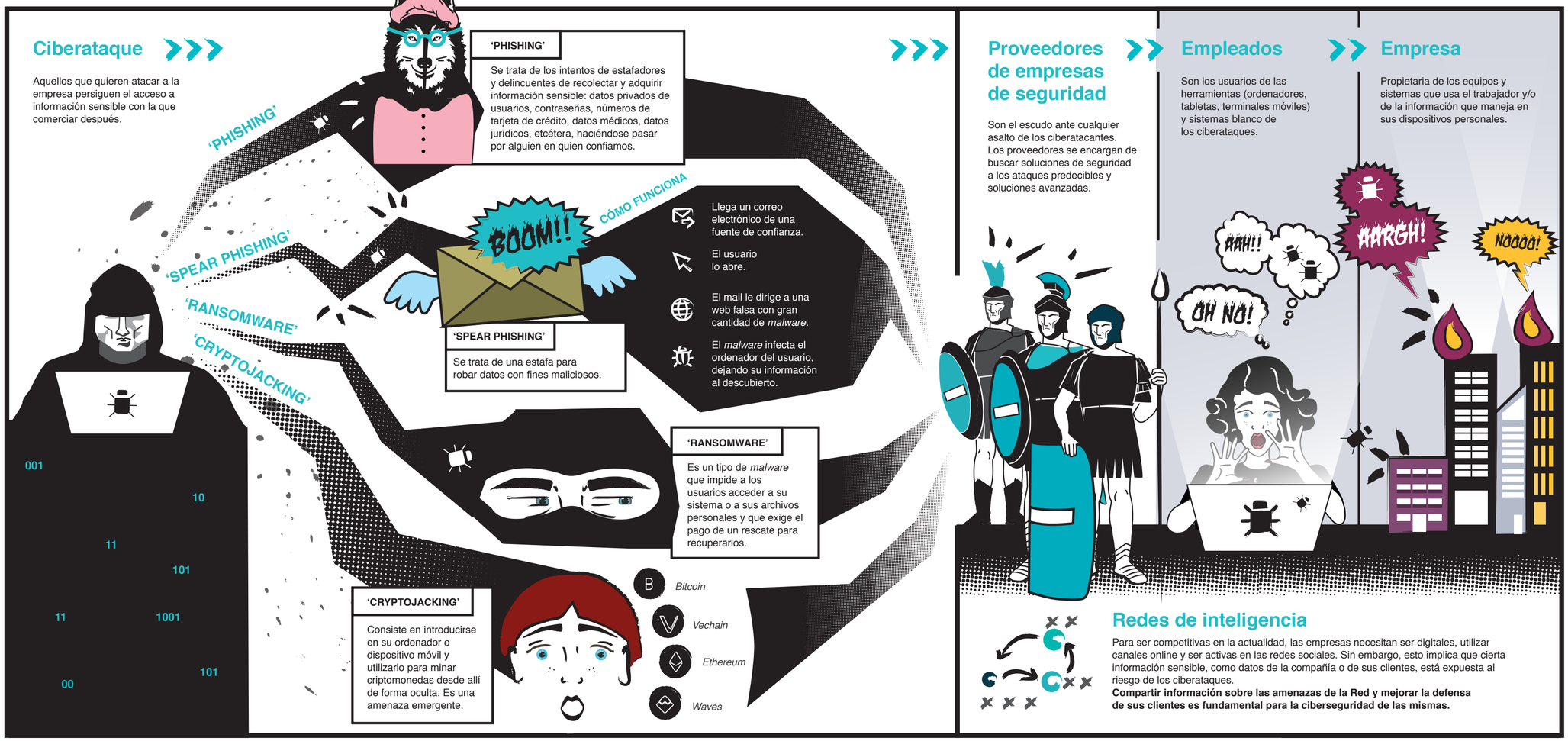
CincoDías
Martes, 25 de junio de 2019

UN PROYECTO DE Telefónica EMPRESAS



Un negocio seguro

En un mundo más digital y conectado, todas las empresas de cualquier tamaño y sector deben blindarse frente a cualquier ciberataque.

Miércoles, 2 de noviembre de 1988. La fecha ha quedado marcada en la historia del mundo digital. Aquel día, Robert Tappan Morris, un veinteañero estudiante de informática, desató el pánico en Arpanet, el padre del Internet moderno. Morris había desarrollado un programa capaz de autorreplicarse y cuya finalidad, según su propia versión, era conocer el tamaño de la red. Sin embargo, terminó por infectar a unos 6.000 servidores, el 10% de esa incipiente red. Fue "una plaga imparable", según los expertos de aquella época, pues volvía los sistemas muy lentos y algunos inoperativos. Desde entonces, distintos software malignos no han parado de extenderse. Hoy se les conoce de distintas maneras (*phishing, spear phishing, spyware, ransomware*, troyanos, etcétera) pero todos tienen el mismo objetivo: causar daño.

Detrás de ellos están cientos de criminales que van a por nuestra información: correo electrónico, datos bancarios, DNI, contraseñas... Ningún dato es insignificante. Todo tiene un precio en el mercado negro y los ciberdelincuentes buscan cualquier resquicio para obtenerlos. El objetivo está en el mundo empresarial, que se enfrenta a dos realidades: busca ser cada vez más digital, pero ello conlleva enfrentarse a un nuevo riesgo, los ciberataques. "Entre las compañías, las amenazas se centran en la pérdida de los datos del cliente o en que estos caigan en manos no deseadas, las denegaciones de servicio (DDoS) o el secuestro de información y la petición de rescate correspondiente (*ransomware*)", dice Juan Hernández Orea, gerente de Desarrollo de Negocio de Seguridad para Grandes Clientes en Telefónica Empresas.

