Internet y nuevas tecnologías

Roberto Plá
Coronel de Aviación
http://robertopla.net/

SEGURIDAD

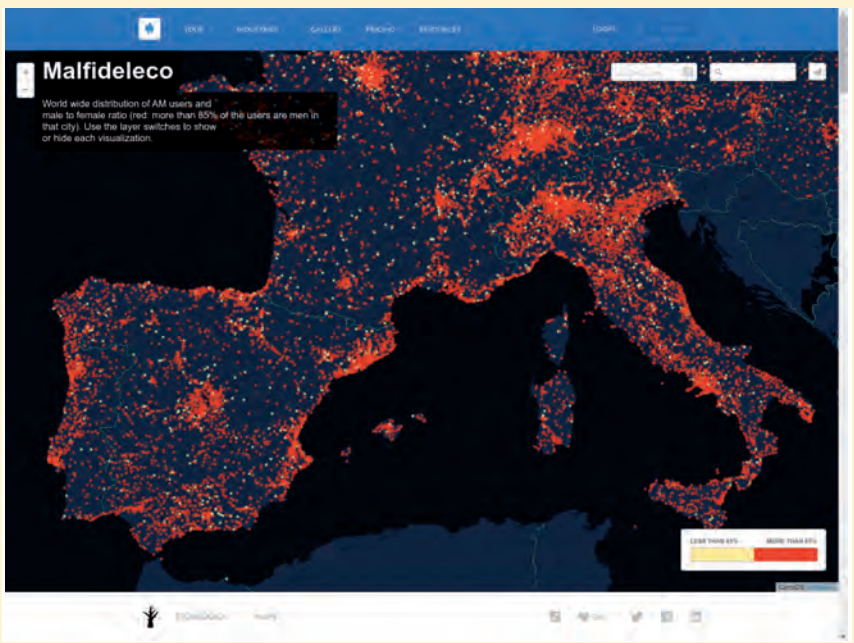
ATAQUE DE CUERNOS

La firma Ashley Madison es básicamente una web de contactos cuyo principal nicho de mercado son los hombres casados que buscan una aventura amorosa extra marital. Atentos a las necesidades de sus clientes uno de los principales reclamos de la firma es precisamente, la discreción, muy bien representada en sus anuncios a través de una bella muchacha que se lleva el índice a los labios en el gesto internacional del silencio.

Un silencio que se ha roto cuando unos hackers han asaltado los ordenadores de la compañía y se han llevado los datos de los clientes.

Hubo unos intentos más o menos absurdos de chantaje, que hacen dudar de que la intención de los hackers no fuera otra que publicar los datos. El 20 de agosto, los asaltantes publicaron los datos robados en la red, arrogandose además el papel de justicieros contra la hipocresía de los clientes y los fraudes de la compañía.

Este suceso reúne una serie de aspectos bastante interesantes, que he visto poco tratados en la prensa, que se ha cebado con las cuestiones más superficiales y socialmente escandalosas de la cuestión. Pero eludiendo los aspectos morales y sociales implicados, creo que hay enseñanzas que podemos sacar de los hechos y un debate interesante sobre cuestiones de seguridad en el uso de las redes. Precisamente porque entre los datos difundidos figuran numerosas cuentas abiertas desde direcciones de correo profesionales, y muchas de ellas pertenecientes a organismos públicos. Sin duda pertenecen a usuarios que no se habían parado a pensar en las cuestiones que expondremos a continuación.



Una Empresa española ha hecho una mapa con la distribución geográfica de los usuarios cuya identidad ha sido filtrada.

Más allá de la cuestión moral y familiar, el adulterio no deja de ser un engaño. En muchos países la imagen que ofrece un adúltero premeditado induce a pensar dos cosas: la primera que si engaña a su familia, también puede que en caso de considerarlo necesario engañe en su trabajo o a sus clientes. Y la segunda que quien necesita el apoyo de una base de datos de dudosa credibilidad es persona de pocos recursos sociales. Todo sea dicho sin juzgar a nadie, pero creo que la posibilidad de ofrecer la imagen que acabo de describir, es un riesgo evidente. Y perjudicial para la vida profesional pudiendo constituir una amenaza para la propia empresa o institución que lo emplea, ya que una persona que lleva una vida oculta es vulnerable como posible víctima de un chantaje.

Por otra parte, hay un debate sobre el uso que se le da a los accesos a internet y las cuentas de correo que las empresas ponen a disposición de sus empleados. En otros medios como vehículos, mobiliario, suscripciones a publicaciones, viajes o comidas, los límites suelen estar más claros o incluso pactados con la empresa. Sin embargo, el hecho de que el correo electrónico sea un medio de comunicación y la Constitución y las leyes protejan las comunicaciones privadas hace algo más enrevesado saber cual es el uso permisible de la cuenta de correo del trabajo. Creo que a nadie se le escapa que por económico que pueda salir cada mensaje, el acceso a la red y las cuentas de correo tienen un coste para la empresa y que esta no se gasta el dinero para el solaz de sus empleados, sino para que los usen en asuntos relacionados con su trabajo aumentando su productividad y no perdiendo el tiempo que se paga con su salario.

