si serán proporcionados por la empresa o no.
3. Puntualice la naturaleza de los servicios que se podrán utilizar en los dispositivos móviles, tomando en cuenta la arquitectura de TI existente.

4. Identifique la manera en que la gente emplea los teléfonos inteligentes, considerando tanto la cultura corporativa, los factores humanos y cómo la ejecución no determinística de procesos a través del uso de dispositivos móviles puede llevar a riesgos no predecibles.
5. Integre los dispositivos que la empresa proporciona en un programa de administración de activos.
6. Describa el tipo de autenticación y cifrado que debe emplearse en los dispositivos.
7. Defina cómo debe almacenarse y transmitirse la información de manera segura mediante el uso de tráfico cifrado, el empleo de PIN (número de identificación personal, por sus siglas en inglés) y contraseñas seguras.
8. Defina qué tareas pueden realizar qué empleados y el tipo de aplicaciones permitidas.
9. Desactive aplicaciones que no son necesarias y establezca una política para restringir la instalación de *software* no autorizado en los dispositivos móviles.
10. Las contraseñas para sitios *Web* deben resguardarse en llaveros digitales para prevenir su almacenamiento en el *cache* de los navegadores *Web*.
11. Instale software de seguridad, incluyendo *firewalls* y antivirus, en los teléfonos inteligentes.
12. Si no se requieren para uso corporativo, desactive características como *Bluetooth, WiFi* y GPS.
13. Incluya los dispositivos móviles en la política corporativa de respaldos.
14. Despliegue capacidades remotas de borrado a través de un sistema central de administración que le permita deshabilitar dispositivos robados o extraviados.
15. Utilice cifrado WPA2, o mejor, para las redes *WiFi*.
16. Asegúrese de que las computadoras que se sincronizan con dispositivos móviles tengan programas de *firewall* y antivirus actualizados.
17. Proporcione entrenamiento a los usuarios para que sepan cómo evitar ataques de phishing por SMS (conocidos como ataques de *smishing*).
18. Establezca mecanismos de acceso cifrado con clientes de VPN que utilicen SSL o IPSec.
19. Incluya los teléfonos inteligentes en el programa de seguridad de dispositivos finales para prevenir la fuga de información por copia de archivos vía USB.
20. Asegúrese de que los dispositivos móviles están contemplados en el programa de administración de parches y actualizaciones.



Conclusiones

La innovación tecnológica ha allanado el camino para la asimilación de los teléfonos inteligentes en el lugar de trabajo. Estos dispositivos han actuado como un catalizador para mejorar la eficiencia, productividad y disponibilidad de las operaciones de negocios y, si bien muchas empresas han optado por utilizar esta tecnología, a menudo no han considerado los riesgos del negocio o las implicaciones normativas que se relacionan con estos dispositivos.

La pérdida, robo o corrupción de información sensible o confidencial, la contaminación con *malware* que puede afectar no sólo a un teléfono sino a toda una red corporativa, y la manera en que los empleados usan estos dispositivos son sólo algunos de los riesgos a tomar en cuenta cuando se emplea esta tecnología. Adicionalmente a la normatividad y sistemas de gobierno corporativo y de TI que ya existen, los riesgos y los controles asociados a ellos, en su caso, deben ser evaluados para asegurar que los activos de información de la empresa se mantengan disponibles y protegidos frente al uso de teléfonos inteligentes.

Las empresas que están considerando el uso de dispositivos móviles de cómputo tendrán que calcular los beneficios que esta tecnología ofrece y los riesgos adicionales que conlleva. Una vez que los beneficios y los riesgos han sido evaluados, el negocio debe emplear su normatividad y sus sistemas de gobierno corporativo para asegurar que los cambios en los procesos y en las políticas son entendidos, implementados y que se aplican los niveles adecuados de seguridad para prevenir la pérdida de datos.

Departamento de Defensa

David Gutiérrez
CISSP y CISA.
dagutierrez@scitum.com.mx

Seguridad de aplicaciones web: state of affairs.

¿No es suficiente mi *firewall*?

