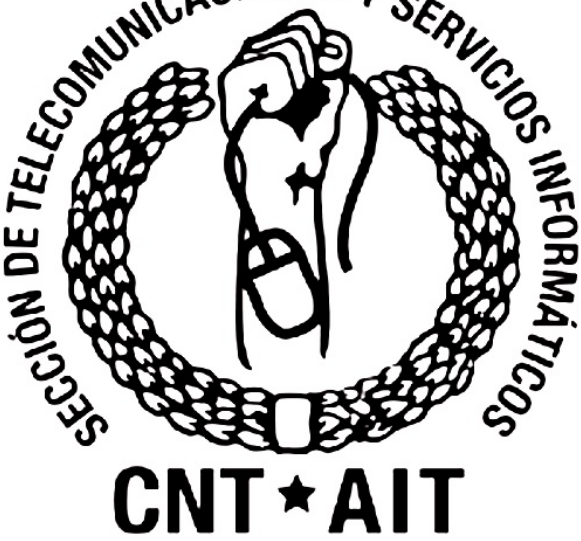
APUNTES

DE DEFENSA DIGITAL



Sumario

Introducción

Generalmente consideramos Internet como el lugar donde podemos exponer líbremente nuestras ideas, compartir imágenes y vídeos, construir debates y relaciones políticas con otras personas sin tener miedo a la represión, porque “Internet por sí misma es una herramienta libre”. Pero esto no es cierto, porque en la mayoría de los casos hay alguien que “escucha” nuestras conversaciones, filtra nuestras búsquedas y censura las noticias.

En España, así cómo en otros estados considerados democráticos o dictatoriales, sobran los casos de represión digital. En estos apuntes vamos a presentar las herramientas básicas para poner nuestros datos a salvo y defendernos de posibles ataques.

Para entender cómo defendernos hay que tener en cuenta que la seguridad informática no es nada más que un termino medio entre riesgos de ataques y medidas de defensa que tomamos. Unos ataques pueden ser sencillos para unos y difíciles para otros.

Por ejemplo, un compañero de trabajo puede leer los correos y descubrir nuestros secretos mientras que nos alejamos del ordenador, pero difícilmente podrá secuestrar vuestro ordenador de casa. La policía usualmente elije la segunda posibilidad, siempre que no logre espiaros mientras vais al baño. Situaciones diferentes, según el tipo de ataque del cual somos objetivo.

Identificaciones

Cuando nos conectamos a Internet para chatear, enviar correos o para cualquiera otra cosa, el servicio que utilizamos (Facebook, Twitter, Google, etc..) almacena muchos de nuestros datos personales, como la dirección IP y el sistema operativo que utilizamos. Todos estos datos se quedan almacenados por mucho tiempo y pueden identificarnos de manera inequívoca.

Estos datos tienen valor legal y pueden ser utilizados para identificarnos delante de la ley. Para evitar de ser identificados se pueden tomar medidas técnicas que permiten ocultar los datos personales de la conexión, como la dirección IP y los programas que estamos utilizando.

Estas medidas técnicas tipicamente funcionan enviando los datos a un intermediario de confianza (proxy, vpn, etc..), que luego enviará otra vez los datos a su nombre hacia el destinatario final (Facebook, Google, etc..). Aquí presentamos las más comunes.

Las VPN

Las VPN (Redes Virtuales Privadas) son túneles que conectan tu ordenador a otra red, que puede estar situada en cualquier otro lugar del mundo. Utilizando esta conexión para enviar y recibir datos en Internet, tu identidad queda oculta a la persona con la que te estás comunicando o a los servicios que estás utilizando (como Facebook, Gmail, Twitter, ecc..).

Además la conexión de las VPN es cifrada, o sea que los datos no pueden ser leídos por los intermediarios de la red entre tu ordenador y la VPN. Es posible usar las VPN con la mayoría de ordenadores, smartphones y tabletas. Os aconsejamos el servicio de VPN de Riseup [1] y de Autistici/Inventati [2].

