UNIVERSIDAD UNIMINUTO

INFORMATICA EMPRESARIAL

Seguridad informática

GINA MARGARITA CEPEDA VILORIA

000672773

22 de septiembre 2018

**INTRODUCCION**

En los últimos años, las redes sociales como Facebook o Twitter han crecido rápidamente, las redes sociales son muy útiles para hablar con amigos que hacía mucho tiempo que no teníamos contacto, o antiguos compañeros de clase.

También nos permiten crear eventos para quedar o salir, sin tener que llamarnos todos por teléfono y por tanto, ahorrarnos dinero en la factura del móvil. También sirve para establecer nuevas relaciones con otros, basados en rasgos compartidos como comunidades, hobbies, intereses y círculos de amistad.

Las ventajas de las redes sociales las conoce todo el mundo, lo que poca gente sabe, es que la privacidad y la seguridad en las redes sociales, está reñida con la sociabilidad y el uso que se les puede dar. Si tenemos un perfil demasiado estricto, no se podrán comunicar amigos de nuestros amigos y eso podría perjudicarnos “socialmente”, sin embargo si tenemos un perfil abierto, se podrá comunicar todo el mundo, ver todas las fotos, todos los comentarios, es decir, la privacidad es nula pero sin embargo la sociabilidad es máxima, justo lo que la gente quiere conseguir en las redes sociales.

Las redes sociales han crecido exponencialmente, y ellas almacenan muchísima información privada de sus usuarios y sus interacciones. Esta información es privada y va dirigida a unas determinadas personas. Sin embargo con toda la información que almacenan, no es de extrañar que las redes sociales también atraigan a personas malintencionadas, para acosar, difamar, hacer spam y phising.

A pesar de los riesgos, muchos mecanismos de control de acceso y privacidad son débiles contra estos atacantes.

En este artículo hablare sobre la seguridad y privacidad en las redes sociales, y nos hacemos la pregunta: ¿cuáles deberían ser los objetivos de los diseños de seguridad y privacidad?

Cuando evaluamos los objetivos, entramos en el conflicto de privacidad contra funcionalidad y sociabilidad. Debe haber un equilibrio entre ellas.

**PRIVACIDAD Y SEGURIDAD EN LAS REDES SOCIALES**

Para comprender el gran reto que supone equilibrar seguridad y privacidad, con la sociabilidad y usabilidad tenemos que ver los principales estándares de seguridad en la red.

* Confidencialidad: requiere que la información sea accesible únicamente a las entidades autorizadas. Es de vital importancia en las redes sociales porque un mal uso de la información podría traer graves consecuencias en la vida de las personas.
* Integridad (requiere que la información sólo sea modificada por las entidades autorizadas).
* Autenticación (el usuario es realmente quien dice ser).
* No repudio (ofrecer protección a un usuario frente a otro que niegue posteriormente que realizó cierta comunicación). [4]

Todo ello aplicado a las redes sociales.

**Principales funcionalidades de las redes sociales:**

Hay varias diferencias entre unas redes sociales y otras, pero todas ellas tienen un punto en común: la comunicación con nuestros amigos, y también con desconocidos.

Una red social es la representación digital de sus usuarios, sus relaciones sociales, sus fotos mensajes etc.

Con dicha res social podemos crear un perfil de uno mismo para mantener relaciones sociales con otra gente que también tiene un perfil, mejorar las relaciones existentes entre nosotros y también nos ayuda a tener nuevas relaciones sociales, basadas en intereses comunes como localización geográfica, actividades etc.

Las redes sociales también nos proporcionan un espacio personal de gestión de nuestro perfil. Nos permiten, – entre otras cosas -, crear, modificar y cancelar nuestro perfil en dicha red social. También nos permite introducir contenido (fotos o comentarios) y editarlos, todo ello para mejorar la relación con otra gente, ya que automáticamente es actualizada en la red social y estará a la vista de nuestros contactos.

Nos permitirán administrar la lista de contactos que tengamos, podremos agregar personas con nuestros mismos gustos, misma edad, ciudad…para establecer una nueva relación.

Si tenemos gente agregada con la que que ya no hablamos, o simplemente porque no queremos tenerlos en nuestra lista de amigos, podemos eliminarlos, y no tendrán los permisos necesarios para seguir viendo nuestras fotos o comentarios (esto si la configuración de seguridad es para sólo amigos y no abierto para todo el público).

