CincoDías

Publicación	Cinco Días General, 10	Fecha	20/12/2021
Soporte	Prensa Escrita	País	España
Circulación	30 782	V. Comunicación	44 345 EUR (49,835 USD)
Difusión	21 772	Tamaño	504,37 cm² (80,9%)
Audiencia	38 000	V.Publicitario	8781 EUR (9868 USD)

Desayuno **CincoDías**

La ciberseguridad, un puzle en el que muchos tienen que aportar piezas

Compartir información de ataques en tiempo real puede marcar la diferencia entre un leve incidente de seguridad informática y un desastre

CINCO DÍAS
MADRID

Los costes provocados por la ciberdelincuencia alcanzaron los 5,5 billones de euros en 2020, el doble que en 2015, según datos del Parlamento Europeo. Fue el año de la irrupción de la pandemia del Covid-19 y, por tanto, el de una aceleración imprevista y brusca del proceso de digitalización de la sociedad, con los riesgos que conllevó.

Pero ese impacto tan específico no significa que la preocupación por la ciberseguridad vaya a dejar el primer plano con el paso del tiempo. Más bien al contrario: según el informe *Digital Trust Survey 2022*, de la firma de servicios profesionales PwC, el 70% de las empresas españolas prevé aumentar sus presupuestos de ciberseguridad en el año entrante.

Y no es solo una cuestión corporativa. Ciudadanos y Gobiernos están directamente concernidos por una amenaza poliédrica que puede desde costar unas decenas de euros por un ataque poco sofisticado de *ransomware* (secuestro de datos) hasta paralizar las infraestructuras básicas de todo un país.

CincoDías, en colaboración con Abanca, organizó en torno a estas cuestiones la mesa redonda *El factor humano en la ciberseguridad: formación y talento para protegerse en un mundo conectado*. Como ponentes, Mar España, directora de la Agencia Española de Protección de Datos (AEPD); Elena Maestre, socia responsable de ciberseguridad en *consulting* de EY España; Roberto Baratta, director de prevención de pérdida, continuidad de negocio y seguridad de Abanca, y el teniente coronel Juan Sotomayor, jefe del departamento contra el cibercrimen de la UCO (Unidad Central Operativa) de la Guardia Civil, coincidieron en la necesidad de mejorar y reforzar la comunicación y coordinación entre organismos públicos y privados para luchar con más eficacia contra el cibercrimen.

Elena Maestre, socia responsable de ciberseguridad en *consulting* de EY España; Mar España, directora de la Agencia Española de Protección de Datos (AEPD); Roberto Baratta, director de prevención de pérdida, continuidad de negocio y seguridad de Abanca, y el teniente coronel Juan Sotomayor, jefe del departamento contra el cibercrimen de la UCO (Unidad Central Operativa) de la Guardia Civil. PABLO MONGE

El valor de la colaboración

Dicen los expertos en ciberseguridad que solo hay dos tipos de organizaciones: las que ya han sufrido un ciberataque y las que lo van a sufrir. No hay, en consecuencia, nada vergonzante en pasar por esa situación, pero sin embargo la mayoría de empresas son reticentes a compartir información sobre los ataques que han sufrido, según expusieron los ponentes. Y es un problema, porque las alertas tempranas son básicas para parar ataques o minimizar sus daños.

"Necesitamos más colaboración público-privada", recalcó Maestre, de EY, "pero nos encontramos con reticencias enormes, en todos los ámbitos, a compartir información". Levantar la mano y reconocer el problema supone todavía cierto estigma reputacional, y también puede faltar clarividencia: "Muchas empresas se miran el ombligo, sin compartir información. No se dan cuenta de que, si ayudan, serán ayudadas", señaló Mar España. "Si España quiere jugar en la primera liga de la ciberseguridad, tiene que compartir la información de los ataques de forma inmediata, y no está pasando", añadió el teniente coronel Sotomayor.

Las organizaciones especializadas en este ámbito, en España particularmente Incibe (el Instituto Nacional de Ciberseguridad), pueden mitigar esos problemas de comunicación, ejerciendo de nodo de alerta, prevención y conocimiento ante los ataques. Pero en opinión de Baratta, de Abanca, sería necesario otro esquema colaborativo, más dinámico y completo: "Incibe no funciona para nuestras necesidades, y habría que reforzar el intercambio en tiempo real de la información. Mi sueño es un organismo como Cirbe [Central de Información de Riesgos del Banco de España]: si los bancos compartimos allí toda la información sobre el crédito de una persona, ¿por qué no algo parecido con la ciberseguridad?".

