PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 3 | OCTUBRE 2009 | *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, en esta ocasión con el tema de: Seguridad en el Correo Electrónico.

El uso del correo electrónico es ya tan común que para muchos de nosotros ya forma parte de la rutina diaria el revisar nuestra bandeja de entrada. Este medio de comunicación se ha vuelto muy práctico debido a lo económico que resulta y sobre todo a su rapidez. Además de que tiene la gran ventaja de permitir compartir archivos de forma sencilla.

De esta forma, este medio de comunicación es usado por diversos grupos de personas y con distintos fines como asuntos de trabajo, comunicación entre amigos, con la familia etc.

Este gran uso que se le da actualmente al correo electrónico lo hace blanco de amenazas de seguridad. En este Número 3 de **.Seguridad** se muestra como funciona el correo electrónico y nos informa de los amenazas a los que nos podemos enfrentar al utilizarlo así como de las prácticas que podemos utilizar para prevenir ser víctimas de ellas.

Rocío del Pilar Soto Astorga
Departamento de Seguridad en Cómputo

Sergio Andrés Becerril López

Hoy en día, el correo electrónico es el principal uso que le damos a Internet ya que un medio de comunicación gratuito, rápido y confiable, que nos permite optimizar nuestros tiempos y ampliar nuestra capacidad de envío. Con unos cuantos clicks, por ejemplo podemos enviar el mismo mensaje a toda nuestra oficina, incluyendo imágenes y otros archivos, de manera sencilla y prácticamente instantánea.

Pero, ¿cómo funciona este sistema? Como usuarios, simplemente tenemos que instalar algún programa como *Outlook*, configurar la conexión y listo; más aún, con la popularidad de los clientes web – clientes que podemos utilizar con nuestro navegador de Internet – solo tenemos que entrar a una página de Internet y ahí podemos administrar nuestra información. Sin embargo, detrás de esto se esconde un proceso que, si bien no es muy complicado, requiere de una explicación más detallada.

Imaginemos, por ejemplo, una oficina postal común y corriente. Como usuarios, nuestra participación en el proceso termina en cuanto entregamos nuestra carta o paquete en el depósito u oficina correspondiente; claro, tenemos que indicar para quién va y como llegar a esa persona (es decir, dar un nombre y una dirección postal correcta), posiblemente pagar alguna tarifa, pero hasta ahí llegamos. Sin embargo, el mecanismo de envío postal tradicional requiere toda una infraestructura: administración local del correo, aviones, ordenamiento y selección, etc. En forma análoga, la infraestructura de correo electrónico en Internet requiere de una serie de elementos que garantizan la llegada correcta de nuestro correo electrónico a otras personas.

La Figura 1 ilustra el esquema general del funcionamiento del correo electrónico explicado mediante un ejemplo. En primera instancia tenemos a dos personas, Ana y Bruno. Pensemos que Ana (cuya dirección de correo electrónico es ana@escuela.com.mx) quiere enviar un correo electrónico a Bruno (cuya dirección es bruno@empresa.com). Congruente a nuestra analogía de correo tradicional, la segunda parte de la dirección de correo (la parte que sigue a la @) corresponde a la ubicación de la persona; su compañía, proveedor gratuito de correo, servidor personal, etc. La primera parte (lo que está antes de la @) corresponde al nombre de la persona dentro de esa ubicación.