Seguramente durante el desarrollo de nuestras actividades como profesionales de seguridad nos ha tocado escuchar: “Sí tenemos seguridad, contamos con un *firewall*” o “Nuestro portal sí está protegido, contamos con un *firewall*”. Lamentablemente no es así y en algunos lugares persisten estos conceptos equivocados.

Las amenazas específicas para aplicaciones *Web* han evolucionado de manera sostenida, y se puede decir que seguirán siendo el blanco favorito de *hackers* en el corto y mediano plazo. La gran mayoría de las tecnologías de seguridad como *firewalls* y prevención de intrusos han probado ser poco efectivas ante el vasto mundo de amenazas específicas para las aplicaciones *Web*. Poco a poco los controles tecnológicos especializados han ido ganando terreno y ahora contamos con firewalls de aplicaciones *Web* (*Web application firewalls*) y *firewalls* de bases de datos (*database firewalls*).

El uso de dispositivos de seguridad de propósito específico, como los *firewalls* de aplicaciones *Web* y de bases de datos, puede ayudar efectivamente al control de amenazas en este ámbito. Sin embargo, si nuestro objetivo es contar con un esquema integral de seguridad aplicativa, el uso de este tipo de tecnología es muy recomendable como la primera aproximación, pero hay que tener en mente que no será suficiente.

Un esquema integral de protección de aplicaciones *Web* tiene que incluir una estrategia encaminada a tratar la raíz del problema: estas estrategias generalmente son desarrolladas con la funcionalidad -y no con la seguridad- en mente. Es necesario que nos ocupemos de diseñar y codificar las aplicaciones con los controles de seguridad embebidos en ellas desde las primeras etapas de desarrollo. Para ayudarnos en esta tarea existen herramientas que analizan de manera automatizada el código y determinan si en alguna línea o función es posible que éste presente vulnerabilidades, aunque es cierto que esto nos obliga a detectarlas después de que se codificó la aplicación, y para remediarlo habría que regresar al principio y volver a revisar todas las etapas de desarrollo de la aplicación hasta el momento en que se pueda verificar que en efecto las deficiencias fueron corregidas.

Lo anterior no suena muy eficiente y va en contra de la teoría moderna de control de calidad, en donde se prefiere corregir los problemas en etapas tempranas del desarrollo, sobre todo porque es mucho menos costoso. De cualquier forma, el uso de este tipo de herramientas se recomienda como una segunda fase en la estrategia de protección de aplicaciones *Web*, ya que la implantación de estos controles y procesos llevará menos tiempo que la utilización de metodologías de desarrollo seguro.

El establecimiento y puesta en práctica de metodologías de desarrollo seguro de aplicaciones se perfila como la solución más efectiva y de menor costo; siempre será más barato remediar las vulnerabilidades antes de que puedan ser explotadas. No obstante lo anterior, muy probablemente la implantación y homogeneización de la práctica de cualquier metodología de desarrollo seguro llevará mucho tiempo lo que nos lleva a sugerir que este control tiene que ser planeado como una tercera, y última, fase de la estrategia.

Ilustración: Silverio Ortega

La estrategia propuesta está construida sobre todo desde el punto de vista de la efectividad en los controles y el tiempo que se lleva implementarlos; sin embargo, resulta imprescindible revisar el presupuesto con el que se dispone para el despliegue de la estrategia de protección de aplicaciones *Web*, ya que el conducir las tres fases propuestas requerirá de fondos significativos que probablemente no existan, al menos eso es lo que indica la tendencia.

¿Hacia dónde va la seguridad para aplicaciones Web?

En el contexto de la industria estadounidense, el Instituto Ponemon (que se dedica a levantar encuestas en materias especializadas de tecnologías de información) reporta dentro de su informe "*State of Web Application Security*" de abril de 2010, los siguientes hallazgos clave:

- Una clara discrepancia entre el número de incidentes de seguridad, que involucra una aplicación o una base de datos, y el presupuesto que las organizaciones destinan a controles de seguridad para protección de éstas.
- Falta de auspicio por parte de la alta dirección en temas de seguridad aplicativa.
- Las aplicaciones *Web* se están moviendo hacia servicios tipo nube (*cloud computing*).

Si bien es razonable decir que el contexto estadounidense difiere de la realidad en México, sí nos sirve como parámetro de referencia para estimar lo que es factible que se reproduzca en nuestro escenario.

