Expansión
miércoles, 22 de noviembre de 2017
Pág: 38
Ocupación: 81,11% Valor: 13.302,21 € Tirada: 38.718 Difusión: 24.981 Audiencia: 136.000

JORNADA EXPANSIÓN

Ciberseguridad: Cómo mitigar el impacto de los piratas informáticos

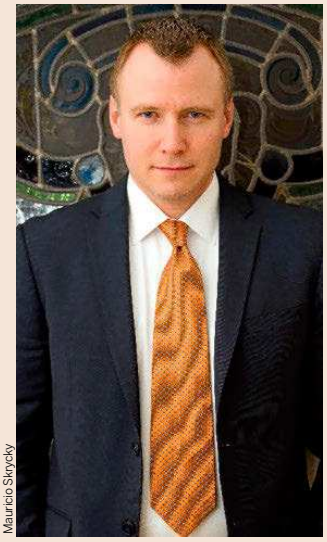
DESAFÍOS/ La digitalización de la economía mundial hace que las compañías deban adoptar medidas para protegerse de los riesgos de ciberataques, apostando por políticas integrales y de colaboración.

DETECCIÓN
Las organizaciones deben detectar **amenazas en tiempo real**, dado que su capacidad de respuesta será decisiva para calibrar los efectos de los ataques.

Jesús de las Casas. Madrid

Hace unos meses, los ataques de *ransomware* Wannacry y Petya sembraron el caos a escala global. Sus virus infectaron los sistemas de cientos de empresas e individuos de todo el mundo. La repercusión de lo ocurrido sacó de nuevo a la palestra el debate sobre la ciberseguridad. En concreto, la obligación de que las empresas desarrollen su capacidad de respuesta ante esta clase de amenazas. Las prácticas más recomendables en este sentido, así como las principales carencias de las compañías españolas, fueron señaladas en el encuentro *Ciberseguridad: Pilar de la economía digital*, organizado por EXPANSIÓN con el patrocinio de FTI Consulting y la colaboración de Hiscox.

"Hoy en día, no hay empresa que no necesite ciberseguridad, porque todas utilizan las tecnologías de la información", recordó Elena García, responsable de empresas y profesionales de Incibe (Instituto Nacional de Ciberseguridad de España). Por suerte, "el nivel de madurez del ecosistema empresarial ha evolucionado mucho en los últimos años", apuntó. Según las encuestas de este organismo, el 70% de las empresas españolas ha revisado recientemente su política de ciberseguridad.


Mauricio Skrycky

Anthony Ferrante, director ejecutivo sénior y director de Ciberseguridad de FTI Consulting.


Pablo Moreno

Alan Abreu, suscriptor sénior y responsable de ciberriesgos de Hiscox España.


Pablo Moreno

Elena García, responsable de Empresas y Profesionales de Incibe.

Un reto integral

"El riesgo cibernético va más allá del aspecto tecnológico y requiere que las distintas áreas de la empresa se involucren y se coordinen entre sí. También tenemos que asumir la transferencia del riesgo como medida complementaria", propuso Alan Abreu, responsable de ciberriesgos de Hiscox España. Asimismo, opinó que el sector asegurador debe colaborar en la formación de sus clientes en las materias más elementales de la ciberseguridad.

"La aproximación que hacemos se centra, por este orden, en los ámbitos de predicción y análisis de riesgos, prevención, detección y respuesta o resiliencia. Uno de los aspectos primordiales es tener los básicos bien cubiertos, porque la inmensa mayoría de los ataques relevantes se producen por carencias de base", señaló Rosa Kariger, 'chief information security oficer' de Iberdrola, que incidió en que la prevención es una labor de todos dentro de la compañía. Kariger imagina un futuro sin disputas internas por quién asume el presupuesto en ciberseguridad, "pues este ámbito estará integrado en el propio diseño y estructura de todos los equipos de las organizaciones".

En la misma línea, "consideramos la ciberseguridad como algo que forma parte de la cultura de la compañía. La diferencia estriba en que, en lugar de poner el foco en el ataque, lo hacemos en el cliente", aseguró Guillermo Llorente, subdirector general de seguridad de Mapfre.

Llorente enfatizó también la necesidad de que exista una mayor cooperación entre todos los actores. "Las empresas queremos ser más partícipes de la sociedad, y por ello somos cada vez más abiertas e interdependientes", apuntó. En definitiva, una mayor transparencia y colaboración puede ayudar a las empresas a protegerse mejor ante los futuros ataques informáticos.

