OPINIÓN

DESPUÉS DE LA PANDEMIA

El desastroso estado de la ciberseguridad

Enrique Dans

Publicada 18 diciembre 2024 02:23h
Actualizada 18 diciembre 2024 10:51h

El mes pasado, una de las agencias gubernamentales más respetadas de los Estados Unidos en todo lo relacionado con la ciberseguridad, CISA (Cybersecurity and Infrastructure Security Agency) informó, junto con el FBI, sobre un ciberataque presuntamente asociado con China, denominado **Salt Typhoon**.

Este ataque habría comprometido, entre otras, a dos de las compañías de telecomunicaciones más grandes del país, AT&T y Verizon, y se considera ya como **uno de los mayores ataques a la infraestructura estadounidense en toda su historia**.

Los objetivos del ciberataque eran en su mayoría **personas definidas como "de alto valor"**. Funcionarios gubernamentales a diferentes niveles, las propias CISA y FBI, la National Security Agency (NSA) y algunos socios internacionales. A raíz de eso, todas estas organizaciones publicaron una guía conjunta con recomendaciones destinadas a ayudar a proteger a los ciudadanos estadounidenses.

Una de las sugerencias más interesantes del informe es la recomendación del uso de **cifrado de extremo a extremo, *end-to-end encryption* o E2EE**, un método relativamente sencillo de utilizar que hace que las comunicaciones digitales sean mucho más seguras.

El cifrado de extremo a extremo ayuda a garantizar que sólo los destinatarios previstos puedan leer sus mensajes mientras se desplazan entre su terminal y el terminal del remitente.

> *La tecnología para proteger nuestras comunicaciones de forma razonablemente accesible, por tanto, existe y está fácilmente disponible.*

Algunas aplicaciones de mensajería utilizan cifrado de extremo a extremo para proteger las comunicaciones de sus usuarios de manera que **ni siquiera los propios proveedores de aplicaciones de mensajería puedan leerlos**.

Recordemos, por ejemplo, **lo ocurrido en países como Brasil o España** cuando algunos jueces pretendieron cerrar determinadas plataformas porque, según ellos, no cumplían sus peticiones de descifrado de mensajes entre encausados, algo que, técnicamente, no tenían modo de hacer.

La tecnología para proteger nuestras comunicaciones de forma razonablemente accesible, por tanto, existe y está fácilmente disponible. Pero esa recomendación, sin embargo, suena enormemente confusa para

muchos usuarios que no tienen ni la más ligera idea de qué plataformas de mensajería permiten utilizar este tipo de cifrado ni de cómo utilizarlo.

¿A qué se debe **un nivel de desconocimiento tan elevado en una tecnología que llevamos ya muchos años utilizando** y que constituye un canal de comunicación fundamental en la sociedad actual? Simplemente, a que no hemos sido capaces, ni como sociedad ni a otros niveles, de desarrollar una cultura de la ciberseguridad.

Una carencia importantísima, que está detrás del **elevadísimo volumen de robos de información, estafas, chantajes, timos y problemas** que sufren personas y organizaciones de forma tristemente habitual.

Los usuarios utilizan habitualmente distintas aplicaciones de mensajería para distintos fines, generalmente sin pensar en absoluto en la ciberseguridad. Pero existen diferencias entre ellas que es importante conocer: por ejemplo, que **Signal y WhatsApp** (que utiliza el protocolo de cifrado desarrollado por la primera) **se consideran las aplicaciones de mensajería más seguras** porque incorporan cifrado de extremo a extremo, lo que las hace preferibles a los SMS o MMS.

> *No hemos sido capaces, ni como sociedad ni a otros niveles, de desarrollar una cultura de la ciberseguridad.*

Signal es una de las favoritas entre muchos entusiastas de la privacidad porque su misión hace **énfasis específico en no recopilar ni almacenar información confidencial**, algo que obviamente las aplicaciones de Meta, conocidas por sus desastrosas prácticas de privacidad, no pueden hacer.

La desventaja de Signal es que no está tan extendida como WhatsApp y si tus contactos no están en ella, no puedes comunicarte. En países como España, con un acusado "monocultivo", **todo lo que no sea usar WhatsApp genera problemas e inconveniencias**. Yo llevo años siendo "el amigo que no usa WhatsApp", y me genera infinidad de contratiempos.

El caso de los usuarios con dispositivos Apple la cuestión es algo más complicada, porque si utilizan iMessage, que en la mayoría de los casos se configura sustituyendo a los SMS, cuentan con cifrado de extremo a extremo, pero si el destinatario del mensaje no tiene también un iPhone, no lo usan. **Telegram y Facebook Messenger**, muy poco utilizado en España, **disponen de cifrado de extremo a extremo, pero no lo utilizan por defecto,** sino únicamente cuando se solicita.

En cualquier caso, poco puede hacerse en un entorno en el que **la mayoría de los usuarios prestan una atención escasísima a sus prácticas de ciberseguridad**: utilizan contraseñas ridículamente sencillas, reutilizan la misma contraseña entre varios servicios, o se lanzan a utilizar redes WiFi públicas sin la menor precaución. El uso de sistemas de doble factor de autenticación, que exigen una incomodidad mínima, es también descorazonadoramente bajo.

> *Yo llevo años siendo "el amigo que no usa WhatsApp", y me genera infinidad de contratiempos.*

Otras cuestiones, como el uso de gestores de contraseñas o de redes privadas virtuales (VPN) son meramente testimoniales entre la población general. **Los bloqueadores de publicidad, que también mejoran sensiblemente la seguridad** y que fueron, de hecho, recomendados por el propio FBI hace tiempo, **tienen algo más de uso**, pero no por una cuestión de protección, sino más bien para evitar el espantoso bombardeo intrusivo y molesto al que nos someten muchas páginas.

Lo mínimo que podemos hacer si utilizamos internet de manera habitual es formarnos mínimamente en las prácticas de ciberseguridad necesarias para evitarnos problemas.

Del mismo modo que nuestros padres, cuando empezamos a caminar solos por la calle, nos explican las prácticas de seguridad mínimas (caminar por la acera y evitar la calzada, no aceptar caramelos de extraños, esperar en los semáforos, cruzar por los pasos de cebra, etc.), esa educación no se produce cuando hablamos de nuestro uso de la red porque **las instituciones educativas renuncian a proporcionarla y prefieren prohibirlo todo**, lo que genera las situaciones que

conocemos.

¿Podemos intentar plantearnos cuáles deberían de ser nuestras precauciones mínimas para utilizar una herramienta como la red sin exponernos a grandes riesgos, y abandonar el estúpido y nocivo pensamiento de "bah, total no soy importante, no tengo nada que ocultar ni nada que proteger"?

Si no nos educan en el uso de la red, tendremos que educarnos nosotros... pero hagámoslo. Es importante, de verdad. Ya me lo agradeceréis más adelante.

*** ***Enrique Dans es Profesor de Innovación en IE University.***