ARTÍCULOS DE OPINIÓN

¿CUÁLES SON LOS DESAFÍOS EN CUANTO A CIBERSEGURIDAD EN 2023?

Victor Poitevin
Editorial & Digital Manager, Stormshield

Después del covid-19 como tema de fondo del año 2021, el año cibernético de 2022 ha estado marcado por otras fuertes tendencias que orientarán el año que empieza: crisis económicas, ecológicas y sociales, conflictos geopolíticos o el surgimiento de una inteligencia artificial accesible para todos... ¿Cuáles serán los retos de la ciberseguridad para 2023? Ejercicio de prospección y tendencias.

EL DESAFÍO DE LA CONTRATACIÓN

El mercado de la ciberseguridad lleva varios años sufriendo una gran escasez de mano de obra. Según el estudio *Cybersecurity Workforce Study 2022*, al parecer hay por lo menos 3,7 millones de puestos de trabajo que cubrir en todo el mundo.

Tras verse sacudido por las oleadas de la «Gran Dimisión» posconfinamiento, el sector de la ciberseguridad también está viendo cómo aumenta su tasa de rotación. En este mismo estudio, el 21 % de los encuestados habría cambiado de trabajo en los últimos 12 meses, un 13 % más que el año pasado. Salario, condiciones de trabajo, razón de ser de la empresa: elementos que se tienen en cuenta a partes iguales en la decisión final de los candidatos.

Una carencia que llega a plantear una pregunta terrible: **¿puede morir una empresa de ciberseguridad por falta de recursos humanos?** Para algunas empresas de servicios de ciberseguridad, el año 2022 nos ha demostrado hasta dónde puede llegar el problema. Una situación destinada a extenderse en 2023: ¿vamos hacia un SOC sin recursos y que no puede reaccionar con la suficiente rapidez ante una alerta crítica? ¿hacia empresas sin RSSI?

Pero el sector se está movilizando y activando. Si bien el contexto geopolítico de 2022 ha empujado a grupos de hackers éticos a apoyar a los gobiernos, el movimiento podría continuar en 2023. ¿Hasta estructurarse? Por otro lado, la sensibilización en las escuelas o incluso el creciente número de cursos de formación en ciberseguridad son verdaderas promesas para el futuro. Pero la creación de estos nuevos talentos plantea otras preguntas: ¿cuándo estarán disponibles? y ¿esto es fiable a largo plazo? Sobre este mismo tema de la contratación, hay que observar con atención lo que ocurre en Google, Microsoft o incluso Meta... **¿Y si la oleada de despidos en tecnología fuera una oportunidad para la cibernética?** Al igual que la pregunta, el mercado de los fichajes está abierto.

EL RETO DE LA COOPERACIÓN ENTRE EDITORES

Con la sofisticación de los ciberataques, el analista cibernético ya no puede basarse únicamente en los datos reportados por el cortafuegos acerca de la red o el agente de protección acerca del equipo de trabajo. Debe tener una visión general de lo que sucede en el sistema de información.

Para ayudarle a tener esta visión general, un producto de ciberseguridad debe agregar, correlacionar y clasificar los datos que produce y recibe. Porque la puesta en común de estos flujos de datos, de diferentes fuentes, como bases de datos de reputación o de información de *Cyber Threat Intelligence* (CTI), es lo que mejor permite detectar la amenaza. **La detección, la protección y la remediación se convierten entonces en las diferentes piezas del mismo engranaje.** La ciberseguridad tal como la conocíamos está evolucionando, con la adopción de tecnologías como EDR, XDR o incluso NDR. Pero este enfoque también puede ir asociado a una acumulación de productos de ciberseguridad en las empresas. Esto implica una organización que prever para las grandes empresas y un quebradero de cabeza para las más pequeñas, por no hablar de la partida presupuestaria. Todo eso hace sentir una necesidad de racionalización. Pero, ¿cómo racionalizar? ¿Y con que herramientas? Una ciberresiliencia que deberá construirse, más que nunca, en torno a la noción de colaboración entre editores.