[1] https://www.riseup.net/es/riseup-vpn/

[2] https://vpn.autistici.org/help/index-es.html

Navegar con Tor Browser Bundle

Tor es un sistema que anonimiza tus comunicaciones, haciendo rebotar los datos de la comunicación entre diferentes nodos de la red Tor, que están distribuidos por todo el mundo.

Tor Browser Bundle es un navegador (basado en Firefox) que te permite utilizar Tor sin tener que instalar o configurar nada. Puedes bajar la última versión desde su página web oficial [1].

[1] https://www.torproject.org/projects/torbrowser.html.en

Los servidores autogestionados

Además de los millones de servicios ofrecidos por empresas que existen en Internet, hay otros que son ofrecidos por colectivos que se empeñan técnicamente y políticamente en ofrecer servicios libres. Estos colectivos ponen la privacidad y el anonimato de los usuarios por encima de todo, tomando medidas técnicas para que las autoridades no puedan sacar informaciones de los servidores y de los ficheros de logs. Entre los colectivos más conocidos, aconsejamos Riseup [1] y Autistici/Inventati [2].

[1] https://riseup.net/

[2] https://www.autistici.org/es/index.html

Anonimizar los ficheros

La mayoría de los ficheros multimedia (ficheros audio, vídeo, pdf, documentos, ...) contienen muchos datos “escondidos” que podrían ayudar a identificar a quién creó, modificó o utilizó el fichero. Por ejemplo, las fotos y los vídeos suelen contener la información del modelo de cámara utilizado y la posición GPS. Para eliminar estas informaciones existen diferentes herramientas que limpian los ficheros de manera muy sencilla. En sistemas GNU/Linux aconsejamos Metadata Anonymisation Toolkit [1].

[1] https://mat.boum.org/

Interceptaciones

Todos los datos que enviamos y recibimos por Internet pasan por muchos nodos de la red, que si quisieran podrían leer el contenido de estos datos. No hay manera de evitar que lean nuestros datos, pero es posible cifrar el contenido para que sólo lo pueda entender la persona con la que estamos hablando en Internet.

La medida de cifrar los datos, es una técnica que puede ser utilizadas para la navegación, el envío de correos, los chats y otros servicios. Aquí vamos a presentar herramientas sencillas para cifrar la información de los servicios más comunes.

Cifrar los correos con GPG

Cuando hablamos de cifrar los correos, nos referimos a transformar un texto que puede ser leído o "robado" por cualquier persona, en otro del que estamos seguros que sólo va a poder ser leído por el destinatario.

¿Cómo se hace eso? Pues para explicarlo de forma sencilla con un símil, podríamos decir que la persona que quiere recibir el correo tiene dos llaves, una que le da a todos los que quieren enviarle el correo (clave pública) y otra que se queda él y no puede dar a nadie. Cuando alguien le envía un correo, lo "cierra" con esa llave que le ha dado el destinatario (lo cifra con su clave pública). De esta manera, nadie lo puede leer, sólo el destinatario de dicho correo, que lo puede abrir con su llave (clave privada).

Todo este proceso de generación de las llaves (claves) se llevan a cabo mediante los programas que enumeramos en este capítulo, que permiten almacenar tanto las claves públicas de tus contactos como tu clave privada.

De todas formas, existen directorios en internet en los que se puede encontrar las claves públicas de personas que las han dejado allí para que los que quieran cifrar los correos que les envían, lo puedan hacer sin problemas.

Thunderbird + Enigmail, GPG Suite y GPG4Win

Thunderbird [1] es una aplicación de correo libre, fácil de configurar y personalizar, y hay versiones para Linux, Windows y Mac OS X. Instalando el plugin Enigmail [2] es posible recibir y enviar correos cifrados de manera automática, además de disponer de un panel para gestionar las llaves de cifradura GPG.

En sistemas Mac OS X aconsejamos GPG Suite para cifrar, descifrar, firmar y verificar correos y ficheros [3]. Si buscas algo similar para los sistemas Windows puedes probar GPG4Win [4].

Cifrar los correos con las llaves GPG es una de las maneras más seguras de comunicar en Internet.