En el caso del primer hallazgo, con certeza muchos nos podemos identificar con la situación. Los presupuestos de seguridad hoy en día se encuentran volcados a la seguridad perimetral y el control de las amenazas de código malicioso. Lo cierto es que tampoco podríamos pedir que no se atiendan estas necesidades de manera prioritaria, lo que nos dejaría con la única alternativa de pedir aumento en el presupuesto para seguridad ¡Vaya situación tan difícil!, sin embargo es necesario que organicemos nuestros argumentos en concordancia con los objetivos de negocio de nuestra empresa o entidad, expresar los riesgos en términos de pérdidas para el negocio (monetarias o de otra índole, pero sobre todo monetarias) y realizar un meticuloso análisis costo/beneficio. Al final del ejercicio habremos ganado de una u otra manera: si el resultado es negativo, nos evitaremos la pena de invertir en controles onerosos; y si el resultado es positivo, tendremos el argumento sólido que necesitamos para presentar nuestro caso a la alta dirección, lo cual de seguro nos reportará un impacto benéfico para contrarrestar la situación que se describe en el segundo hallazgo.

«La gran mayoría de las tecnologías de seguridad como firewalls y prevención de intrusos han probado ser poco efectivas ante el vasto mundo de amenazas específicas para las aplicaciones web»

El tercer hallazgo que seleccioné podría servir como una alternativa muy efectiva en costo para transferir la responsabilidad de la protección de aplicaciones *Web* a un tercero, el cual nos brindaría el servicio con la seguridad necesaria incluida y con todas las ventajas de este modelo de entrega de servicios. Sólo hay un detalle: realmente no sabemos si esto se podrá realizar en México en un futuro cercano.

Historias

José Ramírez Agüero
jramireza@scitum.com.mx

Vías de fuga

En la mayoría de las compañías donde he laborado, me han hecho firmar contratos de confidencialidad con el fin de proteger su información. Como todos sabemos la actividad diaria de las organizaciones genera datos e información de todo tipo y mantener esto bajo control es fundamental, pero ¿realmente se puede evitar la fuga de información?

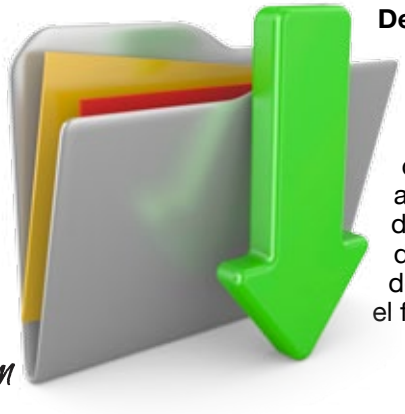
Ahora en México existen algunas normas que obligan a ciertos sectores empresariales a proteger la información, pero ¿y los demás sectores?, podría pensarse que también aplican controles, pero muchos de nosotros que estamos dentro del ámbito de la seguridad de la información sabemos que es algo alejado de la realidad y he aquí el por qué.

Hoy en día no es necesario poner un pie en las instalaciones de la compañía para acceder a la información que es propiedad de ésta. Con la popularidad de Internet, las amenazas pueden venir desde el exterior y si no se cuenta con una protección perimetral de la red informática, así como un control de acceso de sus usuarios, la fuga de información a través de código malicioso está latente. De igual forma pasará cuando los usuarios se conecten remotamente a los centros de trabajo y no cuenten con encriptación de datos, así como con las herramientas necesarias para proteger su equipo móvil cuando se conecte a redes públicas.

Los empleados son también amenazas, pues de manera inconsciente pueden convertirse en un punto de fuga de información; lo único que se requiere es acceso a dicha información y extraerla. En la actualidad esto es muy fácil a través de dispositivos portátiles (*USB Drives*, teléfonos celulares), así como mediante la utilización de servicios gratuitos de correo electrónico, hospedaje y respaldo de datos vía Internet, por eso es importante contar con una política de gestión de usuarios, cada uno con sus permisos correspondientes para acceder a determinadas aplicaciones y/o sitios *Web*. También es preciso definir en los procesos del Departamento de Recursos Humanos algún procedimiento que impida, o al menos dificulte, el que una persona extraiga información de la compañía.

