2015-06-01

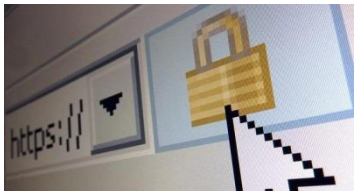
CiberNoticias # 32

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 01: **Descubren LogJam, una grave vulnerabilidad que intercepta datos cifrados**



Los expertos en seguridad informática creen que el 8% de las páginas que incluyen el protocolo de seguridad HTTPS son vulnerables

La sombra de Heartbleed pasea de nuevo. Un grupo de investigadores formado por expertos en seguridad informática franceses y norteamericanos, centros universitarios, los que se encuentran ingenieros de Microsoft, han descubierto una grave vulnerabilidad que es capaz de interceptar datos cifrados.

Según el informe elaborado, la vulnerabilidad informática detectada en un algoritmo de los sistemas de cifrado utilizados permite espiar comunicaciones supuestamente seguras, recoge la cadena BBC. De esta manera, decenas de miles de sitios web HTTPS, servidores de correo y otros servicios son vulnerables al espionaje debido a un defecto en los algoritmos criptográficos.

Proveedores de antivirus ya han sido alertados y preparan una solución al respecto. Los expertos creen que el 8% de las páginas que incluyen protocolos de seguridad HTTPS son vulnerables**,** por lo que este icono situado en la barra de direcciones del navegador tampoco garantizaría a los usuarios comunicaciones totalmente privadas.

Este «bug» afecta a varios servicios de correo electrónico que utilizan el protocolo de cifrado Transport Layer Security (TLS) y, según los expertos, puede ocasionar posibles intromisiones ilegítimas. El fallo se beneficia de Diffie-Hellman, un protocolo criptográfico de establecimiento de claves entre partes que no han tenido contacto previo utilizando un canal inseguro y de manera anónima (no autentificada). Esta fue una de las primeras técnicas desarrolladas para permitir que dos o más partes crearan y compartieran una clave de cifrado. Este sistema es fundamental para otros protocolos informáticos como HTTPS, IPsec, SMTPS o SSH.

El informe asegura que los navegadores más populares como Chrome, Firefox, Safari o Internet Explorer son susceptibles de ser afectados por este «bug», por lo que empresas como Google o Microsoft ya trabajan en resolverlo. Pese a todo, diversos expertos aseguran que los usuarios no deben preocuparse al respecto, ya que para aprovecharse de la vulnerabilidad los hackers y el objetivo deben estar en la misma red.

Fuente: http://www.abc.es/

Noticia # 02: Un congreso analiza las formas de luchar contra el 'phishing'

eCrime 2015 reúne en Barcelona a los principales expertos mundiales en cibercrimen

Las amenazas informáticas persistentes, el phishing, el malware móvil, los ataques de denegación de servicio y el uso de las cripto monedas por los delincuentes son algunos de los temas que desde este lunes debate en Barcelona unos 200 expertos en seguridad informática de todo el mundo que se reúnen en el congreso eCrime2015, que organiza el AntiPhishing Working Group (APWG), la organización estadounidense de lucha contra el cibercrimen.

El phishing es el intento de los delincuentes informáticos de engañar a los usuarios para que proporcionen sus datos bancarios y contraseñas para desvalijar sus cuentas. Un intento que no siempre es directo, según explicaban los expertos, sino que suele ser uno el que roba a través de un malware y otra banda quien utiliza estas contraseñas después de comprarlas en el mercado negro.

Este método, que utiliza más la persuasión clásica que una gran complejidad tecnológica, es cada vez más popular y se adapta a los tiempos. En Malaisia, por ejemplo, ya han descubierto páginas webs fraudulentas adaptadas a los móviles, porque este es el medio con el que la mayoría de los internautas accede a sus cuentas bancarias.

En el congreso, que se celebra en el Caixaforum, participan representantes de grandes empresas y entidades financieras como CaixaBank y Telefónica, Kaspersky, PayPal, los es-CERT y representantes académicos y de los cuerpos policiales.

Fuente: http://www.elperiodico.com/

Noticia # 03: Encriptación: de lo básico a lo estratégico

Los datos siempre están en riesgo de perderse o de que sean robados, aparte de que nunca falta quien olvide la clave para acceder a ellos.

Poco antes de que la máquina de escribir fuera sustituida por la computadora personal y de que los documentos impresos se convirtieran en información codificada en bits, las empresas solían resguardar sus datos más sensibles en carpetas, archiveros y bodegas, cuyo esquema de protección dependía simplemente de controlar el acceso a los mismos mediante el uso de cerraduras, candados, llaves o de avisos con leyendas como “Prohibida la entrada” o “Sólo personal autorizado”.

Pero en el terreno informático, y muy particularmente dentro de un entorno de redes, la propia naturaleza de los documentos obligó a modificar radicalmente tan rudimentario método de protección y hoy en día los negocios manejan complejas estructuras de seguridad que incluyen antivirus, firewalls y aplicaciones de respaldo, por ejemplo, aunque el privilegio de acceder a dicha documentación sigue centrándose en quien tiene “la llave” (usuarios autorizados, administradores de sistemas, etc.) o en quienes necesitan entrar a las redes y los contenidos corporativos para realizar su trabajo ya sea desde sus casas o vía remota.

Debido a lo anterior, tanto las organizaciones como los usuarios deben estar conscientes de la importancia de encriptar sus datosde forma concreta (una carpeta o fichero) o global (encriptado íntegro del equipo). Elcifrado de datoses el proceso por el que una información legible, mediante un algoritmo llamado “cifra”, se transforma en información ilegible (conocida como “criptograma”o “secreto”); en ese sentido, quien cuente con los permisos correspondientes y tenga la clave de cifrado puede volver a hacer legible la información, reduciendo así el riesgo de que sea leída por terceras partes o de que termine en manos inapropiadas.

Los algoritmos, sin embargo, suelen ser públicos, lo cual facilita la intromisión de posibles atacantes, por lo que los expertos sugieren basar la seguridad de un sistema de cifrado enteramente en la clave y no en aquéllos. En materia de cumplimiento, los negocios tienen la obligación de encriptar cualquier equipo portátil con el que vaya a accederse a las redes corporativas, así como hacer copias de seguridad externas y cifrar los datos más sensibles en caso de que la transmisión de los mimos se realice a través de un entorno tan descontrolado e inseguro como lo es Internet, para lo que se recomienda el uso de protocolos criptográficos como SSL (Secure Socket Layer), conformando una capa de seguridad que puede aplicarse en diversos ámbitos, como HTTPS, FTP y/o SMTP

Adoptar VPNs (Virtual Private Network) y cifrar archivos o discos duros son también buenas alternativas para la protección de los datos, aunque tener un fichero o una información cifrada no garantiza absolutamente su integridad o su fiabilidad, ya que pueden presentarse varios problemas aun con los algoritmos más seguros; por ejemplo, la información se perdería en caso de que sea cifrada en un disco duro y éste se estropee; también es probable que un usuario olvide las claves de cifrado o las filtre con la idea de afectar a su compañía, además de que se suele almacenar la clave en el mismo sitio que el fichero cifrado, por lo que si alguien accede a este último también podrá encontrar la clave para descifrarlo.

Una mala gestión de las claves o el manejo de información inválida impedirá que el destinatario acceda a ella aunque el cifrado y descifrado sean correctos, por lo que siempre será necesario realizar backups de los datos, recurrir al método de doble autenticación o garantizar la seguridad de las claves, sobre todo si se tiene a "la nube" como principal repositorio o medio de transferencia.

Pareciera que las soluciones de encriptación fueron diseñadas exclusivamente para las empresas, pero no debemos olvidar que la mayoría de los riesgos a la seguridad tiene como punto de coincidencia al individuo, ya sea como usuario interno o externo de una red corporativa; de hecho, existen tecnologías -como Microsoft BitLocker- que permiten cifrar los archivos de forma local o en el equipo de cada usuario.

El nivel de seguridad que otorga el cifrado depende de la robustez del algoritmo de encriptación, o sea, del modo en que se cifra la información para hacerla ilegible. A fin de satisfacer los requerimientos de las organizaciones en esta materia, la compañía de seguridad ESET estableció recientemente una alianza tecnológica con la empresa DESlock, cuyo producto insignia (DESlock+) permite justamente el cifrado de datos.

Debe mencionarse que el trabajo desde el hogar o desde dispositivos móviles obliga a la extensión de las políticas de seguridad mediante el cifrado más allá del perímetro de una red; en ese sentido, la solución referida ofrece un control completo sin importar dónde se encuentran los usuarios; se trata de una poderosa herramienta de cifrado que, del lado del servidor (DESlock+ Enterprise Server), permite a los administradores de sistemas la fácil gestión de usuarios y estaciones remotas de trabajo de manera independiente o en relaciones de "muchos a muchos".

Esta aplicación facilita además el uso compartido de claves entre clientes en tiempo real, utilizando avanzados algoritmos y estándares para crear claves impenetrables y haciendo posible el cifrado de discos duros, medios extraíbles, archivos y correos electrónicos.

Los datos son una parte crítica de toda organización, pero este valioso activo suele suponer un gran riesgo cuando se traslada o se transmite fuera de la red corporativa. DESlock+ también garantiza una mínima interacción del lado del cliente, mejorando el cumplimiento de normativas por parte del usuario y permitiendo la seguridad de los datos corporativos con un único paquete instalador de Microsoft (MSI).Aparte de la edición gratuita denominada "Personal", DESlock maneja las versiones Pro, Standard y Essential (esta última exclusiva para los clientes de ESET) pensando en los requerimientos de distintos tipos de usuarios y tamaños de empresas. Dependiendo de las necesidades, esta aplicación garantiza prestaciones como cifrado completo del disco duro; cifrado de medios extraíbles, archivos, carpetas, textos y portapapeles; cifrado de discos virtuales, compatibilidad con la administración centralizada, así como cifrado portable con DESlock Go y complemento para correo electrónico y archivos adjuntos de Outlook.

Fuente: http://addictware.com.mx/

Noticia # 04: Las 10 principales estrategias de manipulación mediática según Noam Chomsky

1- La estrategia de la distracción. El elemento primordial del control social es la estrategia de la distracción que consiste en desviar la atención del público de los problemas importantes y de los cambios decididos por las élites políticas y económicas, mediante la técnica del diluvio o inundación de continuas distracciones y de informaciones insignificantes. La estrategia de la distracción es igualmente indispensable para impedir al público interesarse por los conocimientos esenciales en el área de la ciencia, la economía, la psicología, la neurobiología y la cibernética. "Mantener la atención del público distraída, lejos de los verdaderos problemas sociales, cautivada por temas sin importancia real. Mantener al público ocupado, ocupado, ocupado, sin ningún tiempo para pensar; de vuelta a la granja con los otros animales.

2- Crear problemas, después ofrecer soluciones. Este método también es llamado "problema-reacción-solución". Se crea un problema, una "situación" prevista para causar cierta reacción en el público, a fin de que éste sea el mandante de las medidas que se desea hacer aceptar. Por ejemplo: dejar que se desenvuelva o se intensifique la violencia urbana o planear y ejecutar atentados sangrientos, a fin de que el público sea el demandante de leyes de seguridad y políticas en perjuicio de la libertad. O también: crear una crisis económica para hacer aceptar como un mal necesario el retroceso de los derechos sociales y el desmantelamiento de los servicios públicos.

3- La estrategia de la gradualidad. Para hacer que se acepte una medida inaceptable, basta aplicarla gradualmente, a cuentagotas, por años consecutivos. De esa manera condiciones socioeconómicas radicalmente nuevas (como el neoliberalismo) fueron impuestas durante las décadas de 1980 y 1990: Estado mínimo, privatizaciones, precariedad, flexibilidad, desempleo en masa, salarios que ya no aseguran ingresos decentes, tantos cambios que hubieran provocado una revolución si hubiesen sido aplicadas de una sola vez.

4- La estrategia de diferir Otra manera de hacer aceptar una decisión impopular es la de presentarla como "dolorosa y necesaria", obteniendo la aceptación pública, en el momento, para una aplicación futura. Es más fácil aceptar un sacrificio futuro que un sacrificio inmediato. Primero, porque el esfuerzo no es empleado inmediatamente. Luego, porque el público, la masa, tiene siempre la tendencia a esperar ingenuamente que "todo irá mejorar mañana" y que el sacrificio exigido podrá ser evitado. Esto da más tiempo al público, la masa, tiene siempre la tendencia a esperar ingenuamente que "todo irá mejorar mañana" y que el sacrificio exigido podrá ser evitado. Esto da más tiempo al público para acostumbrarse a la idea del cambio y de aceptarla con resignación cuando llegue el momento.

5- Dirigirse al público como criaturas de poca edad. La mayoría de la publicidad dirigida al gran público utiliza discurso, argumentos, personajes y entonación particularmente infantiles, muchas veces próximos a la debilidad, como si el espectador fuese una criatura de poca edad o un deficiente mental. Cuanto más se pretenda engañar al espectador, más se tiende a adoptar un tono infantilizante. ¿Por qué? "Si uno se dirige a una persona como si ella tuviese la edad de 12 años o menos, entonces, en razón de la sugestionabilidad, tenderá, con cierta probabilidad, a una respuesta o reacción también desprovista de un sentido crítico como la de una persona de 12 años o menos de edad

6- Utilizar el aspecto emocional mucho más que la reflexión. Hacer uso del aspecto emocional es una técnica clásica para causar un corto circuito en el análisis racional y por ende al sentido crítico de los individuos. Por otra parte, la utilización del registro emocional permite abrir la puerta de acceso al inconsciente para implantar o injertar ideas, deseos, miedos y temores, compulsiones o inducir comportamientos.

7- Mantener al público en la ignorancia y la mediocridad. Hacer que el público sea incapaz de comprender las tecnologías y los métodos utilizados para su control y su esclavitud. "La calidad de la educación dada a las clases sociales inferiores debe ser la más pobre y mediocre posible, de forma que el nivel de la ignorancia que planea entre las clases inferiores y las clases sociales superiores sea y permanezca imposible de alcanzar para las clases inferiores"

8- Estimular al público a ser complaciente con la mediocridad. Promover en el público la idea de que es moda el hecho de ser estúpido, vulgar e inculto.

9- Reforzar la auto culpabilidad. Hacer creer al individuo que es solamente él el culpable por su propia desgracia, por causa de la insuficiencia de su inteligencia, de sus capacidades o de sus esfuerzos. Así, en lugar de rebelarse contra el sistema económico, el individuo se auto invalida y se culpa, lo que genera un estado depresivo, uno de cuyos efectos es la inhibición de su acción. ¡Y, sin acción, no hay revolución!

10- Conocer a los individuos mejor de lo que ellos mismos se conocen. En el transcurso de los últimos 50 años, los avances acelerados de la ciencia han generado una creciente brecha entre los conocimientos del público y aquellos poseídos y utilizados por las élites dominantes. Gracias a la biología, la neurobiología y la psicología aplicada, el "sistema" ha disfrutado de un conocimiento avanzado del ser humano, tanto de forma física como psicológicamente. El sistema ha conseguido conocer mejor al individuo común de lo que él se conoce a sí mismo. Esto significa que, en la mayoría de los casos, el sistema ejerce un control mayor y un gran poder sobre los individuos, mayor que el que los individuos tienen y ejercen sobre sí mismos.

Fuente: http://pijamasurf.com/

CREDITOS:

Revista de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:
Ing. Marco de la Torre
m.delatorre@scprogress.com

Supervisado por:
Ing. Arturo de la Torre
adltorre@scprogress.com