Yaiza Rubio

Analista de seguridad en ElevenPaths

Desde mayo de 2013 ejerce como analista de seguridad en ElevenPaths tras haberlo hecho en empresas como S21sec e Isdefe, además de ser colaboradora del Centro de Análisis y Prospectiva de la Guardia Civil y coautora del libro *Bitcoin: La tecnología blockchain y su investigación*.

Ha sido nombrada cibercooperante de honor por INCIBE (2017) y premiada como finalista de los Proyectos I+D+i del V Security Forum (2017), segundo premio del hackathon de INCIBE en el Mobile World Congress (2017), tercer premio de la Cátedra de Servicios de Inteligencia y Sistemas Democráticos (2015) y segundo premio del Reto de ISACA de jóvenes investigadores (2015). A nivel universitario, es docente en diferentes postgrados sobre análisis de inteligencia, seguridad, análisis forense, evidencia digital y fuentes abiertas, además de codirigir el Posgrado de experto en Bitcoin y Blockchain de la Universidad Europea de Madrid. En el ámbito técnico, se dedica a la publicación de contenidos científico-técnicos en eventos como Blackhat (2017), Defcon (2017), EuskalHack (2017), MaríaPitaDefcon (2017), ISMS Forum (2016), SummerBootcamp (2016), 8dot8 (2015), Cybercamp (2015 y 2017), NavajaNegra (2015), JNIC (2015) o RootedCon (2015), así como a la participación en numerosas jornadas de formación y concienciación en materia de ciberseguridad y privacidad.

Twitter: @yrubiosec

LOS CLAROSCUROS
de la ciberseguridad

Yaiza Rubio

Sin que se asemeje a una excusa, se torna realmente complicado sintetizar el complejo mundo de los riesgos de Internet y la evolución que está teniendo el sector de la ciberseguridad en un artículo que contiene menos de tres mil palabras. No por la cantidad de titulares pensados desde el *clickbaiting* cuyo efecto es el de aterrorizar al usuario medio de Internet, sino por la calidad y la cantidad de investigación existente sobre este campo que es la que hace que, un medio que no nació concebido desde la seguridad desde el diseño sino más bien el de ofrecer una vía adicional de comunicación a las que disponíamos y al que ha habido que ir implementando parches.

La situación actual no es tan dramática como se percibe desde fuera. Hasta hace bien poco las credenciales viajaban por la red en claro utilizando protocolos como HTTP. No existía la autenticación en dos pasos. No existía concienciación sobre la gravedad de un incidente. Antes, los sistemas estaban pensados para conectarse, no para ser seguros. Una frase que refleja esta situación es la que diría mi querida Mafalda: "No es cierto que todo tiempo pasado fue mejor. Lo que pasaba era que los que estaban peor todavía no se habían dado cuenta".

1 *Sobre la necesidad de ciberseguridad*

El concepto de ciberseguridad es muy amplio porque aplica a numerosos campos pero podría resumirse como la práctica de defender aquellos sistemas informáticos de ataques maliciosos. Uno de los principios más importantes de una estrategia defensiva efectiva es el de la *defensa en profundidad* definida por el Centro Criptológico Nacional (CCN-CERT) como la estrategia de protección consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto. De este principio se desprende una máxima del mundo de la seguridad: "La seguridad al 100 % no existe".

La exposición tecnológica de una determinada organización, así como la tecnología legada o el impacto de no proteger sus activos más valiosos como la

información de sus clientes, entre otras cosas, son desafíos frecuentes que hacen darnos cuenta de que el riesgo de recibir un determinado ataque no es el mismo para todas las organizaciones. El principio existente detrás de este concepto es el de dificultar las acciones del atacante a través de las diferentes medidas de seguridad aplicadas a cada una de las capas de forma que los diferentes sensores que tenga nuestro sistema detecten las actividades maliciosas. Cuando una capa se vea comprometida, las medidas de detección, de reacción y de recuperación nos permitirán reaccionar, disminuyendo la probabilidad de que otras capas se vean comprometidas. De esta manera, evitamos así que la seguridad del servicio en su conjunto se vea burlada, disminuyendo por tanto el riesgo.

