CIBERSEGURIDAD

Según el Centro Nacional de Inteligencia (CNI), los ciberataques se incrementaron un 80% en 2014. Éstos además son cada vez más sofisticados. Teniendo en cuenta que cualquier dispositivo conectable a Internet es susceptible de ser atacado, estamos ante una amenaza que afecta tanto a grandes organizaciones como a pymes, y a los ciudadanos a título individual.

Sistemas de gestión para minimizar ciberamenazas

Alberto Olmos y Fernando Seco
Directores de Gestión y Consultoría S2 Grupo

Aunque resulta difícil dar una breve definición de ciberseguridad, podríamos decir que se trata del conjunto de políticas, herramientas, tecnologías, salvaguardas, formación, buenas prácticas, etc. dirigidas a proteger los activos de las organizaciones, los países y los usuarios del ciberentorno. Es el de la ciberseguridad un tema multidisciplinar con una gran componente tecnológica, extraordinariamente complejo y de un alcance amplísimo, ya que afecta a todo tipo de organizaciones, infraestructuras, gobiernos y administraciones; y a todos sin excepción: tanto en nuestro ámbito profesional como en el privado. Es decir, aunque de manera bien distinta, la ciberseguridad afecta tanto a una gran corporación multinacional como a una pyme; y tanto a un alto ejecutivo como a un niño de 11 años por el mero hecho de disponer de una tableta o móvil con acceso a Internet o una consola de videojuegos. Atañe igualmente a todo tipo de *hardware*, tanto industrial y profesional como el destinado al ocio y uso personal (equipos informáticos en general, cajeros automáticos, tabletas, teléfonos móviles, TPV, cámaras, *firewalls*, routers, PLC, *smartphones*, etc.); y a todo tipo de *software* y plataformas (sistemas operativos, software de control industrial, entretenimiento, multimedia, comunicaciones, control remoto, redes sociales, mensajería instantánea, etc.).

La ciberseguridad afecta muy especialmente, aunque no exclusivamente, a todos aquellos dispositivos conectados o conectables a Internet. Partiendo de la base de que su número no hace más que crecer (se estima que en el año 2020 habrá más de 30.000 millones de dispositivos conectados a la red), y asumiendo que cualquier dispositivo conectable a Internet es susceptible de ser atacado, estamos hablando de un ingente *mercado objetivo* para los ciberdelincuentes, que va desde las pymes a las grandes multinacionales, y desde los gobiernos a casi cada uno de nosotros.

Realidad actual

Las actividades que admiten delante el sufijo *ciber-* están de total actualidad. Casi a diario se pueden ver o escuchar noticias relacionadas con la

ciberdelincuencia, ciberespionaje, ciberguerra, etc. Frecuentemente nos llegan también informaciones sobre denuncias y sentencias relacionadas con delitos cometidos en relación con las nuevas tecnologías como robos de información, suplantaciones de identidad, *hacking*, ingeniería social o casos de ciberacoso, por no hablar de las sofisticadas Amenazas Persistentes Avanzadas, más conocidas como APT.

Datos recientes proporcionados por el Centro Nacional de Inteligencia (CNI) indican que el número de ciberataques ha crecido un 80% en 2014 con respecto a 2013. Se han gestionado desde el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) alrededor de 13.000 ciberincidentes, de los cuáles se estima que algo más del 10% consiguieron su objetivo. También se ha constatado un incremento en la sofisticación de los ataques, tanto a las Administraciones Públicas como a empresas y organizaciones de interés estratégico para España, fundamentalmente de los sectores energético, aeroespacial, farmacéutico y químico.

Pese a todo, el elevado nivel de desconocimiento en la materia hace que haya una escasa conciencia general del riesgo. Hoy en día son todavía muchas las organizaciones pequeñas y medianas que, al igual que ocurre con gran cantidad de usuarios del ciberentorno, piensan erróneamente que la información que poseen y manejan no puede resultar de interés para nadie. El incremento de la externalización de los servicios, el uso del *cloud computing*, la informática móvil, la aparición del BYOD[1], el teletrabajo, etc. hace que ninguna empresa hoy en día pueda permitirse el lujo de no gestionar de manera adecuada la ciberseguridad de su información corporativa y de sus infraestructuras tecnológicas, bien sea utilizando recursos propios o recurriendo a empresas especializadas que presten servicios externalizados de seguridad gestionada. El nivel de riesgo existente no puede obviarse.

CIBERSEGURIDAD

Panorama de futuro

¿Qué nos depara el futuro en materia de ciberseguridad? Considerando las características y complejidad del asunto y la velocidad de vértigo a la que se suceden los cambios, algunos expertos opinan que lo que nos depara el futuro en materia de ciberseguridad se puede resumir en dos palabras: muchas sorpresas. Pero basándonos en la observación de la realidad, y sin ánimo de ser exhaustivos, se puede apuntar como muy probables los siguientes escenarios futuros en esta materia:

• **Mayor número de ciberdelitos.** Aparecerán delitos totalmente nuevos, pero también nuevas versiones de los delitos de siempre cometidos con nuevos métodos. Es esperable, por tanto, el desarrollo de normativa y legislación relacionada que intente establecer la división entre lo permitido y lo no permitido (lo cual no siempre está claro y dista mucho de ser trivial) y fije algunas bases importantes. Aunque siendo realistas, no es muy probable que dicho marco vaya a disuadir a *los malos* de cometer sus fechorías. Y es que se dan una serie de factores (la facilidad de delinquir desde la distancia y el anonimato, la ausencia de sensación de peligro o la dificultad de la atribución de los delitos) que hace previsible un incremento de los ciberdelitos. Algunos expertos aseguran que resulta mucho más barato robar un proyecto industrial o empresarial que emprenderlo desde cero. Y es mucho más *cómodo* intentarlo por medio de ataques informáticos que por medios físicos, por su menor nivel de riesgo.

• **Incremento del *malware*.** El número de dispositivos móviles crece a diario y las apps, tanto gratuitas como de pago, ofrecidas en las tiendas virtuales se cuentan por millares. Muchas de estas aplicaciones cuentan con nuevas funcionalidades y sofisticadas utilidades. Pero, al mismo tiempo, estas aplicaciones cada vez acceden, manejan y *controlan* más información sensible sobre sus usuarios. Toda esta información puede tener un gran valor. Las diferentes vías por las que se interconectan nuestros ordenadores y dispositivos móviles hacen elevar el riesgo de exposición a la industria del *malware*, interesada en toda esa ingente cantidad de información que se maneja en los equipos y que viaja por Internet y las redes sociales. Todo ello hace pensar en un incremento de *malware* para dispositivos móviles, así como un mayor nivel de sofisticación.

• **Aumento de las actividades de ciberespionaje y ciberguerra.** Hace años que el ciberespionaje y la ciberguerra son una realidad. Su incremento es imparable porque, como ya se apunto anteriormente, resulta más barato el ciberespionaje que el espionaje tradicional. Además, los países espían y se saben espiados por medios informáticos, pero dichas actividades son mucho más discretas que el espionaje tradicional y también de difícil atribución. Con la ciberguerra ocurre lo mismo: resulta más discreta y rentable en términos económicos y menos peligrosa para el atacante, en general, que las distintas modalidades de guerra tradicional.

• **Incremento del cibersabotaje.** Los riesgos que ha introducido la conexión de los sistemas de control industrial a Internet han quedado ampliamente demostrados. Esta interconexión tiene grandes beneficios (facilidad de mantenimiento, control y supervisión remotos o disminución de costes, entre otros) pero a la vez introduce problemas de cibersabotaje y ciberterrorismo contra infraestructuras críticas, o de ciberespionaje de sectores estratégicos, como indicábamos antes. La vulnerabilidad de estos sistemas de control industrial conectables a Internet deriva de que muchos

LOS DATOS

Ciberseguridad en cifras:

El **65,9%** de las empresas de más de 10 empleados no disponen de una política de seguridad

El **44%** de las empresas no dispone de personal destinado a la seguridad TIC

El **38,5%** de las empresas adopta una actitud proactiva tras un incidente de seguridad

El **75%** de las empresas que utilizan comercio electrónico como canal de venta no dispone de un sistema de gestión del fraude

El **60,6%** de las pymes desconocen el concepto de Plan de Continuidad de Negocio

Fuente: Instituto Nacional de Ciberseguridad (INCIBE)

de ellos no fueron diseñados y/o configurados para ello, quedando en ocasiones, una vez conectados, totalmente expuestos. Por otro lado, el surgimiento imparable del IoT o *Internet de las cosas* en el ámbito doméstico (neveras, calefacciones, sistemas de riego, cámaras, cocinas, espejos inteligentes, domótica en general) conllevará grandes comodidades y ventajas, pero a la vez provocará que cualquier *cosa* conectada al IoT sea susceptible de ser atacada.

Importancia de los sistemas de gestión

Si disponer de un sistema de gestión resulta necesario para organizaciones de cualquier sector de negocio, dicha necesidad se hace aún más imprescindible en el ámbito de las TIC en general y en el de la ciberseguridad en particular. Los sistemas de gestión se basan en el ciclo PDCA lo que obliga a planificar lo que se va a hacer. En materia de ciberseguridad no todo se puede planificar. Por ejemplo, durante la neutralización de un ciberataque en tiempo real hay un alto componente de imprevisibilidad. Pero los métodos generales de actuación, intercepción y defensa deben estar establecidos y validados. Se necesita contar con los mejores recursos técnicos por un lado y, por otro, con un sistema de gestión extremadamente ágil que sea, a su vez, capaz de aprender casi en tiempo real, fijando, mejorando y diseminando las prácticas que se han mostrado eficaces y descartando el resto.

Ninguna organización a día de hoy puede permitirse el lujo de no gestionar de manera adecuada la ciberseguridad de su información corporativa y de sus infraestructuras tecnológicas

Además de un sistema de gestión basado en la Norma UNE-EN ISO 9001 de calidad que se pueda aplicar de manera global a la organización y que dé respuesta a la necesidad obligatoria de combinar servicio y seguridad, resulta imprescindible la integración de los requisitos incluidos en las Normas UNE-ISO/IEC 27001: 2014 *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI), Requisitos,* para lo que contamos con su nueva versión publicada en noviembre de 2014 y UNE-ISO/IEC 20000-1: 2011 *Tecnología de la información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio*. Además, considerando la velocidad a la que cambian los escenarios en materia de ciberseguridad (los cambios se suceden a una velocidad difícil de asimilar incluso por los propios profesionales del sector) resulta necesario estar siempre en la punta de la lanza. Para ello, es necesaria una inversión en I+D+i, y la Norma UNE 166002 *Gestión de la I+D+i: Requisitos del Sistema de Gestión de la I+D+i* describe un sistema de gestión para las organizaciones que constituye una herramienta de gran utilidad en este campo.

Asimismo, para poder reaccionar al ritmo al que se suceden los cambios, se dispone de una herramienta muy útil en las normas UNE-ISO 22301 y UNE-ISO 22313 que proporcionan un sistema de gestión para la continuidad del negocio. Éste proporciona a la organización un marco para identificar las posibles amenazas y fortalecer su capacidad para afrontarlas, para ayudar a desarrollar un plan de continuidad de negocio que garantice el funcionamiento de las organizaciones durante y después de las interrupciones.

Como muestra de que las normas y estándares internacionales se adecúan a los tiempos que corren, la preocupación por el ámbito de la ciberseguridad es una cuestión ya presente en la estrategia de los organismos de normalización. Desde hace un tiempo se está trabajando en documentos internacionales que forman parte de la familia de normas ISO 27000 de Gestión de la seguridad de la información con un enfoque orientado a dar apoyo a los nuevos escenarios derivados de actividades como la ciberseguridad. ◗

NOTAS

(1) Siglas en inglés de *Bring Your Own Device* (traiga su propio dispositivo): política empresarial en la que se permite a los empleados hacer uso de dispositivos personales (*smartphones*, *tablets*, ordenadores) para acceder a recursos de la empresa como correo electrónico, repositorios de información o aplicaciones corporativas.