Evento patrocinado por

NECSIA

CICLO DE DESAYUNOS FUNDACIÓN ASTIC 2013

¿Podemos responder a las expectativas de ciberseguridad de los ciudadanos?

POR MAOLE CEREZO
Fotos de Aitor Diago

En el desayuno de trabajo celebrado el pasado mes de mayo para abordar el tema de la ciberseguridad, la Directora General de Necsia, Pilar Balcells, se refirió a la presentación del informe anual de los peligros a los que se enfrenta Estados Unidos, en la que el director de la Oficina de Inteligencia Nacional, James Clapper aseguró que "la rapidez con la que el mundo está aplicando tecnologías digitales es mayor que nuestra capacidad para entender las implicaciones que se puedan derivar para nuestra seguridad y para tratar de mitigar los nuevos riesgos".

En este contexto, señaló, "los ataques y el espionaje informático se han convertido en la principal preocupación de las distintas agencias de inteligencia y de seguridad de EEUU, sustituyendo por primera vez al terrorismo internacional en la lista de amenazas del país".

A su vez, apuntó Balcells, el secretario de Estado de Telecomunicaciones, Víctor Calvo-Sotelo, afirmó que "España necesita un sector de ciberseguridad y ciberdefensa fuerte, que sea capaz de innovar, de tener un desarrollo sostenible, de competir internacionalmente por su especialización y sus profesionales". Para ello, y como método de prevención antes de ser ciberatacados, "deberíamos tener un plan creíble, verdadero y sincero, que nos permita seguir desarrollando nuestros sueños como sociedad. Un plan

como el propuesto por la ISO27001 mediante una aproximación holística sobre procesos, infraestructuras (tecnológicas y no tecnológicas) y personas" recalcó la directora general de Necsia, empresa referente en el área de Seguridad, destacando en la Continuidad de Negocio y en Sistemas de Gestión de Seguridad de la Información. Como recordó, nació en 2005 con capital 100% español y cuenta con una plantilla que supera las doscientas personas, entre las que figuran más de treinta consultores de seguridad certificados y que trabajan principalmente en gran cuenta. Entre algunas de ellas se encuentra Privalia, el primer club privado de venta on line, que se presentó como caso de éxito en el desayuno de trabajo.

Al hilo de lo expuesto anteriormente, Rocío Montalbán, Subdirectora General Adjunta de TICs del Ministerio de Industria, comenzó su moderación reafirmando que, efectivamente, los principales gobiernos del mundo, ante las últimas oleadas de ciberataques y fugas de información que están teniendo lugar, están muy concienciados de la necesidad de asegurar su información.

Para ello, según Rodrigo Jiménez, Responsable de Seguridad de la Información de Necsia, hay que partir de los "círculos de confianza", como modelo al que se llega a través de tres grandes cuestiones que buscan explicar el qué, el cómo y el porqué de los ciberataques. De este modo, "interesa definir, en primer lugar, qué nos interesa proteger, identificando dentro de los inventarios de activos aquéllos que se deben considerar críticos". A continuación sería necesario determinar el cómo en las dos vertientes del problema: Por un lado, "investigando el modo en que se materializan las amenazas, sumando a la dificultad de su gran diversidad las continuas mutaciones que experimentan. Entre las técnicas de ciberataque más habituales destaca en estos momentos el phishing dirigido, que tiene lugar a través de un e-mail que suplanta el origen del correo, ofreciendo un link tras el cual se oculta un troyano que permite al atacante tomar el control de la máquina". Por otro lado, y como segunda vertiente, "estudiando cómo protegernos". Y, por último "abordando el porqué de los ciberataques". Daniel Sainz, Consultor de Seguridad de la Información en la Oficina de Seguridad implantada en Privalia.

Adicionalmente, y "como una parte más del problema, debemos considerar la existencia de las llamadas redes oscuras, integradas en Internet pero no detectables por medios convencionales, y que tienen una especial importancia en la distribución del material obtenido por los ciberdelincuentes". Es el caso de la red TOR, "que asegura el anonimato y permite el establecimiento de servicios de venta on line mediante pago en bitcoins".

También "debemos tener claro por qué hemos de defendernos. Poniéndonos del lado de quienes sufren los ataques observaremos que pueden darse diferentes motivaciones y que, en función de las mismas, pueden abordarse las tareas de protección con distintos esfuerzos y de forma más o menos rigurosa".

