ENTREVISTA **Olmo Rayón** Manager de Ciberseguridad en España para Getronics

Ciberseguridad, el nuevo reto directivo

La pasada semana Getronics, empresa especializada en soluciones para la transformación y la evolución digital, participó en Cyber Europe, un evento de ciberseguridad a nivel europeo. Hablamos con Olmo Rayón, experto en ciberseguridad y participante de esta iniciativa.

Getronics ha participado en Cyber Europe, un ejercicio coordinado en la UE para conocer su respuesta ante un ciberataque

Dedicado a la ciberseguridad desde que acabara sus estudios, Rayón posee un amplio conocimiento en este campo. Cuenta con experiencia como consultor para empresas y organizaciones de diversos tipos, tamaños y sectores, lo que le permite tener una visión global de la situación del sector a nivel nacional e internacional. Actualmente, compatibiliza su actividad consultiva y de asesoría con la docencia en un máster universitario en el EAE Business School. Como recalca Rayón; "intentando ayudar a los que están empezando".

¿Cómo llega Getronics a participar en Cyber Europe?

Considero especialmente relevante, como profesional en el campo de la ciberseguridad, mantener un contacto cercano con el ecosistema. Existen multitud de foros, eventos y congresos que facilitan este contacto entre organizaciones y profesionales del sector y donde estar al tanto de este tipo de iniciativas. En el caso de Cyber Europe, recibimos la oportunidad de participar desde el Instituto Nacional de Ciberseguridad (Incibe). Para nosotros, este programa ha sido una forma perfecta de conocer nuestra madurez tanto a nivel interno como de país, y en particular la industria de la salud.

¿En qué ha consistido su participación en el evento?

Cyber Europe es un ciberejercicio a nivel europeo en el que participan 27 países y que dura 48 horas. Durante estos dos días se simula una oleada de ciberataques, a nivel global, contra multitud de sistemas críticos (en este caso, el sector de la salud). Se analiza al detalle las respuestas tanto de los responsables de las organizaciones atacadas (fundamentalmente hospitales) así como la coordinación de estos con los proveedores de servicios (como en este caso Getronics) y, a su vez, la de los proveedores con los cuerpos de seguridad (INCIBE y Departamento de Seguridad Nacional), para frenar los ataques. Es, en definitiva, un ejercicio militar llevado al campo de la ciberseguridad.

¿Qué balance hacen del ejercicio?

En mi opinión ha sido todo un éxito, desde el planteamiento enfocado al sector de la salud, hasta su ejecución. La manera en que tanto el INCIBE, como el ENISA (Agencia de la Unión Europea para la Ciberseguridad) coordinaron todo ha sido excelente, han logrado una simulación muy real. Este ejercicio permitirá extraer muchas conclusiones, tanto de lo bien hecho como de los puntos de mejora de este sector.

En su opinión, ¿estamos preparados para posibles ataques?

Los avances tecnológicos han permitido unas mejoras muy importantes en la usabilidad, agilidad y en la comodidad de muchísimos procesos. Lamentablemente, en muchos casos se ha pensado poco en las puertas que esos mismos avances han dejado abiertas para usos malintencionados. Es impresionante lo que la tecnología posibilita, como poder operar a una persona remotamente o el usar la inteligencia artificial para afinar o agilizar diagnósticos, pero como experto en ciberseguridad me surgen cientos de preguntas y preocupaciones. Respondiendo a su pregunta, creo que queda un gran camino por recorrer. Y ese camino pasa por lograr que el desarrollo y la ciberseguridad vayan de la mano, diseñando sistemas con la máxima seguridad desde las etapas más tempranas.

Sentido común…

Así es. Siempre pongo el ejemplo de la automoción. Sería impensable fabricar coches sin frenos y que, una vez hecho el coche, se le intente poner un mecanismo de frenada. Trasladado esto a la ciberseguridad, hay que dejar de verla como una funcionalidad más y empezar a verla como un elemento clave que va a marcar la diferencia entre sobrevivir empresarialmente o no. No nos podemos olvidar, que, más allá de los ciberdelincuentes que buscan únicamente el lucro financiero de un ataque, hoy en día encontramos muchos otros motivos por los que atacar un negocio: ideológicos, políticos, activismo… incluso empleados descontentos.

Ha dedicado su carrera a la ciberseguridad. ¿cuáles son los retos en esta materia?

El área que considero más relevante, común a cualquier empresa y que puede habilitar un avance real en este campo es el apoyo e implicación de la capa ejecutiva. La ciberseguridad ha llegado para quedarse; por un lado, los equipos directivos deberán adentrarse en la materia y tener una visión de alto nivel de su situación y siguientes pasos y por el otro, los profesionales del sector tienen el papel de simplificar y agilizar el proceso.

