Texto L. Bonilla
Fotografía Santiago Ojeda
Vídeo Jorge Pariente

LOS RESPONSABLES DE SEGURIDAD TIENEN VARIOS CAMPOS DE BATALLA ABIERTOS

Los CISO se quejan de poca cooperación y presupuestos

Un año más, Computing ha organizado un encuentro con algunos de los máximos responsables de Seguridad de compañías privadas y representantes de Administraciones Públicas para conocer cuáles son sus mayores prioridades y desafíos, teniendo en cuenta la vital importancia de la ciberseguridad, una asignatura pendiente a todos los niveles.

Una de las más reveladoras conclusiones apunta a que los CISO no sienten tanto temor ante nuevas amenazas como puede ser el ransomware, sino miedo a la falta de formación y desconocimiento tanto de usuarios como de directivos, así como unos todavía escasos presupuestos que les limitan en su capacidad operativa. Pero además, encuentran muy beneficioso poder lograr una unión para compartir experiencias y cooperación en una lucha que les es común. Se trata de una unión que podría ser muy útil incluso entre compañías que compiten entre sí.

"Estamos viviendo un interesante momento de evolución en el mundo de la seguridad, que es un reto diario. Se añade una nueva vertiente de ciberseguridad que implica nuevos y más re-

Manuel Fernández,
Banco Inversis

Javier Candau,
Centro Criptológico Nacional

Edwin Blom,
FCC

Manuel Barrios,
IECISA

Alberto Hernández,
Incibe

Antonio Calzada,
Instituciones Penitenciarias

Antonio Abellán,
director comercial de Check Point

La seguridad es dinámica: los ataques mutan. La información entrante y saliente debe quedar protegida, pero también es importante poder anticiparse a los ataques

Melchor Sanz,
technology and solutions presales manager de HP Inc.

Como fabricante, debemos garantizar la seguridad. Nos gusta proteger dispositivos como las impresoras, que suelen ser las grandes olvidadas

tos", piensa Antonio Abellán, director comercial de Check Point. Para el ejecutivo, "hoy la seguridad es dinámica: los ataques mutan. Ya no solo nos preocupa que no entren en nuestro castillo, sino que la información entrante y saliente quede protegida, marcando todos los parámetros necesarios para gestionar la información, y también anticiparse e interpretar los ataques antes de que se produzcan. La cantidad de puertas abiertas nos obliga a buscar soluciones para todo". Adicionalmente, Abellán aprovecha para dar las claves de la oferta de su compañía, "llevamos dos años ajustando nuestros productos para adaptarlos a la nube. Creemos también que debemos ofrecer proyectos abiertos y trajes a medida en función de las necesidades y la problemática del negocio. No queremos estandarizar, sino personalizar".

Por su parte, Melchor Sanz, technology and solutions presales manager de HP Inc., también está de acuerdo con las afirmaciones anteriores, pero añade la importancia de dotar de seguridad a los dispositivos, y más concretamente a algunos grandes olvidados como pueden ser las impresoras. "Como fabricante, tenemos una gran responsabilidad para garantizar la seguridad. Nos gusta proteger este tipo de dispositivos, como las impresoras, porque facilitamos las herramientas de gestión y monitorización necesarias para evitar agujeros de seguridad y una posible usurpación de la identidad, por ejemplo". Sanz insiste en la necesidad de securizar las impresoras, porque "muchas veces no sabemos dónde se queda guardada la información, si se puede borrar, etc. porque los hackers saben buscar el eslabón más débil de la cadena: dan por hecho que un servidor está protegido, pero no tanto los dispositivos periféricos".

Tampoco se quiso perder el encuentro Carlos Borja, responsable de soluciones de Ciberseguridad de Informática El Corte Inglés, que aportó su visión como integrador. "Yo añadiría a lo anteriormente comentado la cantidad de normativas de obligado cumplimiento. Igualmente, la movilidad puede ser un problema añadido". En ese sentido, Carlos Borja confirma que "nosotros nos sentimos cómodos porque tenemos más de 20 años de experiencia en el ámbito de la seguridad. Tenemos igualmente un perfil de compañía de desarrollo, por lo que nos sentimos cómodos y capacitados para ayudar a nuestros clientes a abordar la gestión del riesgo, porque pensamos y entendemos las necesidades de cada negocio para acompañarles

Carlos Borja, responsable de soluciones de Ciberseguridad de Informática El Corte Inglés

Es enorme la cantidad de normativas de obligado cumplimiento para los CISO. Igualmente, la movilidad puede ser un problema añadido

Bosco Espinosa de los Monteros, key presales manager de Kaspersky

Hay que olvidarse de la seguridad tradicional e ir más allá: no sirve solo con asegurar el endpoint y el perímetro, sino todo en su conjunto

en el camino".