Caso de Privalia

Daniel Sainz, Consultor de Seguridad de la Información en la Oficina de Seguridad implantada en el cliente, explicó cómo Privalia, presente en Europa y Latinoamérica, "es una empresa con una fortísima dependen- »


Albert Valls de Necsia y Bartolomé Bauzá del Estado Mayor de la Armada


Carlos Turmo de OEPM y Daniel Sanz de Necsia


Eugenio Gómez del Ministerio de Empleo Fernando Martín del Tribunal de Cuentas


Fernando Morón de Informática de la Casa Real y Francisco Alonso del Ministerio del Interior


Francisco J. Matarrubia d ela AEAT e Ignacio Bellido


Ignacio Cudeiro del Ministerio de Economía y Javier de la Cal del Ministerio de Defensa


Jorge Navas de la IGAE y Jose A. García del Ministerio de Hacienda


José R. García de la Biblioteca Nacional y Manuel Alonso de la IGAE

cia tecnológica, y cuyo grado de externalización de servicios implica depositar una gran confianza en sus proveedores de TI". Su mayor activo, como empresa de comercio electrónico, "lo constituye la base de datos de socios, siendo tres sus principales fuentes de amenazas: los ataques de denegación de servicio, las fugas de información y la gestión de la disponibilidad de los servicios críticos para la compañía".

Respecto a la primera de las fuentes, comentó que "cada vez se generan mayores ataques a través de técnicas cuya evolución les lleva a conseguir efectos cada vez mayores empleando recursos mínimos". Como protección frente a esta amenaza "se suele situar una red de distribución de contenidos entre los clientes y los servidores, que absorbe las peticiones que ocasionan exceso de tráfico". También "se pueden establecer mecanismos de diferenciación entre los tráficos legítimo e ilegítimo, éste a menudo automatizado, o utilizar técnicas de geolocalización, con el fin de limitar el tráfico restringiendo determinados accesos".

Por su parte, "las fugas de información tienen lugar tanto por accesos externos no autorizados como por abuso en la utilización de sus privilegios por parte de los usuarios internos y los administradores". En el caso de Privalia, "los datos de sus socios, que incluyen los de sus tarjetas de crédito, constituyen el activo fundamental de la empresa, y requieren el máximo nivel de protección".

Y en lo que se refiere a la posibilidad de afectar a la disponibilidad de servicios críticos, la organización "ha de tenerlos convenientemente identificados, con el fin de planificar esfuerzos tendentes a redundar infraestructuras y servicios relacionados, estableciendo procedimientos de actuación para el supuesto de no disponibilidad". Desde la oficina de seguridad "se aprecia cómo, de forma continua, evolucionan las modalidades de ataque a través de la red. Se observa que, alrededor del 30% de los ataques, vienen dados por intentos de acceso a directorios de Windows, así como una proliferación de los llamados "sistemas araña", que intentan obtener información de terceros de forma automatizada".

Conciencia del peligro

Si bien, para Rocío Montalbán, los círculos de confianza aportan ventajas, "su establecimiento y difusión comunican una imagen de existencia de riesgos a veces poco tranquilizante". En opinión de Rodrigo Jiménez, "continuamente se polemiza acerca de la conveniencia de hacer públicos los incidentes de seguridad. En realidad, este problema se afronta con ópticas distintas según las diferentes zonas culturales. En el caso del Sur de Europa, por ejemplo, los incidentes se ocultan por regla general, a diferencia de lo que se suele hacer en los países escandinavos". Por su parte, Bartolomé Bouza, de la Armada, puntualizó que "por parte de amplias capas de la sociedad existe una baja percepción del riesgo, por lo estéticamente incruento de los ciberataques, a pesar de que puedan estar promovidos por ciberterroristas".

A la vez, Daniel Sainz hizo hincapié en que "en las comunicaciones que se generan a raíz de los incidentes de seguridad hay que tener en cuenta la responsabilidad en que se puede incurrir frente a terceros, lo que motiva que la notificación de incidentes se esté empezando a imponer como práctica habitual". Ello se desarrolla "en la propuesta de

reglamento de Protección de Datos y en la propuesta de Directiva de Seguridad de la Información en las Redes, que contemplan la notificación de los incidentes considerados graves".

El principal problema en materia de seguridad, según Francisco Alonso, del Ministerio del Interior, viene dado "por una falta general de concienciación, a pesar de que la seguridad en las TIC se viene abordando por parte de la Administración desde 2007". Sin embargo, "no se ha trabajado en la sensibilización de los ciudadanos". En este sentido, "el Esquema Nacional de Seguridad supone un gran paso".