¿Cómo Funciona el Correo Electrónico? Protocolo SMTP

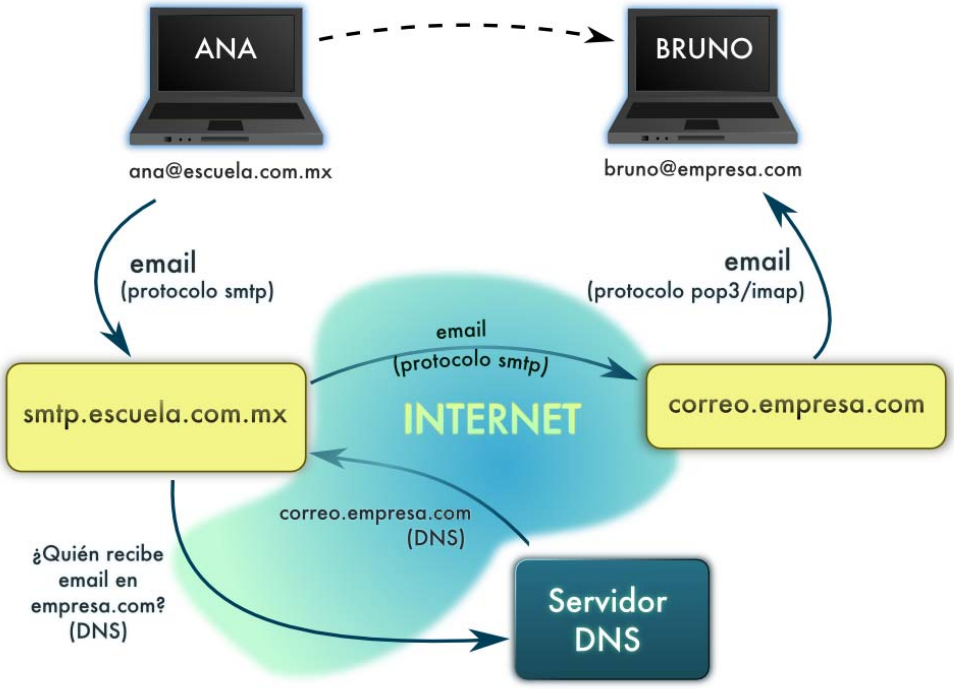

Figura 1

Ana abre entonces su programa favorito de correo electrónico (*Outlook*, *Eudora*, su navegador de Internet posiblemente) y, una vez autenticada (es decir, habiendo introducido su nombre de usuario y contraseña), envía su correo. Es importante resaltar este punto: es imprescindible indicarle a nuestro servidor de correo quienes somos, para poder hacer uso del mismo, aunque a veces esto se realiza de manera automática.

Lo que pasa una vez que Ana hace click en "Enviar" es donde reside la verdadera magia. Dijimos antes que la segunda parte de la dirección de correo corresponde a la ubicación de la persona; en este caso, Ana quiere contactar a 'Bruno' en la ubicación 'empresa.com'. Sin embargo, es posible que el servidor que administra el correo dentro de la organización 'empresa.com' no sea precisamente el servidor 'empresa.com', sino, digamos, otro servidor llamado 'correo.empresa.com'. Esta práctica es muy común y sirve para delegar responsabilidades (un equipo que administre el sitio web, usualmente 'dominio.com'; un servidor de correo, etc.)

Por tanto, necesitamos saber exactamente qué servidor se encargará de recibir nuestro correo en 'empresa.com'. Para ello, contactamos a otro equipo, un **servidor DNS**[1], que nos entrega

1 Servidor que se encarga de relacionar nombres de dominio (e.g. *dominio.com*) y direcciones IP (identificadores numéricos), así como servidores asociados a un dominio (e.g. un servidor de correo).

justamente esta información (como se aprecia en la Figura 1). En este caso, nos contesta que el servidor es 'correo.empresa.com'; esta información se conoce como el **registro MX** del servidor 'empresa.com'. Usualmente, se tiene más de un registro MX, de forma que si algún servidor deja de funcionar, podamos seguir recibiendo correo con algún otro.

Una vez conocido este dato, el servidor 'smtp.escuela.com.mx' contacta a 'correo.empresa.com' y de estar disponible, le enviará nuestro correo electrónico, en donde residirá hasta que Bruno abra su cliente y lea su correo.

Si Ana enviara un correo a múltiples destinos, su servidor de correo realizaría este procedimiento por cada destino diferente. Esto es, si voy a enviar correos a 100 personas diferentes, todas en 'empresa.com', haría este procedimiento una vez, y enviaría 100 correos al registro MX correspondiente; si fueran, en cambio, 100 personas en 100 dominios diferentes, realizaría este procedimiento 100 veces. También es posible que nuestro destinatario se encuentre en nuestro mismo destino (por ejemplo, que Ana quisiera contactar a Carlos, cuya dirección es carlos@escuela.com.mx); en este caso, nuestro servidor de correo simplemente lo copiaría a las bandejas de entrada de cada quien.

Este procedimiento está documentado como un estándar (es decir, es el mismo para todos los servidores de correo que quieran comunicarse utilizando este esquema) y se conoce como el **protocolo SMTP**, cuyas siglas en inglés significan *Simple Mail Transfer Protocol*, o Protocolo Sencillo de Envío de Correo. Como se puede apreciar, hace honor a su nombre.

El protocolo describe una gran cantidad de opciones; un servidor de correo puede presentar mensajes de error, por ejemplo si no tiene registrado al usuario que buscamos (digamos que Ana se equivocara al escribir la dirección, y no existiera ese usuario, recibiría un correo electrónico indicándole el problema). Por otra parte, también es común que un servidor de correo tenga instalado un antivirus y un filtro para distinguir al ***spam***, o correo no deseado, del correo auténtico ya que por ejemplo durante el 2008, el 60.56% del total de casos de incidentes reportados al Departamento de Seguridad en Cómputo UNAM-CERT se trató de *spam*.

Esta breve descripción puede ayudarnos a entender mejor el funcionamiento 'tras bambalinas' la próxima vez que enviemos las últimas fotos de la fiesta o aquél memorándum del trabajo.

Referencias:

http://www.ietf.org/rfc/rfc2821.txt (estándar)
http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol (Wiki específica del SMTP).
http://www.cert.org.mx/estadisticas.dsc

Javier Ulises Santillan Arenas

Muchas de las técnicas utilizadas para conseguir información de forma ilegal contemplan la utilización de mecanismos, herramientas, equipos, etc., y la mayoría de las veces quienes las ejecutan necesitan de sofisticados conocimientos técnicos y amplia experiencia para que los ataques sean efectivos, sin embargo, la llamada "ingeniería social" omite el dominio de cuestiones técnicas y se basa en el aprovechamiento del "eslabón más débil" dentro de la seguridad informática: el usuario.

