“El Kit Digital es una gran oportunidad para que las pymes aprovechen las nuevas tecnologías, si bien estas tecnologías han de ser fáciles de implantar en una solución integral, donde el software y el servicio está contemplado como parte de una solución que incluya así mismo el hardware seguro para su explotación”, asegura Melchor Sanz, CTO de HP.

Olga Romero

Crear soluciones fáciles para todas las pymes que contemplen hardware, servicio y software podría ser el elemento diferencial

Esta es la meta que el fabricante pretende alcanzar antes de que se anuncie la segunda convocatoria de ayudas del Kit Digital. Y es que HP tiene como objetivo impulsar la adquisición de dispositivos seguros que garanticen la protección de todos los activos de la empresa. Un objetivo que se ha materializado con HP Wolf Security, el ecosistema de seguridad que incluyen los dispositivos de HP de manera intrínseca y que, además, las compañías pueden reforzar con otras cuatro soluciones adiciones de ciberseguridad. Entre ellas destaca Wolf Security Pro, la herramienta que la multinacional ofrece a pymes y autónomos a través del epígrafe X del Kit Digital.

Tal y como explica Sanz, los primero días de confinamiento "fueron catastróficos" para estas empresas ya que de la noche a la mañana tuvieron que mover a su fuerza laboral a casa, equiparla con los dispositivos y herramientas necesarios para trabajar y, en esos momentos de caos, la seguridad del puesto de trabajo no estaba en su lista de prioridades. El directivo comenta que poco a poco las pymes, dependiendo del sector y la liquidez de la empresa, fueron implementando algunos "remedios" como parches de seguridad, antivirus, VPN o entornos de virtualización, entre otros. De esta manera conseguían "mitigar los riesgos, pero no cerrarlos completamente". Además, se trataba de soluciones a corto plazo.

Melchor Sanz, CTO de HP

Actualmente, la consolidación del trabajo híbrido como la modalidad laboral de la era postcovid ha obligado a estas organizaciones a "diseñar un entorno híbrido de trabajo que sea seguro y estable en el tiempo", apunta Sanz. Una necesidad que, como el propio directivo lamenta, no pueden cubrir todas las pymes ya que "seguimos en una situación económica difícil y la seguridad del puesto de trabajo depende directamente del sector de actividad al que pertenezca la pyme". Sin embargo, Sanz aplaude "la enorme labor de concienciación que se ha hecho durante estos dos años porque gracias a ella se ha conseguido un alto nivel de concienciación".

En cuanto a la evolución que han experimentado los ataques, Sanz apunta que "el objetivo de los *hackers* siempre ha sido el chantaje a las grandes organizaciones". Una finalidad que por suerte los ciberdelincuentes están consiguiendo menos de lo que esperaban. Pero, como era de

"Incluir el hardware en las próximas convocatorias del Kit Digital es la única manera de que las pymes adquieran una herramienta de seguridad completa"

esperar, no se están yendo con las manos vacías ya que están consiguiendo acceder a empresas más pequeñas a través de la instalación, en los ordenadores de los empleados, de un *malware* como residente a bajo nivel y cuando éstos acceden al sistema de las empresas los malhechores digitales se alzan con su premio.

"Su objetivo no es atacar al ciudadano doméstico, su objetivo es atacar a la empresa y para ello se cuelan por la brecha de seguridad que tiene el ciudadano en su dispositivo", explica Sanz. Quien añade que actualmente el ataque más utilizado es el *phishing* masivo a través del cual consiguen apropiarse de los datos de los usuarios.

Esta brecha de seguridad se seguirá manteniendo ya que, como explica Sanz, "las pymes estarán más expuestas porque invertirán las ayudas del Kit Digital en herramientas como el comercio electrónico o página web con las que aumentarán su presencia en Internet, pero también los riesgos a recibir ataques". Ante esta situación, el directivo subraya la importancia de "garantizar la seguridad de toda la cadena, desde el usuario hasta el dispositivo".

La prioridad como problema, no la concienciación

En la actual era digital las habilidades digitales se han convertido en imprescindibles. Pero en este nuevo escenario la concienciación y formación de los empleados, y usuarios, en materia de ciberseguridad también son claves para evitar ciertos ataques, especialmente el *phishing* que, como indica Sanz, está tan de moda. Sobre estos aspectos el responsable de tecnología de la multinacional está convencido de que "en materia de concienciación y divulgación estamos avanzando mucho".

Sanz defiende que pymes y autónomos son conscientes del riesgo que corren al carecer de herramientas de seguridad, "no se trata de una cuestión de concienciación sino de la situación económica actual y de prioridades, y desgraciadamente la seguridad no está entre sus prioridades ahora mismo", afirma.

Según comenta, el nivel de concienciación entre este segmento de negocio oscila entre el 80 y el 90 %. "Pero el negocio, la situación económica y la urgencia hacen que la vulnerabilidad no esté en un 10 %, sino que sea de un 60 %. Por eso

debemos seguir trabajando para que se convierta en una prioridad", resalta. Sanz, además, añade que "hay que hacer entender a las pymes que la seguridad es una inversión a largo plazo y que, tarde o temprano, obtendrán retorno de esa inversión". Tal y como asegura el directivo, en algún momento del ciclo de vida de la empresa va a ocurrir un desastre de seguridad y entonces "el gasto de la recuperación y de la protección siempre va a ser mucho mayor que la inversión inicial para protegerse", apunta.