[1] http://www.mozilla.org/es-ES/thunderbird/

[2] https://addons.mozilla.org/es/thunderbird/addon/enigmail/

[3] https://gpgtools.org/

[4] http://www.gpg4win.org/

HTTPS Everywhere

HTTPS Everywhere es un plugin para los navegadores Firefox y Chrome que se encarga de utilizar comunicaciones cifradas con las paginas web que visitas, dejándote un alto nivel de defensa contra posibles interceptaciones.

En el caso que la página web no soporte comunicaciones cifradas o las soporte sólo en parte, el plugin no podrá cifrar la comunicación y el envío y la recepción de datos será vulnerables a interceptaciones.

Puedes instalar este plugin con mucha facilidad visitando su página web [1].

[1] https://www.eff.org/https-everywhere

Chatear con Pidgin y OTR

La mayoría de las mensajería instantáneas (Skype, GTalk, Facebook Chat, Yahoo! Messenger, etc..) protegen las conversaciones con el cifrado SSL (o TSL) poniendo más difícil a los compañeros de piso o a un colega leer tus conversaciones.

En estos tipos de mensajerías tu privacidad se queda en mano de las empresas, que con toda probabilidad colaborarán con las autoridades para poderte interceptar y identificarte.

En alternativa a estos servicios comerciales, aconsejamos los servidores autogestionados de A/I [1] y Riseup [2] ofrecen a sus usuarios el servicio de mensajería instantánea Jabber (XMPP) que, combinado con el sistema de cifrado OTR [3], nos proporciona un alto nivel de seguridad contra las interceptaciones.

[1] http://www.autistici.org/es/stuff/man_jabber/index.html

[2] https://help.riseup.net/en/otr

[3] http://www.cypherpunks.ca/otr/

Secuestros

Los datos de todos los dispositivos electrónicos (ordenadores, móviles, tabletas, disco duros, etc...) no están a salvo de posibles secuestros. La contraseña de Windows, el código pin de los móviles y todas las medidas de autenticación, no te protegen de posibles lecturas de tus datos cuando el villano de turno (que sea un ladrón de ficheros o un policía forense) tiene en su mano el dispositivo.

La manera más segura para evitar que estos villanos puedan ver tus datos es la criptografía asimétrica, o sea un sistema que protege tus datos con una contraseña. Esta técnica de defensa se puede usar con los ordenadores, y sólo en parte con los smartphones y las tabletas.

Es posible cifrar todo el disco duro, la carpeta de los usuarios, una carpeta cualquiera o un fichero solo. La medida más segura es cifrar todo el disco duro de manera que los datos no puedan ser leídos y el sistema no pueda ser comprometido.

Cifrar con Mac: FileVault y FileVault2

Con el sistema operativo ya instalado se puede cifrar todo el disco duro o sólo la carpeta de los usuarios, respectivamente con FileVault2 y FileVault.

Para utilizar FileVault2 se necesita Mac OS X Lion 10.7 o superiores, y se puede elegir entre cifrar las carpetas de los usuarios y cifrar todo el disco, que se desbloqueará insertando la contraseña al encender el ordenador. Para más información visita la página oficial de apple [1] y esta otra página en castellano [2].

Con Mac OS X Panther 10.3 o superiores se puede utilizar FileVault y sólo se puede cifrar las carpetas de todos los usuarios.

[1] https://support.apple.com/kb/HT4790

[2] http://www.mimac.es/area/Programas+Mac/Encriptar+tu +disco+duro

Cifrar con Linux: luks y Gnome Disk Utility

Con los sistemas GNU/Linux al momento de instalación es posible cifrar todo el disco duro o solo la carpeta de los usuarios. Si tienes un sistema ya instalado, solo será posible cifrar de manera sencilla las carpetas de los usuarios. La solución mejor es cifrar todo el disco, si instalamos un sistema desde cero el procedimiento es sencillo. Consulte la guía de instalación de Ubuntu [1].

Para poder crear y manipular discos duros externos existen diferentes herramientas incorporadas en las diferentes distribuciones de GNU/Linux. Para las que utilizan Gnome (como Ubuntu, Xubuntu, Debian, ecc...) aconsejamos Gnome Disk Utility [2].

