El gran reto de securizar el Internet de las Cosas

LA PROTECCIÓN DE LOS DISPOSITIVOS MÓVILES, UNIDO AL INTERNET DE LAS COSAS, SON UNA DE LAS PRINCIPALES TENDENCIAS DEL SECTOR DE LA CIBERSEGURIDAD, A LA VEZ QUE SUPONE UNO DE LOS DESAFÍOS MÁS COMPLEJOS A LOS QUE SE ENFRENTA ESTA INDUSTRIA.

La evolución de la tecnología ha traído consigo una serie de cambios a los que las antiguas estrategias de seguridad no pueden hacer frente: Internet, las tecnologías cloud y la penetración de tecnología inalámbrica contribuyen a la extensión de la superficie del ataque. Asimismo hay otra preocupación relacionada con la desaparición del perímetro: cómo pueden salir los datos de la red. "La shadow IT, el uso no autorizado de aplicaciones como Hightail o Dropbox también significa que hay un número de vías por las que los daos pueden salir de la red sin el conocimiento del responsable de TI, haciendo más fácil la filtración de datos resultante de una intrusión en la red", comenta José Luis Laguna, director técnico de Fortinet Iberia.

Ante este nueva situación, para Nicasio de Tomás, Channel Manager Dell Security Spain, el enfoque tiene que ser global, "es decir, contemplar la seguridad de la red, el end point, los usuarios móviles, la seguridad del cloud y su acceso, la formación y concienciación de los usuarios, la estrategia de backup y recuperación de los datos, etc".

También hay otra preocupación relacionada con la desaparición del perímetro, explica Jose Luis Laguna, director técnico de Fortinet Iberia: cómo pueden salir los datos de la red. "La shadow IT, el uso no autorizado de aplicaciones como Hightail o Dropbox también significa que hay un número de vías por las que los datos pueden salir de la red sin el conocimiento del responsable de TI, haciendo más fácil la filtración de datos resultante de una intrusión en la red".

Como resumen bien Ángel Victoria, country manager de G Data para España y Portugal, "no es cuestión de ir "atacando" cada capa en función de coyunturas, es fundamental una política global que atienda todos los aspectos y no se olvide del eslabón más débil, los propios usuarios".

Esta falta de educación y formación en seguridad es más evidente en empresas de menor tamaño, aunque la sofisticación cada vez mayor de los ataques hace que en ocasiones sean difíciles de detectar incluso por usuarios avanzados. "Una de las tendencias actuales es evitar fallos de seguridad de dentro hacia fuera motivado, fundamentalmente, por el uso incorrecto de muchas de las nuevas herramientas de TI que se están implantando por falta de una formación de las mismas", advierte Javier Modúbar, director general de Ingecom. "En un entorno en el cual la evolución tecnológica es exponencial y avanza a un ritmo muy superior al que las personas pueden adaptarse a las mismas, provoca que se convierta en un reto a afrontar en los próximos años. Es decir, adaptarse a esta evolución tecnológica cumpliendo unos mínimos de seguridad".

En esta línea, Félix Muñoz, director de InnoTec, la empresa de ciberseguridad del Grupo Entelgy, considera que aún es necesario un importante esfuerzo para concienciar a empresas y empleados en los riesgos a los que están expuestos en materia de seguridad TIC. "Es necesario potenciar planes de concienciación al ciudadano y apoyar a las pymes en la formación en términos de ciberseguridad. Es también muy importante la labor de los organismos gubernamentales que deben velar porque se definan y cumplan normas de seguridad de información en los dispositivos, al tiempo que concienciar a los usuarios en el uso de las nuevas tecnologías. En este sentido, quiero destacar la importancia de la aprobación, hace apenas unas semanas, de la primera normativa europea de ciberseguridad, un paso necesario y que creo será muy positivo".