Más privado, más seguro

Si una cadena es tan fuerte como su eslabón más débil, una organización es tan cibersegura como su empleado más despistado en estas cuestiones, y más tras el auge del teletrabajo –y el consiguiente aumento del perímetro a defender– que trajo la pandemia. Como explicó Baratta, los ciberdelincuentes están aprovechando esos puntos débiles, con ataques de ingeniería social sofisticados y muy dirigidos, nacidos a partir de fugas de información. "Logran información personal valiosa que les sirve para armar ataques directos. Y esa información valiosa surge de problemas de privacidad en la gestión de los datos", aseguró.

No solo los empleados pueden abrir la puerta de la empresa a los ciberdelincuentes, contactados por una fuga de información personal y engañados por una interfaz prácticamente

El 70% de las firmas españolas prevé aumentar sus presupuestos de ciberseguridad en 2022

Un empleado puede ser usado como cebo para un ataque directo y sofisticado a una empresa

CincoDías

Publicación	Cinco Días General, 11	Fecha	20/12/2021
Soporte	Prensa Escrita	País	España
Circulación	30 782	V. Comunicación	44 345 EUR (49,835 USD)
Difusión	21 772	Tamaño	540,60 cm² (86,7%)
Audiencia	38 000	V.Publicitario	9227 EUR (10 369 USD)

“Los problemas ocurren; hay que asumirlo. Por eso es clave la detección rápida y coser mejor todas las herramientas que tenemos para defendernos”

ROBERTO BARATTA, DIRECTOR DE PREVENCIÓN DE PÉRDIDA, CONTINUIDAD DE NEGOCIO Y SEGURIDAD DE ABANCA

“Es fundamental compartir la información, y se puede hacer sin afectar a la privacidad. Aun así, algunas operadoras y bancos nos ven como enemigos”

JUAN SOTOMAYOR, TENIENTE CORONEL. JEFE DEL DEPARTAMENTO CONTRA EL CIBERCRIMEN DE LA UNIDAD CENTRAL OPERATIVA (UCO) DE LA GUARDIA CIVIL

“La ciberseguridad ya no es solo una preocupación de los ámbitos técnicos. Ha subido al nivel de los CEO y debe formar parte del ADN de las empresas”

ELENA MAESTRE, SOCIA RESPONSABLE DE CIBERSEGURIDAD EN ‘CONSULTING’ DE EY ESPAÑA

“Privacidad y ciberseguridad han de ir de la mano. Y, como nos ocurre con la salud, solo las valoramos cuando las perdemos”

MAR ESPAÑA, DIRECTORA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

idéntica a la de su organización. El mismo esquema se repite con los clientes, y “por eso, como banco, tenemos también que proteger su información. Si no, estaríamos retroalimentando esos ciberataques”, reconoció el directivo de Abanca.

Privacidad y ciberseguridad son, en consecuencia, dos caras de la misma moneda, como resaltó Mar España, de la AEPD: “Deben de ir de la mano, con un enfoque integral”. Y mejorar en ambos ámbitos requiere de una mayor concienciación, en el terreno personal y en el profesional. “Tanto empresas como instituciones públicas están esforzándose en este ámbito y se está avanzando, pero todavía falta por recorrer”, opinó al respecto Maestre, de EY.

Concienciación... y más

La conciencia de la seriedad del problema puede ser individual, pero las soluciones han de ser colectivas, incluso traspasando las fronteras nacionales, un concepto que no manejan los ciberdelincuentes.

Sotomayor, de la Guardia Civil, resaltó la necesidad de armar esquemas complejos pero ágiles, que incluyan cambios legales y estructuras judiciales supranacionales. “El Poder Judicial debería crear una nueva jurisdicción de instrucción de incidentes de ciberseguridad”, reclamó. Y se necesita colaboración de muchos agentes, como de la Secretaría de Estado de Telecomunicaciones, para perseguir mejor las llamadas fraudulentas que piden datos y contraseñas mediante engaños.