En el caso de las organizaciones públicas, creo que se está haciendo un gran trabajo en el área de la normalización. La aplicación de la nueva ley de protección de datos de 2018 (GDPR) fue un gran avance y sentó un precedente importante. Creo firmemente en la función de la normalización y la aprobación de leyes que exijan a las organizaciones medidas para protegerse, tanto a sí mismos, como a sus clientes.

¿En qué consiste un SOC? ¿por qué son unas instalaciones tan críticas y controladas?

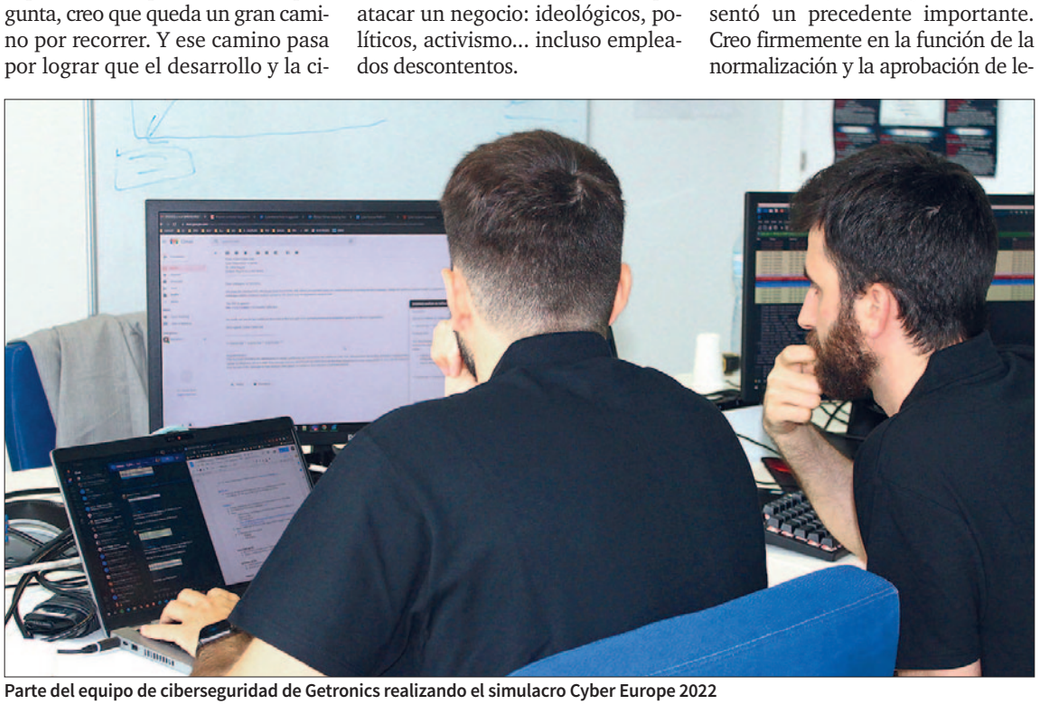
Para entender correctamente la posición del Centro de Operaciones de Seguridad (SOC), es interesante remontarse a la estrategia de ciberseguridad de una compañía. El SOC representa la columna vertebral. Este articula todas las iniciativas de ciberseguridad marcadas en la estrategia y opera todos los servicios definidos para brindar protección en las áreas más críticas.

El SOC es un centro de mando y control, coordinado y operado por expertos de las diferentes áreas tecnológicas que tiene una organización (web, móvil, IoT, redes, etc.) monitorizando y respondiendo en tiempo real a cualquier detección que se pueda dar.

¿Qué le diría a una compañía que esté comenzando con un proyecto de este tipo?

Comienzo respondiendo qué no debería hacer una organización: desplegar tecnología y proyectos de protección sin una revisión objetiva, estructurada y que establezca prioridades dentro de los riesgos a los que está sometida. Son muchas las compañías que encuentro con tecnología desplegada que no tiene razón de ser y que, con un correcto análisis y valoración, podrían haberse ahorrado.

Recomiendo encarecidamente que las organizaciones tomen el tiempo necesario en obtener una visión clara de lo que tienen y de cómo pueden ser atacadas. Entender cuáles son los sistemas que realmente les van a proteger, por qué y quién los va a mantener y operar internamente una vez los despliegues hayan terminado.



Parte del equipo de ciberseguridad de Getronics realizando el simulacro Cyber Europe 2022