La inversión que siguen actualmente las organizaciones se encuentra muy ligada a la correcta percepción sobre la gestión de sus riesgos. Es un error pensar que nunca va a ocurrir un desastre como el que viví y del que tanto aprendimos de Wannacry y que van a ser capaces de proteger sus sistemas ante cualquier ataque por lo que se trata de desarrollar políticas de ciberseguridad ligadas al negocio.

Las empresas medianamente maduras balancean sus presupuestos de seguridad entre soluciones de prevención y de detección realizando un análisis continuo de vulnerabilidades, monitorizando qué está pasando en su red identificando accesos no autorizados porque, sin duda alguna, en algún momento un ataque va a tener éxito. En cambio, las más maduras son las que se plantean qué van a hacer el día que tengan un fallo de seguridad, qué van hacer el día en el que un empleado se lleve información de la empresa o qué van a hacer el día en el que un ataque DDoS deje sin disponibilidad su web. En resumen, qué medidas van a tomar cuando el servicio que utilizan sus clientes siga funcionando.

2 Las diferentes visiones sobre la privacidad

Internet está siendo utilizado con éxito por grupos organizados para satisfacer sus objetivos pero serán las necesidades de cada grupo lo que marcará el tipo de aplicaciones o servicios que utilizarán para llevarlos a cabo. En este sentido, las organizaciones que centran sus esfuerzos en acciones de presión harán uso de la web de superficie (parte de Internet indexada por buscadores tradicionales) como blogs, redes sociales o plataformas de firmas para garantizar la difusión de su mensaje garantizándose su llegada a un público amplio. Por el contrario, aquellos grupos criminales o aquellas organizaciones que lleven a cabo actividades perseguidas por estados optarán por soluciones que provean una capa de anonimato más robusta (Tor, I2P, Freenet, etc.) para dificultar las labores de investigación de las agencias de seguridad.

La masacre de San Bernardino desató una guerra tanto legal como mediática entre gran parte de los fabricantes de tecnología y el FBI después de que Apple se opusiera fuertemente a liberar un iPhone propiedad de un presunto terrorista

En este sentido, la colaboración entre las fuerzas de seguridad y las principales empresas tecnológicas es crucial en cuanto a compartición de información se refiere. Los primeros tratan de hacer su trabajo con la dificultad que entrañan aquellos delitos que se comenten a través de la red o que se ha utilizado como herramienta para la comunicación. Y, algunos de los segundos, en aras de luchar por la privacidad de los usuarios se niegan a compartir su información. La masacre de San Bernardino desató una guerra tanto legal como mediática entre gran parte de los fabricantes de tecnología y el FBI después de que Apple se opusiera fuertemente a liberar un iPhone propiedad de un presunto terrorista.

En 2016, a raíz de aquello, algunos de los fabricantes comenzaron a tomar medidas para adecuarse a las necesidades de los nuevos tiempos en materia de privacidad. La implementación del cifrado punto a punto, como fue el caso de Whatsapp o el reporte periódico que hace Google sobre el número de peticiones de información sobre sus usuarios por parte de las Fuerzas y Cuerpos de Seguridad o el anuncio de la política de privacidad de Apple con el eslogan de fondo *What happens on your iPhone, stays on your iPhone* han sido algunas de ellas. A lo largo de 2018 con Facebook casi siempre en el foco de los escándalos de seguridad es cuando nos hemos dado cuenta que no era tan cierta la percepción que se tenía de que a los usuarios no les importa su privacidad.

El 25 de mayo de 2018 fue el día en el que comenzó a ser de obligado cumplimiento la GDPR donde se hace referencia a dos principios para la implementación efectiva de la responsabilidad proactiva como son los de protección de datos desde el diseño y protección de datos por defecto. El principio de protección de datos desde el diseño tiene como objetivo cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados

El director del FBI, James Comey, y la Fiscal General, Loretta Lynch, en la rueda de prensa sobre el titoreo masivo en San Bernardino / Foto: FBI

y busca que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto.

