PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 5 | MARZO 2010 | *ISSN EN TRÁMITE* | REVISTA BIMESTRAL

Editorial

Una vez más **.Seguridad** es publicada para ofrecer a los lectores un espacio donde se pueden informar sobre asuntos de Seguridad Informática así como fomentar la cultura de la seguridad en cómputo.

En esta edición te presentamos algunos ataques que con frecuencia pueden ser usados en Internet. Es de especial importancia hacer notar que las precauciones a tomar en cuenta para evitar ser víctimas de estos ataques, son tanto a nivel usuario final como a nivel de desarrollador de las aplicaciones que se ofrecen.

De esta forma no debemos de bajar la guardia, ya que nuevas amenazas surgen cada día y todos debemos estar alerta para hacer buen uso de Internet.

Rocío del Pilar Soto Astorga
Departamento de Seguridad en Cómputo

David Jiménez Domínguez

Actualmente vivimos sumergidos en una sociedad que interactúa diariamente con las tecnologías de la información como parte de sus tareas diarias; desde el uso del cajero ATM, el pago en el supermercado hasta la actualización del estado en nuestra red social favorita. Si bien es cierto que la privacidad es un derecho humano, el uso del correo electrónico, tarjetas de crédito y toda aquella actividad que utilice de manera electrónica nuestros datos, requiere que la privacidad de la información de cada ser humano u organización sea protegida durante el uso de estos servicios. Cada individuo vive con una serie de datos como son el correo electrónico, número telefónico, CURP, historial crediticio, etc., los cuales utilizamos e intercambiamos diariamente con personas, compañías e incluso el gobierno. Cada vez que solicitamos un crédito o inclusive al solicitar empleo, estos datos son consultados y juzgados a favor o en contra de nosotros. Básicamente lo que le pase a nuestros datos, nos afecta directamente a nosotros, en medida de que aquella información considerada como privada sea modificada o consultada sin nuestra autorización.

Por otra parte, en las organizaciones cada vez es más común escuchar que la protección de la información es una iniciativa clave para la operación del negocio, desde la información de clientes y proveedores pasando por el material con propiedad intelectual hasta el correo personal de los empleados. Esto ha orillado a varias empresas a implementar estrategias de protección y monitoreo del uso de la información, que permitan reducir el riesgo de que algún empleado pueda ser víctima de un ataque masivo o incluso de un ataque dirigido hacia él en particular, con el objeto de obtener información confidencial de la organización.

Ataques dirigidos

A diferencia de un ataque de tipo broadcast[1] que es más propenso a ser identificado rápidamente por alguna firma antivirus como un código malicioso, en un ataque dirigido el intruso debe ser paciente previo al ataque, buscando la oportunidad correcta para acceder a una sola computadora que pueda contener información confidencial o que permita el acceso a otros sistemas dentro de una red privada. Esta es la característica principal de un ataque dirigido o también conocido como targeted attack, el cual difiere del escenario tradicional de un ataque por malware, spam o phishing.

[1] Ataque en el cual un intruso utiliza la propagación masiva de malware por medio de un sitio web

Por ejemplo, en un escenario tradicional el intruso busca propagar su malware de manera masiva, con el objeto de tener el control de tantos equipos como sea posible, para posteriormente enviar correo spam, generar ataques de negación de servicio o rentar esta red de equipos comprometidos a un mejor postor, entre otro tipo de actividades. Sin embargo, durante la propagación del código malicioso es muy probable que una muestra de este código sea capturada por un honeypot[2] o una honeynet[3] de una firma de seguridad, y sea analizada para generar una actualización de un software antivirus que proteja a los usuarios de dicha amenaza.

En un ataque dirigido no existe una propagación de malware, ni el envío masivo de correo electrónico a varias direcciones, en lugar de ello, el intruso envía cinco, tres o incluso un solo correo electrónico con malware como archivo adjunto. Esto conlleva a que sea difícil obtener una muestra de este malware ya que muy probablemente nunca es capturado por un honeypot, en cambio solo afecta a una sola organización y posiblemente a un solo empleado. Si este usuario no se da cuenta de que este correo tiene un código malicioso como adjunto, pasará desapercibido por la organización y por ende por la mayoría de las firmas antivirus.

