Dudas y certezas sobre las redes sociales en la empresa

Autor: Sebastián Bortnik, Analista en Seguridad de ESET para Latinoamérica
Fecha: lunes 2 de agosto de 2010

ESET Latinoamérica, Av. Del Libertador 6250, 6to piso
Buenos Aires, C1428ARS, Argentina
Tel +54 (11) 4788 9213 – Fax. +54 (11) 4788 9629
info@eset-la.com, www.eset-la.com

Certeza I: los usuarios quieren las redes sociales

En los últimos años, las redes sociales han aumentado en popularidad y ya forman parte de los hábitos cotidianos de los internautas. Casi cualquier usuario de Internet hace uso de al menos una red social, y muchos de ellos participan activamente en varias de ellas. Incluso para muchos usuarios (especialmente los más jóvenes), **las redes sociales son el principal motivo para conectarse a Internet**.

El número de redes sociales es muy extenso dado que es una actividad en constante movimiento donde periódicamente aparecen nuevas alternativas, y cuya popularidad depende tanto de las diversas características que presenten como también del tipo de usuario al que estén apuntadas. Analizando los números de las redes sociales más populares se puede observar la relevancia de éstas en el escenario web.

Facebook se ha posicionado como **la red social más popular del mundo**, y durante el 2010 ha superado los **500 millones de usuarios en todo el planeta**. Es la predilecta entre los más jóvenes y es utilizada principalmente para armar redes de contactos entre amigos, comunicarse con éstos, compartir imágenes y otros usos más. En los últimos años ha comenzado a ser utilizada por empresas y organizaciones para comunicarse con el público.

En segundo lugar aparece otra red social que es muy popular, como es el caso de **Twitter**, la **red social de *microblogging***, donde los usuarios comparten contenidos en un máximo de 140 caracteres. Esta ha sido una de las redes sociales de mayor crecimiento durante 2010 y ya posee **más de 75 millones de usuarios**.

MySpace, es otra **plataforma basada en las relaciones sociales** que permite compartir perfiles de usuarios, amigos, grupos, fotos, videos y música, entre otros. Según datos del 2010 posee **130 millones de usuarios**, a pesar de que con la popularización de Facebook se ha visto desplazada. De todas maneras aún mantiene su popularidad en sectores específicos, especialmente para la difusión de bandas musicales.

En redes sociales más enfocadas, aparece como líder **Linkedin**, la **red social para profesionales**. Es **la más utilizada en el ámbito corporativo**, permitiendo a las personas tejer redes de contactos laborales, además de cargar sus *curriculums vitae* en la web, y disponer de ellos en formato público. Posee además otras funcionalidades desorientadas al ámbito empresarial como foros de discusión, difusión de eventos o búsquedas laborales. A la fecha, cuenta con 70 millones de usuarios registrados.

Existen otras redes sociales y es imposible enumerarlas todas, pero hay algunas que también poseen popularidad en Latinoamérica como **Orkut** (especialmente popular en Brasil), con **100 millones de usuarios**; **Hi5** (80 millones) o **Sonico** (17 millones).

Se estima que **entre 2007 y 2009 el número de usuarios en redes sociales se duplicó**[1]. Estos números, más el conocimiento que el lector tendrá sobre sus costumbres y la de su entorno, certifican la primera certeza: **los usuarios quieren las redes sociales**.

Certeza II: en las redes sociales hay riesgos relacionados a la seguridad de la información

El hecho de que existan millones de usuarios en las redes sociales, publicando contenidos en forma dinámica e interactiva, no ha sido pasado por alto por los atacantes informáticos, que han encontrado en las redes sociales un medio para realizar diversas actividades maliciosas a través de Internet. Los riesgos existentes son variados y con características distintas según la ocasión, listándose en la presente sección los más importantes de ellos, junto con sus medios y principales implicancias para las empresas.

Malware

La relación entre las redes sociales y el malware se ha vuelto más estrecha en los últimos años. Al haber tantos usuarios utilizando estos servicios, éstos aparecen como un medio atractivo para la propagación de códigos maliciosos, ya que haciendo que un mensaje circule entre los usuarios y enlace a un archivo dañino, se puede tener una alta efectividad para los atacantes.

Un ejemplo de esto es el gusano Koobface, un malware que se propagó masivamente durante 2009 y que ha continuado su actividad en lo que va del año, utilizando como principal vectorde propagación Facebook, enviando mensajes a los contactos de los usuarios infectados de forma automática con enlaces

[1] http://mashable.com/2009/07/28/social-networking-users-us/

dañinos. En el artículo "**Utilizando redes sociales para propagar malware**"[2], es posible conocer más detalles sobre su funcionamiento[3].

