MESA REDONDA

El valor del dato en Ciberseguridad.

En el sector de la ciberseguridad, un simple dato procesado y gestionado a tiempo puede evitar una catástrofe. El valor de la información adquiere una nueva dimensión en el momento en el que nuestros sistemas TIC representan servicios esenciales, los activos de nuestra empresa o parte de nuestra vida privada.

D. RAÚL RIESCO
Gerente de Inteligencia y Sistemas de Control Industrial de INCIBE

Con la llegada del IoE (Internet of Everything) se ha producido una explosión del volumen de información que implica un aumento exponencial de los vectores de ataque. Esto nos exige desarrollar capacidades en la automatización de la prevención, detección y respuesta mediante una simbiosis entre nuevos conocimientos y capacidades humanas, y nuevas tecnologías *Big Data* unidas a *Machine Learning* e Inteligencia Artificial, entre otras tecnologías.

En el Instituto Nacional de Ciberseguridad (INCIBE) tratamos cada día de mejorar los servicios públicos que prestamos a ciudadanos, a expertos en ciberseguridad, y a empresas y profesionales que hacen uso de las TIC. Para ello, INCIBE destina esfuerzos a la protección de los sectores estratégicos, imprescindibles para la economía y la sociedad, y a las instituciones afiliadas a RedIRIS mediante diferentes algoritmos e infraestructuras para procesar los grandes volúmenes de información que manejamos, y que representan amenazas de variada naturaleza, como el conocido ataque *ramsonware* Wannacry[1].

Entre las preguntas que nos hacemos en el área de ciberinteligencia, destacan cuestiones como ¿cuál es la probabilidad y tipo del próximo ataque?, ¿quién podría estar detrás?, ¿cuál es la motivación del ataque?, ¿nos puede volver a pasar? ¿necesito la información RT *(real time)* o NRT *(near real time)*? y un largo etcétera. Asimismo, cabe

1 https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-oleada-ransomware-afecta-multitud-equipos

destacar que la información que dará respuesta a esas preguntas deberá ser accesible a diferentes públicos, no solo por nivel de acceso, sino por el tipo de negocio, estratégico, táctico y operativo.

"Las nuevas tecnologías y el IoE (Internet of Everything) nos llevarán a obtener servicios nunca imaginados hasta ahora."

Nuestra recomendación es plantearse continuamente preguntas clave y después modelar las arquitecturas y servicios TIC, y no al revés, Aunque por supuesto, siempre deberemos aprovechar las economías de escala y reutilizar nuestra arquitectura aún en proceso de amortización.

En nuestro caso, además de contar con millones y millones de eventos a procesar y relacionar entre sí, tanto externos como internos, de Internet o de la *Deep Web*, de dispositivos IT y OT, diariamente analizamos muestras de *malware* que producen cantidades enormes de información añadida al resto de eventos, como por ejemplo el modo en que han sido creadas para infectar. Es aquí donde, con el objetivo de dar respuesta a las preguntas clave que nos hacíamos en un principio, entra en juego el valor de los algoritmos aplicados sobre nuestro *Big Data*. Los datos por sí solos aportan gran cantidad de información de valor, si bien, dependiendo de los algoritmos aplicados sobre los mismos, el valor es aún mayor, puesto que nos permitirán prestar servicios que serán mejores o peores según lo buenos o malos que sean nuestros algoritmos y los de nuestros socios o "partners".

En ciberseguridad, como históricamente en el mundo de la seguridad o en muchos sectores, la tendencia es mejorar las capacidades mediante el trabajo en equipo y mediante el intercambio de información (IS – *information sharing*) por lo que es habitual trabajar con socios o "partners". Esta relación exige contar con la confianza suficiente entre las partes antes, durante y después del intercambio. Además, no siempre se podrá compartir toda la información según el tipo de clasificación.

Junto a la confianza y la clasificación, en dicho intercambio se deben cumplir una serie de criterios establecidos en los diferentes marcos regulatorios, tanto nacionales como internacionales, entre ellos, aquellos que velan por garantizar la privacidad de los datos de nuestros ciudadanos (ej. la reforma de la protección de datos en Europa - GDPR[2]). Los modelos de intercambio deben estar orientados a la obtención de una solución o respuesta a las preguntas clave y, por lo tanto, no es estrictamente necesario compartir información a nivel de dato, sino que se puede trabajar en la capa de algoritmos o incluso en la de servicios, como los de detección, prevención, respuesta.

