EXTRA GRANDES EMPRESAS >

Más digitales pero inseguros

Crece la conciencia empresarial de que la automatización de los procesos debe ir acompañada de una cultura de la ciberseguridad

WESTEND61 / GETTY IMAGES

VIRGINIA MIRANDA RUFO
26 SEPT 2021 - 10.19 CEST

Son las nueve de la mañana y, en lo que llevamos de día, en España ha habido 3.077 ataques informáticos. Seguramente, a mediodía rozarán los 6.000*. Félix A. Barrio es subdirector de ciberseguridad para la Sociedad y la Empresa de Incibe (Instituto Nacional de Ciberseguridad). Durante la conversación, permanece atento al panel de control de Internet en España, activo las 24 horas de los 365 días del año.

En este observa "los 14.785 eventos de posibles ciberataques que estamos monitoreando". "Nos encontramos en nivel de alerta amarillo", indica sin alarmarse. La cifra es normal a estas horas y la culpa la tienen los sospechosos habituales, como el *ransomware*, protagonista de la "actual epidemia de ataques", o los bots, siendo el FluBot el más popular a través del mensaje de texto o *smishing*.

La pandemia se lo ha puesto más fácil a los ciberdelincuentes. El incremento precipitado de la digitalización y el teletrabajo y la caída de la inversión en seguridad por la crisis han disparado los ataques. En los años 2019-2020 hubo 133.155 incidentes. Desde el confinamiento hasta julio de este año, 153.720, según datos del Incibe.

Las empresas más vulnerables son las pymes, "el eslabón más débil de un sistema donde todos estamos hiperconectados", explica Barrio. De ahí que los ataques empiecen por ellas, porque son "el caballo de Troya de los ciberdelincuentes para infectar organizaciones más grandes". Del sector de los servicios profesionales y del comercio minorista son el mayor número de consultas que recibe el organismo público a través de varios canales. El más popular es el 017, una línea telefónica donde los operadores ayudan a responder tras los incidentes y ofrecen información para evitar la ciberdelincuencia.

MÁS INFORMACIÓN
Cada vez más digitalizados, pero menos protegidos
Ya hay vacuna para la pandemia de los ciberataques
Teletrabajo, 'ransomware' y juguetes sexuales: los retos de la ciberseguridad para 2021

Porque la mejor respuesta es la prevención y la anticipación. "No se trata solo de proteger, sino de ser resiliente a los ataques y actuar. Uno de los conceptos que las empresas deben trabajar es el de los planes de contingencia, que identifiquen los riesgos y las preparen para responder". Lo explica Marc Martínez, socio responsable de ciberseguridad de KPMG en España, que en su reciente informe a partir de encuestas a los altos ejecutivos de todo el mundo concluye que la mayor preocupación de los directivos son los ciberataques. Sobre las nuevas tecnologías, advierte: "El *big data*, la automatización y la inteligencia artificial aumentan la complejidad de todo el sistema de protección y gestión de riesgos".

Sectores como el financiero o el de las telecomunicaciones son los más atractivos para las mafias organizadas, pero también son los más preparados para hacer frente a las amenazas gracias a su inversión en innovación. Álvaro Garrido, *chief security officer* del grupo BBVA, defiende el uso de la inteligencia artificial, el *machine learning* y la automatización de los procesos para mejorar las defensas ante los ciberataques desde un punto de vista preventivo y proactivo, porque "permiten gestionar un mayor número de alertas y eventos y ofrecer una respuesta más específica y autónoma a indicios e incidentes de seguridad".

"El empleo de estas técnicas requiere un cambio en las capacidades y conocimientos de analistas de seguridad", avisa. Y esta es precisamente la clave de bóveda de la ciberseguridad: el conocimiento.

Si la inteligencia artificial "está basada en el *machine learning*, es necesario nutrirla con gran cantidad de información que sea muy bien analizada por un ojo experto", señala Sergio de los Santos, director de innovación y laboratorio en Telefónica Tech. "Hay que definir muy bien qué se quiere conseguir con ello", como por ejemplo detectar anomalías, "y entrenar mucho con los datos. "Si se está seguro, el resultado puede usarse para automatizar procesos y, de ahí, construir una inteligencia artificial completa".

Deberes cumplidos

"Es fundamental incrementar el conocimiento", coincide Enrique Dans, profesor de innovación de IE Business School. Y no solo al más alto nivel. "Las empresas más preparadas para hacer frente a los ciberataques son aquellas capaces de transmitir a los usuarios la importancia y los riesgos potenciales de determinados comportamientos". Así, además de "auditar la seguridad de la compañía con cierta frecuencia con sistemas de *hacking* ético como HackerOne y otras que organizan cursos para encontrar vulnerabilidades y de emplear herramientas que minimicen determinados riesgos, como redes privadas virtuales y gestores de contraseñas", propone desarrollar entre los empleados "una cultura de seguridad". La idea, sostiene, es evitar que se convierta en algo tan complejo que termine siendo mayoritariamente ignorado.

Y ese es uno de los mayores peligros. La inteligencia artificial también está al alcance de los ciberdelincuentes y es responsable de recopilar información de sistemas vulnerables y de expandir los virus de forma cada vez más rápida y masiva. Por eso es importante recuperar los niveles de inversión previos a la pandemia, concluye Barrio, de Incibe, porque elevar la seguridad "al final es la supervivencia del negocio y la competitividad".

FUERTE IMPULSO TECNOLÓGICO

El 29,5% de los 140.000 millones de euros que llegarán a España para ayudar a la recuperación tras la pandemia está destinado a la transformación digital y "el impulso de la ciberseguridad es una de las vías prioritarias dentro de los planes" del Gobierno para repartir los fondos europeos, apunta Félix A. Barrio, subdirector de ciberseguridad para la Sociedad y la Empresa de Incibe (Instituto Nacional de Ciberseguridad). En el marco del Plan de Recuperación, Transformación y Resiliencia, el Ejecutivo está poniendo en marcha el Programa Digital Toolkit. Dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, está dotado con 3.000 millones de euros para que las pymes puedan adquirir servicios de digitalización. Entre ellos, herramientas de protección frente a los ciberataques.
Otra línea del plan de choque está dirigido a elevar las capacidades de los proveedores de la Administración. "Con un mayor nivel de ciberseguridad en su actividad y servicios", indica el experto de Incibe, "indirectamente se eleva el nivel de protección de los servicios públicos".

ARCHIVADO EN:
Seguridad Internet · Piratería Informática · Incibe · Formación · Informática · Empresas · Digitalización Empresarial · Ataques Informáticos

MÁS INFORMACIÓN

EXTRA GRANDES EMPRESAS
Tecnológicas e inmobiliarias atraen las compras corporativas

EXTRA GRANDES EMPRESAS
Digitalización y sostenibilidad, un binomio indivisible

EXTRA GRANDES EMPRESAS
Servicios clave ante el reto de la recesión