Actualidad aseguradora
España
20/02/17
Prensa: Otra
Tirada: 16.000 Ejemplares
Difusión: 16.000 Ejemplares
Cód: 108731973
Página: 114
Sección: OTROS Área (cm2): 662,0 Ocupación: 100 % Documento: 1/4 Autor: Núm. Lectores: 64000

Ciberataques o la nueva normalidad en las empresas de todo el mundo

QUÉDENSE CON ESTA CIFRA: 4.200 MILLONES REGISTROS DE DATOS ROBADOS EN 2016. ASÍ LO REVELA EL RISK BASED SECURITY EN SU INFORME ANUAL DE DATA BREACH QUICKVIEW EN EL QUE SE MUESTRA QUE EL PASADO AÑO SE ROMPIÓ EL MÁXIMO HISTÓRICO EN CUANTO AL NÚMERO DE REGISTROS DE DATOS EXPUESTOS A VIOLACIONES. DE LAS 4.149 BRECHAS DE DATOS REPORTADAS DURANTE 2016 SE EXPUSIERON MÁS DE 4.200 MILLONES DE REGISTROS. OTRO DATO MUY SIGNIFICATIVO: SE NECESITARÁN 1,5 MILLONES MÁS DE EXPERTOS EN CIBERSEGURIDAD PARA CUBRIR LAS DEMANDAS DE LAS EMPRESAS PARA LOS PRÓXIMOS TRES AÑOS. Y ES QUE EL FUTURO QUE PREDICE EL FORO DE DAVOS POCAS VECES SE EQUIVOCA; EN 2017, YA INCLUYE ENTRE LOS RIESGOS CON MAYOR PROBABILIDAD EL ROBO DE DATOS.

Patricia Ojeda Leiva

¿QUÉ RIESGO CIBERNÉTICO HAY EN 2017? Se preguntó **José Esteves, profesor de Sistemas de la Información de IE** en el Workshop sobre Ciberseguros & Ciberseguridad impulsado por Center for Insurance Research (CIR) de IE. El principal es el relacionado con los riesgos humanos, la peor amenaza que puede haber "porque es el más difícil de corregir, mitigar y controlar". Tras este riesgo, según el experto, destacan Ransomware, Mobile Malware DDoS attacks masivos y globalizados y el Internet de las cosas, "que es la próxima gran amenaza". Además, ahora los hacker se expanden a todos los sectores de negocio, incluso a los de fintech e insurtech. "Los hacker trabajan por prestigios y ponerse la medalla en el hecho de hackear las últimas tendencias tecnológicas, como los móviles más modernos o las empresas más nuevas les da prestigio".

También existen tendencias para mejorar estos riesgos, como el Machine Learning (Aprendizaje automático), la Inteligencia artificial, los Bots (aplicaciones inteligentes), la analítica de datos o Data Science y Big Data, sobre todo para las grandes empresas, la cyberseguridad cognitiva que no solo analiza las transacciones sino que se trata de saber más el comportamiento de los usuarios y conocer los potenciales riesgos. A estos se suman los Sistemas Biométricos o el Blockchain.

A pesar de todo esto, detalla el experto, sigue habiendo una gran barrera: "La gente no entiende el discurso, hay que tener un cambio de mentalidad. El principal problema es la baja conciencia, no le trasmitimos el riesgo potencial que se sufre. Ven la ciberseguridad como un problema de tecnología, no como un problema de ellos: esto hay que mitigarlo". ¿Cómo? Hay que valorar los riesgos más allá de la tecnología, las personas son la última línea de defensa. Para Esteves lo que tiene menos fuerza es lo que corresponde a las personas: "si no saben de ciberseguridad, la tecnología de poco nos va a servir. Smart CyberSecurity, es decir, es necesario un cambio de mentalidad en materia de ciberseguridad".

¿Qué tenemos que impulsar para desarrollar nuestro negocio en 2017? Sería conocer el nuevo rol del CISO, la mentalidad centrada en personas y negocio, el cambio de lenguaje, el modelo cooperativo y desarrollar un Plan...para el fracaso...