Algunas redes sociales también permiten hacer grupos de gente, por ejemplo podemos crear el grupo amigos y meter allí a todos nuestros amigos con unos permisos sobre nuestro perfil determinados. Si creamos el grupo compañeros de trabajo, puede que no queramos que esa gente vea nuestras fotos personales, pues les aplicamos los permisos necesarios para que no las puedan ver, y tener control total sobre lo que ven y no ven nuestros contactos.

La comunicación con los demás, es la principal característica de las redes sociales, y podemos comunicarnos de varias formas. Podemos poner comentarios en un tablón como si de una especie de blog se tratase, estos comentarios estarán a la vista de todo el mundo, podremos mantener conversación personales de una forma pública.

Si queremos más privacidad, podemos enviar mensajes privados, que sólo leerá el propietario del perfil en cuestión, es como enviar un email, pero mediante la red social.

Otra forma de comunicación es el “Chat”, que es como una conversación de messenger, y puede incorporar videollamada.

Algunas redes sociales permiten aplicaciones de terceros, y encontramos por ejemplo los juegos (muy adictivos) de las redes sociales.

Las redes sociales no se limitan sólo a mantener las relaciones existentes (perfiles agregados a nuestro propio perfil), sino que también necesitan (necesitamos) establecer contacto con más gente, y es ahí donde entra en juego el buscador de las redes sociales, donde haremos una búsqueda global por toda la red.

Para encontrar a un usuario deberemos poner su nombre, también podemos acotar su búsqueda por país, provincia, Universidad, colegio, por empresa y por supuesto por sexo y edad. Se nos presentará un listado con toda la gente coincidente, y con la foto principal del perfil podremos decidir si es la persona que buscamos, o de lo contrario nos hemos equivocado y debemos seguir buscando.

También podemos buscar gente que sean “amigos de nuestros amigos”, es lo que llamamos un cruce social. Entramos en su perfil y podremos ver a toda la gente que tiene agregada. Un usuario puede restringir que la demás gente vea a quien tiene agregado, pero esto quita sociabilidad (a cambio de una mayor privacidad).

El principal objetivo de una red social es la sociabilidad, por tanto si tenemos el perfil abierto para que puedan ver a nuestros amigos, potenciaremos esa sociabilidad, y esto es lo que entra en conflicto con la privacidad y la seguridad.

Las redes sociales, también pueden llegar a enmascarar las malas relaciones. Cuando un usuario se quita de la lista de amigos de otro usuario, no te aparece ninguna notificación de que te ha desagregado, solamente aparecen notificaciones sobre las relaciones que son buenas. Es decir, enmascaran los sucesos desagradables.

**Arquitectura de una red social.**

Hay dos formas en las que las redes sociales pueden trabajar, tenemos la arquitectura cliente-servidor donde el servidor será la red social y los clientes nosotros. Y la otra es la arquitectura peer-to-peer, donde la información estará distribuida y no centralizada, como ocurre en el cliente-servidor.

Las redes actuales de hoy en día están centralizadas, basadas en una arquitectura cliente-servidor. Todas las funcionalidades de la red social, como el almacenamiento, edición de los datos, mantenimiento de la web, o el acceso a los servicios que proporcionan la red social, son ofrecidos por la propia red social como Facebook o Tuenti. Esta arquitectura tiene la ventaja de ser sencilla, pero a la vez, es débil a los ataques, como el ataque de denegación de servicio. Si la información que se almacena en el servidor WEB es muy grande, podría provocar el denominado cuello de botella y que todos los usuarios navegaran muy lentamente por la red social. Por eso hay varios servidores en cada uno de los países, varios nodos, aunque están conectados entre sí para el intercambio de información.

La arquitectura peer-to-peer podría ser la próxima generación de redes sociales. Se adoptaría un sistema descentralizado basado en la cooperación de cada uno de los miembros de la red, cada usuario sería cliente de la red social y a la vez servidor de dicha red social, por tanto se almacenarían datos en nuestro equipo. Se apoyaría el intercambio directo de información entre dispositivos, entre usuarios que ya se conocen de antes. La arquitectura P2P puede tener ventaja en redes sociales reales, y proximidad geográfica para proporcionar servicios locales, sin necesidad de internet. El servidor estaría distribuido en cada nodo de almacenamiento, y deberemos tener una “relación social” con ese nodo. El principal problema de esto será, realizar búsquedas de manera global.