En los últimos meses se han reportado diversos casos de relación entre códigos maliciosos y las plataformas sociales, como las propias **campañas masivas de Koobface**[4], los **ataques de phishing a Facebook generados por ZeuS**[5], el **ataque de un rogue a Facebook**[6] o la propagación del código malicioso detectado por la heurística de **ESET NOD32 Antivirus**[7] como *una variante de Win32/Kryptic.ESX* con correos electrónicos **simulando un cambio de contraseña en Twitter**[8], entre muchos otros.

A pesar de estos casos, una encuesta realizada por ESET Latinoamérica en junio de 2010 reveló que **la mitad de los usuarios consideran que no hay malware en redes sociales**[9], lo cual refuerza la probabilidad de éxito para los atacantes.

Privacidad y robo de identidad

La información que publican los usuarios en las redes sociales ha ido aumentando. Ya no se trata sólo del nombre, la edad o el sexo, sino que es posible agregar: fotografías familiares, lugares donde se asiste, opiniones, costumbres, datos de contacto, entre otros. Toda esta información expuesta puede llegar a tener un alto costo para la víctima de algún delito informático.

En primer lugar, la exposición de la privacidad aparece como el principal riesgo para los usuarios, así como también para las empresas. Usuarios publicando situaciones laborales, problemas con compañeros

---

[2] http://www.eset-la.com/centro-amenazas/2034-utilizando-redes-sociales-propagar-malware

[3] También es posible ver un video educativo sobre infección por redes sociales en: http://www.eset-la.com/centro-amenazas/videos-educativos/2035-infeccion-redes-sociales

[4] http://blogs.eset-la.com/laboratorio/2010/04/07/campana-masiva-koobface/

[5] http://blogs.eset-la.com/laboratorio/2009/11/06/ataques-phishing-facebook-generados-zeus/

[6] http://blogs.eset-la.com/laboratorio/2009/09/09/facebook-amenazado-solucion-seguridad-antivirus-falsa/

[7] http://www.eset-la.com/download/

[8] http://blogs.eset-la.com/laboratorio/2010/06/03/cambiar-la-contrasena-de-twitter-o-infectarse/

[9] http://blogs.eset-la.com/laboratorio/2010/06/10/la-mitad-de-los-usuarios-consideran-que-no-hay-malware-en-redes-sociales/

de trabajo (¡o jefes!), temáticas de reuniones, trabajos en proyectos; pueden estar exponiendo datos confidenciales de la empresa, que podrían afectar el funcionamiento de la misma.

Por otro lado, el robo de identidad ha comenzado a afectar a los cibernautas, y el hecho que los empleados de una empresa puedan ser víctimas de este delito, también representa un grave riesgo para la organización; por lo que evitar la exposición de información sensible es la principal herramienta de protección existente. Los ataques de **phishing**[10] aparecen como la principal amenaza informática asociada a este campo, ya que la pérdida de credenciales de acceso puede ser una vía directa para los delincuentes a mucha información personal, incluso aquella que esté configurada como privada.

Fuga de información y reputación de la empresa

Relacionado a la sección anterior, las redes sociales pueden comprometer la reputación de la empresa y la costumbre de los usuarios de volcar en éstas opiniones o experiencias personales aumentan este potencial riesgo.

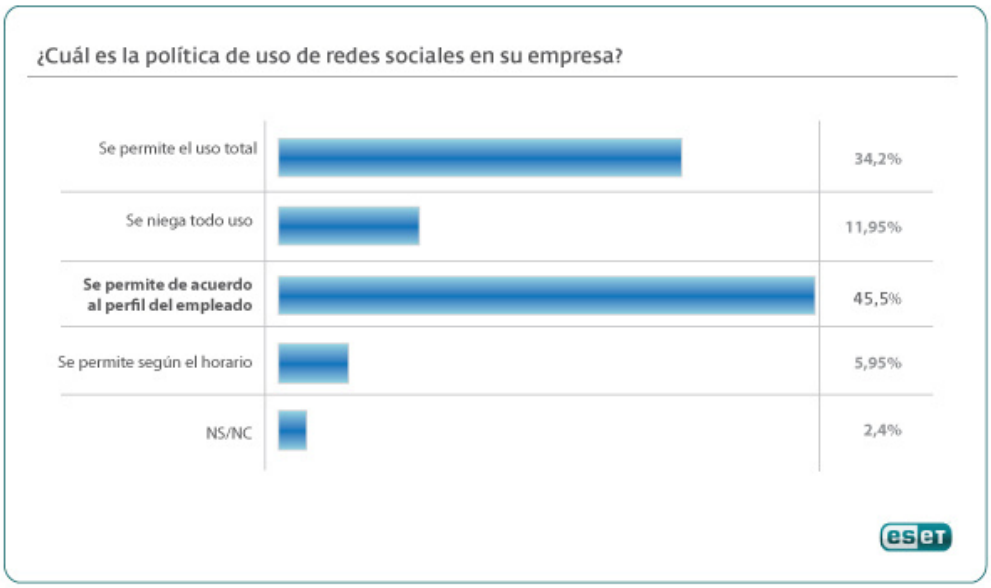
¿Cuál es el costo para la empresa de un empleado o un cliente publicando comentarios negativos sobre la marca en la web? ¿Cuál es el costo de usuarios malintencionados que distribuyen material ilegítimo en nombre de la empresa? Según la ocasión, éstos pueden ser altos, especialmente cuando esas opiniones perjudiciales para la empresa no son detectadas, y circulan por la web afectando la imagen y reputación de la misma. Por lo tanto, las organizaciones sólo pueden enfrentar esta problemática contando con presencia en la web, es decir, tener recursos que permitan identificar contenidos de este tipo, para así poder tomar acciones cuando lo consideren necesario.

