Usuarios no deseados.

Resumen.

La mayoría de las instituciones bibliotecarias reciben diariamente a través de su Web institucional a usuarios no deseados, usuarios maliciosos. Buscando desestabilizar a la biblioteca mediante el acceso a los contenidos que se ofrecen en la misma y a todo aquello que rodea a la misma.

Las consecuencias de estos ataques cibernéticos pueden minimizarse si se toman medias adecuadas. La formación y la concienciación del personal y de los usuarios son una de las herramientas más adecuadas, de lo contrario las secuelas pueden llegar a ser desastrosas.

Palabras clave:

Seguridad en bibliotecas, ciberdelitos, ciberataques, seguridad online, phishing, DDoS, pharming

Introducción.

Hace tan solo unos años hablar de ataques y delitos a través de Internet[1] (de las páginas Web) sonaba a ciencia ficción. A día de hoy, los delitos de la sociedad de la información, los ciberataques, ciberdelitos, etc. son sufridos diariamente por millones de personas y por instituciones públicas y privadas.

Las bibliotecas y centros de documentación soportan una doble problemática. Por un lado tanto usuarios como instituciones pueden ser víctimas de estas actuaciones. Siendo un sencillo blanco por sentirse ajenos e ignorar que pueden ser atacados y carecer de suficientes medios para impedirlos. Por otro lado, la disposición de equipos informáticos, para uso de

[1] La revolución sin precedentes de las TIC se considera todavía insospechado, abarcando la totalidad de los sectores y acciones.

los usuarios, por el propio centro suele ser libre y anónima, pudiendo suscitar cualquier tipo de comportamiento anómalo.

Pero, ¿que es un ciberataque?

Alcanzar definiciones precisas sobre estos términos requieren premisas y discusiones terminológicas que suponen ciertos obstáculos. Debates sobre el inicio de utilización de las palabras, sobre la vía de los ataques, sobre lo virtual, etc.

Cabe destacar que todos los términos referidos (cibercrimen, ciberterrorismo, ciber-hacker, ciberdelitos, etc.) se componen de la raíz *ciber* más la palabra ya utilizada en actividades reprobables tradicionales y conocidas hasta ahora.

Aun así, se podría definir como el conjunto de actividades punibles asociadas con el grupo de tecnologías de la información, a través de medios telemáticos, generalmente Internet. Otra definición podría formularse como un acto ilegal donde se involucra a una computadora, sus sistemas o sus aplicaciones. Siendo las acciones intencionales y nunca accidentales.

Los actos electrónicos abarcan desde objetivos económicos (phishing[2], tabnabbing[3], pharming[4]), relativos a defensa (sabotear, espiar, etc.), documentales (fuentes de información), integridad física de las personas y sus bienes e informáticas (bloqueos de servidores, distribución de malware, robos de datos, virus) con la finalidad de desestabilizar una organización gubernamental y civil hasta la invasión de la intimidad, robos de identidad,

[2] El phishing consiste en el robo de datos bancarios por medio de Internet. El método más habitual es el empleo del correo electrónico para contactar con usuarios y convencerles de que visiten páginas que imitan las de la entidad suplantada y en las que, además, deben introducir datos personales (número de cuenta, PIN, etc.,), que quedan así registrados.

[3] El tabnabbing es una novedosa forma de engañar al usuario. Es también conocido como captura de pestañas. Permitiendo modificar el aspecto de una pagina cuando no tiene el “foco” de la pestaña del navegador.

[4] El pharming es un método más sofisticado que el phishing. el ataque se realiza al ordenador del usuario o al proveedor de servicio de Internet, de modo que cuando el usuario solicita -como hace normalmente- una página de su entidad bancaria, se le redirecciona a otro sitio Web que imita la página original.

actuaciones relacionadas con la propiedad intelectual, con la imagen, crímenes contra la moralidad, etc. de las personas.

Desde finales de los años 90, se observa un creciente cambio de paradigma en cuanto a los crímenes y delitos. El objetivo, de los ciberataques, es el mismo que en los delitos tradicionales pero modificando el canal de actuación. Las nuevas tecnologías, con Internet a la cabeza, permiten todo tipo de ataques. No necesariamente son cometidos totalmente por estos medios, sino también a partir de los mismos.

La evolución de las actuaciones es constante, convirtiéndose en un auténtico problema para ciudadanos e instituciones multiplicándose el poder destructivo gracias al uso de las nuevas tecnologías.

Un ciberataque puede estar dirigido a los equipos y sistemas de computación que se encuentran operando en la red a nivel mundial, o puede ser orientado hacia la información y los datos concretos que son almacenados en bases de datos. Al dirigirse a los equipos y sistemas, pueden buscar la anulación del servicio que éstos prestan, de forma temporal o permanente, introduciendo algún tipo de elemento extraño en dichos sistemas que dificulten su operación normal. Los ataques contra los datos, por su parte, pueden ir desde el robo de los mismos, a la manipulación e incluso el borrado.

En definitiva, las razones de los ataques se pueden clasificar:

- Experimentación y deseo de aprender.
- Confianza equivocada con otros individuos.
- Venganza.
- Espionaje corporativo y/o gubernamental.
- Razones psicológicas.
- Financiero.
- Motivos políticos.

La realidad.

Esta compleja tesitura da pie a que las bibliotecas sufran, al igual que el resto de sectores, ataques e intromisiones con mayor frecuencia de lo que piensan las autoridades, los responsables de las bibliotecas y los usuarios. La información electrónica disponible, desde las Webs de las bibliotecas, está más disponible que nunca para la audiencia mundial y, aunque se desea afirmar que dicha información gubernamental, personal o científica está garantizada en cuanto a su protección, la realidad dice que la seguridad absoluta no existe y que las vulnerabilidades se han multiplicado con el desarrollo de estas nuevas tecnologías de la información y la comunicación.

La encuesta[5] de vigilancia de Seguridad Cibernética 2010, realizada para la revista CSO en colaboración con el Servicio Secreto de Estados Unidos y el Instituto de Ingeniería de Software de Carnegie Mellon CERT[6], y patrocinado por Deloitte, calificó a las acciones cibernéticas de los hackers como la mayor amenaza.

Según la Oficina de las Naciones Unidas contra la Droga y el Delito La red cibernética ofrece oportunidades de lucros ilícitos inimaginables. Superando los mil millones de dólares de pérdidas[7], originando contracciones de la economía y pérdidas de confianza en el comercio electrónico.

---

5 Encuesta sober la Vigilancia de seguridad cibernética, 2010. <http://www.CSOonline.com/documents/pdfs/2010CyberSecurityResults.pdf> [Consultado el 8 de octubre de 2010]

6 Carnegie Mellon University's Computer Emergency Response Team. <http://www.cert.org/> [Consultado el 8 de octubre de 2010]

7 Oficina de las Naciones Unidas contra la Droga y el Delito, ONUDD <http://www.unodc.org/documents/data-and-analysis/tocta/Globalization_of_Crime-ExSum-Spanish.pdf> [Consultado el 8 de octubre de 2010]

Según CSI (Computer Security Institute) la mayor parte de los hechos no se comunican mayoritariamente por miedo a padecer una publicidad negativa y por pensar que los cuerpos de seguridad de los países no pueden ayudar[8].

Según análisis de Symantec[9], para el 42 por ciento de las compañías los ataques on-line son la primera de sus preocupaciones, debido a que el 75 por ciento de ellas sufrió ataques a través de la red durante el año 2009.

Con estos elevados índices, los ataques generados de forma online superan ya en el escalafón al crimen tradicional como la principal preocupación de las empresas.

Destacan las siguientes agresiones que padecen y pueden soportar las bibliotecas a través de la red:

- Obtención, modificación y supresión de documentación disponible online (artículos científicos, libros digitalizados, eBooks, etc.)
- Extracción de datos personales de usuarios y trabajadores de la institución. (nombres, direcciones, DNI, mails, números de cuenta bancaria, etc.)
- Historiales de préstamos y consultas de documentos.
- Acceso a los servicios por medio de de falsas identidades.
- Alterar los registros de ejemplares, de los diferentes soportes documentales. Es posible, por ejemplo alterar las condiciones de de un documento en concreto: el tipo de préstamo, la caducidad, tipo de colección, generar préstamos y devoluciones, etc.
- Modificar el diseño de la página Web de la institución, como el acceso a sus contenidos.
- Anulación y bloqueo de comunicación.
- Los servicios 2.0 (colocan a los usuarios en una situación vulnerable) como los canales Twitter, perfiles en las redes

[8] Estas conclusiones se desarrollaron a través de Computer Crime & Security Survey. 2009.

[9] Estudio sobre el Estado de la Seguridad Empresarial 2010, <http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf> [Consultado el 9 de octubre de 2010]

sociales (Facebook, Tuenti, Orkut, hi5, Sónico), MySpace, Delicious, plataformas de video como Youtube, blogs, foros, Wikis, Flickr, etc. pueden ser igualmente saboteados.

- Internet constituye un instrumento formidable de propaganda que permite alcanzar fácilmente a una gran audiencia (algunos centros superan ampliamente los cien mil usuarios). Fundando en las siguientes actuaciones:
  - La propagación de virus informáticos.
  - El envío masivo de correo no deseado o SPAM.
  - La suplantación de los remitentes de mensajes con la técnica Spoofing[10].
  - El envío o ingreso oculto de archivos espías o Keyloggers[11].
  - El uso de Troyanos para el control remoto de los sistemas o la sustracción de información.
  - El uso de archivos BOT[12] del IRC (Internet Relay Chat) para el control remoto de sistemas y sustracción de información.
  - El uso de Rootkits[13] para los mismos fines anteriores y daños irreversibles, etc.

Durante el año 2010 diversas instituciones han sufrido ataques. Véase los datos:

- En septiembre el Ministerio de Cultura de España padeció un DDoS, denegación de servicio. Consistió en la petición a sus

[10] Spoofing: Hace referencia a la suplantación de identidad para fines maliciosos (en la mayoría de los casos) o de investigación; existen diferentes tipos como el IP spoofing, ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing.

[11] El keylogger es un tipo de software que permite registrar las pulsaciones del teclado, es decir, lo que uno está tecleando para luego almacenar dicho registro y enviarlo a través de Internet.

[12] Un bot (abreviatura de *robot*) es un programa informático que realiza funciones muy diversas, imitando el comportamiento de un humano.

[13] Un rootkit es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible.

servidores de cientos de miles de accesos casi al mismo tiempo, bloqueando sus Webs.

- Twitter, en el mismo mes, ha sobrellevado igualmente ataques[14].
- Google recibió denuncias de sabotajes de diversas cuentas privadas de mail a principio de año[15].
- Blogs de WordPress y usuarios de ZenCart. Los ataques no solo se concentraron en un sólo proveedor de hosting[16], sino que en varios de los más populares proveedores de alojamiento para bloggers,

¿Quienes son los atacantes?

En este apartado se observa una de las grandes particularidades entre los delitos tradicionales y los cometidos a través de Internet: la "deslocalización" de los delitos y del atacante, debido a que la red es global. Deduciendo que los atacantes nunca ven a sus víctimas, lo que facilita su labor, ya que resulta mucho más fácil atacar a alguien que no se ve.

Por tanto, la posibilidad de captura de los autores es mínima, debido a que su ubicación física se desconoce, siendo la única forma de atraparlo la cooperación y colaboración entre países u organizaciones. Aunque existen acuerdos entre países, éstos son lentos y burocráticos perdiendo pistas y limitando el objetivo.

Los autores de los hechos pueden ser personas o máquinas ordenadas para realizar los actos delictivos.

[14] Los ataques fueron tres. Por un lado, cada vez que se pasaba el mouse sobre un Tweet, este se retweteaba automáticamente, provocando así un masivo retweteo. Otro lograba que los colores de nuestro Twitter cambiara constantemente. Y el tercero, rediría al usuario a un sitio pornográfico.

[15] Google advierte que los ataques a Gmail probablemente provegan de China.

[16] Los proveedores de hosting más afectados fueron DreamHost, GoDaddy, Media Temple y Bluehost.

Los procedimientos.

Las características de Internet, como el anonimato, la falta de regulación o el escaso desarrollo actual de sistemas de seguridad, representan el medio idóneo para atacar mediante la Red de redes. Siendo por tanto un arma eficaz, discreta y económica.

Es útil diferenciar las dos posibilidades o niveles de intromisión al sistema informático. Por un lado cabe destacar el nivel de acceso al sistema, (vía email (keyloggers, troyanos), ejecutando programas, etc.) siendo el que más riesgo atañe y el más difícil de lograr (donde el intruso pueda tener control pleno de los recursos con los mismos privilegios y permisos que el propio administrador mediante un terminal remoto), y por otro lado, el acceso a la aplicación a través del código fuente por ejemplo.

Los sistemas de información han evolucionado hacia arquitecturas compartidas, con una interconexión a gran escala. Su apertura, junto con la disponibilidad de las tecnologías IP (Internet Protocol) ha provocado que su seguridad sea extremadamente vulnerable. Las amenazas tecnológicas y las habilidades de los potenciales “hackers” se han incrementado enormemente siendo testigos de agresiones profesionales por parte de criminales informáticos.

Modus operandi

En algunas ocasiones el crimen tiene un alto grado de organización, existiendo “*bandas*” bien estructuradas que realizan estas operaciones en la red y están a la orden de diversos clientes que necesiten cualquier clase de información; en otros casos si el cliente no esta satisfecho con la información, el dinero invertido es devuelto.

Paliativos.

Ante el panorama descrito, las bibliotecas no se encuentran libres de padecer ciberataques, por ello es por lo que las autoridades deben actuar con el fin de prevenir y reducir cualquier ataque generado a través de la sociedad de la información.

No cabe la menor duda de que los principales problemas para poner en marcha planes de contingencia que cubran los ataques informáticos a las redes de las instituciones bibliotecarias, son disponer de una infraestructura tecnológica de respuesta que permita la defensa de los intereses nacionales en el ciberespacio y de una legislación (nacional e internacional) adecuada.

Dos de los pilares básicos y primordiales para el desarrollo de los planes son la formación y la concienciación. Es preciso tomar conciencia de los riesgos (con medidas procedimentales, organizativas y técnicas), utilizar herramientas de seguridad (medidas técnicas) y mantener evaluaciones que acrediten el buen uso de estas prácticas y herramientas.)

Es necesario, para implementar las actuaciones, superar la falta de concienciación, en materia de seguridad, por parte de las instituciones y usuarios de las TICs. De hecho, la ingenuidad, los errores y omisiones del personal autorizado (pero desconocedor de buenas prácticas de seguridad) y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información constituyen una fuente principal de amenazas.

En cuanto a las medidas técnicas que deben instaurase en los centros, con el fin de contrarrestar los posibles efectos de adversos, es necesario usar un amplio espectro de tecnologías de defensa. Existen diversas soluciones que deben instalarse en las computadoras de la biblioteca con el fin de prevenir ataques externos; estas medidas vienen en cuanto a la utilización de software y de hardware. Cabe destacar que las herramientas han ido mejorando con el paso del tiempo generando que su estructura se vuelva mucho más compleja, haciendo que sean más difíciles de analizar.

A continuación se detallará algunos ejemplos de medidas a tomar por las bibliotecas:

- Antivirus Web, filtración de tráfico, analizadores de comportamientos, máquinas virtuales, firewall perimetral, filtro de contenido, antispam, sistemas de análisis de tráfico de red, organizador de comunicaciones por correo electrónico, instalación de un calendario o gestor de contactos y cortafuegos.
- Uno de los métodos más efectivos para defenderse de estas amenazas son las tecnologías que bloquean los sitios Web infectados. Los incidentes provocados por un botnet han demostrado que un antivirus moderno no sólo debe contener tecnologías de lucha contra los rootkits, sino que debe ser capaz de neutralizar sus subespecies, los bootkits.
- La introducción de la criptografía (amigable y transparente) en las organizaciones e instituciones reduciría muchos de estos problemas.
- La informática Forense es un método muy provechoso para prevenir estos tipos de ciber ataques. Esta se encarga de garantizar la protección y seguridad de la información y de las tecnologías que cuentan con esta. Para esto, recolectan datos de diversos medios digitales para luego examinarlos y esto permite que se llegue a una conclusión, es decir, si hay algún caso de ciber ataque o no, todo esto sin alterar los datos de origen. Cabe señalar que siempre deben hacerlo teniendo en cuenta los requerimientos legales para no violar la privacidad de ningún tercero y siempre recolectando las evidencias necesarias para que la justicia dictamine que de verdad está ante un caso de ciber ataque.
- El uso del software libre evitaría un alto porcentaje de ataques. Su flexibilidad salvaría vulnerabilidades y amenazas que aparecen en los sistemas operativos comerciales.

La realidad del ciberespacio hace que sea necesaria la colaboración de todo el mundo. Un elemento esencial es lograr la colaboración de todas las

partes interesadas para resolver los problemas comunes de ciberseguridad y crear un plan de creación de capacidades eficiente.

Existen iniciativas[17] internacionales por parte de organismos y empresas privadas. Un número importante de países se han adherido a estos acuerdos internacionales.

Por otro lado se están tomando y aplicando medidas en el plano estratégico, como la creación de Centros de Respuesta a Incidentes de Seguridad. En relación con los CERT (Computer Emergency Response Team).

Por último, en cuanto a las medidas jurídicas, es necesario adecuar o crear legislaciones y de jurisdicciones adaptadas a esta tipología de delincuencia "de nueva generación". El principal problema estriba en la carencia de una armonización internacional de la legislación sobre la ciberdelincuencia. Se han desplegado esfuerzos para resolver este problema y, pese a que han sido valiosos, siguen siendo insuficientes. Internet es una herramienta de comunicación internacional y, por consiguiente, toda solución relativa a la seguridad debe encontrarse a nivel mundial.

Conclusiones finales:

El proceso de ciberseguridad alcanza a toda la sociedad, en la medida en que todos los individuos están afectados en mayor o menor medida por su implementación.

Al plantear el proceso de ciberseguridad es importante identificar correctamente los activos y recursos que han de protegerse, para poder definir con precisión el alcance de la seguridad para que la protección sea eficaz. Esto exige un planteamiento global de la seguridad, a la vez multidisciplinar y exhaustivo.

[17] Tratado Internacional de Cibercrimen entre la Unión Europea y Estados Unidos. Convenio Internacional sobre Cibercrimen. Guía de ciberseguridad para los países en desarrollo (de la Unión Internacional de Telecomunicaciones). <http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf>

Bibliografía:

- BACALLAO PINO, Lázaro. Representaciones mediáticas de las redes sociales: un estudio de los casos. Revista Latina de comunicación social, Nº. 65, 2010.

- CANONGIA, Claudi; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. Parcerias Estratégicas, Vol. 14, No 29 (2009).

- Communication on protecting Europe from cyber-attacks – 30 March 2009. European Commission: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= COM:2009:0149:FIN:EN:HTML>

- GERCKE, Marco. El ciberdelito: guía para los países en desarrollo. Unión internacional de Telecomunicaciones. División de Aplicaciones TIC y Ciberseguridad Departamento de Políticas y Estrategias. Sector de Desarrollo de las Telecomunicaciones de la UIT. Proyecto de abril de 2009 http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

- GHOSH, Sumit . Nature of Cyberattacks in the Future. Cybercrimes: A Multidisciplinary Analysis. 2010, Part 9, Pág. 379-399.

- LIM, H.; HONG, S.; CHOI, M. S.; LEE, S. J.; KIM, T. W.; LEE, S. W.; HA, B. N. Security Protocols Against Cyber Attacks in the Distribution Automation System. IEEE Transactions on Power Delivery, Vol. 25, Nº. 1, January 2010. Pág. 448-455

- PATEL, Sandip, ZAVERI, Jigish. A Risk-Assessment Model for Cyber Attacks on Information Systems. *Journal of Computers*, Vol 5, No 3 (2010), Mar 2010, Pág. 352-359.

- TAPIA, Gema. *Ciberataque a las redes sociales: Las amenazas también han empezado a introducirse en las redes profesionales*. Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones, Nº. 42, 2009, Págs. 40-42.