Como se percibe, nunca estaremos protegidos al 100% contra un robo de información. Hay amenazas internas y externas que están presentes en todo momento y pueden provocar una fuga hacia algún tercero. La fuga de datos no es nueva, siempre ha existido el espionaje industrial (virus, *spyware*, etc.), los empleados descontentos que roban información o las pérdidas accidentales de datos. Es pues primordial establecer procedimientos y políticas contra este tipo de problema en cada organización, y no necesariamente solo para cumplir con normas o leyes dictadas por el gobierno. A continuación, enlisto algunas de las principales vías de fuga de información:

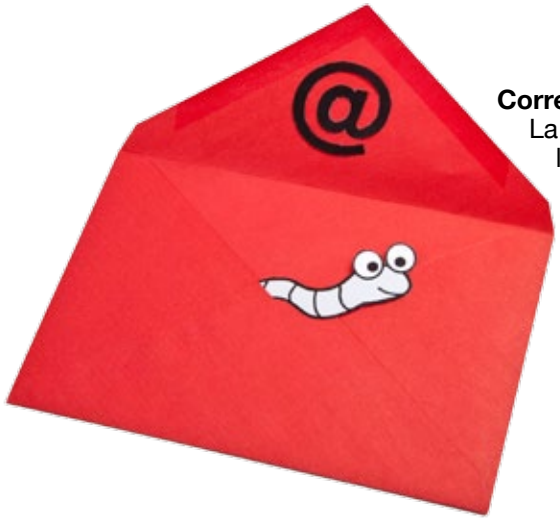
Código malicioso
Troyanos, *spyware, keyloggers*, todos estos desarrollos maliciosos tienen una sola misión: robar información. Ningún lector de esta revista tiene dudas sobre la importancia de protegerse contra esta amenaza a través de soluciones *antimalware* o sistemas antivirus para los troyanos, etcétera.



Descargas
Las aplicaciones de uso doméstico que se descargan vía *Web*, además de ser un dolor de cabeza y un posible agujero de seguridad, es factible que sean utilizadas para transmitir información confidencial. *Skype, 4Shared*, MSN son aplicaciones comunes en los hogares, pero dentro de las compañías son una amenaza que se debe considerar. Una solución para evitar la fuga de datos a través de estos medios es establecer políticas de uso de esas aplicaciones en los equipos propiedad de la compañía, dependiendo del tipo de usuario y la información que maneja, con el fin de bloquear o borrar estas aplicaciones.

Portables
La pérdida o robo de USB, CD y portátiles es una realidad. En México por desgracia la inseguridad está a la orden del día, aunado a los descuidos del personal, y los costos asociados a este tipo de pérdidas son relevantes, no sólo por las posibles sanciones si hay datos confidenciales de por medio, sino por el daño que se puede ocasionar a la imagen de una empresa.

La mejor opción para evitar estas pérdidas es, en primer lugar, controlar la información que intenta ser copiada de la red de la compañía hacia dispositivos móviles. Una vez identificada y controlada la información que se deja copiar, ésta debería ser cifrada para evitar un uso inadecuado en caso de robo o pérdida.



Correo
La vigilancia de esta vía de comunicación debería estar en primer lugar, ya que es el medio más usado por las organizaciones durante las horas laborables para transmitir información tanto legítima como ilegítima. Una vez más, las dos medidas a tomar para evitar la fuga a través de este medio serían controlar la información que está siendo enviada por correo (tanto el de la compañía como el personal) y, en el caso de que se trate de información confidencial, que ésta sea cifrada.

Redes sociales
Son una de las nuevas formas de enviar información y su control es complicado; lo primero que hay que hacer es educar a los empleados y en general a los usuarios porque, aunque parezca increíble, en las redes sociales las personas comparten información que nunca compartirían en su vida "real". Por ello es imperativo contar con protecciones de seguridad que filtren el contenido URL por usuario o grupos de usuarios dentro de la compañía.

