PABLO SAN EMETERIO CHIEF SECURITY AMBASSADOR DE LA EMPRESA DE CIBERSEGURIDAD ELEVENPATHS (TELEFÓNICA)

▶ Prefiere diferenciar entre hacker, «que es una persona apasionada por la tecnología», y delincuentes tecnológicos. Alerta de que nadie está exento de sufrir un ciberataque y recuerda que el primer paso de una buena protección es no picar los anzuelos que nos llegan a diario a través de mails fraudulentos, webs poco seguras y enlaces sospechosos.

«Están las personas que ya han sido atacadas y las que aún no lo saben»

TEXTO: **SANTY MOSTEIRO**
FOTO: **CEDIDA**

JOVEN Y SOBRADAMENTE preparado. Como si de un eslogan publicitario se tratase, Pablo San Emeterio forma parte de esa generación de ingenieros informáticos en los que las grandes empresas depositan su confianza para garantizar al resto de la población la tranquilidad cibernética. En su caso, tiene un papel destacado dentro del equipo directivo de ElevenPaths, la unidad de ciberseguridad de Telefónica.

¿Cuál es su función?

Tengo un doble rol. Por una parte, trabajo en i+D como analista de innovación, revisando vulnerabilidades y fallos, y desarrollando soluciones. Y, por otro, soy embajador de ciberseguridad.

¿Estamos ciberseguros?

En general, sí. Pero a veces se descubren fallos que no se conocen y hay que corregirlos a tiempo. Después también está la parte del usuario, que gracias a casos como el robo de identidades de Facebook, se va concienciando cada vez más y va aprendiendo a ser más cauto y prevenido. Por ejemplo, si no estás esperando un paquete de Correos, no debes responder a un email en el que tengas que hacer click para recogerlo.

¿Qué proporción tiene el error humano en la comisión de un ciberataque?

Depende del propio ciberataque. Hay algunos en los que sí es necesaria la participación del usuario para que se produzca (como que a través de un correo malicioso se cuele un 'ramsomware' en los servidores de una empresa), otras veces se debe a una mala configuración del sistema de seguridad y, las menos, a que ese sistema tenga una vulnerabilidad que permite que alguien lo asalte. Es complicado establecer una estadística debido a la multitud de factores que intervienen en el proceso.

¿Los ciberdelincuentes nunca descansan?

Es su forma de vida, su negocio. Cuando les cierran una puerta, tienen que abrir una ventana por la que seguir manteniéndolo.

Tradicionalmente se han relacionado los ataques informáticos con las famosas 'puertas traseras'. ¿Son fallos necesarios o surgen de forma aleatoria?

Como puerta trasera dejada aposta creo que es más mito que realidad. Lo que sí ocurre es que tanto los sistemas operativos como los navegadores son complejos, y la complejidad suele ser tendente a los fallos. Unas veces son los responsables de seguridad los que descubren esos 'agujeros' y se corrigen, pero otras son los atacantes.

¿Cuáles son las agresiones cibernéticas más habituales?

Lo que se está llevando la palma son, por un lado, las fugas de información, como los casos de Facebook, Equifax o Yahoo, y, por otro, el 'ramsomware', que consiste en colarse en un equipo (ordenador, base de datos, servidor...) y encriptar la información, para poder pedir al propietario un rescate a cambio.

Tanta variedad de amenazas traslada la sensación de que nadie está exento de un ciberataque...

Es que afectan a todos, particulares, empresas, instituciones, corporaciones... Todos somos objetivos y hay dos tipos de personas: las que han sido atacadas y las que aún no lo saben. Detrás de estos ataques solo está el objetivo de conseguir dinero, bien de forma directa (con el 'ramsomware' o robando claves bancarias) o bien convertirte en dinero, bien obteniendo información que pueda ser útil para vender en Internet bien utilizando tu PC para lanzar ataques contra terceros o para minar criptomonedas, que es lo que se está poniendo de moda.

Se dice que España es uno de los países más seguros contra los hackers...

Bueno, antes de nada, me gustaría diferenciar entre hacker, que es una persona apasionada por la tecnología y la seguridad, y los delincuentes que utilizan medios tecnológicos. Es cierto que en España tenemos un alto nivel de seguridad pero, como todo, depende mucho de la concienciación y de la inversión que hagan tanto los ciudadanos como las empresas.

¿Es posible conocer la inversión que hacen los españoles en ciberseguridad?

Es evidente que la preocupación por esta materia ha aumentado notablemente. No tengo datos concretos del mercado español, pero Telefónica, en 2017, vendió en torno a 500 millones de euros en ciberseguridad. Y esta cifra va creciendo en torno a un 30% cada año que pasa.

Durante la campaña electoral en Cataluña se especuló con una posible manipulación de los resultados obra de piratas rusos. ¿Por qué las miradas se fijan en este país?

Es una gran pregunta. No lo sé. La verdad es que suele haber dos países a los que se les pone la etiqueta de atacantes: Rusia y China. No tengo muy claro el porqué. Supongo que porque las ip (direcciones) de los primeros ataques salieron de esos países, pero eso no quiere decir que los atacantes residan ahí.

Se asocia la ciberdelincuencia a los ordenadores y no tanto a los smartphones. ¿Podría decirse que, de momento, están a salvo?

Los móviles son objetivos de ataque, igual que los PC. Sin embargo, los markets oficiales suelen inspeccionar bastante las aplicaciones que se ofrecen para su descarga y es difícil que se cuele malware o programas maliciosos, que también los hay.

Prevención personal

> Si no estás esperando un paquete de Correos, no debes hacer click en un email que te ofrece recogerlo»

Objetivo

> Los ataques siempre buscan dinero, bien de forma directa, bien robando información que se pueda vender en Internet»

Ciberseguridad

«La inversión depende de lo que se quiera asegurar, pero a veces es más caro el collar que el perro»

¿Cuánto cuesta blindarse con un mínimo de garantías contra los delincuentes tecnológicos?

Por una parte, el coste de la licencia de un antivirus doméstico, para una vivienda, está entre 50 y 60 euros al año. También está la opción de securizar la línea, no solo para que no entre malware, sino para filtrar los contenidos que ven los menores. Telefónica ofrece ese servicio a sus clientes a un precio de entre uno y tres euros al mes. En cuanto a las empresas, la inversión depende de lo que se quiera proteger. Muchas veces ocurre que sale más caro el collar que el perro. Hay firmas con grandes volúmenes de información o grandes proyectos (por ejemplo, una constructora que opte a un concurso de millones de euros), en las que está justificado destinar importantes cantidades de dinero a la seguridad. Otro ejemplo que se me ocurre son los entornos militares.

¿Es cierto que existe mucho pirateo en el sector de la hostelería para promocionar ciertos negocios?

Desconozco si es así, si la gente se está organizando de tal forma que si se dejan 20 comentarios negativos en tal restaurante, se puede perjudicar su reputación. Pero lo que ocurre en estos negocios que ofrecen servicios como wifi y no se preocupan tanto por su seguridad es que resultan mucho más vulnerables.