Por Ana Moreno Marín

La delincuencia del siglo XXI

Los ciberataques, una amenaza creciente para la seguridad nacional.

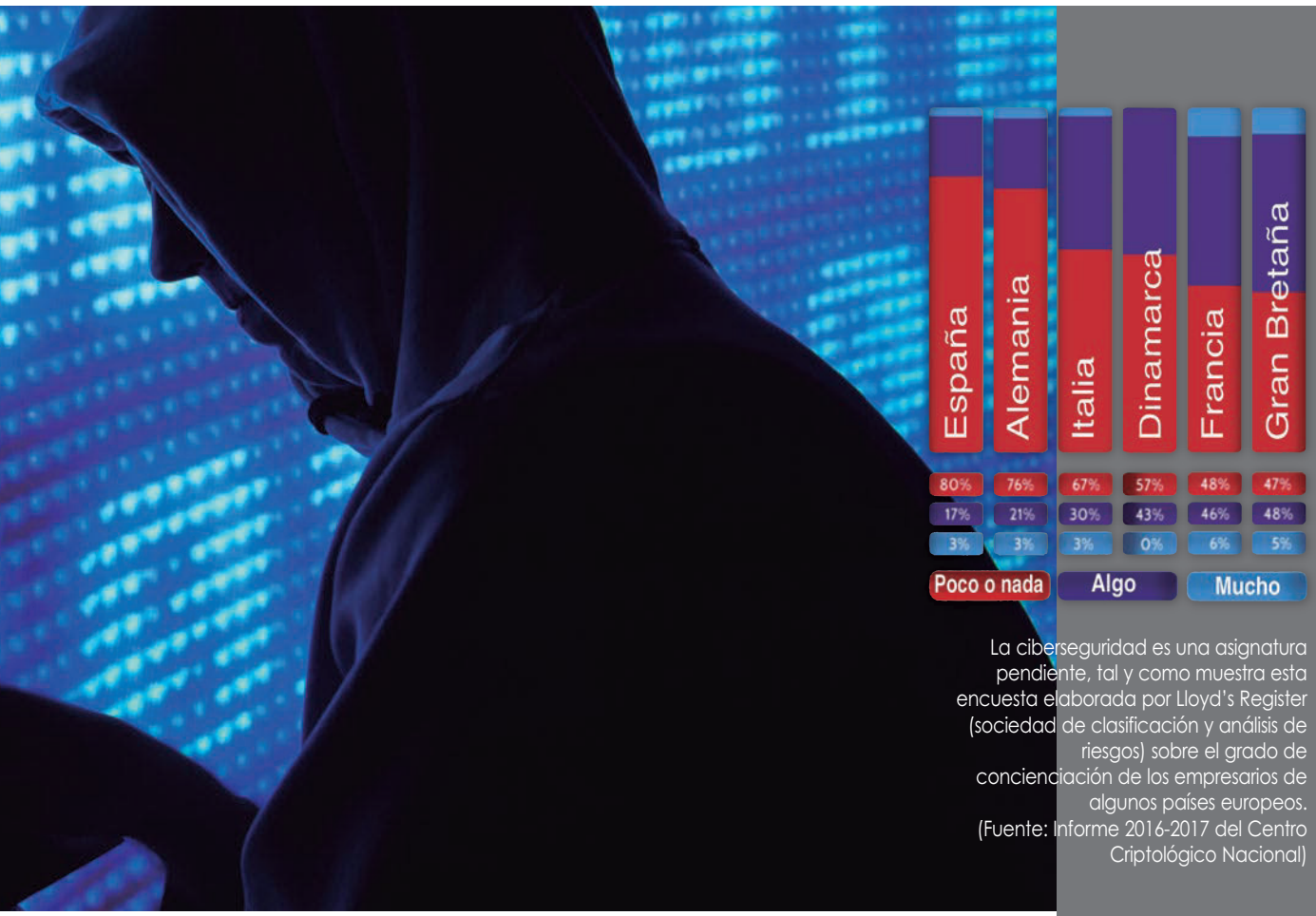
Seguro que todavía recuerdan el ciberataque mundial del virus Wannacry que se produjo el pasado mes de mayo. Más de 300.000 equipos de 180 países afectados de los que al menos 1.200 se encontraban en España. Junto a Telefónica, cientos de empresas españolas sufrieron este virus que bloquea los archivos del ordenador. Es el secuestro de la nueva era.

El Wannacry ha marcado un antes y un después en la conciencia mediática de este nuevo tipo de delincuencia, pero en los últimos años se han producido auténticas barbaridades.

Del robo frustrado de 81 millones de dólares al Banco Central de Bangladés a la publicación de 400 millones de cuentas de una compañía de páginas de citas con datos tan delicados como la orientación sexual de sus usuarios, pasando por la circulación de datos de 154 millones de votantes de Estados Unidos, el robo de 1.000 millones de cuentas de correo electrónico de *Yahoo!* o el primer corte de suministro de electricidad de la historia a más de 600.000 hogares ucranianos en el invierno de 2015. Como ven no es ninguna broma.

Una delincuencia más que rentable

Las pérdidas mundiales se cifran en unos 400.000 millones de dólares, según datos de Khoo Boon Hui, expresidente de INTERPOL. Se calcula que supone cerca del 0,8% del PIB mundial, es decir, ¡hoy los ciberataques mueven más dinero que el tráfico de drogas! Y el precio de los rescates va en aumento. Liberarse de un virus *ransomware*, los que te secuestran el ordenador, cuesta hoy más del doble que en 2015.