Miguel Ángel Martos, director general de Blue Coat para el Sur de Europa, considera que aunque la mayoría de los empleados son conscientes de los riesgos

de seguridad, en la práctica muchos se arriesgan. "En Blue Coat hemos realizado junto con Vanson Bourne un estudio en el que hemos analizado estos comportamientos de los empleados, a pesar del conocimiento que éstos tienen de los crecientes riesgos a los que se enfrentan. Si bien la mayoría de los participantes reconocieron cosas tan obvias como los peligros derivados de descargar anexos que puedan llegar por email desde un remitente desconocido, o utilizar redes sociales y aplicaciones no autorizadas por los equipos de TI, no por ello parece que hayan contenido a la hora de asumir riesgos".

Para Esteban Garijo, BDM de Exclusive Networks Iberia, la principal tendencia de desarrollo de soluciones de ciberseguridad es la seguridad de los dispositivos móviles (endpoint security) debido a que la movilidad de los usuarios y empleados ha promovido que el uso de dispositivos finales se incremente de manera considerable. "de hecho, es una de las principales fuentes de entrada de las amenazas, tanto conocidas como desconocidas", afirma.

Por su lado, Eduard Palomeras, consultor preventa de Seguridad de CA Technologies Iberia, considera que siendo la gestión de las identidades una disciplina madura y consolidada, hoy en día las tendencias es dotar de inteligencia a estas soluciones. "Así, pueden integrar motores analíticos especializados que detecten los diferentes vectores que podrían facilitar el fraude en nuestra organización. Además, el auge de la programación neurolingüística y los motores de perfilado son tendencias clave que vamos a ver integradas cada vez más en la infraestructura del control de acceso. El reto al adoptar estas técnicas avanzadas es mantener el control, por ello el concepto de caja negra es difícilmente aceptable en la mayoría de organizaciones maduras en el tratamiento de la seguridad".

Javier Santiago, responsable del negocio de Ciberseguridad y Network Defense de Trend Micro Iberia considera que en este último año ha habido un desarrollo importante en dos soluciones de seguridad: tecnologías para detección de ataques zero-day o ataques dirigidos, y seguridad en dispositivos móviles. "Las tecnologías de búsqueda de ataques zero-day es algo cada vez más necesario, ya no basta con tener un IPS o un firewall que nos proteja de los ataques conocidos, sino que tenemos que analizar patrones de comportamiento tanto en tráfico como en la ejecución de ficheros. La seguridad en dispositivos móviles es una necesidad cada vez más emergente debido a que llevamos en nuestros smartphones o tablets parte de nuestra oficina y parte de nuestra vida privada".

A todo lo anterior, Borja Pérez, responsable de Canal de Stormshield para Iberia, añade la colaboración entre los distintos elementos de una arquitectura de seguridad (endpoints hablando con el perímetro, por ejemplo). "También veremos a distintos fabricantes

compartiendo información sobre ataques para dar una mejor respuesta global", afirma.

El uso de la nube es asimismo otra de las mayores tendencias en seguridad. "Gran pare de los principales jugadores del sector está implantando soluciones que se benefician da la nube y el big data para mejorar la capacidad de prevención", comenta Luis Corróns, director técnico de PandaLabs. Otro punto que ve donde se está haciendo mucho hincapié es en los dispositivos móviles donde soluciones de control de todos los dispositivos que se conectan a la red corporativa son claves.

Nicasio Martín, Dell, en el caso de los dispositivos móviles, considera que es muy importante dotar a estos dispositivos de acceso cifrado a la corporación, cifrado de sus datos locales, e autenticación fuerte para el acceso, separar la parte privada de la corporativa, etc… son mecanismos básicos que deberían de aplicarse en todas las empresas, con independencia de su tamaño, así como la capacidad de interrogar el dispositivo, antes de realizar la conexión, para hacer que cumpla con la política de seguridad y de otra forma, denegar su acceso.