Con un entorno tan complejo, hay que situar la responsabilidad individual en su justo término: “El error más grande en el que estamos cayendo es poner la responsabilidad en el usuario final”, defiende de Sotomayor. Y advierte de los límites de la estrategia de la concienciación: “La DGT [Dirección General de Tráfico] hace un gran trabajo en eso, pero si han ido bajando los muertos en carretera ha sido también porque se ha invertido en infraestructuras, por las sanciones, por la regulación... No hay que cargar toda la responsabilidad en los ciudadanos”.

Maestre también apuntó a la importancia de las normas: “Aunque nos quejemos de ellas, la regulación hace mucho por mejorar el sistema, como hemos visto en el sector bancario”. “Los reglamentos ayudan a que no nos relajemos”, agregó Baratta.

Todo este contexto, tan complejo y demandante, está obligando a las empresas a invertir en talento especializado en ciberseguridad. Y no es nada sencillo, pues faltan profesionales y además están muy cotizados.

Como se expuso en el panel, en el nicho del mercado laboral de los expertos en ciberseguridad se ha producido una tormenta perfecta. Por un lado, se necesita una formación específica y compleja; no hay una oferta académica completa, pues se empezó a desarrollar hace unos años y apenas ahora empiezan a surgir las promociones formadas; además, la pandemia, según señaló Maestre, “ha provocado un aluvión de reclutamiento internacional, que ofrece mejores sueldos sin la necesidad siquiera de cambiar de ciudad”.

Perfil profesional

Mientras, está cambiando el perfil profesional de los expertos en ciberseguridad. Antes, era una profesión más vocacional, a la que llegaban expertos en tecnología y programadores tras un proceso de formación casi siempre poco estructurado. “Era como estudiar Medicina y ponerse a ejercer sin tener el MIR”, comparó Baratta. Así que ahora se buscan perfiles más específicos ya desde la formación, aunque, como advirtió el ejecutivo de Abanca, “no es necesario que todos los responsables de ciberseguridad sean superingenieros”. La Formación Profesional aparece como una alternativa importante; en esta línea, el Consejo de Ministros aprobó el año pasado dos nuevos títulos de especialización en ciberseguridad, en las ramas de Informática y Comunicaciones y Electricidad y Electrónica.

Por tanto, el reto de la ciberseguridad tiene suficientes frentes e importancia de sobra para ser afrontado, de forma estratégica, en los niveles más altos de la dirección de la empresa, como reclamaron desde EY. Solo con entornos digitales lo más seguros posible se podrá establecer una digitalización basada en la confianza, que permita las nuevas formas de trabajar y colaborar entre organizaciones que se han generalizado con la pandemia. La alternativa es mirar hacia otro lado, pero la realidad de los riesgos de ciberseguridad acabaría por imponerse, y con peores resultados para la empresa.

La estructura judicial y policial está anclada a los territorios, pero el ciberdelincuente no tiene fronteras

Faltan perfiles especializados y la oferta académica era hasta hace poco muy insuficiente

Un reto también social

► **Adolescentes y niños.** La ciberdelincuencia es solo uno de los retos a los que se enfrentan los niños y los adolescentes al entrar en los entornos digitales. Necesitan, por tanto, una formación básica y concienciación, también sobre peligros como el ciberacoso y la llamada “sextorsión”. La Ley Orgánica de Protección de Datos, aprobada en diciembre de 2018 y que derogaba la de 1999, convirtió esta necesidad en una obligación legal en su artículo 83, que establece el derecho a una educación digital: “El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales”.

► **Conversaciones familiares.** Mar España, de la AEPD, recalcó la importancia de que los padres sean conscientes del paso que dan sus hijos al entrar en el mundo digital. “Les advertimos de los riesgos cuando empiezan a conducir con 18 años, pero les damos un móvil con 10 años, lo que es una barbaridad, y no se les conciencia de los problemas que puede suponer dar un clic”, se sorprendió. Un problema añadido es que es muy difícil que los menores de edad presten atención a los mensajes de advertencia que les puedan llegar desde empresas e instituciones.

► **También la empresa.** En un mundo en el que las fronteras entre trabajo y familia son más porosas, las empresas también tienen su papel en este ámbito. Las mejores prácticas contienen jornadas formativas, en la propia compañía, que incluyen a los hijos de los empleados. En el extremo contrario también se han llegado a dar casos de situaciones de ciberacoso a menores a través de teléfonos móviles corporativos, con los consiguientes riesgos legales.