Mientras las nuevas tecnologías de comunicaciones han permitido que la brecha entre usuarios y máquinas sea cada vez menor, los complejos sistemas de comunicación también han desarrollado modelos que dan al usuario la capacidad de intercambiar información de una manera cada vez más rápida, fácil y sencilla. Ejemplos de esto es la evolución de los mensajes de correo electrónico, mensajeros instantáneos, redes sociales, mensajes de texto, etc., los cuales proporcionan una manera efectiva de intercambio de información.

El uso y aprovechamiento de tecnologías de este tipo, conlleva que el usuario confíe en todo lo que hay detrás, es decir, si el usuario ve una interfaz amigable o "conocida", normalmente supondría que el emisor de dicha información es precisamente quien la está publicando. En otras palabras, si ve un correo o cartel electrónico del banco X, supondrá que es efectivamente el banco X quien está emitiendo la información, o al menos es lo que la mayoría de los usuarios que no han sido informados de los riesgos y amenazas de seguridad informática tendrían en mente.

Ingeniería social y las comunicaciones electrónicas

Ahora, ¿cómo se relaciona la ingeniería social en todo esto? El saber que el punto más débil de toda una infraestructura de seguridad es el usuario, da pauta a que puedan omitirse todas las protecciones implementadas detrás de él. La ingeniería social se trata de "prácticas, técnicas especializadas o empíricas, acciones estudiadas, planeaciones estratégicas, etc., cuyo principal objetivo es manipular a una entidad, en este caso a las personas, para que directa o indirectamente realicen acciones que llevarán a conseguir un fin específico para quien las aplica", en palabras sencillas, es la habilidad de engañar para obtener información de una persona o sistema.

En base a lo anterior se puede entender o al menos imaginar gran cantidad de formas por las cuales pueden aplicarse técnicas de engaño en medios como el correo electrónico, mensajes de texto, páginas web, etc., de modo que los usuarios "ingenuos" proporcionen información o realicen acciones que deliberadamente han sido planeadas para lograr objetivos como robo de información, acceso a cuentas de usuario, etc. De hecho, en los últimos años han nacido términos como "*phishing*", "*hoax*", "*shoulder surfing*", etc., los cuales se refieren a un conjunto de acciones aplicadas de ingeniería social.

Abordando ejemplos específicos, el *phishing* consiste en suplantar a una entidad con la finalidad de obtener información tal como contraseñas, número de tarjetas de crédito, información personal de cuentas, etc., y el medio de propagación de esta amenaza se da principalmente por correo electrónico y portales web falsos. Generalmente tratan de dar la apariencia de la entidad que están suplantando, sin embargo, están diseñados de manera que el intercambio de información será entre el usuario y una entidad externa, así, ésta puede utilizar la información proporcionada por el usuario y utilizarla con los fines que se desee. Hay muchas referencias en donde asumen que el término de *phishing* proviene del concepto en que el engaño representa un "anzuelo", y se está a la espera que el más ingenuo sea "pescado".

Realmente técnicas como el *phishing* no solamente pueden ser aplicados en comunicaciones electrónicas escritas como es el correo electrónico, también es utilizado en llamadas telefónicas, carteles electrónicos, etc., pero principalmente se ha dado una tendencia a suplantar portales bancarios porque ha demostrado que es una técnica eficiente para que los intrusos y usuarios maliciosos cometan delitos.

Otra aplicación de la ingeniería social es la propagación de *malware*. Mediante engaños se hace creer a los usuarios por ejemplo que se visita algún sitio o se descarga una aplicación de utilidad, sin embargo, ésta puede estar modificada maliciosamente de modo que a parte de realizar las tareas para las cuales está diseñada, también se aprovecha de la confianza que ha adquirido del usuario y puede, de manera similar que el *phishing*, obtener información como contraseñas, información de cuentas de usuario, números de tarjetas de crédito, etc.

Defensas, consideraciones y buenas prácticas

Con todo lo anterior se puede formular la pregunta ¿existen defensas efectivas en contra de la ingeniería social? La respuesta es totalmente afirmativa, sin embargo los mecanismos a tomar en cuenta van más enfocados a una cultura informática y no tanto a una cuestión técnica.

Se debe entender que una parte muy importante de la seguridad recae en el usuario. Tanto en las comunicaciones electrónicas como en la vida real, siempre se debe tener presente que hay cosas de las que debemos desconfiar, o manejar con particular cuidado.

Hablando de amenazas específicas, podemos citar las siguientes recomendaciones que disminuirían de manera importante la posibilidad de ser víctimas de alguna técnica de ingeniería social aplicada:

- Si se recibe algún correo de remitentes desconocidos, debe tratarse con extremo cuidado, ya que no solamente puede tratarse de un correo con información falsa, sino que puede contener archivos maliciosos adjuntos.
- Como una medida de protección general, se debe saber que las entidades bancarias nunca solicitarán información confidencial por correo electrónico, o incluso cualquier tipo de información del usuario.