Una colaboración que solo puede tener lugar con cierta dosis de humildad, una palabra clave para compartir en la comunidad cibernética.

EL RETO DE LA INTELIGENCIA ARTIFICIAL

Lanzado a finales de 2022, el módulo de conversación ChatGPT ya ha hecho correr ríos de tinta. Y seguirá haciéndolo a medida que los ciberdelincuentes recurran a él. Unos lo presentan como inteligencia artificial y otros como un agente conversacional, pero hay que reconocer que ChatGPT permite sobre todo obtener respuestas elaboradas a casi cualquier petición.

Peticiones tales como escribir líneas de código. **¿Entonces cualquiera podría convertirse en un ciberdelincuente?** Tal vez no, porque los scripts pueden contener una serie de errores y, por lo tanto, las soluciones de protección los detectarían con relativa facilidad. Pero aun con todo permiten a los ciberdelincuentes novatos familiarizarse con el tema y a otros ahorrar tiempo en las fases de compilación del código. Al mismo tiempo, el módulo ChatGPT se puede usar para escribir textos convincentes y, por lo tanto, abrir una nueva era para el phishing… Con la incorporación de avances en materia de deep fake, síntesis de vídeo, audio e incluso de voz, la capacidad ofensiva de los ciberdelincuentes se refuerza. Tanto es así que algunos profetizan la aparición de una verdadera inteligencia artificial maliciosa, como SkyNet en Terminator.

Para los editores, esta forma de inteligencia artificial no es nueva; ya está presente en las soluciones de ciberseguridad desde hace muchos años, como por ejemplo en el análisis del comportamiento. Por lo tanto, el desafío estará más bien aquí al nivel de la capacidad de procesamiento de datos para identificar ataques cibernéticos. En esta guerra asimétrica entre editores y ciberdelincuentes, ¿quién logrará dominar mejor estas nuevas tecnologías? La carrera está reñida...

EL DESAFÍO ECOLÓGICO

El control de la huella ambiental digital es un tema delicado. En junio de 2020, el Senado advirtió que el sector emitía el 2 % de los gases de efecto invernadero en Francia (estimado en un 4 % a nivel mundial, en comparación con el 2,6 % de la aviación civil, por ejemplo). Recientemente, la agencia francesa ADEME advirtió que sin un cambio profundo en el uso de la tecnología digital, esta participación podría duplicarse a nivel mundial para 2025. Y aunque se las señale habitualmente, las plataformas de streaming no son las únicas que tienen algo que hacer al respecto.

El mundo de la ciberseguridad no es responsable de todo este 2 %, pero sí que tiene su parte. Debido a la proliferación de productos de ciberseguridad en las empresas, su huella de carbono está aumentando mecánicamente al generar grandes cantidades de datos, almacenados y replicados en entornos remotos en la nube. Y aparte de generar gases de efecto invernadero, tanto la ciberseguridad como la informática consumen mucha agua. Por ejemplo, los centros de datos de Microsoft en los Países Bajos habrían consumido nada menos que 84 millones de litros de agua en 2022, según el diario neerlandés *Noordhollands Dagblad*. Es decir, el consumo anual de 1750 ciudadanos.

Por tanto, uno de los grandes retos tecnológicos del futuro será mantener el mismo nivel de eficiencia racionalizando los productos de ciberseguridad, reduciendo el volumen de datos recogidos y mejorando el consumo de recursos materiales. En Francia, en octubre de 2022 se inició un proyecto de investigación para «evaluar concretamente los beneficios de los servicios digitales en el borde de la red». El objetivo: tener en cuenta la capacidad de generación de calor de los equipos y distribuirlo mejor en entornos de producción donde sea necesario aportar calor. Digital y ecología, ¿por fin compatibles?