Marcos Gómez - Subdirector de E-confianza del Instituto Nacional de Tecnologías de la Comunicación (INTECO)

«La cultura de la seguridad informática tiene que formar parte de la política de actuación de nuestro entorno corporativo»

La cultura de la seguridad informática resulta determinante en una sociedad que gusta llamarse de *la información.* Los componentes de esta sociedad tienen el deber de conocer el entorno tecnológico, sus usos y costumbres. El Instituto Nacional de Tecnologías de la Comunicacion (INTECO), un organismo vinculado al Ministerio de Industria, Turismo y Comercio, es uno de los encargados de impulsar esta nueva Sociedad del Conocimiento por medio de proyectos relacionados con el ámbito de la innovación y la tecnología. Desde esta plataforma instruyen e informan a usuarios y empresas de los riesgos de la red.

Elisa G. McCausland

Pregunta: ¿Hasta qué punto es posible acabar físicamente con la red de redes, provocar el llamado *caos total?*

Respuesta: El riesgo existe siempre. Lo que ocurre es que es un riesgo, en este caso, muy bajo. Se han dado ataques en algunas ocasiones a uno de los trece servidores, los famosos DNS[1], y cuando han caído dos o tres de ellos la red ha estado bastante ralentizada, en cuanto a respuesta de traducción de nombre de dominio, o lo que es lo mismo, en cuanto a tráfico de información en la red. Como digo, el riesgo existe, pero es muy bajo y el caos es muy difícil que a día de hoy se produzca debido a que la red, tal y como se ha estructurado, ha ido creciendo de subredes en subredes hasta dar lugar a toda la Internet que conocemos; por lo tanto, esas subredes serían lo suficientemente autónomas como para que, según se fueran recuperando esos servidores, se volvieran a unir los nodos principales de la red y así volver a reestablecer el servicio. Luego, un colapso total es muy difícil que se dé como para que toda la red se caiga, pero si se puede dar por áreas.

P.: ¿Qué medidas específicas existen para que esto no ocurra?

Marcos Gómez, subdirector de E-confianza de INTECO.

R.: Una es intrínseca a la naturaleza de la red. Según esta ha ido creciendo se ha dado a si misma una propiedad de distribución de servicios. No solo en los trece servidores de raíz de DNS, sino que además, las empresas están cada vez más deslocalizadas; incluso las multinacionales, que disponen de varios nodos, varias sedes, con posibilidades de respaldo y, por lo tanto, la distribución natural de la red se convierte en una barrera contra este tipo de colapsos. A parte, durante los últimos años tanto la Administración pública como el sector privado, el más concienciado, han incorporado propiedades de alta disponibilidad y alto rendimiento a sus organizaciones. Alta disponibilidad es tener todo replicado, de modo que si tienes una base de datos y se te cae puedes seguir dando ese servicio, y alto rendimiento supone invertir en el mayor potencial tecnológico posible; supone contratar el mejor servidor o varios servidores, por ejemplo. Y, por supuesto, tener centros de respaldo, con sus *backups*[2] correspondientes para que,

1. Un Servidor Raíz es un servidor de nombre de dominio (DNS) y es el servidor que sabe donde están los servidores de nombres autoritarios para cada una de las zonas de más alto nivel en Internet.
2. Copias de seguridad.

en el caso de que suceda un pequeño colapso, tener la capacidad suficiente para recuperarse de este tipo de ataques.

P.: ¿Qué buenas prácticas puede realizar el usuario para contribuir al mantenimiento de la red y su seguridad?