- Al utilizar servicios bancarios en línea, se deben verificar características como que se trata de una “pagina segura” (inicia con https), así como que la dirección del portal realmente pertenezca a la url de la entidad, por ejemplo, si el banco X ofrece servicios en línea, y con total seguridad se sabe que su dirección web es www.bancox.com, entonces cuidarse de direcciones aparentes. Una característica del *phishing* es que paginas auténticas pueden suplantarse con una simple similitud de las palabras, para el caso anterior podría ser que la página falsa fuera www.banncox.com. El simple hecho de que se parezca, hace que muchos usuarios desprevenidos caigan en este tipo de engaños que por muy triviales y sencillos que parezcan, siguen siendo muy efectivos.
- No enviar información de acceso personal por correo electrónico.

El no aplicar este tipo de medidas a pesar de su sencillez, causa que más allá de los términos de seguridad informática, la ingeniería social represente un problema económico. Solo por citar un ejemplo, en el reino unido se alcanzó la cantidad de 52.5 millones de euros en 2008, más del doble 22.6 millones reportados en 2007 de casos de fraude en línea.

En concreto, la ingeniería social realmente representa un problema serio de seguridad. . No se necesita que el usuario sea un experto conocedor de seguridad, pero más allá de las consideraciones básicas se debe tener presente por lo menos cómo o en dónde están las amenazas, que muchas veces no serán virus, programas o equipos infectados, sino simplemente técnicas de engaño.

Referencias:

http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm
http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx
http://www.theregister.co.uk/2009/08/27/online_banking_fraud_survey/

Alejandro Reyes Plata

Con los avances tecnológicos de los últimos años, sobre todo en las tecnologías de la información, una mayor cantidad de personas tienen acceso, a los grandes beneficios pero también a los riesgos de Internet . -uno de los cuales es la propagación de código malicioso a través del correo electrónico.

Una gran cantidad de *malware*[2] y ligas con contenido malicioso se pueden encontrar dentro de imágenes transmitidas a través del correo electrónico, lo que dificulta que los motores antivirus sean capaces de detectarlo. Sin embargo existen antivirus que son capaces de realizar estas acciones.

Cierta parte de este *malware* que se inyecta en imágenes, al ser abiertas en los sistemas operativos, permite la ejecución de cualquier instrucción en los equipos afectados, sin el conocimiento o el permiso de los usuarios. Ésta es una manera hábil de introducir código malicioso a otras máquinas saltándose las alarmas y evitando las herramientas de seguridad en red.

Por ejemplo, el día 5 de enero de 2006 Microsoft, liberó una actualización en su Boletín de Seguridad "MS06-001" que soluciona esta vulnerabilidad. Aunque no deja de ser un peligro latente pues existe una gran cantidad de equipos con sistemas operativos Windows que no son actualizados constantemente. Cabe destacar que gran parte del *malware* que se distribuye a través de correos electrónicos tienen un mayor impacto porque utiliza ingeniería social.
Algunos de los códigos maliciosos más comunes que se inyectan a través del correo electrónico son:

- ***Spywares***. Son programas "espía" se instalan en las computadoras sin el consentimiento del usuario, recopilan información del usuario o de la computadora infectada, enviándola remotamente hacia otra persona. El *spyware* se pude dividir en dos categorías: *software* de vigilancia y *software* publicitario. El de vigilancia se encarga de monitorear todo el sistema mediante el uso de transcriptores de teclado y captura de pantallas. El *spyware* publicitario, también llamado *Adware*, se instala de forma conjunta con otra aplicación, para recoger información privada y mostrar anuncios no solicitados y molestos.
- **Caballos de Troya.** En sus inicios eran programas que se escondían dentro de otro aparentemente inofensivo, en este caso descargado del correo electrónico. Este *malware* engaña al usuario aparentando ser un programa lícito para poder ejecutarse en el equipo víctima. Los nuevos troyanos se pueden definir más concretamente como: "*Backdoor*" o "Puerta trasera", los cuales abren un canal de comunicación en la computadora infectada que permite la conexión de otra computadora que realiza acciones maliciosas sin que el usuario víctima se de cuenta.

2 malicious *software*

- **Virus**. Es código que se replica uniéndose a otro objeto generalmente sin consentimiento ni conocimiento del usuario, algunos toman el control de los programas de correo electrónico, intentando duplicarse a sí mismos. Otros virus pueden destruir o corromper archivos de datos, borrar programas instalados o dañar el propio sistema operativo. Los virus de script son una subcategoría escrita en una variedad de lenguajes de script (VBS, *JavaScript*, BAT, PHP, etc). Una de las principales habilidades de los virus de script consiste en ser capaces de enviarse con gran facilidad a través de programas de correo como Outlook o clientes de IRC como mIRC o PIRCH.
- **Gusanos**. Un gusano es un programa o conjunto de programas que realizan copias completas de sí mismos en distintos equipos informáticos, se reproducen a tal velocidad que pueden colapsar y tirar las redes en las que se infiltran, se propagan a través de las conexiones de una red pero principalmente se extienden a través del correo electrónico. La mayoría utilizan *Outlook* y *Outlook Express* (uno de los clientes de correo electrónico más utilizados en todo el mundo), como transporte hacia otros equipos y así poder propagarse rápidamente. Es necesario destacar que los clientes de correo electrónico menos empleados no son inmunes, ya que todos pueden ser susceptibles de servir de medio de propagación para un gusano. Los gusanos actuales han sido modificados y mejorados de forma que se envían de manera independiente, sin necesidad de utilizar un cliente de correo electrónico determinado. Emplean su propio motor *Simple Mail Transfer Protocol* (SMTP). Para enviarse únicamente requieren de una conexión a Internet y enviar determinados comandos a través del puerto 25/TCP.