¿Cómo funciona un ataque dirigido?

Primero que nada el intruso es paciente, analiza a la víctima y busca la oportunidad apropiada para realizar un ataque exitoso. Previo al ataque, el intruso investiga a su víctima utilizando la información de fácil acceso. Por ejemplo, si la víctima es una organización, el intruso podría identificar el objetivo del ataque por medio del organigrama que está disponible en la página web de la empresa, investigar sobre sus socios de negocio y conocer un poco sobre la industria sobre la que opera la organización de manera que pueda crear un correo electrónico con un mensaje creíble para el usuario y que propicie la apertura del código malicioso. Incluso el intruso podría utilizar ingeniería social en llamadas hechas a individuos identificados en el organigrama de la organización para obtener más información sobre el objetivo.

Una vez que se cuenta con toda esta información, el intruso busca la manera de influenciar al usuario a que abra el archivo adjunto; comúnmente un archivo .doc, .exe, .pdf, .xls o .ppt que puede contener una carta o presentación proveniente de un proveedor o de la editorial de una de sus revistas electrónicas

[2] Sistemas de información que busca ser un anzuelo para su uso no autorizado o ilícito.

[3] Consta de una red de sistemas de información, cuyo propósito es ser comprometida por algún usuario malicioso, con la finalidad de aprender sobre las herramientas, tácticas y motivos que alientan a este tipo de usuarios.

preferidas a la cual está suscrito. Si el usuario obtiene el correo y ejecuta el código malicioso que viene adjunto, el malware tomará control de su computadora y dará acceso remoto al intruso mientras utiliza técnicas para ocultar su presencia en el equipo del usuario, estas técnicas son similares a las utilizadas por rootkits[4].

Ahora es cuestión de tiempo para que el intruso obtenga información confidencial del usuario o peor aún, que pueda comprometer a otros sistemas dentro de la red privada de la organización, sistemas con información de más alto valor para la víctima.

¿Cómo protegerse?

Veamos el caso de una organización con problemas de propagación de spam. Si este correo llega a uno de los empleados, se supone que fue una excepción mal manejada por el filtro anti-spam. Sin embargo, en el caso de un ataque dirigido si uno de los empleados recibe este correo, este empleado es el objetivo del ataque, el cual busca obtener su información personal o de la organización. Por estos motivos hay que proteger el eslabón más débil, el usuario, teniendo en cuenta las siguientes recomendaciones:

1. **Capacitación de empleados.** Que los empleados sepan manejar información confidencial y que sean conscientes sobre el manejo de la información al interior de la organización en un mayor grado, ayudará a que la identificación de este tipo de ataques sea hecha, en la mayoría de las ocasiones, por las propias víctimas.
2. **Asegurar la red.** El intruso buscará información sobre la victima previo al ataque, si esta información no la puede obtener por medio de ingeniería social o de manera directa en la información pública de la organización, buscará obtenerla mediante un ataque sobre la red.
3. **Evitar proporcionar información de más.** Un ataque dirigido requiere que el intruso conozca bien a la víctima y mientras más información le proporcionemos, será más probable que seamos víctimas de este ataque. Consideremos que los datos de contacto y la estructura organizacional de la empresa son datos confidenciales.
4. **Deshacerse de información confidencial de manera adecuada. Se recomienda** implementar procesos para el procesamiento de documentos confidenciales que han sido desechados. No se debe permitir que los empleados se deshagan de esta información directamente en el basurero, se debe utilizar un triturador o mejor aún, un contenedor de documentos para su posterior procesamiento.

[4] Conjunto de programas que un invasor utiliza para ocultar su intrusión y obtener acceso a nivel de administrador en un equipo de cómputo o sistema.

El tener en consideración las recomendaciones anteriores y mientras que el personal de cumplimiento a las políticas de seguridad alineadas a las mejores prácticas para el manejo de la información y mejor aún, que exista un compromiso de la dirección de la organización para el cumplimiento de estos procesos, ayudará a mitigar el riesgo de un ataque dirigido.