Si somos capaces de controlar por lo menos estas vías de fuga de datos estaremos en una buena posición para asegurar que la información confidencial esté a salvo. Recuerden que más vale prevenir que corregir. Si hablamos de información, poco podremos hacer si en algún momento se escapa de nuestro control, ya que hoy en día copiar datos y transmitirlos por la red es cuestión de segundos (o menos).

En el pensar de...

Eduardo Patricio Sánchez
CISSP, GCIH, CISM,
GWAPT, CEH y CHFI
epsanchez@scitum.com.mx

El capital humano, una posible fuente de pérdida de datos

Hace algún tiempo una persona conocida tuvo que viajar por cuestiones laborales a un país que se encontraba inmerso en conflictos internos y por esta razón se consideraba un lugar peligroso. La empresa para la que trabajaba decidió contratar un seguro que protegía no solo la integridad física de esta persona, sino también el valor que tenía como activo en la organización.

No solamente con seguros se protegen las organizaciones; también existen los contratos de no divulgación de información, más conocidos como NDA (*Non Disclosure Agreement*), que son contratos de carácter legal entre dos individuos u organizaciones que les permiten compartir información confidencial con un fin común pero restringen su divulgación a terceros para evitar que se convierta de carácter público. Otra forma en que las organizaciones cubren sus activos de información son las patentes, las cuales son derechos exclusivos que se conceden a un organismo o individuo para evitar que un tercero utilice su tecnología a menos que éste cuente con su autorización explícita. También existen las marcas, protección a derechos de autor, etcétera; todos ellos mecanismos para proteger activos valiosos.

Sin embargo ¿cómo protegemos la experiencia, el instinto, la inspiración o la destreza? Son elementos que cuando una persona clave los pone en acción sobre nuestros datos o información pueden ser la diferencia entre lograr los objetivos o no. Cuando una organización pierde a personal clave por fallecimiento, incapacidad o simplemente porque deja la organización, se puede estar perdiendo el "know how", y con esto se pone en riesgo el negocio, no solo desde la perspectiva financiera sino incluso es factible que afecte los procesos clave que permitan sobrevivir a la organización. En México hay seguros empresariales que apoyan a las organizaciones para recibir una indemnización al perder un talento clave, lo cual ayuda a capacitar a algún sucesor o a sobrellevar la operación del negocio hasta encontrar quién ocupe dicho cargo.

Otro riesgo en cuanto a la fuga de información que maneja nuestro personal, se presenta cuando éste no está consciente de la criticidad de ella. Un par de ejemplos de esto los observamos en dos situaciones: cuando Gray Powell --empleado de Apple--, durante el festejo de su cumpleaños perdió un prototipo del que sería el nuevo teléfono de Apple; y cuando *Kevin Butler* hizo un *retweet* (RT) de la llave maestra del PS3, en un momento en el que Sony se encontraba intentando demandar a todo aquel que publicara esta información. Estos dos ejemplos nos ayudan a visualizar que, sin estar sometidos a algún ataque de ingeniería social o espionaje industrial, podemos cometer errores y divulgar información sensible.

El identificar el 100% de posibles puntos de fuga de información en una organización es muy complejo, sin embargo, el estar conscientes de que no todo es tecnología o procesos, sino también personas, nos permitirá tomar decisiones más eficaces en la protección de lo más importante, la Información.

http://gizmodo.com/#!5520438/how-apple-lost-the-next-iphone
http://games.slashdot.org/story/11/02/09/1412253/Sony-Marketing-Man-Tweets-PS3-Master-Key?from=twitter

Consejos para una implementación segura de VoIP (voz sobre IP)

Tips

Osvaldo Hernández
CCSA e ITIL
lhernandez@scitum.com.mx

Debido al rápido crecimiento de las soluciones de VoIP, muchos hackers están sacando provecho de las debilidades o vulnerabilidades de dicha tecnología a través de ataques de denegación de servicio, inundación, rapto de llamada, espionaje en el medio, *vishing*, etcétera.