Mientras tanto, Bosco Espinosa de los Monteros, key presales manager de Kaspersky, tampoco se quiso perder el encuentro, destacando de su compañía que "llevamos más de 20 años luchando contra el cibercrimen, y es verdad que hay muchos elementos que suelen ser los grandes olvidados a la hora de protegerlos (puntos de venta, ATM en bancos, máquinas de vending…) de las que nadie se suele preocupar, pero con el auge del Internet de las Cosas, hay que tenerlo en cuenta más que nunca". Para Espinosa, igual de importante es tener en cuenta a los usuarios. En ese sentido, su formación es un imperativo. "Hay que olvidarse de la seguridad tradicional e ir más allá: hoy todas las empresas implantan medidas, pero sin los usuarios, de nada sirve: ya no basta con solo asegurar el endpoint y el perímetro, sino todo en su conjunto".

Adicionalmente, Domingo Cardona, Chief Operations Officer de Wise Security Global, asegura que lo importante es tener mucho más en cuenta a las pequeñas y medianas empresas. "La pyme suele estar muy desatendida en el ámbito de la ciberseguridad. Creemos que los grandes proveedores no siempre pueden ofrecerles soluciones adaptadas a su tamaño", confirma. En ese sentido, es importante contar con "soluciones paquetizadas de vigilancia y disuasión: vigilar porque en pyme nadie suele hacerlo, y disuadir porque también hace falta cumplir con las normativas de privacidad", añade Cardona.

A grandes males, grandes remedios

¿Cuáles son los principales problemas de los Chief Information Security Officer? Javier Candau, jefe del departamento de Ciberseguridad del Centro Criptológico Nacional, asegura que, en primer lugar, lo que más preocupa es el cumplimiento normativo. Pero además, "la labor del CISO es cada vez más difícil, ya que la seguridad siempre ha tenido una difícil justificación en las empresas, por lo que suele tener limitaciones de recursos", señala. Se añade como un problema adicional la nube y los dispositivos móviles, elementos que "dificultan la capacidad de control y vigilancia", de acuerdo con Candau. Y es que "tenemos un desequilibrio entre la capacidad ofensiva del atacante con respecto a la capacidad defensiva, algo que se soluciona con el compromiso e implicación de la dirección: gastar en seguridad lógica debería ser igual que gastar en seguridad física, y de ello deben ser conscientes las compañías", opina.

Resulta curioso que en 2017 se siga debatiendo sobre la necesidad de incrementar los presupuestos en seguridad, una partida que, dado el aumento de los riesgos y amenazas, debería prácticamente darse por hecha. Sin embargo, "el presupuesto sigue siendo un factor muy importante", admite Edwin Blom, CISO de FCC, quien añade que "aún estamos saliendo de la crisis y presupuesto para seguridad no hay mucho: necesitamos más, y para mí como CISO sigue siendo un reto importante", explica.

Algo muy similar ocurre en la Administración Pública. Así lo afirma Rafael Santos García, portavoz ministerial, quien señala que "el problema, además, es que no hay una adecuada concienciación, tampoco al más alto nivel directivo. Pero lo más grave es que cada uno se defiende como puede: en la Administración deberíamos empezar a trabajar de la forma más coordinada y eficiente posible. La tendencia lógica debería ser colaborar más de forma conjunta, porque la experiencia puede ser muy útil: nos tenemos que proteger en común", considera Santos.

"Debemos de empezar a cambiar. Me refiero a que hay que crear una cultura desde abajo, en todos los estamentos de la sociedad. Yo como

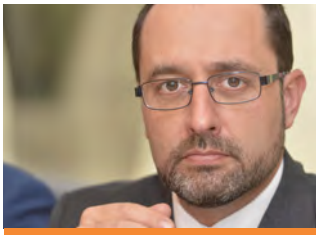
CISO, creo que hay que ir más allá y pensar que vamos a sufrir ataques y amenazas cada vez mucho más elaboradas. Y para ello, no hay más remedio que asociarse. Porque todos tenemos experiencias comunes, en lugar de seguir quejándonos tanto por la falta de apoyos", piensa por su parte Pedro Pablo López, gerente de Gobierno, Riesgos, Commpliance y Protección, Infraestructuras y Continuidad de Rural Servicios Informáticos. Así, López apuesta por trabajar de forma más coordinada.

Al respecto también está de acuerdo José Ramón Monleón, CISO de Orange. "La cuestión presupuestaria no debe ser una excusa ya que la seguridad tiene que venir por defecto, ya que gran parte del presupuesto nos lo gastamos en auditar y corregir los defectos de fabricación de terceros. Si las cosas se hacen bien de inicio te ahorras mucho dinero, o lo podríamos utilizar para otras cosas. También Monleón asegura que "cuando realizamos la contratación de un producto o servicio, lo primero que se eliminan son los requerimientos de seguridad para reducir costes, por lo que el presupuesto del proyecto no debe ser una excusa para eliminar los requerimientos de seguridad. Se debe exigir en el desarrollo seguro de soluciones, puesto que si el desarrollo de software no te ofrece unas garantías, te pueden dar lo que quieran. Hay que saber bien lo que se compra", afirma.

