CÓMO PROTEGERSE DEL CIBERCRIMEN

Con el incremento de las gestiones *online* aumentan los riesgos de convertirse en víctima de cibercriminales que, lamentablemente, son conscientes de que la mayoría de usuarios ni siquiera sabe qué tipo de información les hace vulnerables. Las empresas juegan un rol esencial en la protección del internauta.

Por **Cristina Cunchillos**

Los ciberataques son noticia cada vez con más frecuencia. En mayo de este año, un ataque con *software* malicioso del tipo *ransomware* paralizó el servicio de salud británico y afectó a grandes empresas de todo el mundo incluyendo Telefónica o Iberdrola. Más recientemente, otro virus infiltró los sistemas de la central nuclear de Chernóbil; Deloitte fue víctima de un *hackeo* masivo y hasta el guión inédito de Juego de Tronos fue robado. Nadie es inmune.

400 nuevas amenazas por minuto

Lo que se publica en los medios de comunicación no es más que la punta del iceberg. Miles de pequeñas y medianas empresas se ven atacadas constantemente sin que se difunda en las noticias. El 92% de las empresas europeas han sufrido al menos un ciberataque. Y se estima que hay un promedio de 400 nuevas amenazas por minuto.

En España, las ofensivas contra sistemas informáticos aumentaron un 60% en los últimos cuatro años según la Dirección General de la Policía Nacional. Es un crecimiento que naturalmente evoluciona en paralelo a la revolución digital y el incremento de las gestiones *online*.

Se trata de un crimen que, sin derramar sangre, puede destrozar vidas y tumbar empresas. El Foro Económico Mundial lo considera uno de los cinco principales riesgos globales, con un impacto económico estimado entre 300.000 y un billón de dólares al año. Para las empresas, además del coste de restablecer las infraestructuras saboteadas o el pago de un rescate en *bitcoins* para desbloquear sus sistemas, el verdadero precio a pagar es su reputación y la confianza de sus clientes.

En el sector MICE

En el sector de los viajes y la organización de eventos la digitalización de los servicios está cada vez más generalizada: reservas y facturación *online*, programas de gestión de gastos, comunicación por *chatbots* o plataformas como Whatsapp... Los hoteles y agencias, por ejemplo, almacenan gran cantidad de información sobre sus clientes, no sólo en relación a sus datos personales y bancarios, también detalles de sus preferencias o su vida personal.

Si para estas empresas el *big data* sirve para proporcionar un servicio mejor y más personalizado, para un *hacker* que consiga infiltrarse en sus sistemas es el pasaporte para suplantar con extrema facilidad la identidad de cualquier cliente y utilizarla en actividades fraudulentas. En realidad, tan sólo unos pocos datos como el domicilio personal, el correo electrónico o la fecha de nacimiento del usuario pueden ser suficientes para hacerse pasar por él.

> Para un *hacker* el *big data* sirve de pasaporte para suplantar fácilmente otra identidad

INCIBE, Instituto Nacional de Ciberseguridad español, reconoció el riesgo para las agencias de viajes creando un programa educativo específico con vídeos tutoriales y consejos sobre medidas preventivas como la actualización de los sistemas. La reciente celebración en Tenerife (España) de HackHotel, primer Congreso Nacional de Ciberseguridad Hotelera, muestra la preocupación en este sector.

Legislación más estricta

Las empresas que gestionan a diario miles de datos de sus clientes tienen, por ley, el deber de protegerlos. Existen legislaciones a nivel nacional pero, además, el 25 de mayo de 2018 entrará en vigor el nuevo Reglamento General de Protección de Datos de la Unión Europea. Todas las empresas europeas deberán adoptarlo o afrontar sanciones de hasta 20 millones de euros o el 4% del volumen de su negocio total anual.

Según un estudio de Trend Micro, el 95% de los directivos de empresa son conscientes de ello y el 79% considera que ya cuenta con la mayor protección posible. No obstante, pueden pecar de exceso de confianza si no entienden bien qué debe ser considerado como información extremadamente delicada. El 64% de los encuestados, por ejemplo, no cree que la fecha de nacimiento sea un dato clave.

La nueva normativa será más estricta y obligará a las empresas a estar mejor preparadas, actualizando sus sistemas de manera regular e invirtiendo en nuevas tecnologías que garanticen una mayor protección del *big data*. Sin olvidar que la ciberseguridad es un negocio que mueve millones y no todo lo que se ofrece es efectivo.