[1] http://planetubuntu.es/post/como-instalar-ubuntu-12-10

[2] https://tails.boum.org/doc/encryption_and_privacy/encrypted _volumes/index.es.html

Borrar ficheros

Cuando borramos un fichero en realidad su contenido no se pierde, sino que el sistema borra la dirección donde está almacenado. Existen diferentes maneras para recuperar la dirección del fichero, que sólo funcionan si el sector donde están guardados los datos no ha sido utilizado para otro fichero.

Para estar seguros de que el contenido no podrá ser leído en futuro, podemos utilizar unas herramientas que antes de borrar la dirección del fichero, escriben encima de ello datos casuales más de una vez.

Borrar ficheros con Linux: secure-delete

Las herramientas Secure-Delete [1], son un conjunto de herramientas muy útiles que usan avanzadas técnicas para borrar de forma permanente archivos.

En este paquete encontrarás la herramienta para eliminar ficheros existentes en el disco duro y en la partición de swap, limpiar el espacio libre y la memoria RAM [2].

[1] http://sourceforge.net/projects/securedelete/

[2] http://www.atareao.es/ubuntu/borrado-seguro-o-como-triturar-archivos/

Borrar ficheros con Windows: eraser

Eraser es una herramienta para Windows que permite borrar con seguridad los ficheros guardados en Windows y en otros dispositivos, rescribiendo encima de ellos más veces. Para más información puedes visitar su página oficial [1] o este articulo en castellano [2].

[1] http://eraser.heidi.ie

[2] https://securityinabox.org/es/eraser_principal

Intrusiones

Las intrusiones en los ordenadores, móviles y tabletas, son prácticas utilizadas para espiar a una o más personas en remoto. Con estas medidas el atacante logra obtener el control de los dispositivos con la instalación de un malware, o sea programas que se instalan engañando al usuario o aprovechando de fallos del sistema. Un Malware es algo parecido a un virus: es un programa que se esconde en el ordenador con finalidades malévolas. Quien produce estos malware y los difunde puede hacerlo por diferentes razones, como vender tus datos a empresas que trabajan en publicidad o utilizar tu correo para enviar spam.

Malware de Estado

En los ultimos años la policía de diferentes Estados está empezando a utilizar los malware para espiar personas y buscar pruebas de un supuesto crimen. Por norma general estos malware se encargan de:

- Registrar todo lo que aparece en la pantalla (screenshot)
- Registrar todas las teclas que pulsas (keylogger)
- Permitir desde remoto la navegación en los ficheros del ordenador y copiarlos

En España ha sido redactado un borrador (el Borrador del Código Procesal Penal [1]) en el cual se autoriza a la policía a utilizar malware bajo autorización de la magistradura. En el texto se evidencia que las intrusiones telemáticas por parte de la policía se podrán autorizar sólo para:

- Los casos de supuestos crimenes penales con penas maximas mayores de tres años
- Los casos de terrorismo
- Los casos crimen organizado y crimen informatico

Soluciones especiales

Además de la herramienta que podemos instalar en nuestros sistemas, existen unos sistemas operativos que llevan ya instalado y configurado todo lo necesario.

Estas distribuciones se suelen instalar dentro de una memoria USB y se pueden arrancar en casi todos los ordenadores, sin modificar el sistema y los datos que están en el disco duro del ordenador.

Freepto

Freepto [1] [2] es una de estos sistemas operativos y se focaliza en preservar la privacidad y el anonimato. En ella hay instaladas muchas herramientas para poder navegar con Tor, manejar ficheros y correos criptados, y otras herramienta que hemos mencionado en las páginas anteriores.

Se instala en una memoria USB y es posible guardar con seguridad datos y instalar nuevos programas como si fuera un sistema operativo, porque la memoria USB está totalmente cifrada. Aconsejamos esta distribución para un uso habitual.

[1] https://we.riseup.net/avana/freepto-docs-es

[2] https://github.com/AvANa-BBS/freepto-lb

Tails

Tails al igual que Freepto, se focaliza en preservar la privacidad y el anonimato [1], con todas las conexiones salientes forzadas a salir a través de Tor. El sistema está diseñado para ser arrancado sin dejar ningún rastro en el almacenamiento local a menos que se indique explícitamente. Aconsejamos el uso de Tails cuando estamos en un ambiente hostil.