R.: Tanto el usuario doméstico como el usuario corporativo, sea este de *pymes* o de grandes empresas, tiene arte y parte en la salud de la red. Entre esas buenas prácticas, propias de la cultura tecnológica, está saber utilizar las herramientas de Internet, el correo electrónico, la navegación, el intercambio de ficheros, etc., sin olvidar el fomento de una cultura de seguridad. Al igual que nos dan un manual nada más llegar a una empresa y nos dicen cómo tenemos que actuar frente a un riesgo de incendios, esa actitud tiene que formar parte también de nuestra política de actuación en nuestro entorno corporativo, al igual que en nuestra casa. Si llevamos las buenas prácticas empresariales a nuestros hogares, como el software de seguridad, antivirus, cortafuegos, *antispam,* y a eso añadimos cautela a la hora de utilizar nuestro correo electrónico, no nos metemos en páginas sospechosas, no damos nuestros datos personales en la red, etc, y nos mantenemos informados, como usuarios tendremos una cultura de seguridad a la hora de trabajar en la red lo suficientemente buena como para que no nos convirtamos en un blanco de ataques informáticos.

P.: ¿Cuáles serían las medidas, por parte del Gobierno, para evitar ataques en la Red?

R.: La primera es, evidentemente, elevar la cultura de seguridad. Según los indicadores de Inteco y el Ministerio de Industria, que a través del *Plan Avanza* ha elaborado estudios que así lo indican, una gran parte es la cultura de seguridad del ciudadano. Porque, si el ciudadano conoce una amenaza, es más difícil que caiga en la misma. Si el ciudadano desconoce dicha amenaza, en caso de ataque, por débil que este sea, puede producirle algún tipo de perjuicio. En cuanto al Gobierno, a parte de incentivar la cultura de la seguridad con campañas de difusión, de concienciación en materia de seguridad, en materia de uso de nuevas tecnologías, está trabajando en dos vertientes: una es la coordinación de incidentes, que es la herramienta más reactiva y preventiva. Reactiva porque, ante un incidente de seguridad, permite calcular, por medio de una red de organismos, como Inteco o las fuerzas de Seguridad del Estado, la magnitud del incidente y medir la respuesta adecuada. La parte preventiva alude a los centros de prevención.

Tanto el usuario doméstico como el usuario corporativo, sea este de *pymes* o de grandes empresas, tiene arte y parte en la salud de la red

La otra cuestión importante está en la creciente dependencia tecnológica que hay de las infraestructuras críticas (como la energía, el transporte, la sanidad), de ahí que se deba elevar la seguridad en estas infraestructuras aplicando los mismos protocolos que se han llevado a cabo antes para evitar los colapsos en Internet: alta disponibilidad, alto rendimiento, copias de respaldo, coordinación con otros centros de seguridad y, además, tener algún tipo de mecanismo que permita medir la salud de la tecnología de la que dependen estas infraestructuras. Si somos capaces, día a día, de medir cómo está la red, ante un incidente tendremos mayor capacidad de enfrentarnos al mismo y responder con la suficiente fuerza como para repelerlo.

P.: ¿Cómo se compaginan seguridad y libertad a la luz de la nueva Ley de Protección de Datos?

R.: En el ámbito internacional, hay países, como Reino Unido, que están elaborando normas que permiten que dentro de una empresa el empleado sea contratado con una serie de derechos, siendo uno de ellos que use la infraestructura corporativa para trabajar y no para uso personal. Este paso que está dando Reino Unido no sabemos si se dará alguna vez en España. La nuestra es una cultura más latina, más de compartir y ver la red como una oportunidad, lejos de verla como una amenaza, prueba de ello es que la Web 2.0 está teniendo un éxito en España abrumador. El tema de los *blogs* es un ejemplo de que cada vez se comparten más recursos en la red. Pero analizar un correo electrónico sospechoso, el *malware*[3] que puede llevar incorporado o si se es víctima de un *phishing*[4], tiene unas connotaciones más de análisis forense, de auditoría de seguridad. De ver si ese correo es nocivo o no para un internauta, una corporación o una Administración. La frontera entre lo que es sospechoso y lo que realmente es perjudicial es una frontera muy fina y, a veces, no sabes si la estás pasando de más o te estás quedando corto. ▮

3. Malware (del inglés *malicious software,* también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.
4. Anzuelo o Estafa electrónica (inglés *phishing*. Ver Origen de la palabra) es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). Fuente: Wikipedia