Actualidad aseguradora
España
20/02/17
Prensa: Otra
Tirada: 16.000 Ejemplares
Difusión: 16.000 Ejemplares
Cód: 108731973
Página: 115
Sección: OTROS Área (cm2): 650,8 Ocupación: 100 % Documento: 2/4 Autor: Núm. Lectores: 64000

LA IMPORTANCIA DE CUANTIFICAR LOS RIESGOS

Para **Jérôme Gossé, Head IT/Tech & Commercial Companies - Financial Lines France; Head Security & Privacy - Europe, Middle East and Africa (EMEA), ZURICH GLOBAL CORPORATE** la ciberseguridad es un riesgo pero también una oportunidad. "Como aseguradores tenemos muchos datos y manejamos información que es muy sensible sobre nuestros clientes. Este es el riesgo, pero por eso tenemos el ciberseguro. Cuando hablamos de riesgos sistémicos, éste puede afectar a las aseguradoras, es primordial definir de qué estamos hablando, riesgo operativo de la tecnología y cómo afecta a su integridad. "Afecta a todo el sistema. El acceso no autorizado se puede ver expuesto".

La fuente del ciberseguro puede ser un problema accidental (ser humano, negligencia, etc.) pero es la más difícil de controlar. Gossé remarca la importancia de la gestión del ciberriesgo, resaltando la importancia que tiene para las empresas cuantificar los riesgos y saber gestionarlos. "Llama la atención cómo los ciberriesgos cada vez preocupan más entre los CEOs y los directivos, alcanzando los puestos más altos entre los líderes. Evitar el riesgo es casi imposible a día de hoy, por eso, para intentar mitigarlos es fundamental la integración dentro de las empresas de todos los implicados. Dado el impacto devastador de este riesgo, hay que estar preparado para mitigarlo. Es esencial que bajo este escenario se transfiera el riesgo a las aseguradoras u otras alternativas como las empresas cautivas", afirma.

LA FALTA INFORMACIÓN DIFICULTA PODER CALCULAR LOS PRECIOS

Los retos que tiene el mercado son de diversa índole. Como los riesgos tecnológicos ya que las amenazas están evolucionando de forma muy rápida y constantemente, explica Gossé. Los cambios de los modelos de información, las nuevas tecnologías, así como los riegos para los asegurados se complican: "Se darán cambios en mayo de 2018 con las distintas normativas que se darán en el mundo entero. Además de la madurez en la ciberseguridad en las compañías. No hay una solución estándar ni una barita mágica, hay que entender el negocio a la perfección para valorar el negocio y la cobertura y su exposición al riesgo". El riesgo principal, detalla el directivo de ZURICH, sigue siendo de carácter humano ya que es el eslabón más débil en la cadena de una compañía y para el asegurador es difícil cuantificar la prima porque la información actuarial es escasa, "se establecen precios a futuro basándose en información que puede no ser completa. Hay una acumulación del riesgo sistémico dado el gran número de amenazas y su difícil delimitación".

TIPOS DE COBERTURAS

Dentro de los seguros, éstos combinan coberturas de dos tipos, subraya Gossé. La primera centrada en las que cubren a las personas afectadas; gastos de investigación forense, abogados, la ciberextorsión, cuestiones regulatorias como multas o, incluso, la interrupción del negocio (lucro cesante). En la segunda cobertura estarían integrados los daños a terceros; costes de mejora del sistema informático "porque el objetivo del seguro es indemnizar para volver a la situación actual", la infracción de patente o el spam, aquí estaría incluida los spam que las compañías envían a sus clientes y que forma parte de una violación de normativa de protección de datos. Habría que incluir una nueva tendencia: "más servicios adicionales como los que dan respuesta a una emergencia cuando se produce un fallos en los ordenadores o una red de especialistas para dar asistencia al cliente ante cualquier incidente", concluye.

EL ROL DEL CISO ALINEADO AL NEGOCIO

1. Debe hablar varios lenguajes.
2. Liderar los cambios culturales.
3. Mostrar el valor para la organización.
4. Promover una cultura de ciberseguridad.
5. Sensibilizar, motivar y comprometer la Alta Dirección.
6. Establecer alianzas con stakeholders (modelo cooperativo).

> "EXISTEN 60 COMPAÑÍAS QUE OPERAN EN CIBERSEGUROS EN ESTADOS UNIDOS Y UNAS 10/15 EN EUROPA. ACTUALMETE HAY 3.000 MILLONES DE EUROS EN PRIMAS GLOBALES DE CIBERRIESGO, QUE EN LOS PRÓXIMOS 10 AÑOS PODRÍA ALCANZAR LOS 17.000 MILLONES" (JÉRÔME GOSSÉ)

> "HAY QUE CAMBIAR LA CONVERSACIÓN DE LA SEGURIDAD Y EL CUMPLIMIENTO PARA CENTRARSE MÁS EN LA ESTRATEGIA DE NEGOCIO Y LA GESTIÓN DEL RIESGO" (JOSÉ ESTEVES)