Es por ello que antes de comenzar con la implementación de voz sobre IP (VoIP) debe considerar los siguientes consejos para poner en marcha esta herramienta de modo exitoso y seguro:

Consejo 1

- Garantice que la infraestructura de seguridad y de red, incluyendo *firewall*, IDS y VPNs, están optimizados y configurados para soportar los requisitos avanzados para VoIP, los cuales contemplan:

- **Las reglas tradicionales de políticas estáticas para el control de tráfico de VoIP.**
- **La asignación dinámica de los puertos durante el establecimiento de la llamada, lo cual requiere de apertura y cierre de puertos (SIP, SDP, SCCP, RTCP, RTP y SRTP) en el *firewall* dedicado a VoIP.**
- **La inspección de trafico VoIP no sólo en la capa de red, sino también a nivel de aplicación para detectar problemas con protocolos de VoIP en NAT (*Network Address Translation*).**
- **El ancho de banda, latencia y calidad (QoS) son indispensables para el procesamiento de voz.**

Consejo 2

- Derivado de la identificación regular de vulnerabilidades de seguridad críticas que dejan su infraestructura de VoIP expuesta a ataques de denegación de servicio, espionaje del medio, rapto de registro de llamada e incluso situaciones más grave como ataques de desbordamiento de buffer, debe garantizar que el sistema operativo de su conmutador de IP (IP PBX) siempre esté actualizado con parches de seguridad para vulnerabilidades recientes, así evitara ataques e interrupciones del servicio.

Consejo 3

- Cambie los usuarios y contraseñas por omisión de toda la infraestructura de VoIP (teléfonos, conmutadores, etcétera).

Consejo 4

- Deshabilite cualquier característica de configuración innecesaria como accesos remotos, transferencia de datos (FTP) y *telnet*. En caso de requerirlo, asegure adecuadamente los accesos remotos a un número reducido de empleados ya que los teléfonos de VoIP son los componentes más comunes de entrada a la infraestructura de VoIP.

Consejo 5

- Utilice siempre canales seguros con el apoyo de tecnologías de cifrado de túneles IPsec para proteger el tráfico de VoIP. Aunque muchos de los protocolos de VoIP incluyen capacidades para el cifrado y la autenticación, la mayoría es opcional por lo cual es esencial establecer túneles seguros entre los flujos de VoIP (señalización y control de llamadas, y medios de comunicación) y las redes que no son de confianza.

Consejo 6

- Estructure la red convergente aprovechando las VLAN (redes virtuales) para separar la red de voz y la red con los dispositivos de datos, ya que el despliegue de dispositivos de VoIP en las redes VLAN separadas permite aislar el tráfico de voz y señalización de tráfico para una óptima utilización de calidad del servicio (QoS) y tener un impacto limitado en la seguridad.

Consejo 7

- Monitoree y analice los detalles de las llamadas sospechosas con regularidad, de ser posible diariamente.

Consejo 8

- Limite el número de intentos fallidos para acceder al sistema del conmutador (IP PBX) antes de bloquear por seguridad.

Consejo 9

- Cambie regularmente las contraseñas de seguridad en los dispositivos de VoIP.

Espero que les sea de utilidad.

Saludos

Prevención de fugas de información en comunicaciones unificadas

Marcos Polanco
CISSP, CISA y CISM.
mpolanco@scitum.com.mx

Actualmente las organizaciones tienen la necesidad de contar con mejor comunicación y mayor velocidad y agilidad para ejecutar los procesos de negocio, por otro lado, cada vez es más frecuente que los usuarios que ejecutan estos procesos sean móviles. Es por ello que contar con servicios que les permitan interactuar de forma más eficiente, flexible, rápida y barata son factores clave de éxito para los negocios.

Las comunicaciones unificadas (*Unified Communications*) -integración entre la red y aplicaciones de datos con servicios de comunicación sobre IP (voz, mensajería instantánea y video)- vienen a proveer una plataforma muy importante para generar dichos factores determinantes en las organizaciones.

Este nuevo contexto suena muy interesante pero, ¿se ha detenido a reflexionar en los riesgos que esto podría implicar?, ¿se ha preguntado si algún extraño o delincuente podría escuchar, grabar, alterar o publicar sus conversaciones?, ¿podría sufrir un ataque a la infraestructura que bloquee el sistema y lo deje totalmente incomunicado?, ¿podría alguien hacer llamadas "usurpando" su número e identidad?, ¿podrían cobrarle por concepto de llamadas que usted no realizó?

Cuando se ejecuta un proyecto de comunicaciones unificadas hay que considerar que existen diversos retos desde el punto de vista de seguridad, algunos de ellos muy particulares y otros similares a los que presentan las redes y aplicaciones tradicionales de IP; los más relevantes son:

- Amenazas de intercepción y modificaciones.
- Amenazas de interrupción del servicio.
- Amenazas de abuso del servicio.

Asimismo existen ataques específicos para los cuales debemos contar con mecanismos de protección, por mencionar DoS (*denial of service), call hijacking, call recording, caller ID spoofing, man in the middle,* fraude, SPIT (*SPAM over IP Telephony*), *vishing (voice phishing*), etcétera.

Lo ideal es que la seguridad en las comunicaciones unificadas se contemple desde un inicio, es decir, desde el diseño de la arquitectura y no como una idea de último momento; desafortunadamente, muchas veces la seguridad se considera hasta que se tiene el primer incidente notorio o con impacto para el negocio.

Las estrategias para prevenir fugas de información en las comunicaciones unificadas tienen que pensarse en un esquema multicapas y deben estar dirigidas a cubrir los tres aspectos básicos de la seguridad (confidencialidad, integridad y disponibilidad) y a garantizar la calidad del servicio y la calidad de la experiencia del usuario final. Es necesario tomar en cuenta una serie de controles de distinta naturaleza pero complementarios, tales como los siguientes:

- **Normativos**. Se refieren a contemplar la definición de políticas y normas correspondientes así como a realizar análisis de riesgos y auditorías recurrentes.
- **Tecnológicos**. A través de:
  - Elementos ya existentes como parte de la infraestructura de soporte de la red IP (VLANs, ACLs, endurecimiento de plataformas, etcétera),
  - la infraestructura propia de comunicaciones unificadas,
  - de elementos ya implementados como parte de estrategia de seguridad de la red IP (*firewalls*, IPSs, etc.),
  - de funciones avanzadas y protocolos seguros (IPSec, TLS/DTLS, SRTP, SRTCP, etc.) y
  - de elementos especializados que permiten implementar controles muy granulares como SBC y UCTM.
- **Operativos**. Que toman en cuenta aspectos como administración de parches, control de configuraciones y cambios, administración de activos y monitoreo permanente.

¿Está su organización adecuadamente protegida?

«Las comunicaciones unificadas (Unified Communications) vienen a proveer una plataforma muy importante para generar dichos factores determinantes en las organizaciones»

¿Sabías que

Scitum

es el único
Centro de Entrenamiento
autorizado en México?

(ISC)² EDUCATION AFFILIATE
Authorized Provider

Por lo que ahora puedes:

1.- Tomar el Seminario Oficial de CISSP de (ISC)² del 1° al 5 de agosto de 2011, a un precio especial de $1,500.00 Dlls. +IVA
2.- Presentar el examen de certificación CISSP el 3 de septiembre de 2011, cuyo costo es de $549.00 Dlls.

La sede tanto del seminario como del examen es:
Oficinas de Scitum, Cd. de México.
Av. Paseo de la Reforma No.373
Col. Cuauhtémoc
C.P. 06500 México D.F.

Más informes, comuníquese al 9150 7496, lunes a viernes de 9:00 a 18:00 hrs. o bien al correo electrónico: capacitacion-isc2@scitum.com.mx
La fecha límite de inscripciones es el 22 de julio de 2011.

¿Y si le *envié* este **archivo** a la ***persona equivocada***?

Check Point realmente hace que su sistema de **DLP** funcione.

¿Usted, alguna vez, ya ha enviado accidentalmente un correo para la persona equivocada o ha anexado algún documento que no era para ser compartido?

Check Point realmente hace que su sistema de DLP funcione, combinando tecnología y procesos para evolucionar su negocio de tener apenas detección pasiva a una verdadera prevención, antes que las fugas de datos ocurran.

PREVIENE la pérdida de datos

EDUCA a los usuarios

FORTALECE políticas de datos

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

©2010 Check Point Software Technologies Ltd. All rights reserved. Check Point, the Check Point logo, and Check Point Endpoint Security Full Disk Encryption are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.