Pocas veces he visto a arquitectos o desarrolladores de software tan preocupados por comprender cada uno de los artículos donde se mencionan términos como "dato de carácter personal", "transparencia", "desde el diseño", "por defecto" o "tratamiento" para que la implementación esté realmente alineada con lo que pide la GDPR. Va a hacer un año desde que comencé a liderar un proyecto en la empresa donde trabajo actualmente que está íntimamente relacionado con uno de los proyectos IT con más envergadura que he visto, como es la Cuarta Plataforma.

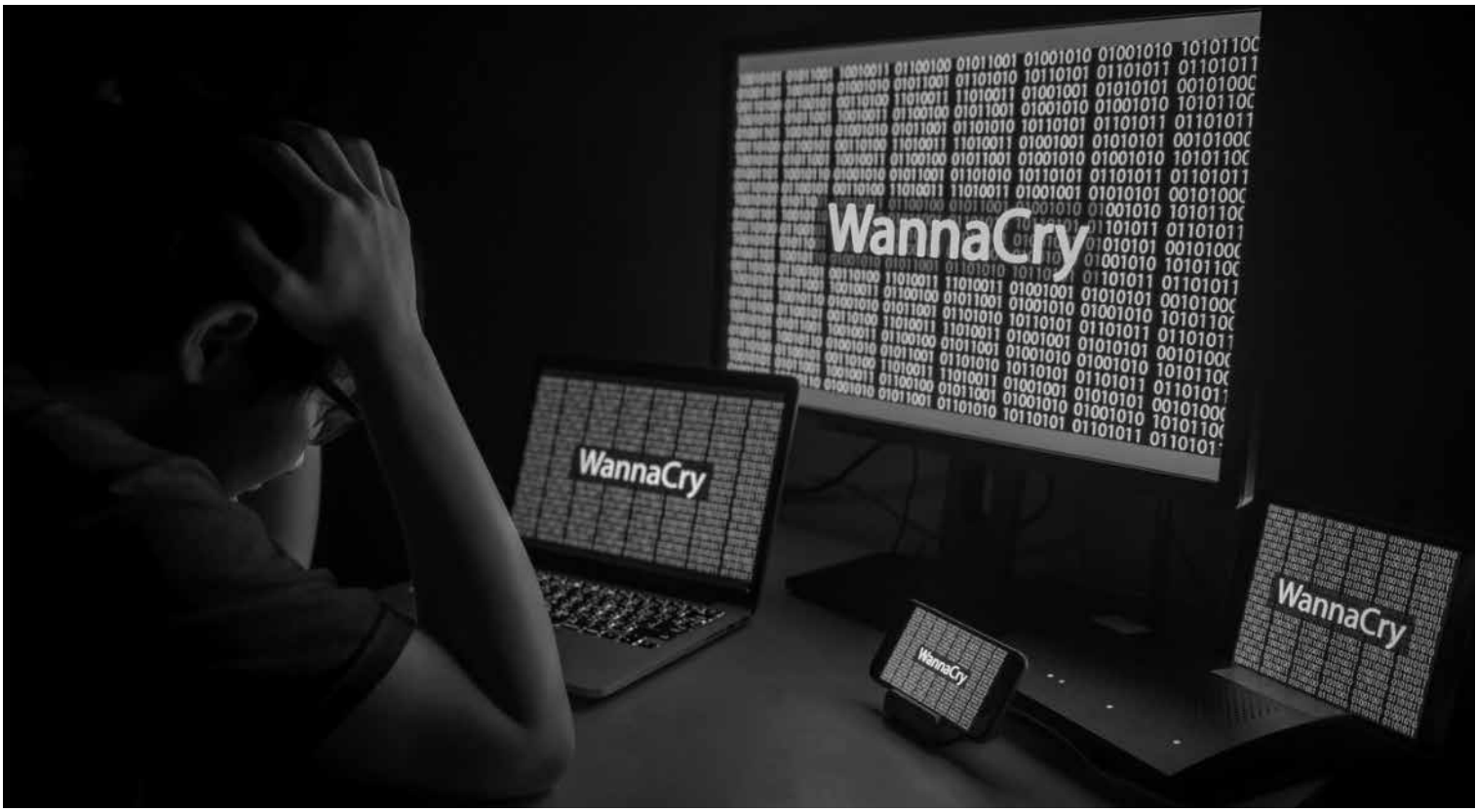
Este proyecto fue diseñado para apoyar y cumplir plenamente con el espíritu y la letra de este reglamento introduciendo una serie de conceptos centrales para definir cómo manejar información personal permitiendo a su vez dotar de capacidades de gobierno de datos, control de acceso, registro y auditoría, entre otras.