Un informe reciente de SITA, Sociedad Internacional de Telecomunicaciones Aeronáuticas, indica que el 96% de los aeropuertos y el 95% de aerolíneas invertirán en iniciativas de ciberseguridad en los próximos tres años. De hecho en el aeropuerto de Múnich se acaba de instalar un centro para combatir los ciberataques a los que el *hub* se enfrenta diariamente.

Por su parte, los proveedores de tecnología desarrollan continuamente nuevas soluciones, tanto para los individuos como para las empresas. La tecnología disponible para combatir ciberataques es variada y, probablemente, no existe una solución única que valga para todos los casos. Lo más efectivo es combinar distintas herramientas. La aplicación de la inteligencia artificial es una de las soluciones emergentes.

Rol del usuario

Si la legislación obliga a adoptar mayores medidas de protección y la tecnología lo facilita, la concienciación del usuario es igualmente importante. En los viajes de negocios es una realidad la necesidad de estar conectado en todo momento. Sin embargo, los viajeros deben tener en cuenta la seguridad de la red antes de introducir cualquier dato privado, contraseña o información confidencial. Una red *wifi* gratuita a la que acceder sin contraseña es mucho más vulnerable que una red que solicita registro.

> Los viajeros deben tener en cuenta la seguridad de la red antes de introducir datos privados

Del mismo modo, la opción de guardar documentos en la nube, en sistemas populares como Google Drive o Dropbox, facilita enormemente la movilidad de los trabajadores ya que pueden consultar archivos desde cualquier lugar y desde cualquier dispositivo. Pero también supone un riesgo: un virus en un ordenador puede acabar infectando a toda la empresa.

Proteger la información con contraseñas idóneas, realizar transacciones únicamente en páginas web que muestren el protocolo de seguridad HTTPS, o evitar colgar documentos confidenciales en la nube son normas básicas que se deberían adoptar siempre y en todo lugar. En un mundo cada vez más digital donde la exposición a ciberataques es cada vez mayor, la responsabilidad de evitarlos nos concierne a todos.

Entrevista

Ángel Pascual

Jefe de Tecnología y Plataformas, Samsung Electronics Iberia S.A.U.

“Aunque parezca trivial, debemos compartir datos con las personas adecuadas”

¿Por qué deben las empresas invertir en ciberseguridad?

Existe una amenaza real y creciente en nuestro entorno. Recientemente hemos visto vulnerabilidades que han conseguido detener la actividad de muchas empresas de forma inesperada. El *smartphone* se ha convertido en una herramienta de trabajo que gestiona información sensible, pero a la vez debe ser accesible y estar conectado: éste es un reto que debemos cubrir los proveedores de soluciones. Más del 90% de los gestores de seguridad en las empresas dice estar preocupado por los desafíos actuales, siendo incluso más acusado en sectores como la banca donde vemos inversión creciente y apuesta por soluciones que integren medidas de seguridad que cubran la necesidad de proteger la información, y no sólo la relacionada con el trabajo sino también la personal.

¿Qué ofrece Samsung a sus clientes para protegerlos?

La plataforma Samsung KNOX vela por la seguridad y confidencialidad demandada por las empresas y ofrece protección de los datos personales del usuario. Nuestra visión pasa por ofrecer la mejor experiencia de plataforma abierta pero sin penalizar la seguridad y KNOX mejora las capacidades haciendo que Galaxy sea una apuesta segura. Se basa en una tecnología multicapa integrada en el *hardware* y en el *software* que monitoriza en tiempo real detectando posibles vulneraciones.

¿Qué consejos daría a los usuarios?

Aunque sea trivial, debemos compartir nuestra información con las personas adecuadas y por el medio adecuado. Aunque parece obvio, hay incidencias de seguridad causadas por descuidos de este tipo. Aconsejo el uso de la Carpeta Segura en nuestros *smartphones*: permite guardar aplicaciones e informaciones sensibles, protegiéndolas con la contraseña más segura, huella dactilar o iris en los modelos que lo integran. Si hablamos del mundo de la empresa es necesario mencionar el gestor remoto de dispositivos, que permite aplicar políticas de seguridad o geolocalizar los aparatos de la empresa.