Óscar Navarro

Director de ciberseguridad industrial en S2 Grupo

"Los especialistas en ciberseguridad son todavía un recurso escaso, comparado con la magnitud de la amenaza"

M. R.

La ciberseguridad nacional es de suma importancia para un país, debido a los riesgos que entraña el nuevo panorama digital. El aumento del número y de la complejidad de los ciberataques que reciben las redes militares en los últimos años, así como las formas de espionaje y el robo de información a través de la tecnología -como el caso Pegasus-, y la guerra fría entre la OTAN y Rusia, han provocado que aumente aún más, si cabe, la importancia que se le da a la ciberdefensa.

S2 Grupo es una compañía de referencia en Europa y Latinoamérica en materia de ciberseguridad, ciberinteligencia y operaciones de sistemas de misión crítica, y forma parte de AESMIDE.

Como miembro de AESMIDE, la Asociación de Empresas Suministradoras del Ministerio de Defensa, ¿cómo se lleva a cabo la colaboración con este Ministerio, desde S2 Grupo?

AESMIDE nace en 1984 con el objeto de servir de interlocutor de las empresas de servicios y suministros ante el Ministerio de Defensa español. Nos permite gracias, a las actividades que organiza, recibir de primera mano las distintas necesidades que tiene el MINISDEF, y también cómo articular sinergias entre los asociados que permitan un mejor cumplimiento de las necesidades de nuestras Fuerzas Armadas. Permite que, de un modo transparente, en mundo empresarial, reciba información y a la vez presente las capacidades de la industria española.

En líneas generales, ¿cuáles son los principales retos y amenazas a los que se enfrenta actualmente el ámbito militar en materia de ciberseguridad?

Pues de forma básica, podemos decir que se trata de los mismos que los del resto de la sociedad y la industria: por un lado, se introduce tecnología que permite a los sistemas de defensa ser más eficientes y efectivos. Pero a la vez, este proceso los haces vulnerables a nuevos tipos de amenazas, los mismos a los que estábamos acostumbrados en el contexto de las TIC. Alcanzar un equilibrio entre funcionalidad y ciberseguridad es imprescindible. Este proceso requiere cambios no solo en tecnología, sino también en organización, ya que es necesario introducir la ciberseguridad en todas las operaciones como un proceso más. Por otra parte, es posible también aprovechar esta situación para el desarrollo de nuevas capacidades en este terreno, tanto desde un punto de vista defensivo como ofensivo.

Óscar Navarro.

¿Qué consecuencias podría tener un ataque cibernético en este terreno?

Todo depende del contexto donde este se desarrolle, pero teniendo en cuenta la evolución tecnológica, un ciberataque en el terreno militar puede afectar directamente a infraestructuras esenciales para la sociedad. En el ámbito cibernético no hay, en principio, limitaciones en cuanto a los objetivos, ya que no son precisos para su ejecución despliegues en el terreno físico, lo que hace que su impacto potencial pueda alcanzar a un elevado número de ciudadanos. Desde el punto de vista estrictamente militar, el propio equipamiento es susceptible de sufrir este tipo de ataques, ya que los sistemas de armas dependen para su funcionamiento de tecnologías operacionales: vehículos blindados, aeronaves, buques e incluso plataformas logísticas o de mantenimiento. En el límite podría afectarse gravemente la capacidad de combatir de un ejército, especialmente si se selecciona adecuadamente el momento y se coordina con operaciones convencionales.

> "Un ciberataque en el terreno militar puede afectar directamente a infraestructuras esenciales para la sociedad"

Teniendo en cuenta los conflictos bélicos actuales, como el de Rusia y Ucrania, ¿se puede afirmar que el ciberespacio es el escenario belicoso de última generación?

Podríamos decir que el ciberespacio ha sido en los últimos tiempos el campo donde se ha estado librando una especie de guerra fría por otros medios, y sin duda se incorpora como un componente más a los escenarios tradicionales. La campaña militar en Ucrania es un ejemplo de estos escenarios, en los que las acciones convencionales se ven precedidas o complementadas con ataques para tratar de limitar la capacidad de combatir del adversario, afectar a su logística, la moral de los ciudadanos o incluso la imagen pública ante sus aliados. En relación con esto, debido a la dificultad de atribución de los ataques, se ha establecido un nuevo

concepto en que la ciberguerra es un punto fundamental: las operaciones en zona gris.

La alta dependencia tecnológica de nuestra sociedad es una realidad constatable, aunque resulta imprescindible para el buen funcionamiento de los Estados, sus Fuerzas y Cuerpos de Seguridad, y sus infraestructuras. En este contexto, cada vez será más necesario actuar en el ámbito de la ciberseguridad, ¿cómo afrontan desde S2 Grupo las nuevas necesidades y amenazas que van surgiendo?
Estamos en continuo contacto con la Administración, empresas que operan en sectores estratégicos, y las Fuerzas y Cuerpos de Seguridad del Estado, para identificar los desafíos a los que se enfrentan y las necesidades en materia de ciberseguridad. S2 Grupo realiza una importante inversión en I+D+i, que se dirige en muchos casos a desarrollar las herramientas que este cambiante panorama de amenazas exige.