Respecto al desarrollo de soluciones de seguridad Felix Muñoz, de InnoTec, destaca como tendencias inteligencia en tiempo real y plataformas de intercambio seguro de información sobre ciberseguridad, seguridad en dispositivos móviles y aplicaciones proactivas de se-

guridad basadas en inteligencia artificial. “Respecto a servicios avanzados de seguridad, una de las principales es el desarrollo de servicios como Red Team. Nos hemos dado cuenta en la industria que de poco sirve lanzar soluciones sin realmente hacer ese paso previo: conocer realmente cómo actúan los ciberdeliencuentes”.

Ningún sector a salvo

En algo que coinciden todos los portavoces de las empresas consultadas, cualquier compañía es susceptible de sufrir un ataque, independientemente de su tamaño y el sector en el que opere. “Lógicamente, para los cibercriminales tiene más interés aquellas que disponen de datos o información sensible que pueden utilizar con fines lucrativos”, advierte José Luis Laguna, de Fortinet. “El sector bancario ha sido tradicionalmente uno de los que más ataques ha sufrido, si bien sus altas inversiones en seguridad han hecho desistir a muchos cibercriminales que han rediseñado su estrategia para alcanzar otros objetivos menos protegidos como el sector retail”, comenta.

“Ningún sector está a salvo. La industria, que tradicionalmente ha estado a salvo por ser redes aisladas, pasa a estar expuesta cuando hablamos de la Industria 4.0. Algunos fabricantes hemos desarrollado soluciones de seguridad que entienden protocolos industriales para poder securizarlos al conectarse a redes IP externas. En otras regiones, como en EEUU, estamos viendo un incremento en ataques a otros sectores como el sanitario”, pone de manifiesto Borja Pérez, de Stormshield.

Para Javier Modubar, de Ingecom, no existe un sector que se pueda decir que es atacado más que otro de manera general sin previamente definir qué tipo de ataque es. “Podemos decir que las mafias delictivas han visto como ataques masivos a usuarios corrientes porque pueden conseguir grandes beneficios. Un ejemplo de ello es la explosión del ransomware. Por otro lado, también se están produciendo ataques de infraestructuras críticas de países donde se incluye sectores como banca, comunicaciones, utilities, etc. en el que el atacante tiene otros fines que pueden ser no sólo económicos”.

Ocurre que en igualdad de condiciones, existen mercado, por ejemplo algunos entornos industriales, hospitalarios, etc., donde los propios sistemas utilizados en estas empresas son muy específicos para sus funciones y se crean sin ningún tipo de seguridad asociados, asegura Javier Santiago, de Trend Micro Iberia. “Estos sistemas que inicialmente no se consideraba que pudieran ser susceptibles de ser atacados están sufriendo ataques que por las implicaciones de su indisponibilidad están generando ingentes beneficios a los atacantes”, comenta.

En definitiva, cada sector ha creado sus medida de protección de forma proporcional al valor de lo protegido y al riesgo estimado”, concluye Eduard Palomeras, de CA. Aunque “más que de sectores, yo hablaría de métodos de conseguir dinero a través del cibercrimen”, comenta Vicente Pérez, Key Account Manager de Sophos Iberia. “No olvidemos que el principal objetivo de los ataques es conseguir un beneficio económico por parte del cibercriminal. En este sentido, es común pensar que para obtener mucho dinero has de atacar grandes organizaciones pero la realidad es que en muchas ocasiones es más sencillo atacar a primer que superan en número a las grandes empresas y están más desprotegidas, lo que les reporta mejores resultados”.

El complejo escenario del IoT

El crecimiento exponencial del IoT en los próximos años (se estima que el número de dispositivos que estará conectado a Internet en 2010 será superior a

26.000 millones) es muy preocupante desde el punto de vista de la seguridad. Para el responsable de Stormshiled, en este escenario estamos más expuestos y por lo tanto debemos protegernos. "Muchos de los desarrollos de IoT no han tenido en cuenta la seguridad en su concepción lo que va a implicar tener que securizarlos a posteriori. Lo hemos visto en la industria del automóvil con hackeo de coches incluido, y lo veremos cada vez más en domótica".