Actualidad aseguradora
España
20/02/17
Prensa: Otra
Tirada: 16.000 Ejemplares
Difusión: 16.000 Ejemplares
Cód: 108731973
Página: 116
Sección: OTROS Área (cm2): 637,0 Ocupación: 100 % Documento: 3/4 Autor: Núm. Lectores: 64000

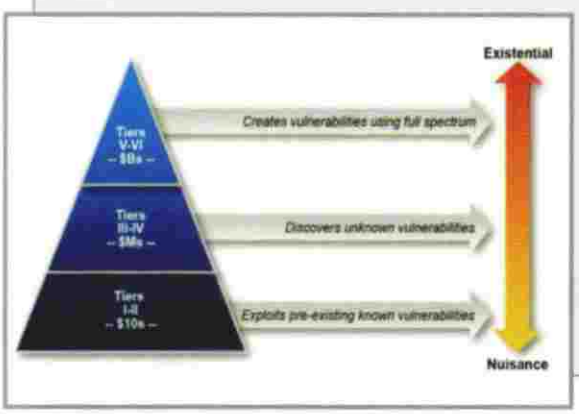
DOS TIPOS DE COMPAÑÍAS: LAS QUE HAN SIDO ATACADAS Y LAS QUE NO LO SABEN

¿Cómo hemos cambiado nuestra forma de enfocar la seguridad? Para **Juan Carlos Crespo, director de la División de Ingeniería, Telecomunicaciones, Ciberseguridad y Analytics de Informática El Corte Inglés**, "nos hemos pasado muchos años intentado proteger nuestros servicios de ciberseguridad, ahora estamos intentando proteger a los usuarios, proteger los negocios por el cambio del paradigma". Para eso -añade- "hemos ampliado a otros stakeholder y también a través de la innovación tecnológica que acelera los procesos. Hemos tenido que crear un servicio de gestión de riesgo continua que nos permita estar al día de todas las amenazas en un sentido proactivo", matiza el directivo.

Según explica, desde la compañía "damos un servicio de mitigación de riesgo, de alerta temprana para anticiparnos a estas amenazas para dar soporte a los posibles riegos de los clientes. No lo hacemos solo en las empresas de banca, sino otras muchas que en la transformación digital han abierto sus protocolos. No obstante, vemos que no es suficiente y apoyamos a los órganos reguladores", asevera Crespo. Ya no tenemos una protección absoluta -añade- tenemos que gestionar nuestro riesgo y además conviene transferir esos riesgos por el bien de las empresas; ahí es donde es esencial el papel del seguro.

LA SEGURIDAD TOTAL ES IMPOSIBLE Y NI SIQUIERA ES DESEABLE

Para **Ignacio Guinea, director Tecnology/Operations Risk en Grupo Santander,** la ciberseguridad en banca es crítica por el propio negocio al que se dedican ya que trabajan con información "incluso el dinero es información". La ciberseguridad no puede tener como objetivo la seguridad total, eso es imposible y ni siquiera es deseable, asevera. Para exponerlo, Guinea habla del Paradigma de la ciudad medieval frente a la moderna, las ciudades hoy en día no se protegen con vallas, sino que los buenos y los malos conviven en el mismo sitio. Puedes tener minivallas, como cámaras de seguridad, policías, y este es el paradigma, ¿cómo enfocamos este paradigma, este desafío? "Nosotros tenemos un modelo basado en seis dimensiones: Identificar, proteger, detectar, responder y recuperar y reportar y gobernar todo esto. Cada una de estas fases tiene sus propios desafíos. Además se incluye todo lo que no conocemos, wifi, páginas web… proteger es en sí un gran desafío, es un juego asimétrico, tenemos que proteger todo y 'el malo' solo debe encontrar un agujero", reconoce el directivo. Dentro de la parte de detectar y recuperar, subraya, "es donde más camino tenemos que recorrer porque o se ha sufrido un ataque o no lo sabes que has sufrido. Todo este esquema en ciberseguro lo vemos en dos sentidos: para entender el ciberseguro que necesitamos y, por otro lado, en la mitigación. No es una estrategia alternativa, sino como parte de este modelo global en el que el seguro forma parte de él".