[1] https://tails.boum.org/index.es.html

¿Quien somos?

La Confederación Nacional del Trabajo (CNT) es una confederación de sindicatos anarquistas y de clase, que agrupan a trabajadores/as de todos los oficios sin distinción en sus sindicatos de ramo. La CNT es una herramienta de lucha para toda la clase trabajadora.

Decimos que es un sindicato de clase porque a él sólo puede pertenecer la clase trabajadora (en activo, parado, jubilado, estudiante, etc.) sin importar sus ideas políticas o creencias religiosas. Basta con que se comprometa a aceptar nuestro pacto asociativo, y a respetar las decisiones que se tomen en asamblea. Como sindicato de clase, no pueden pertenecer a la CNT aquellas personas que no pueden considerarse trabajadores, como son los empresarios, rentistas, grandes propietarios, ejecutivos y altos directivos, cargos políticos de la administración, etc. Policías y cuerpos represivos en general tampoco pueden ser afiliados. Para preservar la independencia, los miembros de partidos políticos o de organizaciones religiosas no pueden emplear el sindicato como foro de propaganda ni ostentar cargos. Finalmente, por coherencia, tampoco admitimos la doble militancia de trabajadores afiliados a otras centrales sindicales.

Nuestras ideas.

Muchas veces nos han llamado utópicos para insultarnos. Sí, somos utópicos pero lo que defendemos en las empresas, en los sectores, en los barrios y en los pueblos donde nos movemos son derechos concretos, reales. No somos ilusos que estamos en las nubes pero queremos cambiar esta sociedad. Una pulga no puede matar a un elefante, pero muchas pulgas pueden llenarle el cuerpo de ronchas, y a lo peor el elefante cambia, o a lo mejor se muere, pues eso...

Desde luego la CNT no ha caído en el "pragmatismo". Insignes pragmáticos de nuestra época son y han sido: Felipe González y todo su PSOE, la UGT con su PSV, Rubio, De la Rosa, Roldán, Juanillo Guerra, Gutiérrez, Redondo y Méndez, etc. Con esos compañeros mejor no vamos.

Nosotros nos modernizamos, nos actualizamos, nos ponemos al día, estamos en el siglo XXI pero no nos volvemos comprensivos con el poder. Hoy como ayer pensamos que el poder corrompe, que desde el poder no se arregla nada (bueno, nada más que el problema del que ocupa el sillón), que los problemas o los arreglamos los de abajo o nos siguen sometiendo. Por eso los parlamentos, los políticos, los comités de empresa, los ejecutivos de las empresas, los gobiernos, los ayuntamientos no nos gustan nada, desconfiamos de ellos y de todos los que aspiran a llegar a ellos.

Hacemos anarcosindicalismo, es decir, un sindicalismo de ideas anarquistas. Otros sindicatos viven de las subvenciones, del dinero que les da el INEM para las cursos de entrenar parados, de los negocios de sus empresas, de las deudas que les perdona el estado, la Seguridad Social, etc. Nosotros/as vivimos de nuestras cuotas y de nuestro trabajo y punto. No queremos "favores" del poder.

Por todo esto, nosotros/as proponemos:

- Frente al sindicalismo corporativo y burocrático de los comités de empresa el sindicalismo participativo y revolucionario de la CNT a través de sus secciones sindicales, sus sindicatos de ramo y sus Federaciones Locales
- Frente al sindicalismo de los dirigentes, el sindicalismo de los trabajadores, de los de abajo
- Frente al sindicalismo comprensivo con el capital, cómplice de la economía capitalista y de sus desastres ecológicos (efecto invernadero, capa de ozono, deforestación, contaminación de las aguas, desertización, etc.) y humanos (hambrunas en el tercer mundo, desequilibrio norte-sur, etc.), este otro sindicalismo, el anarcosindicalismo, radicalmente opuesto a colaborar con esos desastres

La CNT no es comprensiva con las crisis del capital, si tienen crisis que la resuelvan ellos, que para eso las han creado. Nosotros/as luchamos por nuestros derechos.

Versión 1.1 - Imprimido en octubre 2013

http://informaticamadrid.cnt.es/