Referencias:

http://www.honeynet.unam.mx/docs/Intro.pdf
http://www.youtube.com/user/fslabs
http://www.seguridad.unam.mx/usuario-casero/

Angie Aguilar Domínguez

Sergio Iniesta Juárez

Como usuarios de Internet, muchas veces solo nos interesa lo que estamos buscando y en algunas ocasiones nos llama la atención lo que llegamos a encontrar mientras navegamos pero, *¡cuidado!* existen varios tipos de ataques y fallas sobre aplicaciones Web[5] que podrían causar que nuestra navegación por Internet no sea tan agradable y segura como quisiéramos, en donde personas malintencionadas se aprovechan de ciertas vulnerabilidades de la aplicación o descuidos del usuario para explotar y obtener información a la que *se supone* no deberían de tener acceso.

El fallo de aplicación Web se puede ver reflejado en un comportamiento inesperado de la misma, como la devolución de datos incorrectos, páginas en blanco y un conjunto de errores que provocan que los visitantes abandonen la aplicación ya que no saben qué hacer o cómo reaccionar ante el evento, éste tipo de errores resultan molestos y pueden llegar a "permitir" (mediante el uso de técnicas de ataque o intrusión) el acceso a personas maliciosas para ver información privada referente a los usuarios o también acceder a información importante de la aplicación Web en cuestión. Por ejemplo, si la aplicación Web de uso de banca en línea de nuestro banco no toma las medidas preventivas correspondientes (como utilizar cifrado en la transmisión de la información), un usuario malintencionado puede obtener información sensible (como número de cuentas bancarias o contraseñas) .

> Entre las fallas que podemos llegar a encontrar, están los mensajes de error, esto ocurre cuando la aplicación no permite visitar cierta parte de la aplicación (por ejemplo, una galería de fotos) que debería ser posible ver y entonces muestra mensajes como "404 Archivo no encontrado" o "500 Error interno del servidor" (ver Figura 1). Estos mensajes conllevan a que los usuarios dejen de visitar la página o servicio y así la compañía vaya perdiendo clientes.

[5] Aplicación Web: aplicación que puede ser vista desde un navegador de Internet.

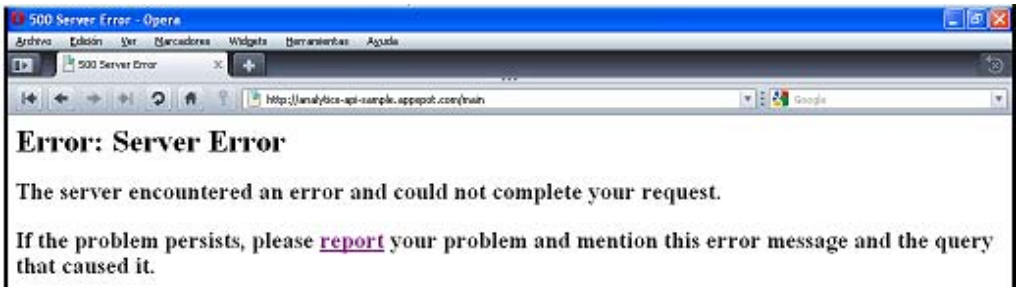

Figura 1. Mensaje de error en una aplicación Web

Una mala práctica recurrente es ocultar valores o funciones de una aplicación Web que se saben no es seguras, para tratar de evitar el riesgo de comprometer al sistema (por ejemplo, tratar de ocultar la parte de nuestra aplicación donde se administren los datos que normalmente debería estar protegida con credenciales de usuario). Ocultar los errores en la aplicación ciertamente no los elimina y un usuario con conocimientos especializados puede encontrarlos con relativa facilidad empleando software y técnicas maliciosas.

Ejemplo de esto es un ataque llamado XSS (Cross Site Scripting) en el cual se puede esconder de varias maneras algún programa malicioso (virus, caballo de Troya, gusano, etc.) en una liga, de modo que al darle clic se instalan programas indeseables sin que nos percatemos de ello. Estos programas permiten posteriormente el acceso a la información que tenemos almacenada en nuestra computadora, nombres de usuario, contraseñas, datos personales, preferencias y cuentas bancarias que se ven expuestas al atacante poniéndonos en serios problemas.

