La ciberseguridad no es opcional en un mundo digital

Pilar López // Presidenta de Microsoft España

El mundo es cada vez más digital. Nos encontramos en un nuevo entorno de mercado donde la digitalización es la única respuesta para garantizar el crecimiento y competitividad de nuestras economías y mejorar la vida de las personas.

Si bien es cierto que en los últimos años estábamos asistiendo a la transformación tecnológica de muchas empresas, la pandemia ha acelerado la digitalización de la forma en la que trabajamos, aprendemos y en definitiva vivimos. Tanto es así que, en los dos primeros meses de la COVID-19 muchas organizaciones avanzaron el equivalente a dos años en sus procesos de digitalización. Por ejemplo, tecnologías como el *cloud computing*, la nube, ha permitido a las empresas habilitar escenarios de teletrabajo en cuestión de horas. En España, hemos pasado de un 15% de empresas con una estrategia de teletrabajo a un 83%.

> Las actividades de los ciberdelincuentes se han vuelto más sofisticadas y han aumentado los ataques que se centran en objetivos de alto valor, como gobiernos o infraestructuras críticas

Ahora es momento de avanzar con lo aprendido y entrar en una etapa de "reimaginación" donde la tecnología juega un papel principal. Si antes de la pandemia confiábamos en el potencial de las tecnologías, tras la situación que estamos viviendo, esta confianza es, si cabe, aún mayor. Pero, en este proceso, además de con una enorme oportunidad, nos encontramos con nuevos desafíos. En los últimos meses se han incrementado los ciberataques que afectan a todas las organizaciones, independientemente de su tamaño o sector. Además, las actividades de los ciberdelincuentes se han vuelto más sofisticadas y han aumentado los ataques que se centran en objetivos de alto valor, como gobiernos o infraestructuras críticas.

En este sentido, en Microsoft disponemos de un programa denominado Government Security Program[1] gracias al cual proporcionamos información a las autoridades de más de 45 países, entre ellos España, sobre amenazas de seguridad que pudieran afectar a nuestra tecnología. El objetivo último es dotar de la mayor información posible, de forma transparente y proactiva, a los responsables de ciberseguridad a nivel nacional.

COVID-19 como señuelo para los ciberataques

Los ciberdelincuentes aprovechan las debilidades de las organizaciones. Así, los datos del informe anual de defensa digital[2] que realizamos en Microsoft señalan que la pandemia está provocando ataques dirigidos a los más vulnerables, aprovechando los escenarios tan frecuentes como el trabajo remoto, las cadenas de suministro o servicios esenciales como los del sector sanitario. Conscientes de la sobreinformación acerca del coronavirus, los ciberdelincuentes se aprovechan del estrés y de este caos informativo y de la facilidad que tenemos de hacer clic en cualquier enlace, para llevar a cabo técnicas de *phishing*.

Según datos de nuestro último Índice de Civismo Digital (ICD), "Civismo, seguridad e interacciones online-2020"[3], un informe anual en el que analizamos el comportamiento y el riesgo que corren adolescentes y adultos en la red, España, con un 44% se ha situado 13 puntos por encima de la media mundial en cuanto a engaños, estafas y fraudes en Internet. En esta categoría se incluyen la difusión de rumores falsos como las "cartas en cadena"; intentos criminales para obtener información personal; o los correos electrónicos falsos que llegan de un destinatario conocido y que esconden software malicioso. Además, un 34% dice haber recibido contacto no deseado en Internet y un 26% afirma haber sido víctima de *"sexting"*, un término que hace referencia al envío no deseado y recepción de mensajes, imágenes, vídeos u otros recursos, con

1 https://www.microsoft.com/en-us/securityengineering/gsp
2 https://www.microsoft.com/en-us/securityengineering/gsp
3 https://www.microsoft.com/es-es/security/business/security-intelligence-report

contenido sexual a través del móvil u otro dispositivo en la red.

Todos los países del mundo han sido víctima, al menos, de un ataque con temática COVID-19. De los millones de emails sospechosos que Microsoft analiza cada día, aproximadamente 60.000 incluyen archivos adjuntos o enlaces maliciosos relacionados con la COVID-19. Aunque esa cifra parece muy grande, es menos del 2% del volumen total de amenazas que rastreamos y contra las que protegemos activamente a diario. En definitiva, el volumen y la complejidad de los ciberataques ha crecido de forma notable en los últimos meses y, de hecho, se espera que las amenazas de seguridad puedan suponer un coste de 8.000 millones de dólares en 2022 en todo el mundo.

Las empresas han respondido a la pandemia aumentando los presupuestos, incorporando personal especializado y acelerando el despliegue de tecnologías de seguridad basadas en la nube para adelantarse a los ataques de *phishing* y avanzar hacia arquitecturas de *Zero Trust*. Ante la presión para reducir los costes y la incertidumbre que ha traído consigo la COVID-19, muchas organizaciones están dando prioridad a las inversiones de seguridad. Pero… ¿cómo deberían asignarlas?

Las empresas tienen que aprender a protegerse y diseñar un plan global de seguridad que incluya la correcta gestión de la identidad, la detección de amenazas, la protección de datos y la monitorización unificada. El reto para las organizaciones es elegir proveedores tecnológicos que garanticen una nube segura y preparada para el cumplimiento regulatorio allá donde desarrollen su actividad, así como crear una cultura empresarial responsable que evite que el factor humano se convierta en el eslabón más débil de la cadena ante los ataques basados en ingeniería social.

Microsoft, estrategia Zero Trust y apuesta por la Inteligencia Artificial

Es una lucha para las organizaciones de cualquier tamaño, y para el sector público y privado por igual. A medida que nos adentramos en esta nueva fase de transformación digital, con la tecnología cada vez más entretejida en nuestras actividades más básicas, las preguntas que debemos plantearnos como defensores de la seguridad son las siguientes ¿Cómo ayudamos a las personas a confiar en la seguridad de sus dispositivos, sus datos y sus acciones online? ¿Cómo protegemos a las empresas y organismos para que tengan tranquilidad y puedan innovar y hacer crecer nuestra economía y ofrecernos un futuro alentador? ¿Cómo fomentamos la confianza en un mundo de confianza cero?

En Microsoft nos tomamos muy en serio este desafío. Con la seguridad en nuestro ADN, somos apasionados partidarios de una mentalidad de confianza cero –*Zero Trust*–, que abarque todo tipo de amenazas, tanto las de fuera como las internas. Creemos que el enfoque correcto es abordar la seguridad, el cumplimiento, la identidad y la gestión como un todo interdependiente, y extender la protección a todos los datos, dispositivos, identidades, plataformas y nubes, sean o no de Microsoft. Es decir, una apuesta decidida en cada uno de los cuatro grandes aspectos que permiten una protección de 360 grados: gestión de identidades y autenticación, detección proactiva y avanzada de amenazas, protección de los datos, cumplimiento y monitorización unificada. Nuestra estrategia en ciberseguridad es única en la industria, de extremo a extremo, por un lado, con un enfoque integrado y por otro aprovechando la Inteligencia Artificial y la automatización.

> Las empresas tienen que aprender a protegerse y diseñar un plan global de seguridad que incluya la correcta gestión de la identidad, la detección de amenazas, la protección de datos y la monitorización unificada

La explotación de los datos es la nueva ventaja competitiva y la Inteligencia Artificial es la tecnología que va a permitir realizar un análisis de los datos que se convierta en inteligencia de negocio y en mejora de la competitividad. Y este proceso debe hacerse desde una perspectiva de confianza, que garantice los aspectos de ciberseguridad, privacidad, transparencia y cumplimiento.

Si hay algo que marca una tendencia clave, tanto en el presente como en el futuro, es la apuesta por la Inteligencia Artificial como base para potenciar una seguridad proactiva que permita seguir la acelerada evolución cualitativa y cuantitativa de las ciberamenazas. Esta tecnología permite construir sistemas de alerta temprana mucho más efectivos, que hace posible enfrentarse de la forma más eficaz posible ante los crecientes riesgos de ciberseguridad.

La Inteligencia Artificial, además, hace posible que los profesionales de ciberseguridad se centren en tareas que aporten el máximo valor, reduciendo las labores administrativas y repetitivas para ayudarles a procesar grandes cantidades de alarmas de seguridad, detectar anomalías y responder a las mismas en el menor tiempo posible. En definitiva, con la Inteligencia Artificial ganamos un aliado de grandísimo valor que colabora con los equipos humanos y ayuda a mejorar el trabajo de estos profesionales altamente capacitados.

En nuestro caso, es el aliado perfecto para los más de 3.500 especialistas que tenemos en la compañía dedicados específicamente a velar por la protección, defensa y respuesta a las ciberamenazas que aparecen cada día. Contamos con varios equipos de expertos especializados en diferentes ámbitos de seguridad; Digital Crimes Unit (DCU), Microsoft Threat Intelligence Center (MSTIC) especializado en el seguimiento de amenazas avanzadas, Detection and Response Team (DART) especializado en Respuesta a Incidentes y un centro de operaciones, el Microsoft Cyber Defense Operation Center (CDOC)[4], desde el que nuestros especialistas vigilan la actividad mundial 24x7, analizando más de 8.000 millones de señales diarias.

Foto: iStock.com/the-lightwriter

Riesgo por falta de personal cualificado en competencias digitales

Es importante incidir en el riesgo que supone la falta de profesionales con competencias digitales avanzadas, como las del ámbito de la ciberseguridad. Las previsiones apuntan a que este año 2021 habrá un déficit de 3,5 millones de profesionales de la seguridad en el mundo. Desde Microsoft abogamos por el fomento de las competencias digitales[5], y ponemos a disposición de todo aquel que quiera formarse, un completo itinerario formativo con cursos online gratuitos desde nuestra plataforma Microsoft Learn[6]. Hemos anunciado recientemente cuatro nuevas certificaciones de seguridad[7], cumplimiento e identidad adaptadas a las funciones y necesidades de cada persona o entidad, independientemente del punto en el que se encuentre en su viaje de capacitación.

Si hay algo que ha demostrado el comienzo de 2021 es que mantener el mundo seguro no es fácil. Los recientes ciberataques de alto nivel han puesto de manifiesto la creciente sofisticación de los actores de las amenazas y la complejidad de la gestión del riesgo empresarial en un mundo cada vez más conectado. Nuestro compromiso en Microsoft es de trabajo y aprendizaje continuo para ayudar a nuestros clientes a mitigar los riesgos a los que se exponen. La seguridad en el ciberespacio exige que gobiernos, empresas y sociedad civil trabajemos para encontrar soluciones conjuntas a los desafíos a los que nos enfrentamos. ●

---

4 https://www.microsoft.com/en-us/msrc/cdoc
5 https://news.microsoft.com/es-es/2021/03/30/microsoft-y-linkedin-han-ayudado-a-30-millones-de-personas-en-todo-el-mundo-a-adquirir-habilidades-digitales-durante-la-covid-19/
6 https://docs.microsoft.com/es-es/learn/
7 https://docs.microsoft.com/en-us/learn/certifications/browse/?resource_type=certification&terms=security