En una empresa como Mapfre, "vemos que estamos viviendo la tormenta perfecta. El número de ataques aumenta y además son más sofisticados que nunca. Además nuestro perímetro aumenta debido a la cantidad de cosas que hacemos: cloud, movilidad, Big Data… impactan en el negocio a nivel de presupuestos y recursos. En ningún momento dejamos de hacer lo que hacíamos antes: se añaden cosas nuevas. Al mismo tiempo, nos impacta la presión regulatoria", revela José María García, responsable de Seguridad en Infraestructura digital de la entidad aseguradora.

Alberto Hernández, director general de Incibe, también acudió al encuentro, y desveló que "en 2016, gestionamos más de 100.000 incidencias en España, mientras que en 2015 eran 50.000 y 18.000 en 2014. Por tanto, las amenazas aumentan, pero también nuestra capacidad de detección. Esto es positivo, porque detectamos más, y un mayor número de incidentes supone un aumento en la concienciación de los CEO". Esta situación también conlleva un "aumento en las primas de los seguros y operadores. Por eso, los comités de dirección están cada vez más concienciados e invierten más. El problema son las pymes, que suelen tener muchos agujeros de seguridad". Para Hernández, la incidencia de ransomware es "dramática" en el caso de pequeñas y medianas empresas, y muchas de ellas se ven incluso obligadas a parar su negocio. "Nos queda mucho por hacer todavía, y también apuesto por la colaboración: la seguridad es tarea de todos", confirma el director general de Incibe.

"Nosotros somos una empresa pública que ofrecemos soporte a organismos públicos, y por supuesto que el ransomware es un problema, pero la nube es una solución muy válida para poder combatirlo. Lo que quiero decir es que hay momentos críticos de cambios pero también de oportunidades: una buena política de integración de la pyme en la nube también puede generar una oportunidad de garantizar la continuidad", opina Óscar Pastor, gerente de Seguridad de Isdefe. Igualmente, el responsable ha querido incidir en la importancia de "que la legislación se cumpla: que haya multas, porque detectamos que la alta dirección en cuanto siente el riesgo, se conciencia. La concienciación se aplica mejor con impactos reales y con responsables que asuman dicho impacto". Igualmente, Pastor aprovecha para manifestar sus dudas en torno a la coordinación y compartición en seguridad. "Es muy difícil que ocurra



Domingo Cardona,
Chief Operations Officer de Wise Security Global

La pyme suele estar muy desatendida en el ámbito de la ciberseguridad. Los grandes proveedores no siempre les ofrecen las soluciones adecuadas

Óscar Pastor,
Isdefe

José María García,
Mapfre

Rafael Santos

José Ramón Monleón,
Orange

Pedro Pablo López,
RSI

porque hay una alta competencia: un fabricante no le va a contar a otro lo que está haciendo". Sin embargo, a este respecto, Javier Candau del Centro Criptológico, cree que "entre empresas que compiten es difícil intercambiar, pero entre organismos públicos es muy fácil y deseable. Porque Incibe por ejemplo no es nuestro competidor". Alberto Hernández de Incibe, está de acuerdo, "compartir supone una ventaja competitiva. En nuestro caso, ya estamos compartiendo información con otros países, especialmente de América Latina, y así conseguimos que nuestra capacidad de influencia sea cada vez más alta".

Por su parte, Antonio Calzada, jefe del servicio de Seguridad Informática de Instituciones Penitenciarias, piensa que "no creo que la concienciación de los directivos tenga que pasar por sufrir un incidente grave. Es cierto que nuestros directivos no suelen estar concienciados, pero también es verdad que no hemos tenido incidentes de seguridad tan relevantes. Mi labor diaria es la de intentar concienciar a mis superiores, pero tengo un doble problema: en primer lugar, el presupuesto, donde tengo todas las limitaciones, pero también pienso que el compromiso de la dirección debería venir por norma legislativa. Por ley debería haber más lucha contra la ciberseguridad y el cibercrimen".

Manuel Barrios, CISO de Informática El Corte Inglés, opina que "uno de los mayores riesgos son las modas que a veces nos ciegan, olvidándonos del primer factor, que es el humano. Es fácil echar la culpa al usuario, pero el factor humano somos todos. Si tengo un buen administrador que no es consciente, de nada sirve tener los mejores sistemas de seguridad. Porque muchos problemas vienen de la formación y concienciación, y no solo del presupuesto".

Finalmente, Manuel Fernández, director de Seguridad y entorno corporativo del Banco Inversis, admite que "hay que analizar los problemas que se tienen, pero también tener en cuenta cómo te tienes que proteger, en qué medida y con qué coste. Por otro lado, plantearse si estamos haciendo lo correcto. Hay que buscar fórmulas para hacer las cosas de otra manera. La concienciación es fundamental, pero a veces no sabemos contarle a cada uno lo que deberíamos". ■

"No creo que la concienciación de los directivos tenga que pasar por sufrir un incidente grave"