José Antonio García, del Ministerio de Hacienda, apuntó que "la sensibilización del personal directivo de la administración tendrá que seguir la misma tendencia que experimentada por los directivos de las organizaciones privadas".

Es importante reseñar que, "las empresas jóvenes y con mayor porcentaje de personal menor de treinta y cinco años registran políticas distintas respecto a cuestiones como la conexión a servicios no corporativos, incluso en algunos casos de carácter lúdico". Empresas más arraigadas, por contra, "cortan radicalmente el acceso a dichos servicios, aunque se contemplen excepciones que, en general, dependen de la visión personal del responsable", matizó el Responsable de Seguridad de la Información de Necsia

A la vez, Jorge Navas, de la IGAE, comentó que en de las auditorías de seguridad que se llevan a cabo en organismos públicos, por lo general, "se comienza por una reunión con el personal directivo del organismo en cuestión, que es quien tiene que establecer y asumir las políticas de seguridad", observándose en la mayoría de las ocasiones "que la principal preocupación viene dada por todo aquello relacionado con el cumplimiento de la LOPD, por sus importantes repercusiones". Navas suscribió que "el obligado cumplimiento del Esquema Nacional de Seguridad generará una mejora de las políticas".

Pero Carlos Gómez, del Ministerio de Empleo, advirtió que "el paulatino incremento del uso de la administración electrónica por parte de los ciudadanos, así como su progresiva incorporación a la toma de decisiones a través de dicho canal, podría dar lugar a que el Esquema Nacional de Seguridad se quede corto".

Sin embargo, Miguel Ángel Amutio, del Ministerio de Hacienda, puntualizó que "la entrada en vigor del Esquema nacional de Seguridad debe impulsar un cambio de mentalidad en la Administración, que debe predicar con su ejemplo ante los ciudadanos, liderando el empleo de buenas prácticas y adoptando medidas organizativas tendentes a minorar los riesgos y a garantizar la continuidad". También "debe concienciar a los ciudadanos a través de la educación".

La implantación del Esquema Nacional de Seguridad, Rocío Montalbán la percibe compleja, interesándose por conocer la opinión de la empresa privada. Para Necsia, "en España las PYMES casi no destinan recursos a seguridad y, en las grandes empresas, la inversión depende mucho del sector". Para Rodrigo Jiménez, "una mayor regulación se corresponde con mayores medidas de seguridad, mayor control vía auditorías y mejor asunción de la influencia de la seguridad en la cuenta de resultados". En todo caso, "la propia sociedad terminará por generar una fuerte demanda en materia de seguridad".


Manuel G. de Vaz del Ministerio de Fomento y Miguel A. Amutio del Ministerio de Hacienda


Miguel A. Rodríguez del Ministerio de Industria y Pedro Varela del Ejército de Tierra


Pilar Balcells de Necsia y Rafael Santos del Ministerio de Fomento


Rocío Montalbán del Ministerio de Industria y Rocío Tuda de Necsia

En esta línea, Ignacio Cudeiro, del Ministerio de Economía, expuso que "el centro de la seguridad lo constituyen las personas, dado que son la principal fuente de riesgo". En cuanto a las organizaciones, "en unos casos prima la eficiencia y en otros la seguridad, dependiendo estas posiciones de múltiples factores". Evitar fugas de información depende, principalmente, "de la cultura y de la formación de las personas". En todo caso, "no se pueden transferir responsabilidades si los riesgos no se asumen de forma adecuada por parte de los directivos".

Para concluir, salió a colación el caso concreto del procedimiento de solicitud de marcas, poniendo sobre la mesa si la seguridad podría, a su vez, convertirse en un freno para el acceso. En la solicitud de marcas, como relató Carlos Turmo, de la Oficina de Patentes, los ciudadanos acceden a un sistema de certificados que gestiona el 60% de las solicitudes y en el proceso se detecta que un 40% de ellas corresponden a personas que no tienen capacidad para utilizar un certificado electrónico". Ante esto, cuestionaba si no sería posible dar el servicio sin extremar tanto las medidas de seguridad, de forma que no se convirtieran en un inhibidor de acceso de un gran número de ciudadanos. ❋

Rodrigo Jiménez de Necsia y Román Díez de la AEAT

Santiago Luna del Ministerio de Defensa