En su opinión, ¿es todavía insuficiente la inversión en I+D+i en el desarrollo de tecnología propia, como único camino para crear soluciones que permitan a Europa ser independiente tecnológicamente en el ámbito de la ciberseguridad?
Desde luego es fundamental disponer de tecnología propia en ámbitos fundamentales como son, por ejemplo, las comunicaciones y, por supuesto, la ciberseguridad. En este sentido y como compañía que desarrolla tecnología propia, española y europea, para la detección y respuesta ante amenazas, se está realizando una fuerte inversión en I+D+i en este campo, pero se requiere de un apoyo todavía más decidido por parte de las administraciones públicas nacionales y europeas. Afortunadamente, en los últimos tiempos, y en parte a causa de los cambios en el contexto internacional, se ha tomado conciencia por parte de los gobiernos de esta necesidad y se están dando pasos en la dirección correcta.

¿Cuáles son los últimos avances tecnológicos que se están experimentando en la ciberdefensa?
Pues las principales líneas de trabajo se están dirigiendo a aumentar las capacida des defensivas de los equipos de ciberseguridad. Los especialistas en ciberseguridad son todavía un recurso escaso, comparado con la magnitud de la amenaza, por lo que la incorporación de técnicas

> "Afortunadamente, se ha tomado conciencia por parte de los gobiernos de esta necesidad"

de automatización en las herramientas utilizadas en la detección y respuesta a amenazas es una línea de trabajo fundamental, como lo es el uso de inteligencia artificial aplicada a la ciberseguridad. Esto se complementa con el desarrollo de herramientas que permitan a los equipos y autoridades, con competencias en la gestión, disponer de una conciencia situacional que permita una mejor asignación de los recursos y una respuesta más ágil. S2 Grupo está colaborando con el Centro Criptológico Nacional en todas estas líneas.

¿Qué proyectos están desarrollando en estos momentos en S2 Grupo, incluido el ámbito de la industria?
Además de lo comentado anteriormente, en el ámbito de la industria se están implementando un número creciente de iniciativas, como consecuencia del incremento de madurez en estas cuestiones del sector y las nuevas exigencias regulatorias, como las derivadas de las directivas europeas NIS2 (2022/2555) y de resiliencia de las entidades críticas (2022/2557). En particular, S2 Grupo está colaborando con clientes de distintos sectores industriales, como energía, construcción naval, ferrocarriles, etc., en la incorporación de la ciberseguridad desde el diseño en los procesos de ingeniería y construcción, incluyendo la definición de criterios que se incorporan a las pruebas FAT y SAT. Otras líneas de trabajo cada vez más demandadas son la consultoría especializada sobre arquitecturas seguras y la evaluación técnica de dispositivos. Por último, cabe destacar el desarrollo de sondas embarcadas para la monitorización de alertas de seguridad en plataformas móviles como buques, trenes o automóviles.

¿Cómo se encuentra el mercado laboral en lo que respecta a la ciberseguridad? ¿Hay una alta demanda de estos expertos?
En general hay importantísima demanda no cubierta de perfiles tecnológicos y en particular de especialistas en ciberseguridad. INCIBE estimaba que en 2021 había unas 24.000 posiciones no cubiertas en España. Se trata de un fenómeno a escala global. Es cierto que se está haciendo un esfuerzo en la incorporación de la ciberseguridad en

> "En general, hay una importantísima demanda no cubierta de perfiles tecnológicos y en particular de especialistas en ciberseguridad"

los planes de estudios existentes, así como la creación de estudios específicos, pero siguen siendo claramente insuficientes. De hecho, S2 Grupo ha creado su propio programa de formación en ciberseguridad, denominado Enigma, que ya acumula 8 promociones de alumnos, que en muchos casos se incorporan como empleados a la compañía.

Los ciberataques son fenómenos relativamente nuevos y con ciertos agujeros legales, ¿qué sería necesario legislar a corto y medio plazo?
Pues precisamente en este momento, la expectativa está en la transposición a la legislación española de las nuevas directivas europeas, especialmente en lo relacionado con el nuevo esquema de certificación de productos. Básicamente, todo equipo o dispositivo con capacidades de conexión a una red va a precisar de un proceso de validación desde un punto de vista de ciberseguridad, para poder ser empleado en la Unión Europea. Esto implica desde un robot aspirador doméstico o una cafetera, hasta el equipamiento que forma parte del sistema de control industrial de una central de generación. Esto va a suponer un cambio fundamental a la hora de extender la demanda de requisitos de ciberseguridad a lo largo de toda la cadena de suministro, e implicará una transformación profunda del sector industrial, lo que servirá de base para garantizar una efectiva transformación digital en la industria.