Basta con mirar los datos. De los 111.519 incidentes informáticos que gestionó el Instituto Nacional de Ciberseguridad (Incibe) en 2018, el 92% correspondió a ciudadanos y empresas, mientras que el resto se

> Las implicaciones económicas de un ataque pueden ser desastrosas

centró en la red académica y operadores estratégicos. "El mundo cada vez es más digital y menos seguro", afirma Hernández Orea. "Debemos ser conscientes de que estamos siendo atacados constantemente", añade. Además de los atacantes, hay que sumar que en el mercado existen personas que se dedican a analizar vulnerabilidades de software. Buscan las debilidades de los sistemas y cuando encuentran una pueden comunicárselo al fabricante, que destina partidas de su presupuesto para pagar a estos cazarrecompensas. Otra posibilidad es vender los datos en el mercado negro. Para anticiparse a este tipo de amenazas, las empresas han creado las Redes de Inteligencia, una herramienta donde las compañías comparten esas vulnerabilidades que detectan a través de soluciones avanzadas. Dicha red permite evaluar los peligros, identificarlos y analizarlos para actuar contra ellos rápidamente.

En este sentido, el mayor riesgo para la empresa está en el empleado, que ahora lleva en sus dispositivos móviles la puerta de entrada a los sistemas de las compañías. "Allí es donde los atacantes ven la mayor posibilidad de éxito para el inicio de una ofensiva", explica. La nube y los móviles son el eslabón más débil de la seguridad y solo el 1% de los usuarios protege sus dispositivos contra *malware*, según la empresa Check Point. De acuerdo con esta firma, el 33% de las organizaciones a nivel mundial ha sido víctima de un ataque de *malware* móvil. El objetivo de los principales atentados ha sido el sistema operativo Android. Las cifras son alarmantes, pero ¿cuáles son las consecuencias? "En términos económicos sus implicaciones pueden ser desastrosas", arguye el experto de Telefónica Empresas. "Un virus produce, a corto plazo, disrupciones en los negocios y en las cadenas de suministro y destruye infraestructuras", explica.

92%
de los 111.519 incidentes informáticos que gestionó el Incibe en 2018 correspondió a ciudadanos y empresas.

33%
de las organizaciones a nivel mundial ha sido víctima de un ataque de *malware* móvil.

"El mayor riesgo lo enfrentan las pequeñas y medianas empresas", dice Hernández Orea. "Las grandes compañías han adoptado novedosos sistemas de seguridad, pero las pymes son las más vulnerables porque aún no cuentan con un presupuesto para ciberseguridad y creen que nunca serán víctimas", subraya. Hoy, ninguna empresa está a salvo. A finales de 2019, cada 14 segundos alguna compañía será víctima del *ransomware*, según Cybersecurity Ventures. Esta firma prevé que el coste por este delito ascenderá a 11.500 millones de dólares al final de este año, un repunte del 130% respecto a 2017. "Nadie está a salvo de sufrir un ciberataque porque la seguridad al 100% no existe", agrega el experto de Telefónica Empresas.

OPINIÓN

La seguridad es más que un antivirus

José Luis Gilpérez López
Director Ejecutivo de Administraciones Públicas, Defensa y Seguridad de Telefónica Empresas.

El mundo de la ciberseguridad cambia vertiginosamente y cada vez son más frecuentes las amenazas en torno al empleado digital y sus herramientas de trabajo. Varios son los factores que están volviendo más inseguras a las empresas. Uno de ellos es el uso de los dispositivos móviles como herramienta de trabajo, que ha acrecentado la convergencia de lo personal y laboral (BYOD: *Bring Your Own Device*), o la generalización de los portátiles, sin que haya aumentado la concienciación de seguridad.

Esta falta de concienciación está brindando a los atacantes una vía de entrada sencilla para vulnerar la seguridad de cualquier empresa. En el contexto actual es patente que, independientemente de su tamaño, las empresas carecen de los medios de protección adecuados cuando un atacante o *hacker* ataca directamente a sus herramientas de trabajo.

La peligrosidad aumenta ante la existencia de una falsa percepción de seguridad pensando que con un antivirus tradicional o quizás un cortafuegos (*firewall*) es suficiente. Craso error. Con la mayor sofisticación de los ataques y el creciente volumen de *malware* que aparece cada día en el mercado (en muchos casos pequeñas variantes de otros existentes), estas soluciones no solo son insuficientes sino también ineficaces. Por ejemplo, un antivirus tradicional basa su protección en comparar lo que tiene previamente identificado con lo que se está ejecutando en un momento determinado. Esto es muy eficaz contra los virus conocidos o estandarizados, pero menos efectivo contra ataques dirigidos o diseñados *ex profeso*, para lo que se necesitan soluciones complementarias.

En este sentido, desde Telefónica Empresas llevamos mucho tiempo poniendo a disposición de las compañías las herramientas necesarias no solo para mejorar la seguridad de sus empleados, sino también para incrementar su productividad. En cuestión de seguridad somos una de las firmas más concienciadas, y nuestra credibilidad se basa precisamente en nuestro *know how*. Es decir, tenemos todas las soluciones implementadas en nuestras propias infraestructuras y en nuestros empleados.

Cuando hablamos de redes de inteligencia es porque las conocemos y las usamos. En Telefónica Empresas no solo vendemos soluciones sino que ayudamos a las compañías de cualquier tamaño a adoptar sistemas de protección avanzada del puesto de trabajo, con un asesoramiento continuo, desde nuestra propia experiencia, para que sean capaces de analizar e identificar amenazas o comportamientos anómalos en tiempo real. En caso de que la empresa haya sido vulnerada, actuamos con planes reactivos para contener el ataque y analizamos cuál ha sido la brecha de seguridad para poder solucionar el problema en el menor tiempo posible.