La ciberseguridad es una asignatura pendiente, tal y como muestra esta encuesta elaborada por Lloyd's Register (sociedad de clasificación y análisis de riesgos) sobre el grado de concienciación de los empresarios de algunos países europeos. (Fuente: Informe 2016-2017 del Centro Criptológico Nacional)

España es el tercer país más atacado después de Estados Unidos y Reino Unido. Tres de cada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años, según el Instituto Nacional de Ciberseguridad (Incibe). Sin embargo, apenas el 37% tiene un plan de respuesta para estos incidentes.

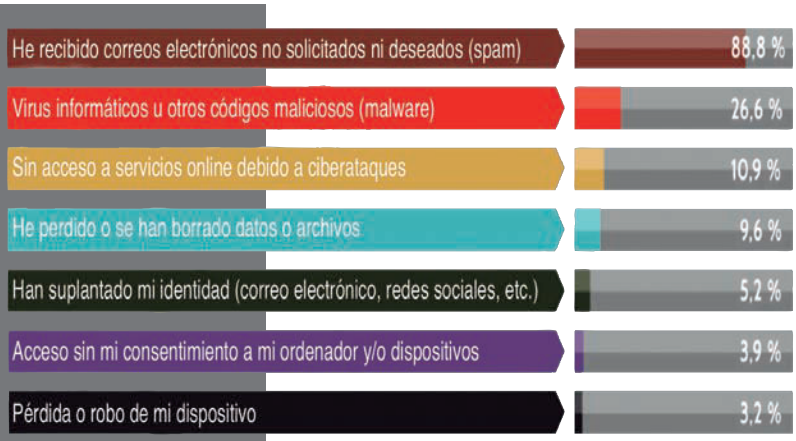
«Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo», explicaba recientemente José Antonio Nieto Ballesteros, Secretario de Estado de Seguridad del Ministerio del Interior en unas jornadas sobre ciberseguridad. En 2016 hubo 115.000 ciberincidentes en España, una media de 315 ataques al día, lo que supone un 130% más que el año anterior según el balance del Incibe.

¿Qué se ataca y quiénes están detrás?

Aeropuertos, hospitales, centrales eléctricas o plantas de agua son algunas de las infraestructuras críticas atacadas en 2016 en España. En su informe *Ciberamenazas 2015/Tendencias 2017*, el Centro Criptológico Nacional detecta un importante crecimiento del ciberespionaje económico, especialmente dirigido a las industrias de defensa, alta tecnología, industria química, energía y salud, que buscan acceder a desarrollos avanzados.

Pero ¿quiénes están detrás de estos ataques? En primer lugar los Estados, muy especialmente los servicios de inteligencia, seguido de organizaciones criminales que buscan el beneficio económico, también organizaciones de ciberespionaje, cuyo objetivo es obtener información, y ciberterroristas, entre los

> Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos.



Usuarios particulares que han sufrido algún ciberincidente en 2016. (Fuente: Informe 2016-2017 del Centro Criptológico Nacional)

que destacan los ciberyihadistas, que utilizan la red para su propaganda y reclutamiento.

Un sector con mucho trabajo

Recientemente, Enrique Cubeiro, jefe de Operaciones del Mando Conjunto de Ciberdefensa, lamentaba que España invierta más en vallas que en ciberseguridad. «¿De dónde creen que vendrá el próximo ataque, de la valla o de un *firewall*? No se está respondiendo a esa amenaza ni con la agilidad ni con la contundencia que hace falta».

Además, pedía que las autoridades dejen de ver a los expertos en ese tema como «los tipos raritos del cuarto sótano» y a las fuerzas de ciberdefensa como a una especie de «cazafantasmas». Hoy se requieren recursos económicos y personal altamente cualificado y especializado. Algo que no es tan fácil de encontrar.

En España hay 1.302 investigadores, repartidos en 104 equipos de trabajo. La mayoría son ingenieros de telecomunicaciones o ingenieros informáticos. Ante el aumento de los ataques y la mayor necesidad de protección se prevé un crecimiento exponencial de la demanda de estos profesionales especializados.

La concienciación en ciberseguridad, asignatura pendiente

La contraseña «1234» sigue siendo la más usada en España, según el Incibe. Cambiar con regularidad las contraseñas digitales, activar un código de seguridad en el móvil, no abrir correos electrónicos sospechosos ni hacer clic en los ficheros adjuntos dudosos son medidas básicas.

Las empresas, foco cada vez mayor de los ciberataques, tienen también mucha responsabilidad. «Todavía en muchas organizaciones la única medida de seguridad es el software antivirus, muchas veces desactualizado», dice el informe del Centro Criptológico Nacional. Para mejorar la seguridad de nuestros dispositivos el INCIBE ofrece en su web aplicaciones para empresas y particulares como el *Conan Mobile*, que indica, entre otras cosas, si tenemos instalada alguna aplicación maliciosa en el móvil o tableta.

Una cosa está clara, tanto el gobierno como las empresas y los usuarios tenemos que hacer los deberes si queremos permanecer seguros en la red. Algo cada vez más complicado. ❐

Los incidentes de seguridad informática en las empresas tienen un coste que algunos organismos estiman en unos 400.000 millones de dólares en todo el mundo. Según el último informe del Centro Criptológico Nacional, los costes más significativos son:

- **Tiempo de inactividad:** pérdidas económicas y daños de reputación. En el caso de empresas de servicios públicos, la falta de energía o agua puede afectar a millones de personas.
- **Costes económicos** derivados de la respuesta a los incidentes, la responsabilidad ante los clientes e incluso el pago de sanciones por motivos legales.
- **Pérdida de datos:** información de los clientes o la propiedad intelectual puede afectar a las finanzas, la marca o la reputación.
- **Pérdida de vidas:** en el caso de un hospital, por ejemplo, la vida de los pacientes puede ponerse en riesgo. Los registros e historias clínicas podrían quedar inaccesibles, provocando retrasos en los tratamientos.