Estos conceptos centrales son los llamados consentimientos (una acción explícita y voluntaria que el cliente realiza para permitir que se realice una acción por ejemplo una firma en un papel, una grabación de voz o un clic en el botón "Autorizar" de un sitio web), los propósitos (la razón por la que se desea procesar información personal. Por ejemplo, una aplicación puede querer manejar información personal para crear una recomendación de película para un cliente) o procesamiento de datos (almacenar, transformar o acceder a información personal se considera procesamiento de datos).

3 *La importancia de la colaboración*

La realidad es que la ciberseguridad no consiste solo en estar preparado a nivel individual. Es necesario implantar normas, políticas y establecer relaciones con otros organismos capacitados para tomar decisiones en todo el entorno para acotar el campo de actuación de aquellos que quieren aprovecharse de la situación. La ciberseguridad es una cuestión de carácter global que necesita de la colaboración de todos los países para hacer frente a los retos que se plantean.

En España, es el Consejo Nacional de Ciberseguridad es el encargado de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privado tanto en el ámbito nacional como en el internacional. Como parte de este, el Instituto Nacional de Ciberseguridad de España (INCIBE), como sociedad dependiente del Ministerio de Economía y Empresa, a través de la Secretaría de Estado para el Avance Digital es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y



especialmente para sectores estratégicos contribuyendo así a construir ciberseguridad a nivel nacional e internacional.

Una de las relaciones centrales del Gobierno de España es la mantenida con la Organización de los Estados Americanos (OEA) bajo un acuerdo de colaboración para el desarrollo de diferentes acciones de cooperación que buscan reforzar los niveles de protección y resiliencia a nivel internacional. Algunas de las actividades llevadas a cabo han sido las siguientes:

- **International CyberEx:** consiste en la ejecución de un ciberejercicio virtual en donde se buscó fortalecer las capacidades de respuesta ante incidentes, así como una mejora de la colaboración y cooperación ante este tipo de incidentes en formato Capture The Flag (CTF). Este formato está basado en un modelo de competición de ciberseguridad diseñado para servir como un ejercicio de entrenamiento que permita otorgar a los participantes experiencia en el seguimiento de una intrusión, así como trabajar en las capacidades de reacción ante ciberataques análogos que sucedan en el mundo real.
- **Cybersecurity Summer BootCamp:** un programa de capacitación especializado en ciberseguridad dirigido a personal técnico que trabaje en Centros de Respuesta a Incidentes (CERTs o CSIRTs), miembros de Fuerzas y Cuerpos de Seguridad que trabajen en unidades operativas relacionadas con la ciberseguridad y personal en activo perteneciente a las carreras judicial o fiscal, abogacía del Estado, funcionarios de la Administración de Justicia y personal de organismos reguladores o legislativos que trabajen en áreas relacionadas con los aspectos jurídicos y normativos de la ciberseguridad.
- **Ibero-American Cybersecurity Challenge (ICSC):** el objetivo de esta iniciativa internacional es fomentar el talento en ciberseguridad y animar a los jóvenes a seguir una carrera técnica profesional en un sector con gran demanda y oportunidades, además de promover el conocimiento, el liderazgo y el fortalecimiento de las relaciones entre los países participantes.
- **Foro Internacional de Género y Ciberseguridad:** sus objetivos principales son el de promover el intercambio de información y el desarrollo de conocimientos sobre género y ciberseguridad, analizar la situación actual y problemática de género tanto a nivel nacional como internacional en relación al sector de la ciberseguridad y debatir sobre los principales problemas en relación a la violencia de género en el ámbito digital.