En resumen, la arquitectura cliente-servidor, requiere conexión a internet para comunicarse a través del servidor centralizado de nuestra red social. Por otra parte el P2P conectaría localmente, ya que el papel de servidor se distribuye en cada nodo de almacenamiento.

**Las 10 peores amenazas que se han detectado últimamente en redes sociales son las siguientes:**

1. **Virus de redes sociales:** A través de *botnets* o robots informáticos, los hackers toman el control de las computadoras enviándoles correos no deseados que promueven hacer clic en un enlace.
2. **Phishing Bait:**El mail que lleva al usuario a entrar a su cuenta de Facebook, esperando que no se identifique la página en su buscador, y así hackean sus contraseñas.
3. **Trojans.**La zona URL es similar a un banco *Trojan*, pero más astuto. Puede calcular el valor en la cuenta de su víctima y ayudar a decidir la prioridad para el ladrón.
4. **Infiltración de información:** Los usuarios comparten demasiada información acerca de la organización, proyectos, productos, finanzas, cambios organizacionales, escándalos y otra información sensible en las redes.
5. **Abreviación de enlaces:** Los servicios que ayudan a abreviar enlaces (ej. Bit.ly y Tinyur) para que quepan en lugares más pequeños, también hacen un buen trabajo escondiendo los enlaces malware permitiendo que las víctimas no se den cuenta que están haciendo clic para instalarlo.
6. **Botnets:** Las cuentas de Twitter han sido usadas para dirigir y controlar los canales de algunos *botnets*.
7. **Amenazas avanzadas persistentes (ATP):** Ésta es la inteligencia que recopia los datos de personas de alto nivel (ej. Ejecutivos, oficiales, individuos de alto poder adquisitivo) para quienes las redes sociales pueden ser una fuente importante de información.
8. **Cruce de páginas web para falsificación de solicitudes (CSRF):** Este tipo de ataques aprovechan la confianza que brindan las aplicaciones de las redes sociales, al ingresar en el buscador de los usuarios. Siempre y cuando la aplicación de las redes sociales no refleje el encabezado del sitio referido, será más fácil iniciar un ataque. En el momento en el que un usuario comparte una imagen en una secuencia de eventos, otros usuarios podrán hacer clic para difundirlo.
9. **Impostores:** Muchos impostores han colectado cientos y miles de seguidores en Twitter. Los personificados han sido avergonzados cuando los impostores se han hecho pasar por ellos.
10. **Confianza:** Cuando un correo electrónico se vuelve popular o un mensaje instantáneo se convierte ubicuo, las personas confían en los enlaces, las fotos, los videos y ejecutables cuando vienen de parte de “amigos”.

Para prevenir este tipo de amenazas es necesario hacer una revisión detallada de las políticas que tiene su empresa en la utilización del internet por parte de sus empleados, y así determinar si es necesaria una estrategia de seguridad para tomar las acciones correctas antes, durante y después de cualquier ataque.

A continuación presento el caso donde un programador de computadores palestino, **Khalil Shreateh**, encontró una falla de seguridad en Facebook que permitía a sus usuarios publicar mensajes en los muros privados de personas que no los habían aceptado como amigos.

Y al no recibir una buena acogida del equipo de seguridad de la red social, decidió mostrarle a su propio fundador, Mark Zuckerberg, como funcionaba. Y en su propio muro:

**El error que "no es error"**

El "bug" –o error- se saltaba todas las normas de privacidad del sitio y dejaba de manifiesto una falla en el sistema de seguridad de Facebook.

Tras descubrirlo, el experto en sistemas publicó un video de Enrique Iglesias en el muro de una vieja amiga de la universidad de Zuckeberg con la que no tenía nada en común ni estaban conectados.

Shreateh reportó el error a través del sistema "Sombrero Blanco" de la red social, una página especialmente creada para encontrar errores y vulnerabilidades la cual premia monetariamente a quienes aportan a la seguridad del sistema.

Según lo manifestado por el programador, le escribió al equipo de Facebook sobre su descubrimiento, con todos los detalles básicos.

**"Lamento tener que violar su privacidad y escribir en su muro (...) No tengo otra opción".Mensaje de Khalil Shreateh a Mark Zuckerberg.**

Sin embargo, el equipo de seguridad de la red social rechazó sus advertencias, afirmando que la cuestión "no fue un error", ya que el video posteado sólo pudo ser visto por los amigos de la amiga de Zuckeberg.

Frustrado por la respuesta de los expertos en seguridad quienes supuestamente deben velar porque se cumplan las normas de privacidad de los usuarios, Shreateh tomó una drástica decisión.

El controlador decidió mostrarles el 'bug' hackeando la página del número uno y rostro innegable de la red social, su fundador Mark Zuckerberg.

"Lamento tener que violar su privacidad y escribir en su muro", decía el mensaje de Shreateh, cuya lengua materna es el árabe. "No tengo otra opción", escribía el palestino en el muro de Zuckerberg, como advertencia tras haber sido ignorado por su equipo de seguridad.

En menos de un minuto la cuenta de Facebook de Shreateh fue suspendida y un ingeniero de seguridad de la red social lo contactó para pedirle todos los detalles de su acción.

**La ira de Facebook**

ser escuchado.

El hackeo al muro del mandamás de Facebook desató la ira de su equipo de seguridad.

Matt Jones, quien se identificó como miembro del equipo, salió en defensa de sus compañeros a través del foro de tecnología "*Hacker News*".

Según el empleado, el error sí existió y fue "limpiado" el jueves pasado. Sin embargo, asegura que el reporte inicial del hacker a través de "Sombrero Blanco" fue un link a muros que él mismo habría hackeado.

"Lo único que presentó fue un enlace al mensaje que ya había hecho (en una cuenta real cuyo consentimiento no tenía, lo que viola nuestros Términos de Uso y la Política de Fuente Responsable). Este decía 'el bug permite a los usuarios de Facebook compartir enlaces con otros usuarios de Facebook'".

A través de su iniciativa "Sombrero Blanco", Facebook paga un mínimo de US$500 como recompensa por cualquier falla de seguridad reportada. Sin embargo, la empresa se ha negado a pagarle a Shreateh debido a que sus acciones violaron las políticas por las que se rige el programa.

Jones agregó que la forma en que actuó Shreateh, mostrando el error "a través de las cuentas de personas reales sin su permiso", era un "comportamiento inaceptable" que iba contra la política de "Sombrero Blanco", por lo que no recibiría ninguna recompensa por su descubrimiento.

**REFLEXION DEL CASO:**

Hoy en día el tema de la inseguridad es algo que nos preocupa en todos los ámbitos de nuestra vida. Especialmente en nuestro país estamos cada vez más expuestos a los maleantes que quieren dañarnos o apropiarse de nuestros bienes y con esto se multiplica la demanda de mejores alternativas para estar protegidos.

Este mismo esquema se ha expandido vertiginosamente hacia el sector digital. Virtualmente estamos vulnerables ante una oleada de personas mal intencionadas y hackers que están al acecho de encontrar los puntos vulnerables de nuestras redes para accesar a ellas y utilizar nuestra información con distintos fines.

Como empresarios, este tema es preocupante, ya que los empleados utilizan sus dispositivos móviles para trabajar y accesar a las redes sociales, como una herramienta indispensable para una comunicación eficiente.

Sin embargo, estos sitios sociales tienen altos índices de vulnerabilidad en donde los ciberdelincuentes pueden obtener fácilmente acceso a las cuentas de los usuarios. Una vez que el hacker obtiene entrada a una cuenta, puede extraer más información e infiltrarse en otras cuentas. El gran problema es que el 87% de las pequeñas y medianas empresas no cuentan con políticas formales para el uso de internet y 70% de éstas carecen de políticas para empleados sobre el uso de las redes sociales.

Actualmente ninguna de las redes sociales más visitadas, como Facebook y Twitter, tienen un fuerte puntaje de privacidad, por lo que las empresas deberían revisar sus políticas de seguridad en la utilización de internet por parte de sus empleados. Aunado a esto, los empleados utilizan cada vez más sus propios dispositivos móviles para uso de la empresa, por lo que la utilización de las redes sociales queda totalmente vulnerable, así como la información de la empresa.