Una labor en la que los agentes digitalizadores tienen un papel fundamental ya que son los encargados de guiar, acompañar y aconsejar a las pymes dónde invertir los bonos digitales. "El agente digitalizador es imprescindible en este momento, pero al final, por lo general, son pymes con un amplio catálogo de soluciones de diferentes ámbitos que venden a otras pymes", recuerda.

Por este motivo y con el objetivo de que para los agentes digitalizadores fuese más fácil vender seguridad que otras soluciones, HP ha trabajado para simplificar todo el proceso. "Hemos creado diferentes guías, PDF y página web, también les hemos explicado a todos nuestros *partners*, —muchos de ellos se están acreditando como agentes digitalizadores—, la oferta de una manera sencilla. Todo esto para conseguir que vender nuestra herramienta de seguridad sea un proceso fácil para los agentes digitalizadores", explica.

Un epígrafe X, dedicado a la ciberseguridad, que en esta primera convocatoria es el único en el que la multinacional puede ofrecer sus soluciones a las pymes. "Nuestro objetivo para las próximas convocatorias es conseguir que entren otras características del puesto de trabajo, no solo seguridad, en las que también podamos entrar y ofrecer un mayor abanico de soluciones", asegura.

"Entre el 80 y el 90 % de las pymes están concienciadas sobre la importancia de la seguridad, pero no es una prioridad para ellas"

HP Wolf Security

HP decidió lanzar HP Wolf Security, el ecosistema de seguridad en el que la multinacional engloba toda su oferta de seguridad, como resultado del éxito que obtuvieron sus vídeos junto a Christian Slater. A través de estos vídeos, llamados The Wolf, el fabricante pretendía concienciar y sensibilizar a la ciudadanía en general y a las empresas en particular de la importancia de tener un dispositivo seguro. Actualmente bajo el paraguas de HP Wolf Security se encuentra un amplio abanico de soluciones de ciberseguridad que forman parte de los dispositivos de la multinacional desde el momento de su fabricación. Además, la compañía ofrece, de manera adicional, otras tres soluciones: Wolf Pro Security, Wolf Enterprise Security y Wolf Protect and Trace, que permiten aumentar la seguridad de los dispositivos.

"HP Wolf Pro Security es la única solución, de estas tres soluciones adicionales que tenemos, que va dirigida a pymes y que tenemos incluida en el programa de ayudas del Kit Digital", comenta Sanz. El valor diferencial de Wolf Pro Security es la incorporación de un sistema de aislamiento capaz de hacer frente a los ataques *zero days*. "Gracias a este sistema de aislamiento la herramienta aísla cualquier aplicación o virus que no conoce y analiza su comportamiento.

El ecosistema HP Wolf Security

1. **HP Wolf Pro Security: solución dirigida a pequeñas y medianas empresas, que puede instalarse en cualquier ordenador, aunque no sea HP, y que brinda una solución de seguridad diferencial gracias a su capacidad de aislamiento.**
2. **HP Wolf Enterprise: esta solución de seguridad esta destinada a grandes corporaciones, instalable en cualquier dispositivo y que contiene tanto una solución de aislamiento como una solución de protección ante conexiones remotas.**
3. **HP Wolf Protect & Trace: solución única de dispositivos HP que gracias a una solución en BIOS permite localizar, borrar y bloquear un dispositivo, tanto en caso de perdida como de robo y sea cual sea su estado.**

En el momento en el que esta aplicación o virus tenga un comportamiento sospechoso el sistema se pone en alerta y aumenta su vigilancia", explica Sanz.

En definitiva, HP Wolf Pro Security frena todos los virus conocidos y sospecha de todo aquello que desconoce, lo que se llama *zero trust* o confianza cero. Además, del sistema de aislamiento, "verdadero valor diferencial de HP Wolf Pro Security", la solución de la multinacional incluye un antivirus, el cual está basado en inteligencia artificial, con protección ante el robo de credenciales.

El rompecabeza de la seguridad en 2022

Los ciberdelincuentes evolucionan sus ataques constantemente. De hecho, hoy en día las empresas se enfrentan a ciberataques más sofisticados y de gran eficacia. "Los ataques de ingeniería social son los que más están avanzando", asegura el directivo. Como explica Sanz los malhechores digitales utilizan la información que los usuarios exponen en las redes para explotarla y a través de inteligencia artificial conocer sus patrones de comportamiento. De esta manera consiguen suplantar su identidad y conocer las vulnerabilidades de la empresa.

Para Sanz el mayor reto en materia de seguridad de este 2022 seguirá siendo que "las pequeñas empresas tengan la capacidad de ejecutar las estrategias de seguridad que saben que necesitan para garantizar la seguridad de sus negocios". Esto únicamente es posible a través de ayudas económicas y poniendo la ciberseguridad entre los primeros epígrafes en el Kit Digital.

El directivo asegura que las soluciones existen pero que las pymes necesitan más recursos para implantarlas porque, como subraya, "las pymes están bastantes concienciadas, pero no tienen el dinero suficiente para acometer todas las mejoras que necesitan, en lo que se refiere a la implementación de soluciones digitales para su digitalización, y entonces necesitan priorizar".