Recomendaciones:
Sin duda mucho del *malware* que infecta nuestros equipos se instala sin nuestro consentimiento y muchas de las veces ni siquiera nos enteramos de ello, nuestra misma computadora puede ser parte de una red de zombis en este momento. De manera general se recomienda no abrir correos electrónicos de remitentes desconocidos, no reenviar correos que sean cadena, instalar un *software* antivirus y mantenerlo actualizado. No dar clic en ligas que nos dirigen hacia ligas con videos de algún personaje público. Aunque conozcamos al emisor del mensaje no nos garantiza que el contenido esté libre de riesgos, debemos de ser muy precavidos.

Referencias:

www.tech-faq.com/botnet.shtml
http://www.terra.es/tecnologia/articulo/html/tec10570.htm
http://es.wikipedia.org/wiki/Adware
http://www.antivirusworld.com/articles/pharming.php
http://www.pharming.org/index.jsp
http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx
http://www.monografias.com/trabajos15/virus-informatico/virus-informatico.shtml

Rocío del Pilar Soto Astorga

El día jueves 4 de mayo del 2000 una alarma sacudió al mundo de las computadoras, se trató de un gusano informático que se propagaba rápidamente vía correo electrónico. Esta amenaza fue conocida por varios nombres, entre los más mencionados se encuentran: "ILOVEYOU" y "LOVE LETTER" y fue la causante incluso de que varias empresas cesaran sus actividades. El asunto del correo electrónico era "ILOVEYOU", con un adjunto de nombre "LOVE-LETTER-FOR-YOU.TXT.vbs". En el cuerpo del mensaje se leía: "*kindly check the attached LOVELETTER coming from me*".

Resultó tentador para muchas personas el proceder a abrir dicho adjunto suponiendo que se trataba de una verdadera carta de amor proveniente de una dirección electrónica conocida.

Como ataca el gusano

El sistema operativo afectado por el gusano fue *Windows* con el *Windows Scripting Host* activado. ILOVEYOU es un programa, realizado en *Visual Basic*, que tiene la habilidad de mandarse a si mismo vía correo electrónico a todas las direcciones contenidas en la libreta del programa *Microsoft Outlook* de la computadora infectada. Después de instalarse en la computadora, el gusano altera imágenes y archivos de audio.

De acuerdo al CERT *Coordination Center*[3] el gusano actúa de la siguiente forma:

- Remplaza archivos con copias de él mismo.
- Crea código mIRC4 con el fin de propagarse.
- Modifica la página de inicio de Internet Explorer a una página en blanco.
- Manda copias de si mismo por correo electrónico.
- Modifica llaves de registro.

3 Computer Emergency Readiness Team, Coordinación ubicada en la Universidad de Carnegie Mellon, que se ocupa de la seguridad en internet.

4 Lenguaje embebido en mIRC, un cliente de IRC –Internet Relay Chat-

Figura 1

Búsqueda del autor

Ese mismo jueves el FBI comenzó con las investigaciones del responsable del ataque originado en Filipinas. La procedencia del virus se supo ya que una compañía de servicios de Internet en Filipinas, Sky Internet , comentó que albergaba parte del código del gusano.

La identificación del culpable se hizo más fácil cuando la Escuela de Informática AMA en Filipinas informó a la policía que la tesis de un alumno se parecía mucho a lo que sucedía con el virus, esta tesis fue rechazada por la escuela debido a no mostrar un trabajo ético. Las investigaciones condujeron al estudiante de 23 años, Onel de Guzmán quien se encontraba viviendo en un departamento junto con su hermana y el novio de esta.

Las autoridades de Filipinas no sabían que hacer ya que no se contaba con una legislación para el crimen cibernético en el país, por aquel entonces. Durante la defensa, el abogado de Onel argumentó que sí era posible que el joven estudiante hubiera liberado el virus pero solo como un accidente y negando la autoría directa.

Los cargos fueron retirados bajo argumento de que los estos no aplicaban al caso o que no se contaban con las suficientes pruebas para demostrarlo. Tampoco tuvo caso una demanda por

parte de las empresas afectadas ya que además de que los cargos no pudieron ser aplicados, Onel era un estudiante que vivía incluso de dinero prestado.

Consecuencias

Entre algunas de las compañías que resultaron afectados se encuentran la editorial *Axel Springer*, la compañía de telefonía *Vodafone*, Pacific Bell en San Francisco, las fábricas de Dell en Irlanda, el periódico español el País, la Ford de Reino Unido entre otras muchas empresas de todo el mundo de varios países que llegaron a tener una cantidad considerable de computadoras infectadas, por lo cual varias de estas compañías tuvieron que desconectar sus servidores de correos.