Es bueno que cada trabajador conozca las normas y la política de su empresa al respecto en vez de hacer supo-

siciones que pueden llevarnos a un disgusto con la empresa.

También está la cuestión de la imagen. No creo que nadie considere sensato que el nombre de su empresa o el cargo que ocupa pueda asociarse con actividades tan completamente ajenas a sus obligaciones profesionales como el ocio o las relaciones y actividades socialmente reprobables. En definitiva, el uso de los medios de la empresa para actividades privadas, salvo que así haya sido autorizado expresamente por la empresa es en mayor o menor medida un caso de fraude o corrupción.

Sobre los cargos y funcionarios públicos cuyas direcciones han aparecido en la base de datos filtrada hay que decir que los procedimientos de seguridad de la web asaltada no eran ninguna maravilla, bien sea por incompetencia o por codicia. Por ejemplo, las cuentas de correo no se comprobaban. Algo tan simple como que te envíen una primera clave al correo que has registrado, comprueba que es realmente tuyo. Eso da pie a pensar que algunos datos de la larga lista de usuarios son datos robados de gente que ha entrado en la web por curiosidad usando los datos de otra persona. Incluso que hayan sido introducidos maliciosamente para desprestigiar o dañar de alguna forma al propietario real de la cuenta.

También se ha sugerido que la propia empresa creaba perfiles falsos -especialmente femeninos- a fin de inflar sus cifras y las opciones de sus usuarios. En estos perfiles las direcciones de correo se 'recolectaban' en la web, en las mismas fuentes donde se recolectan millones de direcciones para convertirlas en blanco del SPAM o fraudes por correo. Esto se sospecha por la aparición de cuentas que en realidad son como "pozos" sin otra finalidad que precisamente atrapar SPAM y correos no deseados.

Obviamente, la estupidez acompañada de deshonestidad, nunca es descartable. Porque la única forma de calificar a alguien que usa su dirección de correo oficial o laboral para un asunto de este tipo es la de "escasamente inteligente y poco dotado para las comunicaciones telemáticas". No es el momento ni el lugar de explicarlas, pero hay numerosas formas de mantener el anonimato al inscribirse en una web, con diferentes niveles de seguridad, desde el "prudente" al "paranoico" y

para llevar a cabo la mayoría de ellos no hay que ser ningún gurú de las comunicaciones. Yo diría que, simplemente, conocer la dirección y el uso del famoso buscador.

También debería formar parte del sentido común más elemental la certeza de que no hay nada que sea secreto siempre. Los que no estén entre esos millones de usuarios cuyos datos se han desvelado, tienen ocasión de ver esta afirmación demostrada en cabeza ajena. Por mucha discreción que nos aseguren, si leemos las condiciones del servicio -claro, nadie lo hace nunca, ¡que aburrimiento!- veremos que advierte que la empresa no se responsabiliza de incidentes informáticos que den lugar a pérdida o publicidad de los datos del usuario.

Además de las cuentas de correo y los datos personales o preferencias intimas de los usuarios, entre los que se ha especulado sobre si había datos de tarjetas de crédito -extremo negado por la empresa- entre el botín de datos, un segundo grupo de hackers ha sido capaz de poner al descubierto millones de claves de acceso. Entre tantos usuarios habrá un número importante de los descuidados que usan la misma clave en todos los sitios, lo cual implica que sus cuentas en esos otros sitios han sido comprometidas: redes sociales, cuentas bancarias, acceso a información de la empresa, otras cuentas de correo,...es como perder el llavero con todas nuestras llaves etiquetadas explicando qué abren y donde encontrarlo.

Como conclusión, creo que al margen de la anécdota y los detalles morbosos suficientemente aireados por la prensa, el caso del asalto a la web Ashley Madison nos puede ofrecer las siguientes enseñanzas:

– Si eres deshonesto en una parte de tu vida, los demás probablemente pensarán simplemente que no eres de fiar.

– Los medios de la empresa son para el trabajo y el uso privado de los mismos puede comprometer tu vida profesional y perjudicar a tu empresa.

– Para tener una expectativa razonable de seguridad, hay que proteger nuestros datos, siendo cuidadosos al compartirlos, incluida nuestra dirección de correo.

– La web es cambiante. Lo que hoy parece seguro, mañana no lo es, la empresa más solida puede quebrar o desaparecer. Las garantías eternas, simplemente, no existen.

– Hay que ser estricto en el uso y la creación de palabras clave seguras para el acceso a nuestras cuentas porque son la barrera que protege nuestra vida privada y nuestro trabajo y patrimonio.

http://delicious.com/rpla/raa847a

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto