La incertidumbre acerca de que nuestras conexiones estén protegidas crece

¿Cómo asegurar las redes?

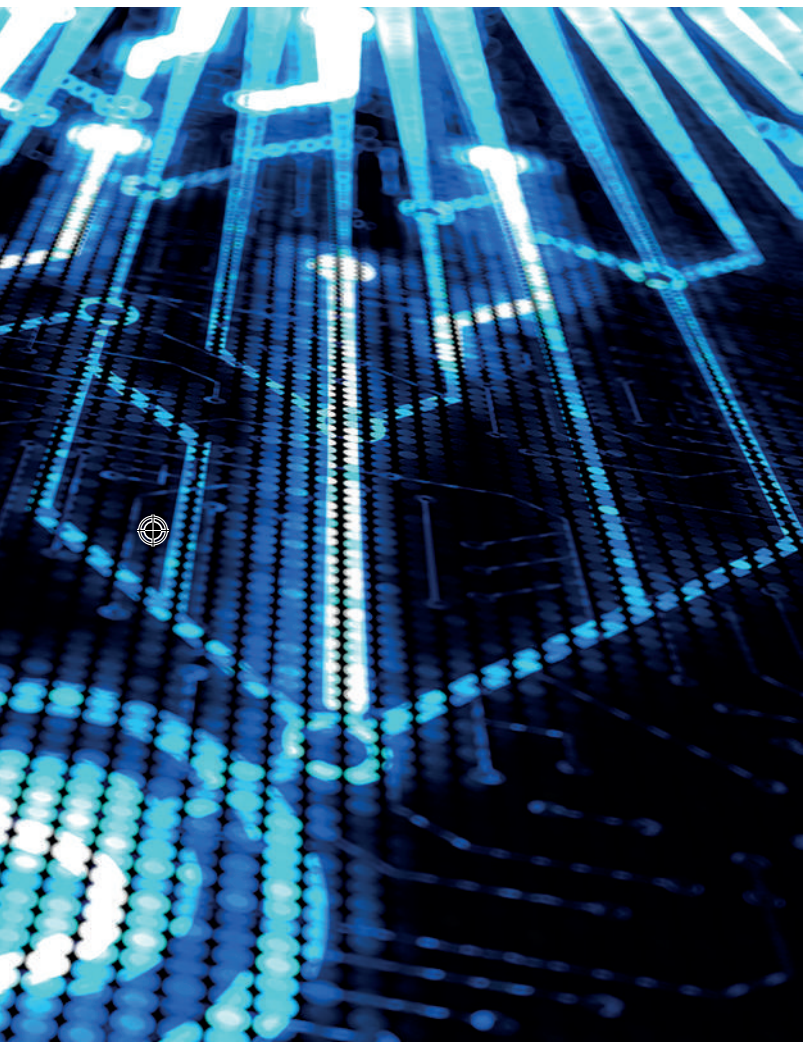
Con la criptografía como principal medida de protección de las comunicaciones, se estudian nuevas alternativas para combatir los ciberataques en un mundo cada vez más conectado. Conseguir una mayor concienciación del usuario, mantener la privacidad y preparar el terreno para la consolidación de la Internet de las Cosas son los grandes desafíos a los que se enfrenta la industria.

Cristina López Albarrán
cristina.albarran@bps.com.es
@Redesbps
www.redestelecom.es

A principios de octubre, Google anunció el cierre de la versión de consumo de Google+, su plataforma social. El motivo oficial de este cese de actividad (poca, dicho sea de paso) fue un fallo de seguridad que expuso los datos personales de, al menos, 500.000 usuarios. Esta violación, que se inició en 2015, fue localizada por la compañía en marzo de este año y la solucionó a través de un proyecto interno denominado Strobe que le permitió descubrir el error de una API llamada "People". Sin embargo, el mal estaba hecho y de nuevo volvía a ponerse sobre la mesa la preocupación acerca de la protección de nuestros datos en la Red de redes. Internet, esa carretera sobre la que fluye, con mayor o menor intensidad de tráfico, la información. Y sobre la que, a día de hoy, no tenemos un control completo, ¿o sí?

Ya hablemos de fija o móvil, cableada o inalámbrica, la incertidumbre acerca de que nuestra conexión sea segura crece. Las ciberamenazas son cada vez más frecuentes

y conocidas. Conviene, pues, estar alerta. Pero, sin afán de ser pesimista, por muy protegidos que estemos se van a producir ataques, así que tendremos que convivir con ello, dicen siempre los expertos del sector. La clave estará en cómo podemos mitigarlos y, en la medida de lo posible, prevenirlos.



Lo bueno es que existen herramientas disponibles y tecnología capaz de hacer frente a amenazas complicadas y sofisticadas, pero de nada sirven si no se utilizan por un usuario concienciado. Reflexionemos. En el mercado podemos encontrar antivirus para dispositivos móviles, ¿cuántas personas tienen el programa instalado en su smartphone? Profundicemos más en el tema, ¿al descargar una aplicación leemos las condiciones de privacidad?, o ¿reseteamos el router regularmente o sólo cuando el VPN Filter de turno se cuela por las noticias tomamos cartas en el asunto? En nuestra mano está aportar nuestro granito de arena. Bien es cierto que no todo el mundo posee una alarma en su casa, rejas en las ventanas, triple cerrojo, y un largo etcétera, pero raro es aquél que deja la puerta abierta conscientemente.

Herramientas para proteger una red

- Antivirus. Programas informáticos que detectan, bloquean, analizan, desinfectan, eliminan y previenen infecciones.
- Firewalls o cortafuegos. Actúan como barrera entre la red y el exterior. Habilitan el acceso seguro a usuarios y servicios, alertando de intromisiones.
- IDS (Sistema de Detección de Intrusos). Mecanismo que analiza el tráfico en la red detectando actividades anormales o sospechosas. Hay dos tipos, N-IDS (garantiza la seguridad en la red) y H-IDS (garantiza la seguridad en el host).
- IPS (Sistema de Prevención de Intrusos). Dispositivos de hardware o software encargados de revisar el tráfico de red con el objetivo de detectar y responder a posibles amenazas.
- Redes Privadas Virtuales (VPN). Red que lleva los paquetes de datos a distintos puntos remotos mediante infraestructuras públicas de transporte. Tiene que estar capacitada para verificar la identidad de los usuarios y restringir el acceso a los no autorizados.

Mayor concienciación

Los fabricantes de seguridad lanzan continuamente versiones de sus últimas soluciones para proteger equipos e infraestructuras y no se cansan de repetir una y otra vez que tiene que ser el ciudadano / empleado de a pie el que asuma también la responsabilidad de sus actos pues está comprobado que el DISPOSITIVO (con mayúsculas), se ha convertido en la puerta de entrada de los ataques actuales. Parece ser que el mensaje está empezando a calar en nuestro país. Según el Cyber Ready Barometer de Vodafone que la operadora presentó a principios de octubre, prácticamente la mitad de los usuarios españoles consultados (55%) no sabe cómo protegerse frente a ciberataques, una cifra 11 puntos por encima de la media global (44%). Sin embargo, el desconocimiento de qué medidas tomar no está alineado con la preocupación por las amenazas, ya que el 92% de los españoles se declara preocupado por el phishing o ataques de ingeniería social, frente al 81% de los encuestados a nivel global. Además, el 88% afirma estar preocupado por la pérdida de datos personales.

El barómetro asimismo se centra en el ámbito laboral y, en virtud de las respues-

> *Es posible aplicar principios cuánticos para intercambiar una clave entre los extremos de un canal de comunicaciones, de manera que esa clave sea segura frente a cualquier ataque e incluso que cualquier intento de ataque sea inmediatamente detectado*

ficar a la autori-
rvicios e incluye

s procesos de
dichos incidentes
fe en su actua-

guridad que les

un millón de

Real Decreto de seguridad de las redes y sistemas de información

El pasado sábado 8 de septiembre, el Boletín Oficial del Estado, BOE, publicó el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, después de que fuera aprobado en el Consejo de Ministros del viernes anterior. De este modo, se incorporó al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, más conocida como Directiva NIS, que busca identificar los sectores en los que se debe garantizar la protección de las redes y sistemas de información y establecer las exigencias de notificación de ciberincidentes. El objeto del Real Decreto (RD) es "regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes", al tiempo que "establece un marco institucional para la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario".
El artículo 11 de este documento establece tres CSIRT de referencia, que se coordinarán entre sí y con el resto de equipos nacionales e internacionales en la respuesta a incidentes y gestión de riesgos. Así, para el sector público actuará el CCN-CERT, del Centro Criptológico Nacional.
Los otros dos son el INCIBE-CERT para la comunidad que no pertenezca al CCN-CERT, ciudadanos y entidades de derecho privado y el ESPDEF-CERT, del Mando Conjunto de Ciberdefensa, que cooperará con los otros en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos que tengan incidencia en la Defensa Nacional.

Obligación de notificar incidentes

El RD contempla la obligación de los operadores de servicios esenciales y los proveedores de servicios digitales (artículo 19) de notificar a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios e incluye aquellas notificaciones de sucesos o incidencias que aún no hayan tenido un efecto adverso real (peligrosidad potencial).
El texto también señala que las autoridades competentes y los CSIRT utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes. Además, se detalla que los empleados y el personal que notifique sobre dichos incidentes "no podrá sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación".
Los operadores de servicios esenciales y los proveedores de servicios digitales tienen la obligación de resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada cuando no puedan resolver por sí mismos los incidentes.
En este sentido, el RD incluye un régimen sancionador que puede ir desde multas de 100.000 euros para las infracciones leves hasta un millón de euros para las muy graves. No obstante, se decanta por la subsanación de la infracción, antes que el castigo (art. 39).

tas de los trabajadores, el 72% reconoce haber recibido algún curso sobre ciberseguridad en el trabajo, orientado a ampliar conocimientos y mejorar las capacidades de los empleados frente a las ciberamenazas. En la misma proporción, un 72% también confía en la estrategia de ciberseguridad de su empresa y en su capacidad para responder ante estas amenazas. Pero sólo el 45% cree que las políticas corporativas de seguridad se cumplen por todos los empleados, lo que indica que la teoría se conoce, pero no siempre se pone en práctica.

Por último, el documento destaca a España como un país muy sensibilizado sobre las posibles consecuencias que un ciberataque o una pérdida de información confidencial puede suponer para su imagen de marca y su reputación. En este sentido, el 67% de los directivos españoles consultados está preocupado por el efecto que estos incidentes pueden tener en su organización, una cifra por encima de la media global, que se sitúa en el 60%.

Criptografía para comunicaciones seguras

Desde la perspectiva de las firmas de seguridad, la protección de las comunicaciones se basa en el uso de la criptografía, de manera que la información se cifra utilizando una clave que permite que sólo los participantes que la conocen sean capaces de descifrar los mensajes intercambiados entre ellos. Las técnicas actuales de criptografía están sustentadas en problemas matemáticos que son complejos de resolver. A medida que la capacidad de computación crece, el tiempo de resolución de estos problemas, y por tanto la seguridad de las claves, disminuye.

El tamaño de las claves y la complejidad de los algoritmos de encriptación

han
cap
sist
obs
dor
prir
la r
inso
gen
crip
de l
com

C
nica
de M
de j
red
con
tecn
Def
a la
ingl
que
la c
mos
na u
cua
técn
de f
pilo

tificial, alytics, y expe- son las cias de centers

han tenido que aumentar a medida que la capacidad de cálculo iba creciendo. Y estos sistemas pueden quedar completamente obsoletos con la aparición de los ordenadores cuánticos, capaces de aplicar los principios de la Mecánica Cuántica para la resolución de problemas actualmente insolubles, incluyendo el romper las claves generadas por los métodos actuales de criptografía, haciendo inútiles la mayoría de las infraestructuras de seguridad en las comunicaciones.

Con esta problemática en ciernes, Telefónica, Huawei y la Universidad Politécnica de Madrid (UPM) demostraron a mediados de junio la aplicación de criptografía en redes ópticas comerciales y su integración con la operación de la red por medio de tecnologías basadas en SDN (Software Defined Networking). Para ello recurrieron a la Distribución Cuántica de Claves (del inglés QKD, Quantum Key Distribution) que resuelve el problema de la amenaza de la computación cuántica para los algoritmos criptográficos en uso y que proporciona un nivel de seguridad mucho más alto a cualquier intercambio de datos. Eso sí, esta técnica requiere una infraestructura física de fibra óptica de alta calidad. Además, este piloto utilizó una nueva tecnología aplicada a QKD basada en “variables continuas” (del inglés, Continuous Variables).

Una característica especial de los dispositivos usados es que son muy flexibles, pudiéndose controlar completamente por software. Los sistemas están óptimamente adaptados para su integración en un entorno dinámico como el de las redes de nueva generación basados en SDN y virtualización de funciones red (NFV – Network Function Virtualization), donde la creación y los cambios en los caminos ópticos y el

Los ataques a las redes pueden ser pasivos o activos

Proyecto FENTEC: compartir datos de forma segura a través de redes no seguras

Atos coordina un consorcio formado por nueve empresas e instituciones para la implantación del proyecto FENTEC (Functional ENcryption TEChnologies) que permitirá a los usuarios compartir datos de forma segura a través de una red no segura o no confiable. El proyecto tiene una duración de tres años y está financiado por la Comisión Europea dentro del proyecto Horizonte 2020, el Programa Marco Europeo de Investigación e Innovación.

Hasta la llegada de la clave pública de cifrado, el método más común para compartir datos de forma segura era establecer una contraseña secreta entre los usuarios. Este método puede funcionar para pequeñas organizaciones o pymes, pero resulta inviable para redes más grandes como las actuales.

La clave pública de encriptación es una tecnología muy desarrollada que se usa habitualmente para construir soluciones de comunicación web, cifrado de disco y distribución de parches de software. Sin embargo, el acceso controlado criptográficamente a los datos o al programa que gestiona los datos no era posible hasta ahora. Esta barrera que se resuelve con el Cifrado Funcional, un nuevo modelo versátil y poderoso de sistemas de encriptación.

El objetivo de FENTEC es desarrollar el cifrado funcional como una alternativa eficiente al enfoque tradicional del cifrado (todo o nada), permitiendo vistas parciales de los datos encriptados y mejorando la seguridad de los sistemas. En el proyecto trabaja un equipo multidisciplinar de criptógrafos, expertos en software, especialistas en hardware y representantes de la industria de TI, con el objetivo de desarrollar sistemas de cifrado funcionales eficientes e innovadores, capaces de adaptarse a un amplio espectro de escenarios. FENTEC diseña, desarrolla, implementa y demuestra la utilidad de las aplicaciones reales de encriptación funcional, ofreciendo ventajas tangibles para la industria de TI y para los usuarios que necesitan operar en entornos donde la confidencialidad de los datos y la privacidad es necesaria.

La seguridad, eficiencia, expresividad y versatilidad de este nuevo enfoque se demostrará en tres casos de uso, el primero es la Moneda digital, para preservar la privacidad, aplicando modelos de auditoría flexibles. El segundo abordará el Análisis anónimo de datos, que permite el cálculo de estadísticas sobre datos encriptados, protegiendo los derechos fundamentales europeos de protección de datos y privacidad. El último se basa en el procesamiento resistente a la pérdida de datos de los dispositivos de Internet de las cosas (IoT).

Con un presupuesto estimado de cuatro millones de euros, FENTEC desarrollará nuevos sistemas de encriptación funcionales capaces de aumentar la confianza en los servicios europeos de tecnología de la información.

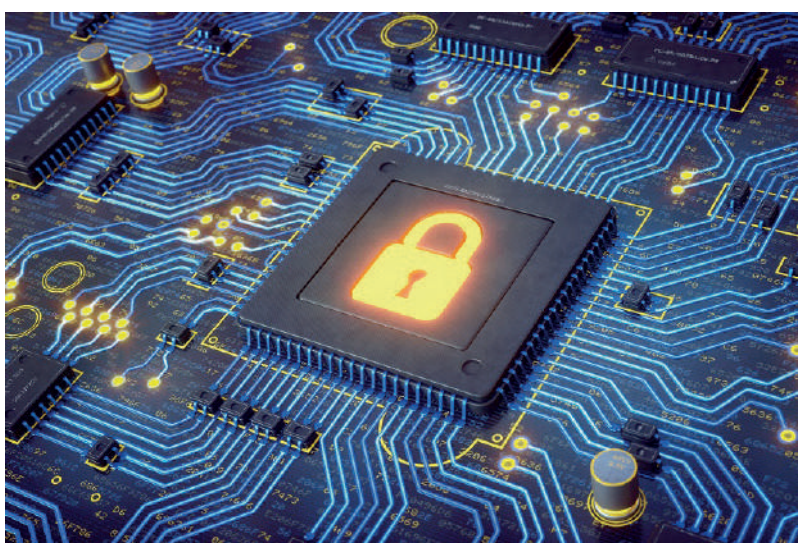
El proyecto comenzó en enero de 2018 y reúne a un consorcio, coordinado por Atos. Cuenta con socios como Ecole Normale Superieure (Francia), Hochschule Flensburg (Alemania), Katholieke Universiteit Leuven (Bélgica), Universidad de Helsinki (Finlandia), Nagravision (Suiza), XLAB (Eslovenia), Universidad de Edimburgo (Reino Unido) y Wallix (Francia).

60,00%
40,00%
20,00%
0,00%

necesario cifrado dejan de ser estáticos y predefinidos, realizándose mediante interfaces de control basadas en software. Estas funcionalidades se aseguran integrando dispositivos CV-QKD con dispositivos estándar de transporte óptico. La integración de QKD y SDN-NFV abre un nuevo camino para dotar de un alto nivel de seguridad a estas nuevas redes.

Protección sin cables

Si hablamos de las redes radio, esas infraestructuras inalámbricas que se propagan por el aire o, dicho de otra manera, que emplean la radiofrecuencia como medio de transmisión (Wi-Fi, Bluetooth, ZigBee,



las sucesivas generaciones de la telefonía móvil e IoT), también tienen sus estándares de seguridad.

En el caso de Wi-Fi –la más utilizada en la actualidad– encontramos diferentes protocolos encargados de mantener protegidas nuestras comunicaciones. Tal y como comentábamos en el anterior número de la publicación, la industria ha ido pasando por WEP, WPA y WPA2, este último vigente desde 2004. Este tipo de redes parecían invulnerables, pero el KRACK attack demostró que esta creencia no era cierta. A raíz de este ataque, la Wi-Fi Alliance anunció la necesidad de incorporar nuevos mecanismos de autenticación y cifrado en el Wi-Fi Protected Access (WPA) dando lugar al nacimiento de WPA3, tanto para el campo particular como el empresarial. En concreto se han perfilado dos modelos: WPA3-Personal, que pretende dificultar el hackeo de contraseñas (protección de las claves y datos); y WPA-Enterprise WPA3, incluye una suite de seguridad con un cifrado de 192 bits. Se trata de un paso importante para proteger la privacidad de los usuarios, utilizando algoritmos más robustos de los que hay en uso y equivalentes a los que se emplean en el ámbito militar y de defensa.

Si esta alternativa se queda corta, una de las medidas de seguridad recomendada es la de cambiar la SSID (Service Sed Iden-

Mantener la privacidad

Un informe de la Agencia Europea para la Cooperación en el Cumplimiento de la Ley (más conocida como Europol), sobre la Evaluación de las amenazas de la delincuencia organizada en Internet (del inglés, Internet Organised Crime Threat Assessment, IOCTA), indica que las próximas redes móviles 5G junto con el nuevo Reglamento general de protección de datos (GDPR) complicarán el rastreo de los delincuentes cibernéticos.

Gary Barton, analista de tecnología de GlobalData, explica por qué los gobiernos y los reguladores deberían tener en cuenta cómo los delincuentes pueden usar la conectividad 5G para sus fechorías. De acuerdo con el consultor, gran parte del debate en torno a 5G se ha centrado en si el usuario medio de un teléfono móvil realmente necesita velocidades de quinta generación. Sin embargo, un aspecto de esta tecnología sobre el que no se ha prestado mucha atención es cómo será aprovechada por los criminales. "El ciberdelito es un frente de batalla abierto y, quizás, antes de que la 5G esté disponible, los gobiernos y los reguladores deberían considerar cómo los delincuentes pueden usar la tecnología como aliada", explica.

El informe de IOCTA de 2018 señala que "la tecnología 5G inhibirá la atribución y la intercepción legal" de los delincuentes. La razón principal de esto es que la tecnología de virtualización subyacente necesaria para hacer frente a la complejidad y el ancho de banda de 5G hace que sea mucho más difícil identificar y localizar usuarios individuales. Las redes 4G dan a cada usuario un identificador único. Por el contrario, la 5G sólo asigna identificadores temporales.

La Inteligencia Artificial permitirá a la policía y a los servicios de seguridad superar este desafío. Sin embargo, esta tecnología tardará tiempo en desarrollarse y las leyes de GDPR diseñadas para proteger la privacidad individual significan que las bases de datos necesarias para respaldar estos procesos pueden ser ilegales.

Cifrado de datos

En el lado positivo, habrá beneficios de seguridad directos de 5G. Las empresas y organismos del sector público tendrán más opciones para cifrar los datos, lo que hará que cualquier posible infracción sea menos probable y menos perjudicial. Las tecnologías de Iot que usan 5G también admitirán mejoras en otros aspectos de la seguridad, como el CCTV y el seguimiento de objetos (por ejemplo, teléfonos / ordenadores portátiles robados). "Las nuevas tecnologías siempre traen nuevos desafíos y la batalla contra el crimen cibernético y el crimen organizado plantea dilemas para los gobiernos y las poblaciones. En el Reino Unido, la propuesta "Carta de Snoopers" (Proyecto de Ley de Datos de Comunicaciones) generó muchas críticas y fue descartada. La Ley de poderes de investigación (The Investigatory Powers Act) que posteriormente llegó al Parlamento del Reino Unido solo obtuvo el respaldo de la mayoría de los diputados británicos después de que se hicieran concesiones a la privacidad. Pero demasiada protección de datos también tiene sus consecuencias. Puede ser que la UE (y, después de Brexit, el Reino Unido) deban considerar las revisiones de GDPR una vez que el 5G entre en vigencia en toda Europa".

tifer) –esa secuencia alfanumérica de 32 caracteres que deben compartir los dispositivos para conectarse– regularmente y desactivar la función de difusión o broadcast para que al usuario no le aparezca la red.

IoT: el gran desafío

A la protección de las infraestructuras y los dispositivos se suma un gran desafío que afecta a ambos mundos: la Internet de las Cosas. Según Gartner, los dispositivos IoT crecen a un ritmo de un 32% interanual desde 2016 hasta 2021 y alcanzarán una base instalada de 25.100 millones de unidades. Centrándonos en España, IDC Research vaticinó en su último informe de abril de 2018 que el gasto en IoT en nuestro país alcanzará los 19.000 millones de euros en 2021. Además, indica que el 20% de las organizaciones españolas ya ha desplegado proyectos reales de IoT, de las cuales un 70% se están planteando ampliar el proyecto en los próximos 18 meses. Por sectores, la consultora confirma que consumo y retail serán los motores de crecimiento ya que el foco de las empresas se va a centrar en la experiencia del cliente y en la multicanalidad. En la actualidad, la industria, influenciada directamente por la Industria 4.0, representa el mercado más grande. Eso sí, el 69% de las empresas usuarias de IoT han creado o piensan crear políticas de seguridad.

No en vano, la superficie de ataque aumenta y los administradores de seguridad necesitan salvaguardar todos los dispositivos en todo momento, mientras que los ciberdelincuentes sólo necesitan un puerto abierto, un equipo comprometido o desconocido, o una gran amenaza para eludir todo el esfuerzo realizado para proteger la red. El futuro que se nos avecina contempla la conexión tres puntos de fisura para los ciberdelincuentes: al propio objetivo (frigorífico, cafetera, TV, smartphone, etc), la nube y la red.

Y en este convulso escenario comienzan a sonar los thingbots, sistemas maliciosos que introduce un hacker en un objeto con conexión a Internet aprovechando una brecha de seguridad con la intención de integrarlo en una red zombi. ■

La concienciación del usuario es fundamental para mantener seguras las redes