Duda: ¿Qué hacer con las redes sociales en la empresa?

Las dos certezas anteriormente presentadas entran en conflicto: **los usuarios quieren usar las redes sociales, pero a la vez éstas pueden ser un riesgo para la información de la empresa**. ¿Qué hacer entonces con ellas? Esta es la gran duda que acecha a gerentes, administradores de red y cualquier posición que implique una responsabilidad sobre la seguridad y el uso de los recursos tecnológicos en la empresa. A priori, esta paradoja obliga a tomar una decisión sobre una oposición binaria: **permitir o no permitir el uso de redes sociales en la empresa**.

[10] http://www.eset-la.com/centro-amenazas/amenazas/2144-Phishing

A partir de las encuestas realizadas por ESET Latinoamérica en diversos eventos y congresos durante el 2010, y habiendo sido consultados los profesionales del sector gerencial y de IT, se puede observar que la mitad de ellos han manifestado resolver la problemática por uno de estos dos caminos, siendo mayoritario el permiso total para utilizar redes sociales en horario laboral. Sin embargo, la otra mitad ha manifestado definir políticas intermedias, como por ejemplo, permitir el uso de redes sociales según el perfil del empleado (la opción más seleccionada); tal como se puede ver en los resultados completos de la encuesta:



Es decir que lo que parece ser un dilema, tiene en realidad otras alternativas y caminos a tomar que, aunque involucran procesos de decisión más complejos o extensos, pueden ser más acordes a las necesidades reales de la organización, así como también permiten encontrar un equilibrio entre las dos "realidades conflictivas" presentadas en la secciones anteriores a la presente.

Sin lugar a dudas no se trata de una decisión sencilla de tomar: permitir las redes sociales puede acarrear riesgos, mientras que prohibirlas puede causar problemas tanto con los empleados, como para la propia empresa que puede necesitar utilizarlas.

Conclusión

Las redes sociales se han incorporado a las costumbres de los usuarios en muy poco tiempo lo que las ha convertido en una herramienta muy poderosa, y lo serán cada vez más con el pasar de los años. La existencia de amenazas y riesgos asociados a éstas no es ni más ni menos que el natural interés de los atacantes por las posibilidades de ataque que les brinda un servicio utilizado por millones de usuarios en todo el mundo.

Cualquiera de las acciones a tomar en este aspecto por las empresas es válida, y cada una de estas posee sus ventajas y desventajas, así como también habrá implementaciones puntuales a las características de cada empresa.

Sin embargo, aunque denegar el acceso a las redes sociales en la red corporativa puede ser una alternativa válida, es importante destacar que el permitir su uso no es necesariamente una exposición indiscriminada a los riesgos asociados, sino que es posible contar con otras medidas de protección para minimizarlos mientras se utilizan este tipo de servicios.

La utilización de un **antivirus con capacidades proactivas de detección**[11], para prevenir las infecciones de malware que circule por las redes, la definición de **Políticas de Seguridad**[12] para evitar incidentes relacionados a la fuga de información o reputación de la empresa, y la implementación de **campañas de educación y concientización** para evitar que los usuarios sean víctimas de ataques que usen Ingeniería Social; son las medidas a tener en cuenta para no sufrir consecuencias negativas a partir del uso de las redes sociales en el entorno corporativo.

Si las empresas aprovechan estas medidas de seguridad, será posible utilizar las redes sociales, con todo el valor asociado que éstas tienen, además de minimizar los riesgos de cualquiera de los incidentes informáticos que se propagan por estos servicios.

[11] http://www.eset-la.com/download/

[12] http://blogs.eset-la.com/laboratorio/2009/10/29/politicas-de-seguridad-en-pymes/