CLASIFICACIÓN DE ATACANTES

- Tier I y II principalmente explotan vulnerabilidades conocidas: Atacante "amateur"
- Tier III y IV están mejor financiados y tienen un nivel de conocimientos y sofisticación suficiente para descubrir y explotar nuevas vulnerabilidades: Atacante profesional
- Tier V y VI pueden invertir grandes cantidades de dinero (billones) y tiempo (años) para crear nuevas vulnerabilidades en los sistemas, incluyendo aquellos sistemas normalmente bien protegidos: Organizaciones Ciber-Criminales

Actualidad aseguradora
España
20/02/17
Prensa: Otra
Tirada: 16.000 Ejemplares
Difusión: 16.000 Ejemplares
Cód: 108731973
Página: 117
Sección: OTROS Área (cm2): 630,7 Ocupación: 100 % Documento: 4/4 Autor: Núm. Lectores: 64000

JONATHAN KEWLEY, ABOGADO CLIFFORD CHANCE LONDON:
"Los sistemas y protocolos deben modificarse para poder cumplir con las obligaciones de información de la GDPR"

'AA'.- ¿Cómo cree que afectará el Reglamento Europeo de Protección de Datos a la ciberseguridad y a los ciberriesgos?

Jonathan Kewley.- La GDPR es el cambio más importante en cuanto a privacidad de datos y ciberseguridad. Un cambio profundo y bastante llamativo es la exigencia de notificación al regulador dentro de las 72 horas de haber sufrido un ataque serio o en el caso que se haya producido una pérdida de datos. Este es un cambio relevante que implica que los sistemas y protocolos deben modificarse para poder cumplir con los obligaciones de información. Todas las empresas estarán sujetas a un escrutinio mucho más amplio en lo relacionado con sus protocolos de seguridad de datos – en sus políticas y procedimientos- además de en lo relativo a su manera de contratar con terceros para proteger datos y ficheros, y el grado de diligencia con sus proveedores. Es necesario un nivel mucho más elevado de coordinación entre los equipos de la empresa, creando un equipo multidisciplinar.

'AA'.- Una vez que ha ocurrido una violación de la seguridad, ¿cuáles son los vectores legales a cumplir?

Jonathan Kewley.- En el caso de que se produzca un ataque serio la notificación al regulador es la prioridad. Raramente es un ciberataque aislado a un único país o a un único grupo de individuos de una nacionalidad en particular. Esto significa que es probable que se requieran notificaciones coordinadas a través de territorios múltiples y la planificación ante este tipo de incidentes es vital. Una buena *due diligence* interna que identifique la causa principal de la incidencia también será necesaria. Lo importante es que esta investigación post-ataque esté protegida por la confidencialidad legal, consultores externos que no son abogados pueden comprometer esta protección.

'AA'.- Y en el caso de prevención, ¿qué medidas legales se deben implantar para lograr mayor seguridad?

Jonathan Kewley.- Los contratos con proveedores externos, por ejemplo, proveedores de la nube, son un riesgo que hay que cuidar. Si no son visibles los procedimientos de seguridad de los proveedores, el negocio puede estar expuesto. En los contratos entre las partes se deben incorporar las identificaciones apropiadas y prever las notificaciones de posibles ataques. Se debe llevar a cabo una *due diligence* para identificar los posibles riesgos y desarrollar un procedimiento contra los ciberataques que prevea la obligación de notificación al regulador y los pasos a seguir.

> "EL SEGURO NECESITA DESARROLLAR PRODUCTOS MÁS SOFISTICADOS QUE SEAN ÚTILES EN EL CASO DE UN ATAQUE"

'AA'.- ¿Cuáles son las principales dificultades técnicas, legislativas y actuariales?

Jonathan Kewley.- El mayor obstáculo legislativo es el alto nivel de legislación global sobre ciberseguridad. En Europa implica multas de hasta un 4% del total del volumen de negocio de una empresa en el caso de una infracción grave. Hasta la fecha sólo hemos identificado multas de ese nivel en las investigaciones de competencia. La mayoría de las empresas están completamente desprevenidas y, por eso, pueden ser propensas a ser sancionados con multas muy serias que ponen en peligro su reputación. Reducir el riesgo requiere que todos los departamentos de negocio – legal, riesgos, recursos humanos, seguridad informática y comunicación- trabajen juntos para asegurar una respuesta coordinada. Este es un reto enorme para las grandes multinacionales.

'AA'.- ¿Cómo puede ayudar el sector asegurador?

Jonathan Kewley.- Hoy en día, la mayoría de los productos de seguros contienen tantas exclusiones que no cubren el escenario de un verdadero ciberataque. Los ciberataques son un riesgo en evolución y la industria de seguros está, lógicamente, preocupada ante la exposición a un riesgo no cuantificable. El resultado final es que actualmente las empresas tienen pocas opciones en cuanto a la compra de pólizas de ciberseguros. La industria necesita desarrollar productos más sofisticados que sean útiles en el caso de un ataque.