El entorno IoT supone un gran reto para la seguridad, siendo la inspección basada en la red el único camino a seguir para la protección del mismo, advierte Jose

⇨ Luis Laguna, de Fortinet. “Cada red requerirá de un dispositivo de seguridad lo suficientemente inteligente para inspeccionar en profundidad el código escrito para estas plataformas no tradicionales. Nos referimos a esto como plataforma de inspección agnóstica, y es la mejor manera de escalar junto con el IoT”.

Respecto a los dispositivos IoT, como cualquier otro que conectado a Internet, “desde Sophos queremos que los usuarios entiendan los riesgos. No consiste en estar en contra de su uso, ni mucho menos, pero una buena práctica cuando vas a adquirir alguno sería tomar un tiempo en revisar la configuración de los mismos”, aconseja Vicente Pérez.

El año pasado, según la edición 2016 del informe Cyberthreat Defense del CyberEdge Group. El 76% de las empresas fueron víctimas de algún ciberataque con éxito. Y esto sucedió a pesar de que el 85% de las compañías invirtieron en seguridad al menos el 5% de sus presupuestos IT, y de que un sorprendente 30% de las empresas llegaron a invertir hasta el 16%, según desvela el mismo estudio. Para Miguel Ángel Martos, Blue Coat, hay varias formas de interpretar estos datos. “O bien las empresas confían en exceso en sus defensas, bien infravaloran la creciente superficie que puede llegar a ser objetivo de los ataques, o bien no son conscientes del impacto que en sus defensas pueden llegar a representar las últimas tendencias en ciberseguridad”. Como explica el responsable de Blue Coat, en la empresa han identificado seis importantes tendencias que inciden, de modo significativo, en la seguridad de las empresas:

- Unos extremos/end points en continuo cambio
- Un perímetro en expansión.
- Visibilidad del tráfico cifrado
- La adopción de Office 365.
- Uso de aplicaciones en la nube.
- Respuesta ante incidentes y malware avanzado.

En BlueCoat nos referimos al tráfico cifrado como “el asesino silencioso”, porque en muchas ocasiones transporta malware pero nunca nos enteremos ya que no dispara ninguna alarma. El cifrado protege la privacidad del usuario y las comunicaciones empresariales sensibles, pero también facilita un escondite para el malware porque las herramientas de seguridad tradicionales en las que las compañías han invertido no son capaces de descifrar el tráfico en tiempo real. Así se crea un punto ciego para la seguridad, lo que supone un importante creciente problema, básicamente por dos motivos principales; porque el tráfico cifrado crea una falsa sensación de seguridad porque los administradores nunca llegar a ver ninguna alerta de seguridad y segundo porque el uso de cifrado SSL y TLS está creciendo. Esto quiere decir que, dada las magnitudes en las que nos movemos, va a ser bastante complicado poder llegar a gestionar completamente el riesgo del tráfico cifrado que se mueve en una empresa”.

Por otro lado, Microsoft Office 365 ofrece un punto clave para el modelo de nube pública pero desde una perspectiva de seguridad, un movimiento completo a la nube no debe disfrazarse bajo la apariencia de un acuerdo con Microsoft. Debemos preguntarnos también si contamos con la protección adecuada al movernos desde una infraestructura propia a la nube de Microsoft, como pueden ser controles para prevenir la ⇨

pérdida de datos (DLP), visibilidad de fallos de seguridad y amenazas persistentes avanzadas, gestión de acontecimientos y recuperación y respuesta ante incidentes. Debemos tener muy en cuenta que no podemos aprovechar las oportunidades que nos aporta la nube si comprometemos la seguridad".