A veces el XSS se puede ejecutar automáticamente cuando se abre un correo electrónico, archivos adjuntos del correo, al leer un artículo, o en un post. Por ello hay que ser cuidadosos al realizar alguna de éstas acciones. Una forma de evitar caer en este tipo de ataque es instalando alguna herramienta de software de seguridad (como antivirus o antispyware) que impida ejecutar el código script[6] en nuestro navegador de Internet.

Otro problema es que nos podemos encontrar con enlaces o redireccionamientos a páginas no válidas pero que “parecen” ser legítimas, llevándonos a una copia de la página que solicitamos originalmente y en la cual se intenta instalar un programa malicioso en

[6] Código Script: Conjunto de instrucciones que son ejecutadas por un interprete de línea de órdenes y usualmente son archivos de texto.

nuestra computadora o incluso engañar a la usuario para ***revelar*** información confidencial. Lo que podemos hacer en este caso es ser precavidos e ir solo a sitios Web en los que confiemos no utilizar ligas alternas o que estén dentro de un correo electrónico del cual dudemos de su procedencia.

Un ataque menos común, se lleva cabo cuando un atacante usurpa nuestra sesión autenticada, por ejemplo, en una aplicación Web de nuestra empresa ejecutándose a través de nuestro navegador para ingresar o realizar acciones en la aplicación a la que tenemos acceso. Este tipo de ataques se deben a la falta de verificación de las credenciales de usuarios en las aplicaciones por parte de los desarrolladores, por ejemplo, con el uso de cookies[7] o variables de sesión de manera no segura. La aplicación Web no tiene manera de detectarlo (pues para ella, es un acceso válido) y el atacante realiza acciones o peticiones en nombre de un usuario sin su consentimiento. Lo que podemos hacer en este caso para disminuir el riesgo es:

1. No mantener una sesión abierta en aplicaciones Web que no estemos usando.
2. Configurar nuestro navegador para no permitir que guarde nombres de usuario ni contraseñas.
3. No utilizar el mismo navegador para acceder a aplicaciones sensibles y para navegar por Internet libremente.

Un ataque directo a la aplicación Web es el que ocurre cuando un intruso intenta modificar la aplicación y obtener con ello información confidencial ya sea de la misma aplicación o bien dejarla fuera de servicio (tanto la aplicación como la computadora del usuario en algunos casos) logrando bloquear o detener el servicio, a esto se le conoce como *Denegación de Servicio*. La denegación de servicio ocasiona que uno como usuario no pueda tener acceso a cierta información, servicio o cuenta provocando en algunos casos, que no podamos realizar cierta tarea o trabajo.

Es importante que tanto los usuarios de aplicaciones Web como los desarrolladores de las mismas, tomen conciencia de los problemas de seguridad que se pueden presentar. Un reporte de la firma de seguridad Cenizc indica que en la primera mitad del año 2009, el 78% del total de la vulnerabilidades reportadas eran de aplicaciones Web, en la siguiente figura (Figura 2), se muestran los tipos de vulnerabilidades Web reportadas. Es por ello que debemos ser muy cuidadosos a la hora de navegar.

[7] Cookie: información que se almacena en el disco duro del visitante a un sitio Web, que puede ser recuperada por el navegador a petición de la página.

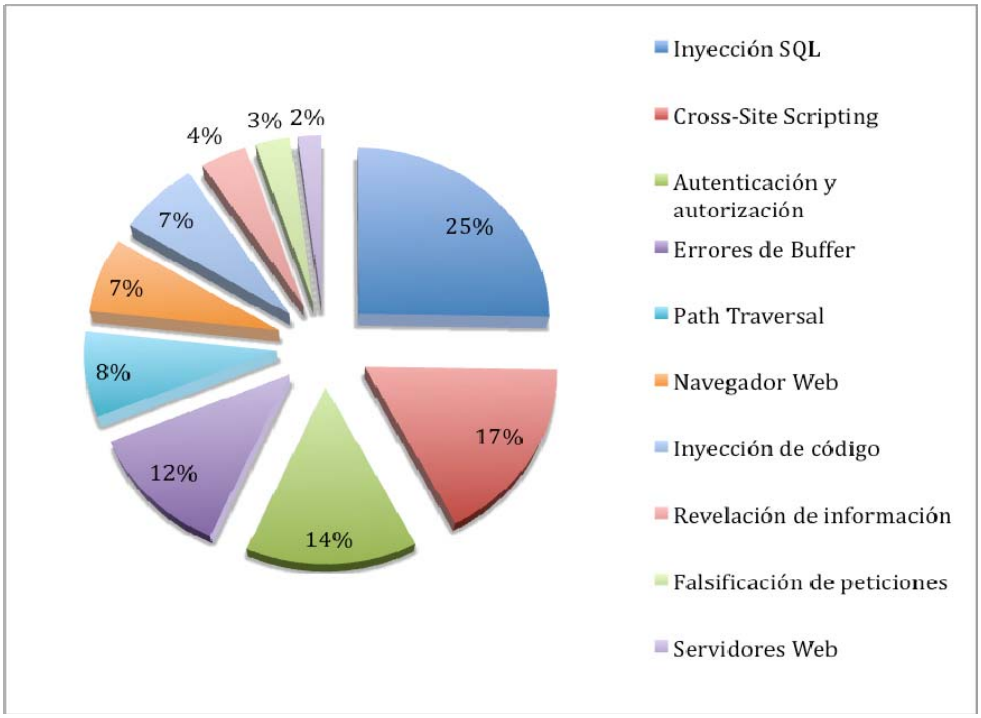

Figura 2. Vulnerabilidades reportadas de software comercial y libre.

Más información

Es importante señalar que estas no son las únicas amenazas al usar aplicaciones Web. Te invitamos a consultar más información que te ayudará a mantenerte protegido mientras navegas.

Referencias:

http://www.seguridad.unam.mx/
http://www.seguridad.unam.mx/usuario-casero/eduteca/
http://www.owasp.org/index.php/Top_10_2007
http://www.w3.org/Security/Faq/wwwsf6.html
http://www.maestrosdelweb.com/editorial/falloapl/
http://www.magenta.cl/servicios/netplus2.asp
http://www.cenzic.com/downloads/Cenzic_Survey_emedia-200910.pdf
http://www.cgisecurity.com/csrf-faq.html

Javier Santillán Arenas
José Roberto Sánchez Soledad

Dentro del mundo de la computación estamos acostumbrados a escuchar términos como gusanos o virus, pero para la mayoría de las personas el escuchar la palabra botnet, no tiene mucho significado. Este artículo tiene como objetivo dar al lector un panorama de esta amenaza en la red.

Una botnet es un conjunto de computadoras o dispositivos conectados a una red, que están a disposición de un equipo central al cual se le suele llamar -.Estos equipos son controlados por una persona maliciosa cuyo objetivo es atacar redes de computadoras o servidores.

A los equipos que se encuentran a disposición del C&C se les conoce como equipos zombi, el tamaño de una botnet se determina por el número de máquinas zombi que esta llegue a tener. Se han encontrado botnets de cientos de miles de equipos.

Las botnets han empezado a jugar un papel muy importante, específicamente en el área de la seguridad en cómputo. El motivo es que este tipo de redes se ha utilizado para fines maliciosos teniendo un impacto negativo en muchas de las actividades normales de un entorno de red.

¿Para qué se usan las botnets?

Debido a la suma de recursos computacionales reunidos en una botnet, resulta muy conveniente realizar actividades en las cuales se necesite de una “organización” o distribución de los recursos para tener logros masivos. Esto se traduce en actividades como las siguientes:

- Envío de correo basura (spam).
- Ataques de negación de servicio distribuido (DDoS)
- Distribución de malware
- Creación de redes P2P
- Robo de información
- Fraudes cibernéticos

¿Cómo funcionan las botnets?

Básicamente siguen los siguientes pasos:

1. El equipo es infectado de alguna manera, comúnmente por medio de una infección de malware en páginas web, correo spam, archivos maliciosos, etc.

2. El equipo principal o C&C toma el control de la máquina por medio de bots[8].

3. Siguiendo las órdenes del C&C, los equipos pueden ejecutar de manera coordinada cualquiera de las acciones antes mencionadas.