Porque, como recordaron los expertos participantes en este evento, no se trata de si los *hackers* llegarán a atacar a una organización, sino de cuándo lo harán, y de cómo estar lo mejor preparado cuando esto ocurra.

ELENA GARCÍA
Responsable de empresas y profesionales de Incibe

"Todas las empresas necesitan ciberseguridad, porque hoy en día todas utilizan las tecnologías de la información"

ENRIQUE ÁVILA
Director del Centro Nacional Excelencia Ciberseguridad

"Una opción para poder controlar la ciberresiliencia a largo plazo sería implantar una identidad digital"

EDUARDO ARRIOLS
'Manager' del servicio Red Team de Innotec

"Las compañías tienen que mejorar su capacidad para detectar las amenazas a nivel interno"

ALBERTO LÓPEZ RUIZ
Director de operaciones de ciberseguridad de Minsait

"Las aproximaciones tradicionales para la estimación de riesgo no son suficientes, porque hoy hay más variables"

GUILLERMO LLORENTE
Subdirector general de seguridad de Mapfre

"Consideramos que la ciberseguridad es algo que forma parte de la propia cultura de la compañía"

ANTHONY FERRANTE
Director ejecutivo sénior de FTI Consulting

"La ciberresiliencia es un enfoque estratégico desde las empresas para identificar y responder a amenazas críticas"

ALAN ABREU
Responsable de ciberriesgos de Hiscox España

"Estos riesgos van más allá del apartado tecnológico y requieren que todas las áreas de la empresa colaboren"

KAREN GAINES
Responsable de 'enterprise cybersecurity' de Microsoft

"La nube mejora el nivel de seguridad, siempre que las empresas conozcan qué información manejan"

ROSA KARIGER
'Chief information security officer' de Iberdrola

"La mayoría de los ataques relevantes se producen por carencias básicas en la seguridad de las empresas"

Resiliencia

Esa preparación toma el nombre de ciberresiliencia. "Hay tres fases clave a la hora de encarar un ciberataque: la preparación, la respuesta y la resiliencia. Esta última es el elemento más crítico de esta ecuación, porque permite a las compañías recuperarse con eficiencia", afirmó Anthony Ferrante, director ejecutivo senior de FTI Consulting.

Ferrante se refirió a la importancia de que las compañías aprendan acerca de "los adversarios potenciales a los que se enfrentan, que son diferentes en función del sector. Por ejemplo, un Gobierno podrá enfrentarse a activistas o ciberterroristas, mientras que un banco se enfrentará probablemente a actores con motivaciones financieras".

A pesar de la creciente concienciación, "pocas organizaciones en España conocen realmente su capacidad de dar respuesta a una amenaza", subrayó Eduardo Arriols, manager del servicio Red Team de Innotec. Esta compañía se dedica a realizar simulaciones reales y determinar la habilidad de una organización para detectarlas. Las compañías necesitan incrementar su capacidad para detectar las amenazas a nivel interno", confirmó.

"La clave es actuar hacia dentro y hacia fuera. Los despliegues analógicos también son necesarios para tener ciberresiliencia, para no depender siempre de la tecnología. Por otra parte, una opción para poder controlar este fenómeno a medio y largo plazo sería la implantación de una identidad digital, tanto para las personas físicas como jurídicas", propuso Enrique Ávila, director del Centro Nacional de Excelencia en Ciberseguridad. Este centro es el responsable de formar a fuerzas y cuerpos de seguridad del Estado y al mando conjunto de ciberdefensa.

"Las aproximaciones más tradicionales de estimación de riesgos no son suficientes, porque todas las variables del contexto influyen e introducen nueva información. No podemos limitarnos a procesos formales sino que debemos complementarlos con procesos técnicos", según Alberto López Ruiz, director de operaciones de ciberseguridad de Minsait, la unidad de transformación digital de Indra.

En cuanto al *cloud*, ¿supone una ventaja o una desventaja en términos de ciberseguridad? Desde Microsoft defienden lo primero. La clave, para Karen Gaines, responsable regional de *enterprise cybersecurity group* de la multinacional de Windows, radica en que las organizaciones conozcan cuál es la información más relevante de la que disponen. A partir de ahí, fabricantes tecnológicos como Microsoft trabajan para "proporcionar a los clientes una plataforma lo más segura posible", aseguró.