El hecho de trabajar en la capa de servicios requiere según el caso, cierto nivel de garantía y de auditoría sobre los algoritmos con el objetivo de conocer el nivel de calidad del servicio, de la eficacia y de la eficiencia de los mismos. En nuestro caso, a modo de ejemplo, y aunque tengamos información de redes infectadas por "bots", nuestro servicio Antibotnet requiere colaboración activa con socios o "partners" como los ISPs *(Internet Service Providers)* para poder identificar al usuario final, avisarle y enviarle la guía de desinfección aportada por INCIBE. De otro modo, si el usuario de manera activa desea comprobar si está infectado, puede validar con nuestra base de datos de infecciones si hemos detectado recientemente alguna infección del tipo "bot" en su conexión. En todo el proceso, desconocemos la identidad del afectado y cumplimos la regulación en torno a la privacidad del usuario, si bien es cierto que quizá no sea el método más rápido de ayudarle en la desinfección.

Las nuevas tecnologías y el IoE (internet of Everything) nos llevarán a obtener servicios nunca imaginados hasta ahora. Estos datos, además de masivos, serán de variada naturaleza (ej. imágenes obtenidas con drones), complicando aún más nuestro trabajo ya que aumentará el vector de ataque de cada uno de nosotros y el de nuestras organizaciones. Por otro lado, el mayor número de datos permitirá entrenar aún más algoritmos de *machine learning* e inteligencia artificial: tecnologías que serán prácticamente necesarias ante la explosión del número de dispositivos, eventos e incidentes y sobre todo, ante la incapacidad de intervención humana en todos esos casos.

Así, los recursos humanos deberán focalizarse cada vez más en trabajar en conjunto con las máquinas, en simbiosis, tratando de afrontar los problemas de forma conjunta, y en muchos casos, atajarlos sin intervención humana. Algunos experimentos se están realizando ya, a modo de competición, en EEUU a través de DARPA Cyber Grand Challenge[3].

2 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

3 http://archive.darpa.mil/cybergrandchallenge/

Las reglas y algoritmos se podrán por tanto definir no solo por parte de los operadores, sino mediante inferencia, esto es, mediante razonamiento automático.

Por tanto, el presente y futuro inmediato es retador a la vez que interesante, puesto que ofrece oportunidades en torno a la eficiencia, la detección preventiva e inferencia, o la obtención de nuevo conocimiento de valor mediante la capacidad que nos aportarán los sistemas.

Si bien, en base a nuestra experiencia, nos encontramos ya con diferentes problemas que necesitamos ir salvando, como por ejemplo el presupuesto limitado (especialmente desde la Administración General del Estado), los procesos de contratación pública o de compra pública innovadora, la necesidad de mejorar la estandarización, la falta de conocimiento multi-disciplinar (incluyendo a nuestras empresas proveedoras), la gestión de la privacidad, la dificultad para ciertos usuarios a nivel estratégico y táctico para la definición de sus propias reglas y alertas (ya que en general se requieren conocimientos técnicos en lenguajes como SCALA o metalenguajes como Apache Pig[4]), e incluso la clasificación que algunas de estas tecnologías *Big Data* realizan de los eventos que, en nuestro caso, hemos debido modificar para una mayor eficiencia en las búsquedas.

En todo caso, por lo que conocemos del sector de la ciberseguridad, España está posicionada como referencia fundamentalmente en la aportación de talento que aporta a la comunidad internacional. Quizá nos falta aún por mejorar las capacidades para identificar y poder retener el citado talento, más aun cuando el futuro inmediato prevé que este tipo de profesionales serán fundamentales incluso para cuestiones de seguridad nacional. Desde INCIBE estamos tratando de mejorar la identificación de este talento mediante competiciones y pruebas de habilidad como CyberCamp[5], así como su retención y gestión a través de diversos programas[6].

"El futuro inmediato prevé que este tipo de profesionales serán fundamentales incluso para cuestiones de seguridad nacional."

Teniendo en cuenta que siete de cada diez personas trabajarán en profesiones que aún no existen[7], nuestros más pequeños ya están comenzando a recibir un cambio en el sistema educativo orientado a adquirir determinadas destrezas en la resolución de problemas complejos así como en el trabajo en equipo desde su esencia. Si sumamos la ética profesional, la implicación en la conservación del planeta, y la restauración de los valores y principios como el de la familia y las relaciones personales, seguro que tendremos grandes profesionales en España como hemos tenido siempre, y la tecnología no será un problema o una amenaza por los riesgos que estamos viendo que también conlleva cada avance, sino que será una gran solución. Esto requiere asimismo de medidas que permitan retener el talento, lo cual podría no ser difícil, aunque es cierto que deberían cambiarse algunas cuestiones de calado en la profesión.

Como opinión personal, creo que algunas de las futuras profesiones que aún no se conocen compartirán, como mínimo común denominador, la capacidad de trabajar en simbiosis con la tecnología para aportar eficiencia y mayor conocimiento de valor. Sin duda, habrá grandes descubrimientos gracias a un uso adecuado de técnicas *Big Data*, *Machine Learning* e Inteligencia Artificial. ✱

4 https://pig.apache.org/

5 https://cybercamp.es/

6 https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe_infografia_0.pdf

7 http://www.abc.es/economia/20140922/abci-siete-cada-diez-bebes-201409191727.html