Otra consecuencia fue la creación de leyes en Filipinas que castigaran los delitos informáticos. Esto se dio mediante la conocida como "Acta de Comercio Electrónico de Filipinas" en la que se penalizan actos de *hacking* o *cracking* tales que interfieren en un sistema de información o acceden con el fin de corromper, alterar, robar o destruir mediante el uso de la computadora o cualquier otro dispositivo de comunicación sin consentimiento, así como la introducción de virus informáticos o semejantes que alteren o destruyan información, siendo por ello, los que incurran en estos delitos, merecedores al pago de una fianza o tiempo en prisión.

Dentro de este gran caos, se tuvieron lecciones aprendidas como es el tener cuidado con los mensajes de correo electrónico que contengan adjuntos a pesar de que sean enviados por direcciones conocidas ya que en ellos pueden estarse transportando virus y programas maliciosos. Si se sospecha de algún correo de remitente conocido es mejor enviar un correo a este remitente aclarando la situación.

No debemos olvidarnos de este caso histórico ya que su importancia radicó en que fue diseminado con gran rapidez debido al gancho de las relaciones personales. Con el auge de las redes sociales y el hecho de que gran parte de los usuarios son jóvenes menores de edad, es muy fácil que esta treta pueda ser utilizada nuevamente con fines de propagación de *malware*. Es por esto que debemos estar bien informados sobre las amenazas actuales y no olvidarnos de los hechos sucedidos en el pasado para poder estar siempre alertas y poder hacer uso seguro de Internet.

Referencias:

http://www.cert.org/advisories/CA-2000-04.html
http://www.sophos.com/pressoffice/news/articles/2000/08/va_guzman.html
http://www.ua.es/es/novedades/comunicados/2000/iloveyou.htm
http://www.elmundo.es/navegante/2000/05/05/ailofiu_virus.html
http://news.bbc.co.uk/2/hi/uk_news/736080.stm
http://news.zdnet.com/2100-9595_22-107318.html?legacy=zdnn
BROADHURST y GRABOSKY. Cyber-Crime, The Challenge in Asia. Hong Kong University Press, Hong Kong, 2005. ELECTRONIC COMMERCE ACT OF THE PHILIPPINES.

Privacidad: El Hombre de en Medio y el Cifrado Electrónico

Miriam J. Padilla Espinosa

El ataque de **MITM** por sus siglas en inglés (*Man in the middle*), consiste en intervenir la comunicación que establecen dos partes entre ellas, sin que éstas puedan percibir la intromisión, el atacante puede estar ubicado de forma física o lógica. Un ataque de tipo **MITM** compromete principalmente las siguientes características de seguridad:

- **Confidencialidad**: al escuchar la comunicación entre dos personas o equipos
- **Integridad**: al interceptar la comunicación y modificar la información
- **Disponibilidad**: al desviar o destruir los mensajes de tal forma que se provoque el fin de la comunicación entre las dos partes que se comunican.

Para contribuir al entendimiento de este tipo de ataque, supongamos el siguiente escenario donde se afecta la confidencialidad, la integridad y la disponibilidad:

Entre dos miembros de una empresa se realizará el envío de un archivo vía correo electrónico, hay un tercero (el intruso) que durante una conversación, sin ser descubierto ha escuchado la hora en la cual se realizará un intercambio electrónico afectando así **la confidencialidad** (Figura1), de esta forma el atacante durante la transmisión del archivo interceptará la comunicación y modificará el documento dañando así **la integridad** (Figura 2) de tal forma que cuando el destinatario lo reciba, no percibirá la modificación; por último, si el atacante destruye la información obtenida durante la intercepción está ya no llegará al destinatario, lo que ocasionará el fin de la comunicación afectando así **la disponibilidad** (Figura 3).

Figura 1

Figura 2

Figura 3

Como medidas preventivas para este tipo de ataque se recomienda a los usuarios el empleo de claves públicas de cifrado, cifrado de la información, uso de certificados y firmas digitales.

Debido a la importancia que en la actualidad ha adquirido el uso de correo electrónico, para el intercambio de información, por ser una herramienta de comunicación rápida, económica, directa y personalizada; se ha vuelto un blanco de amenazas que atentan contra la seguridad de esta herramienta de comunicación. De esta forma surge como una medida de protección contra intrusos el uso del correo electrónico cifrado, que consiste en utilizar un algoritmo de cifrado para transformar el mensaje en una representación incomprensible para aquella persona que no cuente con autorización para recibir la información.

Entre los mecanismos más utilizados en la actualidad para el cifrado de correo electrónico destacan **PGP** y **S/MIME**, los cuales se detallan en la Tabla 1:

ESTÁNDARES DE CIFRADO DE CORREO ELECTRÓNICO		
NOMBRE	PGP (*Pretty Good Privacy*)	S/MIME (Secure Multipurpose Internet Mail Extensions)
FUNCIONAMIENTO	**a.** Generación de claves de sesión aleatorias. **b.** El mensaje es cifrado utilizando las claves aleatorias generadas y utilizando un algoritmo de cifrado simétrico (misma clave para cifrar y descifrar). **c.** La clave de sesión es cifrada utilizando la clave pública del destinatario. **d.** Se utiliza un algoritmo SHA que genera un extracto del mensaje (*hash*), el cual es firmado con la clave pública del remitente creando una firma digital. **e.** La clave de sesión cifrada se adjunta en el mensaje. **f.** El mensaje es enviado al destinatario. **g.** El destinatario invierte los pasos antes mencionados, recupera la clave de sesión y descifra el mensaje.	a. Para cifrar el mensaje es necesario conocer la clave pública del destinatario y para que el destinatario pueda ver el contenido del mensaje requiere utilizar su clave privada. b. Para la autenticidad del remitente se hace uso de la firma digital, de esta forma el mensaje es cifrado utilizando la clave privada del remitente y es enviado con un certificado (éste valida la autenticidad de la clave pública del remitente). El destinatario puede descifrar el mensaje con la clave pública del remitente, que está disponible de forma gratuita Es importante aclarar que no debe confundirse el cifrado y el firmado de mensajes, en el primer caso el mensaje es

		cifrado utilizando la clave pública del destinatario. Ya que en algunos casos el remitente sólo puede requerir la firma del mensaje o ambos (el cifrado y firmado), si éste es el caso (el mensaje debe ser cifrado con la clave pública del destinatario y después con la clave privada del remitente). S/MIME no especifica el orden en que debe realizarse (la firma y el cifrado).
DIFERENCIA	La gran diferencia entre PGP y S/MIME consiste en el modelo de gestión de claves, ya que PGP utiliza un modelo denominado "Circulo de confianza", en éste modelo no hay un emisor central de claves o autoridad de aprobación, es decir se basa en los usuarios para el control y la gestión de claves, este modelo es apropiado para usuarios y organizaciones pequeñas, por otro lado S/MIME utiliza un modelo jerárquico en el cual existe un registro maestro y una autoridad de aprobación denominada como "Autoridad de certificación" con autoridades locales de registro subordinadas.	
VENTAJAS	**1.** Apropiado para grupos pequeños y usuarios individuales. **2.** Mayor seguridad con soporte para AES. **3.** Versiones *freeware* disponibles **4.** No requiere (pero soporta en caso de ser requerida) una infraestructura externa de clave pública (PKI). **5.** Puede ser utilizado, con cualquier aplicación de cliente de correo tales como (*Netscape Messenger, Eudora y Microsoft Outlook*).	**1.** Apropiado para grupos grandes y organizaciones. **2.** Compatible ampliamente con el estándar de cifrado de correo electrónico. **3.** Soportado en la mayoría de las principales aplicaciones de cliente de correo electrónico. **4.** Más transparente para el usuario final.
FUENTES	• International PGP Site http://www.pgpi.or g/ • MIT PGP Freeware Distribution http://web.mit.edu/network/pgp.html • PGP Site (versión comercial) http://www.pgp.com/ • OpenPGP Site http://www.openpgp.org	Autoridades de certificación • Baltimore http://www.baltimore.com • Entrust http://www.entrust.com • Verisign http://www.verisign.com

Tabla 1.

Para la selección adecuada del algoritmo de cifrado de correo electrónico es necesario considerar los siguientes aspectos:

- **El valor de la información** para la organización (considerando el impacto que conllevaría la divulgación, perdida o modificación no autorizada), ya que al intercambiar información de alta confidencialidad será requerido un algoritmo de cifrado riguroso para su protección.

- El **tiempo de valor de la información**, esto considera aquella información que adquiere valor por un periodo determinado de tiempo (contraseñas que sean cambiadas regularmente y que para protegerlos pueda utilizarse tamaños más pequeños de llave).
- El **riesgo de amenaza** para la información, es decir, para aquella que tenga mayor exposición hacia alguna fuente amenazada que implique un nivel de riesgo elevado se recomienda utilizar un método robusto de cifrado.
- Con relación a **infraestructura**, es necesario considerar que los correos electrónicos cifrados requieren un ancho de banda mayor, el cual depende del algoritmo de cifrado utilizado, el número de destinatarios, el tamaño de la clave y del mensaje.

De esta forma el cifrado de correo electrónico se convierte en una alternativa como mecanismo de protección que contribuirá a reducir el riesgo de ser dañados por las amenazas a las cuales pueda estar expuesta toda la información que es intercambiada diariamente mediante el uso de correo electrónico. Además es necesario que los usuarios de este medio de comunicación estén al tanto de los mecanismos disponibles que contribuyan a reforzar las medidas de seguridad implementadas para proteger su información, porque la seguridad es responsabilidad de todos y cada uno de los usuarios que hacen uso de nuevas tecnologías de comunicación.