Todo dispositivo u objeto conectado a Internet es susceptible de recibir un ataque y las grandes cantidades de datos que manejan las empresas son muy jugosas para los ciberdelincuentes. "Por esto hoy es más importante que nunca estar protegidos. En especial porque los fabricantes de IoT están buscando funcionalidad son pensar en la seguridad, saltándose normas básicas y privacidad", apuntan desde la compañía Check Point.

En el caso del IoT, debemos exigir que las empresas cumplan con las medidas de seguridad adecuadas, así como también conocer cuándo nuestros datos han sido robados, explica Guillermo Fernández, sales enginner de WatchGuard para España, portual y PALOPs. "El hecho de que en las noticias aparezcan bre-

⇨ chas de seguridad de empresas americanas no significa que en España o Europa no suceda. La diferencia es que allí tienen obligación de hacerlo público por ley, algo que en breve sucederá en la UE".

Aunque es cierto que amenazas como el ransomware ha estado presente desde hace mucho tiempo, nunca ha sido tan popular o rentable como lo es ahora. Los datos sobre Cryptolocker son rotundos. "Una de cada tres empresas se han visto afectadas en España por esta amenaza", advierte Vicente Pérez, de Sophos.

"A diferencia de otros tipos de malware que intentan robar datos, el ransomware pretende provocar alteraciones, ya sea escriptando archivos o datos valiosos, o bloqueando el acceso al sistema hasta que se cumplan las exigencias. Robar un número de tarjeta de crédito y utilizarlos para cometer un fraude es cada vez más difícil, ya que es necesario realizar muchos pasos, y los bancos y los establecimientos disponen de controles en cada etapa del proceso para detectar e impedir las operaciones fraudulentas", comenta Nicasio Martin, Dell.

Para evitarlo es importante la concienciación de los usuarios y contar con herramientas que mitiguen dichos ataques. "Una solución contra malware avanzado es clave en cualquier estrategia. Por otro lado, y aunque parezca una contrariedad, no conviene pagar los rescates sino que hay que denunciarlos pues el hecho de que se pague no quiere decir que se vayan a recuperar los datos", apunta Guillermo Fernández, WatchGuard. "Hay que negarse a pagar ya que así se incentiva a los criminales para que continúen realizando ataques y dispuestas contacta con una empresas de ciberseguirdad que ayude a recuperar los datos y mantendrá protegidos antes futras posibles infecciones", indican desde Check Point.

"Es peligrosísimo, puede llegar a provocar el cierre de una empresa", avisa Luis Corrons, PandaLabs. "Esto puede sonar muy drástico, pero en pequeñas empresas donde no hay una política de copias de seguridad, que te secuestren los datos pueden llevarte a la quiebra. Recientemente vimos un caso donde a un despacho de abogados les cifraron todos los documentos legales y de clientes. Sin esa información no sólo es que no puedan trabajar, sino que están perdiendo el fruto de meses o años de trabajo".

"Ante este panorama y para evitar este tipo de ciberataques, las empresas deben periódicamente hacer copias de seguridad, además de contar con una solución de seguridad fiable que incluye métodos de detección de comportamiento, protección contra exploits y control de aplicaciones. Asimismo es recomendable que las compañías definan un plan de formación y concienciación sobre seguridad a todos los empleados con el fin de reducir los incidentes", apunta Alfonso Ramírez, Kaspersky Lab Iberia.

Para Javier Modubar, Ingecom, el responsable de definir una estrategia de ciberseguridad debería ser el CISO, "pero no olvidemos que el responsable de abrir un correo que llega por una campaña de phising es el propio usuario". Aunque para el responsable de Sophos, para que la figura del CISO tome fuerza en una organización, el primero en estar implicado y concienciado ha de ser el máximo responsable de la empresa, pasando porque todos estén comprometidos con ello. Pero, si nos ceñimos al tejido empresarial español, donde más del 80% son pequeñas y medianas empresas, "nos encontramos más con el perfil de responsable de informática, que ha de encargarse desde configurar ordenadores y redes, hasta de gestionar la seguridad". ✦