Los bots, como la mayoría del malware, desde el inicio de la infección tratan de aprovecharse de las vulnerabilidades en los programas de software de los equipos víctima. Sin embargo, una vez que han tomado el control del equipo generalmente utilizan el protocolo de comunicación IRC (Internet Relay Chat) para poder emitir las órdenes a los zombis

El IRC generalmente trabaja en los puertos 6666, 6667, 6668 y 7000 del protocolo TCP (*Transmission Control Protocol)*, pero pueden ser configurados para comunicarse por cualquier otro puerto.

Los bots pueden estar ejecutando cualquier sistema operativo, pero como en muchos casos, los sistemas con equipos Windows comúnmente son los más afectados debido a su gran presencia mundial.

Estadisticas

En los últimos años se han identificado miles de botnets, donde cientos de ellas han causado impactos significativos. A pesar de que puede haber botnets con solo cientos de equipos zombis, se han identificado botnets de casi 2 millones de equipos. En un estudio hecho en 2008, se identificó que el promedio de equipos en una botnet de bajo a medio tamaño podría llegar arriba de 50,000 , sin embargo en estos años se ha notado un incremento en el número de elemementos.

Solo por dar un ejemplo, en cuanto a spam se refiere, se calcula que diariamente se mandan casi 90 mil millones de mensajes de spam en todo el mundo. Esto representa un serio problema ya que significa que un porcentaje muy alto del tráfico de Internet es correo basura o malicioso.

[8] Bot es un programa malicioso utilizado para que un intruso obtenga los recursos de un equipo

En la Tabla1 se muestra una lista de las botnets más significativas que se han detectado durante 2009 y que fue publicada por la empresa de seguridad internacional Message Labs..

Nombre	Periodo de actividades	Cantidad de bots	Actividades realizadas
Rustock	agosto - septiembre	1.3 – 2 millones	Aproximadamente 18% del spam mundial.
Cutwail	Todo el año	1 – 1.5 millones	Aproximadamente 17% del spam mundial y propagación de malware.
Bagle	Finales 2009	600,000 – 800,000	Aproximadamente 16% del spam mundial.
Bobax (aka Kraken)	Finales 2009	80,000 – 120,000	Aproximadamente 13% del spam mundial.
Grum	Junio - septiembre	600,000 – 800,000	En su actividad máxima, llegó a enviar aproximadamente el 20% del spam mundial.
Maazben	Marzo – finales 2009	200,000 – 300,00	Aproximadamente el 2% del spam mundial.
Festi	Agosto 2009	100,000 – 200,00	Envío de spam
Mega-D	Todo el año	300,000 - 500,000	Spam, propagación de malware, actividades de phishing
Xarvester		500,000 – 800,000	Aproximadamente 1% del spam mundial.
Gheg	Principio del año	150,000 – 200,000	Aproximadamente 0.5% del spam

			mundial.
Donbot	Principal actividad en el primer cuarto del año. Terminó con aprox. 150,000 equipos al final del año.	800,000 – 1.2 millones	Envío de spam

Tabla 1. Botnets más significativos durante el 2009

Como se puede observar en esta tabla, el número de equipos zombie en una botnet es elevado. La actividad predominante es el envío de correo spam porque representa un gran negocio para quienes los ejecutan.

¿Cómo protegerse de las botnets?

Para estar mejor protegidos contra los bots que podrían infectar a nuestro equipo y hacer que forme parte de una botnet, debemos seguir las mismas recomendaciones que generalmente se siguen para cualquier otro tipo de malware. Entre las principales actividades se encuentran:

- Tener instalado un software de seguridad, preferentemente con características de soluciones completas (spam, phishing, antivirus, firewall, etc.)
- Estar al pendiente de las últimas actualizaciones del software que ejecute nuestra computadora.
- Aumentar las configuraciones de seguridad en nuestros programas como son los navegadores web o cualquiera que realice una conexión a Internet.
- Limitar la información que compartimos en la red y los privilegios de la misma al compartirla.
- Evitar abrir o visualizar archivos adjuntos de remitentes desconocidos.
- Seguir buenas prácticas de seguridad en general.

Como conclusión podemos decir que el problema de las botnets es un problema en crecimiento, en parte debido a las grandes posibilidades en términos maliciosos que abre el tener miles de equipos a la disposición de una computadora principal, y por otro lado

debido al exitoso aprovechamiento de vulnerabilidades en los programas de software que siguen haciendo de ellas el medio perfecto para actuar de manera masiva.

Referencias:

http://www.honeynet.org/papers/bots
http://www.net-security.org/secworld.php?id=8599
http://www.symantec.com/es/mx/norton/theme.jsp?themeid=botnet
http://www.consumer.es/web/es/tecnologia/internet/2009/07/20/186416.php

Jesús Mauricio Andrade Guzmán

Un ataque cibernético es un acto intencional por parte de un usuario malicioso con el fin aprovecharse de una vulnerabilidad en el diseño o desarrollo de una aplicación. La diferencia entre una vulnerabilidad y un ataque cibernético es que un ataque es algo que un usuario malicioso podría hacer y una vulnerabilidad es una debilidad en la aplicación.

Existen varios tipos de ataques que representan amenazas y cuyo riesgo depende de la manera en cómo actúa la herramienta maliciosa, la debilidad que explota y la importancia de la información que está siendo comprometida.

El riesgo que corre una aplicación ante un ataque varía de acuerdo al criterio que se utilice. Es posible calcular el riesgo que corre nuestra aplicación considerando el número de vulnerabilidades reportadas para el software que utilizamos consultando fuentes de información como la base de datos CWE[9] que almacena prácticamente todas las fallas reportadas para cualquier aplicación, independiente de su plataforma, arquitectura o sistema operativo. Otra fuente de información relacionada con los ataques Web es OWASP[10] que se enfoca en difundir información para desarrolladores y administradores de sistemas con la finalidad de prevenir ataques desde el diseño de una aplicación para lo cual ofrecen guías de desarrollo seguro, listados de riesgos potenciales de ataques y herramientas didácticas y de diagnóstico.

Imagen 2. CWE - http://cwe.mitre.org

Imagen 1. OWASP - http://www.owasp.org

[9] Common Weakness Enumeration - http://cwe.mitre.org/
[10] Open Web Application Security Project - http://www.owasp.org

Existen muchas formas en que los atacantes pueden explotar debilidades de una aplicación Web, un ejemplo de esto son las relacionadas con la **interacción insegura entre los componentes de una aplicación**. Estas vulnerabilidades se refieren a que el autor de la aplicación no ha tomado las debidas precauciones a la hora de validar los datos que permite en su sistema (por ejemplo al validar los datos que se envían a través de una forma HTML). Los ataques de **inyección de código** también toman ventaja de este tipo de debilidades al insertar código especialmente creado para engañar a la aplicación y obtener con ello acceso a información confidencial.

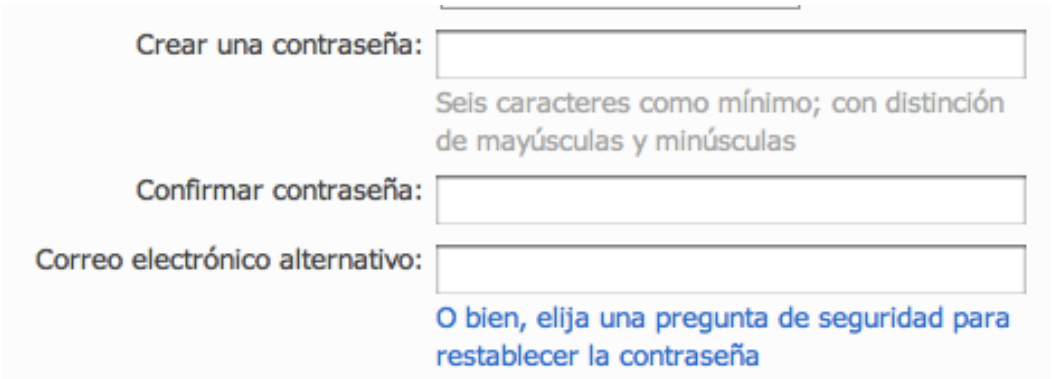

Imagen 3. Ejemplo de forma HTML

Los ataques tipo XSS (**Cross Site Scripting**) permiten a los atacantes ejecutar código malicioso en el navegador del usuario de la aplicación, que podría resultar en la obtención de información confidencial o incluso la toma de control de una sesión de usuario con el objetivo de suplantar la identidad de un sitio legítimo o redirigir a otros usuarios de la aplicación a sitios Web maliciosos.