Referencias:

http://www.sans.org/reading_room/whitepapers/dns/dns_spoofing_by_the_man_in_the_middle_1567?show=1567.php&cat=dns
http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf
http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245341.pdf.
http://blog.s21sec.com/2009/06/firmado-y-cifrado-de-e-mail-con-smime-y.html

Juan Patiño Corona

A raíz del gran impacto que han tenido las tecnologías de la información en la vida diaria, en el aspecto laboral o para el entretenimiento y sumado a las enormes ventajas que nos ofrecen, estas herramientas se han vuelto algo más que indispensables para un gran número de personas, el cual crece a cada segundo.

Son pocas las personas o instituciones que actualmente no cuentan con una dirección de correo electrónico, y no es para menos, ya que el e-mail es uno de los servicios más populares y útiles que se nos ofrecen en el amplio mundo de la red.

Gracias a éste servicio podemos comunicarnos con cualquier persona alrededor del mundo, compartir todo tipo de información y evitar los diversos inconvenientes del correo ordinario y todo de manera prácticamente gratuita. Pero, si hay millones de personas haciendo uso legitimo de un servicio, entonces también debe haber una forma de aprovecharlo para fines ilegítimos, y eso es lo que ha ocurrido con el correo electrónico, donde existe un gran número de amenazas ocultas, mismas que se han incrementado debido, entre otras cosas, a que la gente no presta el suficiente cuidado al abrir su correo, menospreciando o desconociendo los riesgo que existen.

Amenazas como los virus, gusanos, troyanos y demás fauna cibernética conocida como *malware*, o ataques de *spam*, *pharming* y *phishing*, han encontrado un verdadero nicho de acción en el correo electrónico. Por lo que a continuación se presenta una serie de recomendaciones para mitigar el riesgo y poder estar tranquilos al revisar nuestra bandeja de entrada.

1) Tener control sobre a qué personas o instituciones se les proporciona la cuenta de correo electrónico. Ésta dirección es parte de nuestra información personal y no debe ser difundida indiscriminadamente, así mismo es muy recomendable revisar las políticas de privacidad que maneja cada institución y saber que harán con nuestros datos antes de proporcionarlos.
2) No abrir, responder, ni dar clic en enlaces o descargar archivos adjuntos, que recibamos en correos no solicitados o de los cuales se desconozca el remitente. Como se ha comentado, éste medio es una puerta para la propagación de *malware* y otras amenazas.
3) Ignorar las cadenas. Este tipo de mensajes son muy comunes y abarcan un volumen importante de los buzones. En la mayoría de los casos los usuarios sólo reenvían la información, provocando que en el cuerpo del mensaje se acumulen cada vez más referencias de correos electrónicos, lo cual conforma una rica fuente de direcciones para los *spammers*. Quienes podrán recabarlas fácilmente haciendo uso de herramientas automatizadas.
4) No contestar el correo basura. Estos mensajes se relaciona principalmente con ofertas, publicidad, avisos de haber ganado un premio, o prácticamente cualquier cosa con el objetivo de llamar la atención. Cuando se envía una respuesta se le está confirmando al

atacante o spammer que la cuenta se encuentra activa; la recomendación principal es hacer caso omiso de estos correos y eliminarlos inmediatamente.

5) Emplear una contraseña con características robustas de seguridad, modificándola periódicamente. Se sugiere emplear una longitud mínima de 8 caracteres, intercalando letras, números y símbolos especiales, evitando utilizar datos personales como la fecha de nacimiento o el mismo nombre de usuario. Así mismo es importante modificarla con cierta periodicidad, con el objetivo de proteger del acceso no autorizado y del robo de identidad a través de nuestro correo electrónico.
6) Cifrar el correo electrónico. En caso de que se requiera preservar la confidencialidad de la información, existen soluciones para cifrar nuestros mensajes. Aplicaciones como *Freenigma, GmailEncrypt o FireGPG*, trabajan sobre servicios de correo basado en web como lo son *gmail, hotmail* o *yahoo*. Así mismo los clientes de aplicaciones como *Outlook* o *Thunderbird* cuentan con sus opciones de configuración o aplicaciones para hacer posible el cifrado y descifrado de la información.
7) Recordar cerrar la sesión al finalizar. Principalmente en lugares públicos como salas de cómputo o cibercafés, es importante no olvidar cerrar la sesión del correo electrónico, así se evitará que otra persona que haga uso de la misma computadora, sea capaz de ingresar a la cuenta.

8) Contar con un programa antivirus y mantenerlo actualizado. Éste *software* se encargará de revisar los archivos adjuntos, previniendo la contaminación y propagación de *malware*.

Estas son sólo algunas recomendaciones fáciles de llevar a cabo pero que elevarán en gran medida el nivel de seguridad de nuestra información y reducirán el riesgo de que seamos víctimas de algún ataque a través del correo electrónico.

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

2009 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

Sergio Andrés Becerril López
Miriam J. Padilla Espinosa
Juan Patiño Corona
Alejandro Reyes Plata
Iván Santa María González
Javier Ulises Santillán Arenas
Rocío del Pilar Soto Astorga
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

Diana Chávez González
Liliana Minerva Mendoza Castillo
Formación

2009 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico