Conceptos básicos de cifrado para programas Atención a las personas sobrevivientes de la violencia de género

El cifrado ayuda a proteger la información del acceso indeseado o sin autorización. Las opciones de cifrado están disponibles en la mayoría de los dispositivos inteligentes y las plataformas en línea.

Siempre que sea posible, los programas de servicios para víctimas deben utilizar el cifrado para proteger los datos, las comunicaciones y los sitios web. Las personas sobrevivientes también pueden utilizarlo para ayudar a proteger sus dispositivos y comunicaciones. Este manual proporcionará una visión general de lo que es el cifrado y la manera en la que puede ser utilizado por las personas sobrevivientes y proveedores de servicios para víctimas con el objetivo de proteger información confidencial.

¿Qué es el cifrado?

El cifrado protege los datos para que únicamente las personas autorizadas puedan tener acceso a ellos. En términos sencillos, el cifrado codifica los datos de tal manera que solo las personas que tienen la contraseña electrónica correspondiente pueden descifrarlos. El contenido original podría ser un mensaje u otra información que su computadora está enviando a través de Internet. Para leer contenido cifrado, alguien debe proporcionar una clave de descifrado para demostrar que la persona está autorizada para ver el contenido. Esta clave puede ser una contraseña o presentarse de alguna otra manera. Todo esto es sencillo para la persona usuaria; no es necesario entender cómo funciona la tecnología para utilizar el cifrado. Si ha enviado un mensaje de WhatsApp o ha utilizado una aplicación de banca móvil, usted ya ha utilizado el cifrado.

Existen distintos tipos de cifrado para diferentes necesidades. Algunos protegen la información almacenada en la computadora, otros protegen la información que

circula entre distintos equipos. Si un producto o servicio dice que "está cifrado", es posible que aun así no se esté utilizando el tipo de cifrado adecuado para satisfacer sus necesidades.

¿Por qué es importante el cifrado para los programas?

El cifrado es importante para la confidencialidad. Almacenar información personal no cifrada sobre las personas sobrevivientes supone un riesgo. Lo mismo ocurre con el envío de mensajes no cifrados con información personal de las personas sobrevivientes. En ambos casos, personas ajenas a la organización podrían obtener esa información. El cifrado no impide todas las fugas de información de las personas sobrevivientes. Sin embargo, es necesario para reducir el riesgo.

¿Por qué es importante el cifrado para las personas sobrevivientes?

Comunicaciones seguras

El cifrado permite a las personas sobrevivientes usar la tecnología de manera estratégica y segura. Las personas sobrevivientes pueden usar la tecnología para hacer planes, almacenar y enviar evidencia y buscar ayuda. Para realizar este tipo de cosas de manera segura, las personas sobrevivientes deben evitar que sus comunicaciones no sean vulneradas o que alguien las espíe. Esto significa que necesitan acceso a canales de comunicación en línea fiables. Necesitan acceder a herramientas que proporcionen cifrado para, entre otras cosas, el almacenamiento de archivos, el envío de correo electrónico y la conexión a Wi-Fi. Es importante señalar que, aunque el cifrado puede ofrecer una seguridad importante, no es una solución absoluta para las personas sobrevivientes que buscan comunicaciones seguras. Por ejemplo, no impide que una persona agresora obligue a una persona sobreviviente para que le dé una contraseña o que utilice programas de software de vigilancia *(stalkerware)* en su dispositivo. Tampoco les impide a estas personas, verificar de qué manera la persona sobreviviente utiliza el dispositivo, si ya tienen acceso físico a éste y si ha iniciado

sesión. El cifrado puede ser una de las muchas herramientas útiles de seguridad tecnológica para la persona sobreviviente.

Protección frente a la fuga de datos

Una fuga de datos se produce cuando alguien accede a información privada sin autorización. Casi todas las personas, incluidas las personas sobrevivientes, nos hemos visto afectadas por una fuga de datos en algún momento. Las fugas son comunes y crean muchos riesgos para las personas sobrevivientes. Una persona que acecha o agrede podría encontrar esta información en línea o comprarla a un intermediario de datos para localizar a alguien. Esa persona o cualquier otra podrían utilizar la información delicada para robar la identidad de la persona sobreviviente. En el caso de una fuga en la que los datos estén cifrados, la persona no autorizada seguirá sin poder leer o acceder a la información si no tiene las claves para descifrarla. El cifrado es una herramienta fundamental para ayudar a mitigar los daños que pueden causar las fugas de información.

¿Cómo deben utilizar el cifrado las personas proveedoras de servicios?

Los requisitos de confidencialidad de los programas de servicios a las víctimas son estrictos. Los programas solamente pueden compartir la información de identificación personal (IIP) de una persona sobreviviente mediante instrucciones escritas, documentadas y por un tiempo limitado otorgado por la persona sobreviviente. Debido a que la IIP de la persona sobreviviente puede filtrarse a través de intercepciones o fugas de datos basadas en la tecnología, los programas necesitan contar con algunas precauciones también basadas en la tecnología. Al elegir e implementar tecnología, los programas deben buscar las opciones más seguras. En nuestro artículo, Seleccionando una base de datos, se explica cómo se aplica lo anterior a la selección de bases de datos. Las siguientes son las mejores medidas de cifrado:

Cifrado del lado del cliente, de conocimiento cero y sin conocimiento

Una práctica recomendada en materia de confidencialidad, consiste en almacenar la información de identificación personal de las personas sobrevivientes en una base de datos o en un sistema de intercambio de archivos con una forma de cifrado denominada cifrado del lado del cliente, de conocimiento cero o sin conocimiento. Estos términos se refieren al cifrado que está diseñado para que nadie, excepto las personas autorizadas (es decir, las personas de su organización), puedan acceder a la información, incluyendo a la empresa de tecnología que proporciona el servicio si está vinculado a la nube. Esto evita varios de los siguientes riesgos:

- Personas agresoras o que acechan (o sus amistades) que trabajan o están contratadas por una empresa tecnológica y que hacen uso indebido al acceder a los recursos de la empresa para obtener datos de las personas sobrevivientes.
- Los datos personales de las personas sobrevivientes que aparecen públicamente en Internet debido a que los servidores de la empresa fueron jaqueados y los datos publicados en Internet.
- La empresa de tecnología comparte la información de la base de datos de la persona sobreviviente con las fuerzas del orden u otras agencias gubernamentales, sin el consentimiento de la persona sobreviviente. Esta puede ser la decisión de la empresa tecnológica o su respuesta a un proceso legal, como una orden judicial válida.

Si una empresa de base de datos utiliza el cifrado, pero también tiene la clave de descifrado para sus datos, eso se denomina *cifrado del lado del servicio o del lado del servidor*. Esto significa que la empresa puede seguir accediendo a los datos. Podrían proporcionárselos a un tribunal o a las fuerzas del orden sin el consentimiento de la persona sobreviviente si así se les ordenara hacerlo. La ley federal exige que las personas beneficiarias tomen medidas razonables para evitar la divulgación involuntaria. La mejor manera para cumplir este requisito es utilizar un sistema en el que solamente su organización pueda acceder a los datos

almacenados de las personas sobrevivientes. El cifrado del lado del servidor es el predeterminado en la mayoría de los servicios. A menos que un proveedor afirme que un producto o servicio ofrece cifrado del lado del cliente o conocimiento cero, es probable que el proveedor pueda acceder a sus datos. Es posible que los proveedores no estén familiarizados con las necesidades de confidencialidad de los proveedores de servicios a las víctimas, ya que suelen ser más estrictas que las de otros sectores. Cuando almacene información de identificación personal de las personas sobrevivientes usando la tecnología, debe optar por un cifrado del lado del cliente y preguntar específicamente al proveedor al respecto.

Cifrado de extremo a extremo

Otro término que puede escuchar es el cifrado de extremo a extremo (E2EE). En E2EE, los datos se cifran en cada paso de su transmisión. Por ejemplo, si envía un mensaje en una aplicación de mensajería cifrada que tiene E2EE, la aplicación cifra el mensaje mientras aún está en su dispositivo. Permanece cifrado en su trayectoria a los servidores de la empresa tecnológica, a medida que pasa a través de los servidores y en su camino al dispositivo del destinatario. A continuación, la aplicación en el dispositivo del destinatario puede descifrarlo. Imagínelo como en un túnel protegido. E2EE protege los datos cuando están *en movimiento* (por ejemplo, entre un dispositivo emisor y otro receptor). El cifrado del lado del cliente o cualquier cifrado que solamente se aplique a los datos "en reposo" limita la protección a los datos cuando están en los servidores de un proveedor de la nube, no mientras están en tránsito.

E2EE y el cifrado del lado del cliente no compiten entre sí. Sirven para diferentes propósitos, y usted debe buscar soluciones que incluyan ambas características.

HTTPS y su sitio web

Al navegar por Internet, probablemente haya notado la presencia de las siglas "http" o "https" al principio de las direcciones de los sitios web (URL). "HTTP" es el acrónimo de Hypertext Transfer Protocol *(Protocolo de transferencia de hipertexto)*. Un "protocolo" es un conjunto de instrucciones comunes y consensuadas, y el protocolo HTTP se utiliza para estructurar la comunicación en red en la World Wide Web *(Red informática mundial)*. HTTPS es una variante segura de HTTP. A diferencia de HTTP, encripta el tráfico de Internet. HTTPS se utiliza ahora de forma predeterminada en la mayoría de los sitios web.

El cifrado con HTTPS es importante para la confidencialidad y privacidad de las personas sobrevivientes o de cualquier otra persona (incluyéndole a usted) que visite el sitio web de su organización. Puede obtener más detalles sobre este tema, y sobre cómo funciona HTTPS, en nuestro artículo de Seguridad y Privacidad Wi-Fi. Si su sitio web no utiliza HTTPS, cualquier persona podría redirigir el navegador de un visitante desde el sitio web hacia su propio dispositivo. La persona cuyo navegador es redireccionado ni siquiera se enteraría. El HTTPS es muy importante para la seguridad web y las organizaciones de servicios a las víctimas deberían utilizarlo en sus sitios web. La mayoría de los navegadores muestran una alerta de seguridad cuando un usuario intenta visitar un sitio que no admite HTTPS, y algunos navegadores reducen la clasificación de la búsqueda de dichos sitios; ya que de este modo las personas sobrevivientes tendrán menor probabilidad de encontrar ese sitio a través de las búsquedas.

Puede comprobar si su sitio web admite HTTPS visitándolo y comprobando la URL completa. Si la letra "S" no aparece, Google tiene una guía para habilitar el uso de HTTPS en su sitio web.

Asegurarse de que su sitio admite el uso de HTTPS es un primer paso importante, pero no el único que debe tomar. No debería ser responsabilidad de las personas sobrevivientes entender HTTPS frente a HTTP. Su sitio web puede aparecer como

un enlace en otros sitios web. Estos sitios pueden incluir un enlace HTTP en lugar de uno HTTPS. Sin otras medidas de seguridad, un intruso podría modificar la conexión de un usuario de su sitio de HTTPS a HTTP sin que el usuario lo advierta. Por lo tanto, HTTPS debe ser el valor *predeterminado* en su sitio web, no debe ser solamente compatible. Si los usuarios hacen uso de enlaces HTTP anteriores, sus conexiones a su sitio deben seguir siendo HTTPS. Para ello, utilice HTTP con protocolo de transferencia de hipertexto seguro (HSTS). Su servicio de informática o proveedor de servicios puede encontrar la información en el sitio web del Consejo de Directores de información de Estados Unidos US Chief Information Officers Council . Este sitio también describe el por qué este método es más seguro que las otras alternativas.

Hay muchos aspectos del diseño de un sitio web más seguro además del cifrado. Para obtener más información sobre sitios web más seguros, consulte nuestro artículo sobre el diseño de sitios web para aumentar la seguridad y la privacidad de las personas sobrevivientes.

Nota: HTTPS no evita otros riesgos de espionaje de "baja tecnología". Alguien podría tener acceso físico a un dispositivo, haber instalado un programa de vigilancia *(stalkerware)* en él, o tener la cuenta de una persona sobreviviente o contraseñas de navegador y aun así poder ver lo que ha hecho o está haciendo en línea.

El cifrado es una herramienta, no una solución integral de seguridad o confidencialidad

El cifrado es, entre muchas cosas, una herramienta esencial para la confidencialidad y la privacidad de las personas sobrevivientes. Sin embargo, el cifrado no es una solución integral ni para la seguridad ni para la confidencialidad. Las personas intercesoras y el resto del personal siguen necesitando capacitación sobre prácticas de confidencialidad. Deben distinguir cuál es la información que

es confidencial. Deben saber cómo utilizar la tecnología cotidiana, como las listas de distribución o los sistemas de mensajería interna, sin alterar la confidencialidad. Entre las prácticas de seguridad importantes, además del cifrado, se incluyen las siguientes (entre otras).

- Medidas de seguridad de contraseñas efectivas. Son tan importantes para el personal de la organización como para las personas sobrevivientes.
- Garantizar un nivel de acceso adecuado a los datos. Las personas deben tener acceso solamente a la información que necesitan para hacer su trabajo. De esta forma, si la cuenta de un miembro del personal resulta jaqueada, el daño que el hacker puede hacer a través de esa cuenta es limitado.
- Implementación de sitios web por personal informático o contratistas que representa el OWASP Top Ten. Se trata de una lista anual de las fallas de seguridad más comunes en las aplicaciones web.
- Uso de dispositivos de seguridad cortafuegos (firewalls) en los dispositivos, redes y sitio web de un programa. Estos filtran el tráfico de red entrante y saliente.
- Conjunto de herramientas de confidencialidad – Siempre se deben cumplir las instrucciones explícitas de las personas sobrevivientes sobre qué tipo de información propia se puede diseminar y quién puede hacerlo. No se permite que una persona intercesora decida compartir la información de las personas sobrevivientes con nadie fuera de su programa sin el previo consentimiento de dichas personas. Lea más sobre las obligaciones de confidencialidad de los proveedores de servicios a las víctimas en nuestro Manual de Confidencialidad.

necesariamente los puntos de vista del Departamento de Justicia de los Estados Unidos.

Actualizamos nuestros materiales con frecuencia. Visite TechSafety.org para consultar la última versión de este y otros materiales.