Actualmente, España ocupa el puesto quinto y séptimo a nivel europeo e internacional, respectivamente, en el Índice Global de Ciberseguridad que labora la ITU, un organismo de las Naciones Unidas que se centra en las

Tecnologías de la Información y la Comunicación. Cada año realiza una encuesta que mide el compromiso de los Estados Miembros con la ciberseguridad y que muestra cómo España está por encima de otros países europeos en este ámbito.

4 De profesión hacker

No solo ha ido cambiando la percepción de los conceptos de privacidad y seguridad, sino también las profesiones que se necesitan para llevar a cabo el cambio. El proceso que estamos presenciando sobre la digitalización de las compañías está llevando a un crecimiento de ofertas laborales solicitando perfiles bajo el título de analistas en ciberseguridad. Enmascarado bajo este formalismo, se encuentra la filosofía de la profesión del hacker.

El término 'hacker' no es algo nuevo. En realidad, fue definido en 1993 en un glosario realizado por el Grupo de Trabajo de Ingeniería de Internet (IETF). Ellos los definieron como aquella persona que se deleita en tener una comprensión íntima del funcionamiento interno de un sistema, de los ordenadores y de las redes informáticas en particular.

Esta inquietud por saber cómo funcionan los sistemas tiene un trasfondo muy lejos del estereotipo que se ha proyectado desde hace unos años en los medios de comunicación. El fin último de estas personas es hacer de Internet un mundo mucho más seguro, tanto para las compañías, organismos públicos o cualquier usuario que vaya a hacer uso de él. Sin embargo, el término es a menudo mal utilizado en un contexto peyorativo, donde cracker (o cibercriminal) sería el término correcto. Al final, un conocimiento tan profundo sobre una tecnología puede también ser utilizado con fines maliciosos llegando incluso a paralizar empresas por completo como fue el sonado caso de WannaCry.

Principalmente durante días como esos, es cuando las empresas que han invertido en seguridad y en este tipo de perfiles tienen que demostrar el nivel de madurez que han alcanzado y responder así a lo que está sucediendo sin apenas información. No solamente para identificar cuanto antes dónde se encuentra el problema y así dejar de ser vulnerables, sino también para compartir el conocimiento adquirido con el resto de compañías y organismos públicos para evitar que también lo sean.

Además de ese sentimiento por compartir, también les caracteriza el de ayudar a los demás. Comparten lo que saben de una forma completamente altruista cuyo único objetivo es concienciar a aquellos segmentos de la población que pudieran no estar tan concienciados con los riesgos que conlleva Internet. Una mínima formación en seguridad entre los más pequeños y su entorno, es ya esencial en un mundo que tiene los vestigios de convertirse completamente digital.

El término hacker no es algo nuevo. En realidad, fue definido en 1993 en un glosario realizado por el Grupo de Trabajo de Ingeniería de Internet (IETF). 'Hacker' es a menudo es un término mal utilizado en un contexto peyorativo, donde 'cracker' (o 'cibercriminal') sería el término correcto

Este tipo de proyectos que llegan a todo el mundo también sirven para visibilizar y hacer más atractivo el sector de la seguridad inculcándoles que no es una profesión imposible de acceder y que no es una profesión únicamente de hombres. Es importante que comencemos a cambiar entre todos el estereotipo impuesto en el pasado sobre el perfil del hacker para que nadie se quede fuera a la hora de elegir profesiones técnicas a las que dedicarse.
En conclusión, qué voy a decir yo, mi profesión mola. Tiene retos constantes cuyos días son muy diferentes, pero en mi opinión quizá lo más importante sea el poder que tenemos a día de hoy de abrir los ojos a la sociedad dando a conocer que no es cierto que todo tiempo pasado fue mejor. Si tuviera que elegir un momento de la historia para nacer y no supiera de antemano quién sería yo también elegiría el presente.