Otro problema que se puede presentar es que la aplicación **no realice una adecuada gestión de los recursos que utiliza**. Pocas precauciones al almacenar datos de identificación como nombres de usuario o contraseñas pueden conducir a que intrusos aprovechen esta debilidad y puedan llegar usar la identidad del usuario sin autorización. Este tipo de ataques también pueden ser explotados si existen **archivos utilizados por la aplicación sin los privilegios configurados de manera adecuada**, comprometiendo la confidencialidad de dichos recursos. Fallas de este tipo se pueden atribuir a **errores de configuración de seguridad**, por ejemplo, al no cambiar ajustes predeterminados al momento de la instalación que pueden no ser suficientes para garantizar la seguridad de los recursos de la aplicación Web.

Las consecuencias de que un atacante realice con éxito alguno de estos ataques son muy variadas para el usuario, pasando de una simple molestia o baja temporal en el servicio hasta la divulgación o uso no autorizado de información altamente confidencial como es el caso de información de cuentas bancarias. Para los administradores de las aplicaciones afectadas, estos ataques pueden lesionar gravemente la reputación de la empresa disminuyendo la confianza de sus usuarios y por lo tanto disminuyendo también sus ganancias económicas.

Para prevenir estos ataques tanto administradores de sistemas como desarrolladores y nosotros mismos como usuarios, debemos estar conscientes de los riesgos de que la información que usamos esté siendo transmitida a través de Internet. Tomando precauciones simples desde el diseño de la aplicación podemos prevenir muchos de estos problemas. Como diseñadores de la aplicación debemos validar siempre los datos que se obtienen del usuario suponiendo siempre, que los usuarios pueden tener malas intenciones al usar nuestra aplicación. Como administradores de sistemas debemos analizar las características de las herramientas que se utilizan para estar seguros de que las configuraciones que usamos sean las adecuadas para poder garantizar que se preserva la privacidad, confidencialidad e integridad de la información que se maneje al ser transmitida por red. Como usuarios debemos revisar siempre que las aplicaciones Web que utilicemos tomen las medidas básicas de seguridad como lo es el solicitar siempre nuestro nombre de usuario y contraseña antes de realizar alguna operación con nuestros datos privados. Si usamos portales de banca en línea o servicios que manejen información confidencial debemos asegurarnos de que el sitio utilice mecanismos de cifrado (que utilice el protocolo HTTPS en lugar de HTTP) al manejar esta información para mantener al mínimo los riesgos de que un atacante pueda capturar los datos de navegación de la aplicación Web.

Referencias

http://www.owasp.org
http://www.sans.org
http://cwe.mitre.org

DIRECTORIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. José Narro Robles
Rector

Dr. Sergio Alcocer Martínez de Castros
Secretario General

DIRECCIÓN GENERAL DE SERVICIOS DE
CÓMPUTO ACADÉMICO

Dr. Ignacio de Jesús Ania Briseño
Director

Ma. de Lourdes Velázquez Pastrana
Directora de Telecomunicaciones

Ing. Rubén Aquino Luna
Responsable del Departamento de Seguridad en Cómputo UNAM-CERT

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico

CRÉDITOS

PUNTO SEGURIDAD, DEFENSA DIGITAL

M en I. Rocío del Pilar Soto Astorga
Edición

Angie Aguilar Domínguez
Jesús Mauricio Andrade Guzmán
Sergio Iniesta Juárez
David Jiménez Domínguez
José Roberto Sánchez Soledad
Javier Ulises Santillán Arenas
Colaboraciones

Ing. Rubén Aquino Luna
Responsable del Departamento de Seguridad en Cómputo UNAM-CERT

Rocío del Pilar Soto Astorga
Rubén Aquino Luna
Manuel I. Quintero Martínez
Revisión de Contenidos

Act. Guillermo Chávez Sánchez
Coordinación de Edición Digital

Lic. Lizbeth Luna González
Dolores Montiel García
L.D.C.V. Carolina Silva Bretón
Diseño Gráfico

Liliana Minerva Mendoza Castillo
Formación

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico