CIBERSEGURIDAD

SCP

Privacidad de los datos

Parte I

Cyberoam

Avira

CRYPTOPHONE

NEXXT SOLUTIONS

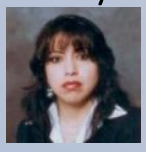
open source

Índice

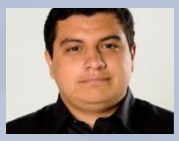
CRÉDITOS:

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

Recopilación y edición:



Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)



Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Revisado por:

Arturo de la Torre
adltorre@scprogress.com (+593 999025294)

Síguenos en:

SCProgress

www.scprogress.com

Facebook

Twitter

¿Por qué es importante proteger tus datos personales?

La importancia que tiene la seguridad de la información y el poder que implica administrarla, es un tema muy delicado que no está en el conocimiento de muchas personas. La diversidad de la información que está asociada a una persona es amplia, los datos considerados como personales (apellidos y nombres, número de identificación, números de cuenta, claves, etc.), son utilizados para muchas actividades cotidianas (pagos, transferencias bancarías, consultas, etc). Con el avance tecnológico muchos datos relacionados a los individuos se almacenan, procesan o transmiten en formato digital.

Esto expande el abanico de opciones para los cibercriminales que buscan lucrar con la información, ya que ahora se utilizan los medios tecnológicos para cometer delitos, es en este punto donde la seguridad de la información cobra relevancia, sobre todo porque cada brecha de seguridad relacionada con una fuga de información conlleva a distintas consecuencias, (suplantación de identidad, copia de claves, etc.) mismas que están en función de los datos que son robados, el tipo de empresa que ha sido afectada, así como, la industria a la que pertenece dicha organización.

En el contexto de internet, muchos usuarios no le dan mayor importancia a la información que publican en la red y de qué forma lo hacen, más aún, muchos no diferencian lo privado de lo público, no por que no quieran o porque no prefieren diferenciar una cosa de la otra, simplemente es por desconocimiento. Para mucha gente es normal pertenecer a redes sociales y publicar su vida, mientras más conocidos sean y más amigos tengan en esa red social, creen que son más importantes, es esta “vulnerabilidad” sin duda alguna, la que se está explotando la ingenuidad del usuario.

Por otro lado están las empresas, las cuales son las encargadas de administrar la información privada y/o pública que los usuarios les confían, por ejemplo en el caso de un concurso, típicamente los datos que piden son nombre, apellido, ciudad, número de cédula, etc., sin embargo las empresas no cuidan o no proporcionan las seguridades de los datos de las personas.

Muchos dicen: “No importa, si en ese correo no tengo nada”. Eso no es una excusa ya que por más que el usuario no tenga nada en esa cuenta de correo, la información le pertenece a él, y el hecho de que alguien tenga su clave y acceda a algo que no le pertenece, tenga información importante o no, debería preocuparle.

Por lo anterior, y debido a que los datos personales pertenecen a su titular y no a las entidades que utilizan las bases de datos, se han puesto en marcha iniciativas alrededor del mundo para proteger los datos personales que se encuentran en posesión de particulares o de gobiernos, haciendo de la tarea de protección de la información, una responsabilidad compartida entre los usuarios, las empresas que tienen acceso a los datos y gobiernos que deben legislar al respecto, así como, crear las instituciones encargadas de controlar, regular y hacer cumplir las leyes.

Es evidente que la información es apreciada por muchos aspectos relevantes, su adecuada administración permite en todos los niveles una correcta toma de decisiones, por ejemplo, en el ámbito organizacional conocer información financiera, de marketing, producción, de sus clientes, del personal, de su competidores, etc., utilidad para la toma de decisiones y a su vez se debe proporcionar la seguridad respectiva por su calidad de secreto industrial, por lo que en muchos casos es considerada el activo más importante de las personas e instituciones.

En otros casos, la información es fundamental para las operaciones de todos los días, aunque no siempre es propiedad de las empresas, sobre todo si consideramos que estos datos pueden pertenecer a los clientes o usuarios. Por ello, en los últimos años ha cobrado relevancia la protección de datos personales.

Los datos personales y las brechas de seguridad.

Debido a la importancia de los datos y a los beneficios que pueden generarle a los cibercriminales que buscan adueñarse de ellos, continuamente observamos brechas de seguridad relacionadas con la fuga de información, en los cuales se utilizan distintos vectores de ataque para lograr los fines maliciosos.

En los últimos años se conocieron casos de fuga de información relacionados con malware Point of Sale, en compañías como Target, Home Depot o UPS, donde los atacantes lograron obtener más de 40 millones de números de tarjetas de crédito y débito de usuarios. Empresas como eBay o Yahoo, también se vieron en la necesidad de notificar a miles de usuarios que sus cuentas y contraseñas habían sido filtradas a través de un ataque.

Grandes industrias se han visto afectadas, tal es el caso de Comunity Health System (CHS) en los Estados Unidos, que fue víctima de la fuga de 4.5 millones de registros médicos. De acuerdo con el comunicado de la entidad, sus sistemas fueron víctimas de una APT. Otro de los casos más conocidos, fue el robo de datos confidenciales a Ashley Madison, sitio de citas online especializado en relaciones extramaritales, que puso en potencial peligro a sus 37 millones de usuarios.

Sin importar las actividades de las empresas, la industria a la que pertenezcan, su tamaño o ubicación geográfica, e independientemente del ataque utilizado para afectarlas, la consecuencia más común suele ser la fuga de información, con los conocidos daños a la imagen de las organizaciones. En esta lista se cuentan empresas, gobiernos y otras entidades, impactado de manera negativa a sus miles, e incluso millones de usuarios.

Por estas razones, en distintos países se han emitido leyes orientadas a la protección de los datos personales, que deben cumplir entidades del sector público o privado que traten información de carácter personal. La protección de los datos es un derecho ciudadano que brinda la facultad para controlar a voluntad la información personal de cada individuo,

El Ecuador consciente de las ventajas y desventajas del avance de la tecnología, se encuentra encaminado a precautelar la información, razón por la cual se presentó en septiembre de 2016, el Proyecto de Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales, que se encuentra en la Asamblea Nacional para el proceso correspondiente.

Definición y clasificación de los datos personales.

Por datos personales se entiende cualquier información concerniente y asociada a una persona, la cual permite identificarla. Estos datos nos caracterizan como individuos y determinan nuestras actividades, tanto públicas como privadas. Debido a que cada dato está relacionado directamente con las personas, cada quien es dueño de sus datos personales y es quien decide si los comparte o no.

Entre estos datos se encuentran los que identifican a la persona o aquellos que permiten tener comunicación con su titular. También, entre estos datos tenemos los relacionados con el empleo, sobre características físicas como la fisonomía, anatomía o rasgos de la persona. Además, considera información relacionada con la formación y actividades profesionales, datos relativos a sus bienes, así como, información biométrica. En este contexto se puede dividir a los datos en:

Algunos datos personales pueden resultar sensibles. En esta categoría se incluyen aquéllos que involucran el ámbito privado de su titular, cuyo uso indebido podría derivar en alguna afectación negativa, como la discriminación, por citar un ejemplo. Incluyen aspectos como el origen étnico, estado de salud, creencias religiosas, preferencia sexual, afiliación u opiniones políticas. Las categorías pueden clasificarse de la siguiente manera.:

Adicionalmente al tema de la información, de cómo la usemos o qué tratamiento le demos a la misma, se encuentra el caso de las claves o contraseñas, encontramos personas que usan las mismas contraseñas para la mayoría o todas sus cuentas de distintos servicios, lo que es inaceptable en la seguridad de la información, esto hace que los datos en cuestión sean totalmente vulnerables en cualquier momento.

Un análisis de los tipos de claves que son inseguros, los han clasificado de la siguiente manera:

- **Numéricos**: Generalmente del 1 al 10000000, por ejemplo 18528287, 20398476, 00000000, todas las combinaciones posibles. Muchas personas utilizan este tipo de contraseña ya que puede pertenecer a su número de identificación, número de teléfono de casa o celular o simplemente porque es su número de la suerte. Lo que no saben es lo FACIL que es romper este tipo de contraseña. Si pensamos en 10 millones de posibilidades (como mínimo), seguramente obtendremos la contraseña en 6 o 7 días.
- **Nombre + número**: Con este tipo, se refiere al tipo de contraseña como 'fernando2008', es decir, nombre, apellido, nick + fecha de nacimiento, edad o algún número que lo identifique. La mayoría de los nombres y apellidos están en diccionarios de datos y los números son fáciles de generar y no complicarían mucho el querer romper la contraseña. Este tipo de contraseña es una de las más fáciles e incluyen claves como: 123nombre456, qwertynombre, nombre123, nombre2009, nombre1975, etc.
- **Nombre**: Aunque parezca absurdo e increíble, es la realidad. Si, existen personas que utilizan su nombre como contraseña de una o más de sus cuentas, y si, lo hace con minúscula.
- **Palabra**: Al igual que el anterior, aunque parezca increíble, existen personas que usan una palabra común y corriente como clave, como pájaro, computador, celular, system, etc., palabras que están en cualquier diccionario de palabras y que son fácilmente crackeables.

Estos tipos de claves son fáciles de romper vía fuerza bruta ya sea con repetidos intentos de login en un sistema inseguro (por ejm. Un sistema sin captcha) y son sencillos de encontrar su hash correspondientes ya sea de sha, md5 u otro.

Las entidades encargadas de la creación de claves para sus usuarios, ya sea de una intranet, un sistema bancario, etc., deben ser más responsables con el tema de asignación de claves por defecto, ya que en algunos casos la que entregan es el nombre más el año actual o bien algo más sencillo como 123456, o el número de cédula de identidad o fecha de nacimiento.

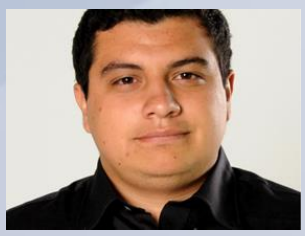
Las claves por defecto DEBEN ser aleatorias y no arriesgarse a que algún intruso ingrese donde no deba.

En este contexto, **SCProgress** cuenta con personal altamente calificado para asesorar y colaborar con las empresas para afrontar las amenazas existentes, a través de hardware y software del más alto nivel, y con ello entregar una solución global en seguridad de la información. Para mayor información, visite la página web www.scprogress.com o solicite una demostración al correo electrónico: ventas@scprogress.com.

FUENTES: http://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/
http://www.fundamedios.org/wp-content/uploads/2016/09/proyecto-ley-de-datos.pdf
https://blog.zerial.org/seguridad/la-importancia-de-la-seguridad-en-la-informacion/

Capacitación en Ciberseguridad y Antimalware

Arturo de la Torre
Asesor de TIC´s SCProgress



Marco de la Torre
Gerente Técnico SCProgress

Consuelo de la Torre
Capacitadora SCProgress

"La necesidad de capacitación surge por la diferencia entre lo que uno debería saber y lo que sabe realmente"

El personal responsable de las áreas de sistemas, así como los usuarios, deben conocer sobre la infinidad de ataques informáticos amenazas, ataques a la información y a las infraestructuras tecnológicas, los mantienen como áreas vulnerables permanentes, facilitando las actividades fraudulentas de hackers, quienes han visto como un gran negocio lucrativo, la sustracción de datos, ya sea personal, financiera, confidencial, etc.

La capacitación en seguridad informática, se vuelve relevante e importante para evitar que las empresas e instituciones, se vean afectadas ante este tipo de amenazas.

SCProgress cuenta con asesores altamente especializados a nivel internacional, lo que nos permite brindar cursos de capacitación en diversos temas tecnológicos, especialmente en el área de seguridad informática, su amplia experiencia y conocimientos, les ha permitido participar en eventos nacionales e internacionales como la conferencia organizada por la CEPOL Research & Science Conference (Organismo acreditado de la Unión Europea), realizada en Budapest el año 2016.

En esta ocasión SCProgress, consiente de la importancia que prestan las instituciones a la seguridad de la información, y ante el incontrolable crecimiento de las amenazas, ha organizado y pone a disposición de sus lectores y clientes, capacitación en los siguientes temas:

Certificación en Ciberseguridad de la RED	Introducción al análisis y comportamiento del malware
Contenido: • Fundamentos de red de computadoras y defensa • Amenazas, vulnerabilidades y ataques a la red • Controles, protocolos y equipos para la seguridad de la red Diseño e implementación de políticas de	**Contenido:** • Análisis de malware • Indicadores de infección • Malware signatures • Categorías de malware • Mass vs Targeted malware

seguridad en la red • Seguridades físicas • Seguridades en los Host • Configuración y administración segura de Firewalls • Configuración y administración segura de IDS • Configuración y administración segura de VPNs • Protección de redes inalámbricas • Monitoreo y análisis del tráfico de la red • Gestión de riesgos y vulnerabilidades • Data backup y recuperación de datos • Respuesta y manejo de incidentes	• Metodología de análisis de malware • Herramientas Antimalware • Malware empaquetado y oculto • DLL Hijacking • Magic labels • Formatos de archivos • Dynamic Link Libraries • Detección de virtualización de malware • Dependency Tracing • Modificación de registros • Manipulación de archivos del sistema • Análisis de tráfico de la red • Sandboxes

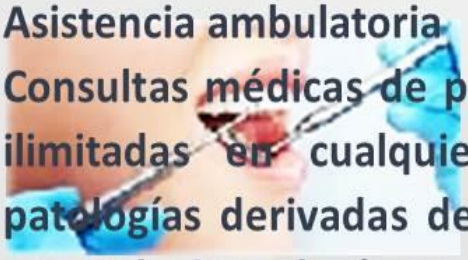
Los cursos se dictan en las instalaciones de SCProgress ubicadas en el edificio Plaza de Vizcaya, tercer piso, en La Pradera E7-21 y Mariana de Jesús,

Para mayor información visite nuestra página web: www.scprogress.com, o comuníquese directamente al correo electrónico: **ventas@scpgrogress.com**.

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- Créditos sin garante hasta 3.000 dólares.
- Otorgamos créditos para consumo, emprendedores y microempresarios.
- Las tasas de interés más bajas del mercado.
- Inversiones a plazo fijo.
- Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.



- Asistencia ambulatoria
- Consultas médicas de primer nivel ilimitadas en cualquiera de las patologías derivadas de: medicina general, ginecología y pediatría.
- Cobertura en asistencia dental.
- Examen clínico y diagnóstico.
- Higiene dental, alivio del dolor.
- Rayos X periapical, profilaxis (Limpieza dental profunda).
- Restauraciones en resina simple.
- Extracciones simples.

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204

www.cooprumi.fin.ec

Tu huella digital y la privacidad de tus datos.

Tu huella digital te pinta como persona.
Asegúrate de que esta descripción sea precisa.

Lo deseemos o no, todos los días la mayor parte de las personas contribuimos a crear un retrato creciente de quiénes somos en línea – un retrato que probablemente sea más público de lo que suponemos.

Este retrato ayuda a las empresas a orientar los contenidos hacia mercados y consumidores específicos, apoya a los empleadores a analizar nuestros antecedentes, así como, a los anunciantes, a seguir nuestros movimientos a través de múltiples sitios web. Sin importar lo que hagamos en línea, es muy posible que estemos dejando atrás nuestras huellas digitales.

Es por ello que, sin importar qué realicemos en línea, es importante saber qué tipo de rastro estamos dejando y cuáles son los potenciales efectos.

Si bien es imposible que nuestra huella sea nula, los primeros pasos para reducir nuestra huella digital y gestionar nuestra identidad digital no son muy difíciles.

A continuación presentamos algunas cosas que pueden ser de mucha ayuda para evitar dejar rastro de nuestra huella digital.

¿Qué es una huella digital?

Nuestra huella digital está formada por los rastros que dejamos al utilizar Internet. Comentarios en redes sociales, llamadas de Skype, el uso de aplicaciones, registros de correo electrónico, todo esto forma parte de nuestro historial en línea y, potencialmente, puede ser visto por otras personas o almacenado en una base de datos.

¿Cómo dejamos nuestras huellas digitales?

Estamos acostumbrados a mirar todo tipo de información en Internet, pero, aparentemente, Internet también nos está mirando. Cada vez que visitamos un sitio web para buscar información, cada vez que

compartimos algo en las redes sociales o enviamos un mensaje instantáneo o correo electrónico, vamos dejando algo de nosotros. Nuestras huellas digitales son los rastros que dejamos al utilizar Internet.

Las huellas digitales tienen tanto costos como beneficios. Por ejemplo, pueden ofrecer comodidad al ahorrarnos tiempo cuando iniciamos una sesión o al no tener que volver a ingresar nuestros detalles personales.

La mayoría nos damos cuenta de que al compartir conscientemente información o subir fotografías a las redes sociales estamos perdiendo algo de privacidad. Pero es probable que pensemos menos en las huellas que creamos por defecto, simplemente por utilizar un buscador, realizar compras en línea o habilitar los servicios de localización. Como dice el refrán: "*ojos que no ven, corazón que no siente*". Es difícil gestionar algo que nunca hemos visto.

Algunas formas en que dejamos nuestra huella digital:

- **Sitios web y compras en línea.-** A menudo las tiendas minoristas y sitios de reseña de productos dejan en nuestro sistema cookies que pueden seguir nuestro recorrido de un sitio a otro, permitiendo la entrega de anuncios dirigidos que nos muestran productos sobre los cuales hemos estado leyendo o que hemos buscado recientemente.

- **Redes sociales.-** Todos esos +1, retweets y comentarios en Facebook (incluso los privados) dejan un registro. Es importante conocer cuáles son las configuraciones de privacidad por defecto de nuestras cuentas en las redes sociales y estar atentos a las mismas. Muchas veces los sitios introducen nuevas políticas y configuraciones que aumentan la visibilidad de nuestros datos. Puede que confíen en que el usuario simplemente hará clic y aceptará todos los términos que están introduciendo, sin siquiera leerlos.

- **Teléfonos móviles, tablets o computadoras portátiles.-** Algunos sitios web generan un listado de los diferentes dispositivos que utilizamos para acceder a los mismos. Aunque muchas veces esto se utiliza como una forma de ayudarnos a proteger nuestras cuentas, es importante comprender qué información recogen sobre nuestros hábitos.

Administrar nuestra huella digital:

No nos equivoquemos: cada vez que utilizamos la red, Internet está escuchando. Es importante comprender qué estamos dejando atrás cada vez que visitamos un sitio web.

Gestionar nuestra huella digital no es tarea fácil, para ello se requiere: pensamiento, tiempo y esfuerzo.

Debemos autoeducarnos contra nuestra propia inercia ante las configuraciones por defecto que son cómodas pero socaban nuestra privacidad y contra los esfuerzos coordinados y persistentes de diferentes organizaciones que tienen un interés económico e intentan persuadirnos de sacrificar nuestra privacidad en su propio beneficio.

Existen cuatro niveles que permiten gestionar nuestras huellas:

- **Mejorar nuestra comprensión de los problemas**.- Piense en las implicancias que tiene el hecho de que todo lo que compartimos en Internet, en mayor o menor grado pone en riesgo nuestra privacidad.

- **Desarrollar hábitos de higiene básica**.- La privacidad es contextual, utilizar diferentes personas para los diferentes aspectos de nuestra vida en línea, ya sea utilizar una dirección de correo electrónico para nuestro trabajo y otra para los asuntos personales, utilizando una tarjeta de crédito para compras en línea y otra para todo lo demás, ayuda a mantener separadas y en diferentes partes nuestra huella digital. Tenga cuidado con lo que comparte a través de las redes sociales y en otros sitios, probablemente esta información sea más publica de lo que piensa.

- **Convertirnos en usuarios sofisticados de las herramientas y servicios en línea**.- Vale la pena tomarse el tiempo necesario para investigar y verificar las configuraciones por defecto de los navegadores, para estar seguros que estamos cómodos con las mismas, cuando una aplicación solicita permiso para enviar notificaciones automáticas y utilizar sus datos de ubicación, tómese un momento para pensar si esto es lo que desea realmente, las cámaras y teléfonos inteligentes generalmente registran la fecha, hora y ubicación en cada fotografía, al compartir estas fotos, a menos que se bloquee específicamente, es posible que estamos publicando esta información.

- **Encontrar y utilizar herramientas específicas para mejorar nuestra privacidad**.- Existen muchas herramientas para mejorar la privacidad especialmente para los navegadores, estas herramientas se pueden utilizar no solo para proteger áreas específicas de nuestra huella digital, sino también para mantenernos al tanto y comprender que es lo que están buscando los proveedores de servicios

Avira Pro permite que navegue con total confianza, bloqueando sitios web maliciosos, descargas ocultas e intentos de secuestro del navegador web, además evita los ataques de suplantación de identidad a través de redes sociales y correo electrónico.

La seguridad avanzada de Avira Pro ha obtenido las mejores puntuaciones de la industria en detección, usabilidad, autodefensa, reparación y bajo impacto sobre el equipo.

Para obtener mayor información sobre Avira Antivirus Pro, visite el sitio web **www.scprogress.com**, o solicite una demostración directamente al **correo electrónico: avira@scprogress.com**.

FUENTE: https://www.internetsociety.org/es/tu-huella-digital

Rincón de los expertos

La privacidad en Internet se pude definir como la privacidad personal de las transacciones en Internet o en la transmisión de datos. El término cubre también, el control individual sobre el tipo y volumen de información personal que se comparte en la red y las personas a quienes esta información se comparte.

La lectura más recomendada sobre este tema, la podemos encontrar en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Privacidad_y_Seguridad_en_Internet.pdf

"El problema no es la tecnología, sino el mal uso que otro ser humano le pueda dar"

— Jeff Jarvis —

Noticias

Descubierta una vulnerabilidad en Linux que estaba presente desde hace 12 años

Se ha descubierto recientemente en Linux otra escalada de privilegios, un tipo de vulnerabilidad muy común en el sistema Open Source, aunque este tiene la particularidad de llevar presente desde hace 12 años.

La escalada de privilegios, cuyo código es CVE-2017-6074, fue descubierta por el investigador en seguridad Andrey Konovalov mientras examinaba el Protocolo de Control de Congestión de Datagramas (DCCP/Datagram Congestion Control Protocol) utilizando Syzkaller, una herramienta de fuzzing liberada por Google.

La vulnerabilidad que provoca la escalada de privilegios es del tipo “usar después de liberar”, siendo el origen la manera en que la implementación del protocolo DCCP del kernel Linux libera recursos de SKB (buffer de socket) para un paquete DCCP_PKT_REQUEST cuando la opción IPV6_RECVPKTINFO está establecida en el socket.

Esta vulnerabilidad en DCCP podría permitir a un usuario sin privilegios alterar la memoria del kernel de Linux, permitiéndole causar un cuelgue en el sistema o escalar privilegios hasta conseguir acceder como administrador.

Por su parte, DCCP es una capa de protocolo de transporte orientada a mensajes que minimiza la superposición del tamaño de una cabecera de un paquete o un procesamiento de nodo final tanto como sea posible, proporcionando el establecimiento, mantenimiento y desmontaje de un flujo de paquetes no confiable, además del control de la congestión de ese flujo de paquetes.

La vulnerabilidad no ofrece ninguna manera para que alguien de fuera pueda acceder al sistema afectado, esto quiere decir que no puede ser explotada de forma remota y que el atacante necesita tener acceso de forma local.

La vulnerabilidad ya ha sido parcheada por los mantenedores del kernel Linux, así que los usuarios más avanzados pueden aplicar el parche directamente o bien esperar a que los mantenedores de la distribución en uso lo suministren a través de una actualización estándar.

Fuente: http://muyseguridad.net/2017/02/24/vulnerabilidad-linux-12-anos/

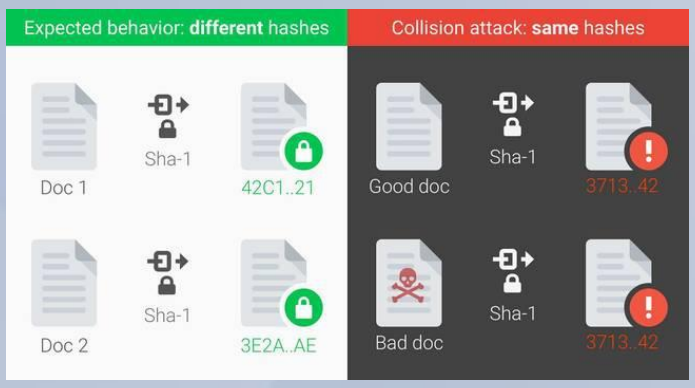
Google ha roto definitivamente el hash criptográfico sha1

SHA1 es un algoritmo criptográfico de hash creado en 1995 y que, durante mucho tiempo, ha sido utilizado ampliamente para asegurar datos, comprobar su integridad y para garantizar la seguridad de las conexiones a Internet. Sin embargo, la tecnología ha cambiado mucho en los últimos años, por lo tanto, este algoritmo ha sido cada vez menos seguro hasta el punto de conseguir la primera colisión de Hash, demostrando así que este está ya totalmente roto.

No es la primera vez que se dice que **el algoritmo SHA1 es inseguro y está roto**. A finales de 2015 ya pudimos ver cómo se habían encontrado varias debilidades en el mismo que, en la teoría, podía ser roto, aunque para poder demostrarlo se necesitaría un sistema de más de 100.000 dólares y varios años de computación. Ahora, Google lo ha roto en la práctica.

Desde este anuncio de 2015 hasta ahora las cosas han cambiado y, tal como nos informan los compañeros de AdslZone**,** Google ha hecho pública la primera colisión en el Hash SHA1, demostrando así la ineficacia del antiguo algoritmo así como su nula seguridad. Cuando calculamos la suma de Hash de un fichero conseguimos una serie de caracteres hexadecimales que, en teoría, debería ser única. Gracias a esto podemos saber si un archivo que originalmente tenía un Hash "abc", tras enviarlo por Internet, el destinatario consigue la misma suma "abc" y no una suma diferente que podía indicar que el archivo ha sido modificado en un punto intermedio de la transferencia e incluso que se ha descargado mal.

Lo que ha hecho Google ha sido conseguir que dos archivos diferentes tengan el mismo Hash, demostrando así que es posible una colisión y que este algoritmo está ya, oficialmente, roto.



De todas formas, el proceso no ha sido fácil, ha requerido de 9.223.372.036.854.775.808 de ciclos. Mientras que romper este algoritmo por fuerza bruta llevaría más de un año utilizando 12 millones de tarjetas gráficas trabajando a la vez. Ccon la nueva técnica "solo" han sido necesarias 110 tarjetas gráficas trabajando durante un año para llegar al resultado.

En el caso de los algoritmos MD5, la cosa es mucho más sencilla, y es que estos pueden romperse en tan solo 30 segundos utilizando un simple smartphone.

Por suerte, aunque Google acaba de demostrar la ineficacia de este algoritmo y dejarlo completamente roto, hoy en día prácticamente no se utiliza para nada, ya que existen varias revisiones como SHA2 y SHA3 totalmente seguras. Además, a finales del año pasado, los navegadores web han empezado a bloquear estos algoritmos por defecto, así como muchas páginas web, como Facebook, que incluso los han eliminado de sus servidores al ser ya totalmente inútiles, además de inseguros.

Las grandes empresas de Internet como Google y Microsoft trabajan a diario en hacer las conexiones más seguras, por lo que, poco a poco, todo va cambiando hacia protocolos y algoritmos más seguros, siendo uno de los predilectos hoy en día SHA256**.**

Fuente: https://www.redeszone.net/

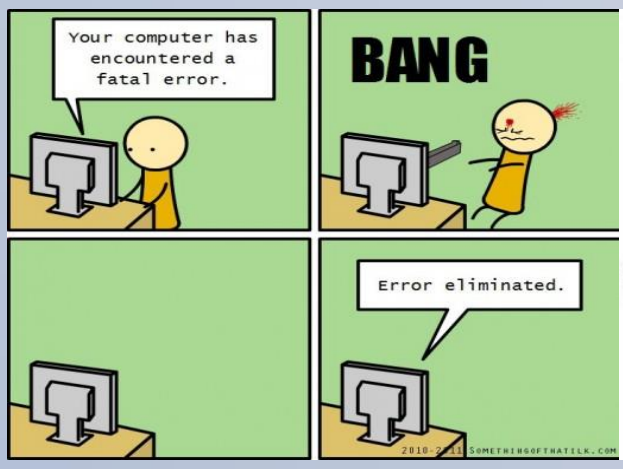
SCProgress brinda cursos de capacitación en diversas áreas tecnológicas enfocadas en las TICs. Nuestra amplia experiencia y la de nuestros técnicos, tanto a nivel nacional como internacional, nos da las competencias necesarias para brindar una formación completamente certificada en las siguientes áreas:

- Ciberseguridad
- Seguridad perimetral de la red
- Seguridad endpoint
- Zimbra - Correo electrónico y listas de difusión
- Comercio electrónico/E-business
- Criptografía
- Análisis forense de datos en la red

Humor


Deberías leer tus mails más a menudo. Hace tres semanas que te despedí.
paisdelocos.com


zeebarf00
"OK, TU PADRE CONSIGUIO EL RATON. ¿AHORA COMO LO USAMOS?"


Your computer has encountered a fatal error.
BANG
Error eliminated.


CONOCÍ A MI NOVIO POR INTERNET!!
NO ME DIGAS! Y ESTO?!
ME ENTRÓ UN VIRUS.


Creo que ha habido un pequeño eror informático al establecer las coordenadas

¿Qué dinámicas operan en el mundo de las huellas digitales?

"Espero que usemos la red para atravesar barreras y conectar culturas"
- Tim Berners-Lee -

El mundo virtual ha penetrado tanto nuestras vidas que muchas veces es difícil desenmarañar las dinámicas que determinan su comportamiento. No obstante, hay tres temas que se destacan del resto: la dinámica cultural, la dinámica económica y la dinámica de la comodidad.

Aunque se pueda acceder a los mismos desde cualquier lugar del mundo, todos los servicios en línea deben originarse en algún sitio, esto muchas veces les infunde una perspectiva cultural particular. Cada país trae a Internet sus propias normas culturales, sus propios modelos jurídicos y regulatorios, y sus propios marcos económicos. Como recurso global, Internet se ha convertido en un fascinante estudio de contrastes.

Las huellas digitales, que tocan los temas de la privacidad personal, el intercambio de datos, el control por parte del usuario final y el anonimato, produce diferentes reacciones en los diferentes grupos que forman parte de Internet. Lo que es aceptable y habitual para un grupo, muchas veces es inaceptable e inusual para otro. Esto forma parte de la naturaleza de Internet.

Para algunos, la respuesta parece sencilla: si no le gusta el modelo de un determinado servicio en Internet, escoja un servicio alternativo. Los usuarios finales pueden votar con sus clics, evitando los servicios que no satisfacen sus expectativas.

Sin embargo, este consejo solo funciona si se cumplen dos condiciones:

- Primero, los usuarios de Internet deben ser conscientes de las implicancias de la privacidad y de la protección de los datos en todos los servicios que utilizan; y,
- Segundo, realmente se debe poder escoger entre una variedad de servicios.

Nuestra experiencia colectiva indica que estas dos condiciones no siempre se cumplen. No todos los usuarios de Internet saben cómo cada servicio comparte su información, no todos los servicios se pueden reemplazar por otro, y algunas veces las alternativas presentan los mismos inconvenientes.

Incluso los usuarios de Internet que controlan activamente sus huellas digitales no tienen más opción que confiar en un conocimiento imperfecto. Algunas veces es un resultado directo de las opciones del proveedor del servicio. Por ejemplo, a una red social le conviene alentar a sus usuarios para que ignoren el hecho de que todo lo que hacen dentro de su círculo social es inspeccionado y monetizado por un tercero.

La dinámica económica incentiva fuertemente a los proveedores de servicios para que recopilen datos y no les proporcionen a los usuarios toda la información sobre este aspecto de los mismos.

Y aunque Internet es increíblemente diversa, no siempre hay una variedad de servicios disponibles. En algunas áreas como las redes sociales, incluso si hay otros servicios alternativos disponibles, puede que estos otros servicios no sean atractivos. Por ejemplo, una red social no tendrá ningún atractivo si ninguno de nuestros amigos la utiliza.

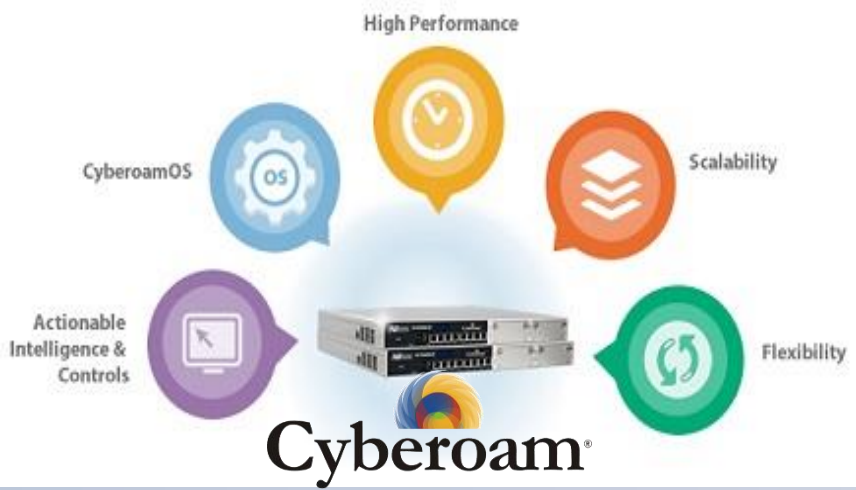
Por último, está la dinámica de la comodidad. La mayoría de las personas preferimos usar algo que sea cómodo aunque erosione un poco la privacidad, antes que un producto que nos haga la vida más difícil.

Nuestra preferencia por la opción más “cómoda” se refuerza si no vemos ninguna prueba de que nuestra privacidad está siendo socavada. Al igual que muchas otras conductas humanas (fumar, comer comidas excesivamente grasas, una mala postura), si nuestras acciones no producen un daño visible de inmediato, tendemos a pensar que estas acciones son inofensivas. La combinación de la comodidad y la falta de daño aparente nos atraen hacia hábitos que socavan la privacidad. Al igual que lo que ocurre con cualquier otro hábito, las posibilidades de modificar nuestra conducta dependen del valor que le asignemos a nuestra privacidad con relación a las alternativas más “cómodas”.

No existe ninguna respuesta sencilla. El primer paso consiste en reconocer los diferentes modelos culturales involucrados, y comprender que los usuarios de Internet llegan a la mesa con diferentes antecedentes, expectativas y valores. Una discusión abierta entre todos los actores relevantes puede ayudar a educar sobre estos temas tanto a los usuarios finales como a los proveedores de servicios. No obstante, en última instancia, depende de nosotros como individuos el ser claros sobre nuestras elecciones, sobre los valores que estas elecciones representan, y sobre los resultados a los cuales nos enfrentaremos como resultado de las mismas.

FUENTE: https://www.internetsociety.org/sites/default/files/Digital_footprints_March%2028_SPANISH.pdf
http://www.slideboom.com/presentations/1598159/Huella-Digital---Eder-Gonzalez%C2%BFQu%C3%A9-din%C3%A1micas-operan-en-el-mundo-de-las-huellas-digitales_
https://issuu.com/marifer61/docs/huella_digital____que___dina__micas
https://www.reference.com/technology/digital-footprint-mean-555fde8e55b9adab

El mejor sistema de seguridad perimetral para Internet



La mayor parte de los ataques a las infraestructuras tecnológicas de las empresas, se realiza a través de Internet, por lo que es necesario que los administradores de las redes, tomen las precauciones necesarias para protegerse contra los ataques de red a nivel de aplicación, asegurando a las organizaciones contra intentos de intrusión, malware, troyanos, ataques DoS y DDoS, transmisión de código malicioso, actividades de backdoor y amenazas combinadas.

Cyberoam cuenta con el Sistema de Prevención de Intrusos basado en firmas, cuenta con miles de firmas actualizadas de forma automática, lo que permite protegerle contra las últimas vulnerabilidades. Soporta múltiples protocolos: HTTP, FTP, SMTP, POP3, IMAP, P2P, IM support. Automáticamente detecta/bloquea tráfico sospechoso, previene violaciones a la seguridad de la red y ataques provenientes de la capa humana y de aplicaciones.

Cyberoam NGFW ofrece inspección y control de aplicaciones en línea, filtrado Web, inspección HTTPS, sistema de prevención de intrusos, VPN (IPSec y SSL) y controles de ancho de banda granulares. También se encuentran disponibles características adicionales, tales como: WAF, puertos expandibles (FleXi), Antivirus y Antispam perimetrales.

Los dispositivos de seguridad de Cyberoam ofrecen un alto rendimiento, seguridad, conectividad, productividad y una arquitectura de seguridad extensible (ESA) para la seguridad en las empresas preparadas para el futuro.

La serie NG de Cyberoam ofrece seguridad compatible con requerimientos futuros para las PYMEs mediante sus características de seguridad grado empresarial, puertos gigabit y los mejores rendimientos de la industria para este segmento. Los equipos de la serie NG cuenta con el mejor hardware de su clase, así como un software igualmente de primer nivel, para ofrecer hasta 5 más veces los rendimientos promedio de la industria.

Recuerde que la productividad y crecimiento de su negocio, depende principalmente de la seguridad de su infraestructura tecnológica. **SCProgress** cuenta con la mejor tecnología y personal especializado en seguridad informática. **Solicite una demostración al correo electrónico:** ventas@scprogress.com.

SCProgress cuenta con todo lo que necesita para su infraestructura de cableado estructurado

Los sistemas de cableado estructurado constituyen una plataforma universal para la transmisión de voz, datos y video, el diseño e implementación de infraestructuras de fibra óptica y cableados que cumplan con los estándares se vuelven cada vez más imprescindible para el éxito de sus empresas.

SCProgress brinda el mejor servicio en:

- Diseño e instalación de sistemas de cableado estructurado con las mejores marcas.
- Certificación de sistemas de cableado estructurado
- Diseño e instalación de fibra óptica.
- Asesoría técnica para la implementación de sistemas de cableado estructurado.
- Personal altamente calificado, certificado y con amplia experiencia.

En caso de requerimiento del cliente, nuestro personal cuenta con experiencia en marcas como Panduit, Dexon, así como marcas nacionales.

Para más información no dude en contactarnos en ventas@scprogress.com

GESRICA
COMPAÑÍA DE GESTIÓN DE RIESGO Y CAPACITACIÓN S.A.

Nuestro país se encuentra ubicado sobre el cinturón de fuego del pacífico, por lo que nos encontramos expuestos a eventos naturales que pueden afectar nuestras actividades, razón por la cual, debemos tomar acciones y ejecutar procedimientos para mitigar posibles siniestros, ya sean causados por la fuerza de la naturaleza o por accidentes humanos.

Contamos con personal especializado en la gestión, planificación, capacitación e implementación de estrategias para la reducción de riesgos y ponemos a su disposición , asesoramiento en la elaboración de planes de gestión de riesgos, diseñados exclusivamente para las características de su empresa, así como, capacitación en áreas a fines, principalmente en:

- ***Primeros auxilios.***
- ***Brigadas de emergencia.***
- ***Prevención de incendios***
- ***Seguridad industrial.***
- ***Normas de seguridad.***
- ***Prevención y manejo de emergencias y evacuaciones.***

www.gesrica.com
E-mail: info@gesrica.com
Teléfonos: 0984489267 - 0996620889 – 0979003123
Dirección: 18 de Septiembre 07-04-009 y Panamericana Norte.

www.scprogress.com

Marzo 2017