A por un notable alto en ciberseguridad para nuestro despacho

Susana GONZÁLEZ RUISÁNCHEZ
(1)
Abogado en CARNICER Y ZAMORA, SLP. Asociada de ENATIC (Asociación de Expertos Nacionales de la Abogacía TIC)

Diario La Ley, Nº 8550, Sección Tribuna, 29 de Mayo de 2015, Ref. D-213, Editorial LA LEY

LA LEY 3824/2015

¿Qué acciones debemos tomar frente a una brecha de seguridad o fuga de datos para superar una situación en la que los recursos de la organización puedan verse comprometidos?

Hiperconexión, dependencia tecnológica, imprevisión… actualidad diría yo.

Vivimos en una sociedad hiperconectada a la que Murphy se

adapta constantemente a la perfección. Apuesto a que todos hemos vivido alguna vez esa sensación de «gran catástrofe» de llegar al despacho y que se haya caído la red o la base de datos, justo ese día en que nos fina un escrito en el que hemos estado toda la noche en vela pensando en los cambios que íbamos a hacer nada más llegar y, nos encontramos con que debemos esperar toda una mañana de nervios para poder acabar nuestro plazo. O seguro que a todos nos ha pasado esperar ese correo electrónico importante que justo creemos debía llegar el día que el sistema falla. Para quienes no hayan vivido en primera persona una infección o ataque a sus sistemas, espero que este artículo les transmita al menos las sensaciones de impotencia, riesgo e inseguridad que se pueden sentir durante largas horas, y a ser posible algunas pautas para prevenir esos ataques o minimizarlos.

Eficiencia, productividad, flexibilidad y movilidad son algunas de las grandes ventajas de la incorporación de la tecnología a nuestros procesos. Los sistemas informáticos nos facilitan la gestión, nos aportan información, nos conectan fácilmente con nuestros clientes y además, nos permiten hacerlo incluso fuera de la oficina y a cualquier hora. Frente a ello, no debemos obviar que tenemos **reforzadas obligaciones de confidencialidad, de secreto profesional y protección de datos.**

En la actualidad cualquiera de nuestros despachos trabajan con un activo que ha adquirido un incalculable valor: la información, los

Lo + Leido | Lo + votado

- El delito de cohecho en la reforma del Código Penal
- Contratación de productos bancarios complejos: examen de la reciente jurisprudencia de la Sala Primera del Tribunal Supremo
- El Supremo fija los criterios para aceptar como pruebas los mensajes en redes sociales: no valen los «pantallazos»
- Importante apertura y mayores posibilidades de acceso a la casación: nuevos criterios del Tribunal Supremo

NÚMEROS DISPONIBLES

Mes Junio ▼ Año 2015 ▼

<< < 6 / 2015 > >>

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

datos propios y de terceros que almacenamos y tratamos en nuestros equipos. Cada vez tenemos más tipos de dispositivos a proteger y la variedad de versiones de aplicaciones, software y de sistemas operativos es cada vez mayor en cualquier organización.

Incluso en los despachos más concienciados en seguridad de la información podrán decirnos que tienen instalados y actualizados sus antivirus; sus equipos cifrados; sus sistemas de correo electrónico con firma digital; que realizan periódicamente copias de seguridad en soportes múltiples y que llevan a cabo correctamente su plan de seguridad. Sin embargo, aún en estos casos, y muy a pesar de ser una frase consabida, se suele olvidar **que el eslabón más débil en materia de seguridad somos las personas,** por lo que es vital la implicación de todo el equipo humano de todo nuestro despacho en la puesta en acción y mantenimiento de las medidas de seguridad sobre todos los soportes de la información.

Conviene insistir en el término «todos», ya que no podemos olvidar que en la actualidad somos trabajadores con un alto nivel de movilidad, y los dispositivos móviles están siendo en la actualidad una golosa fuente de información para los cibercriminales. Cualquier miembro de nuestro despacho bien intencionado pero mal informado puede estar utilizando su smartphone, tablet y portátil personal para el trabajo o los dispositivos corporativos para sus actividades personales; tomando sus propias decisiones sobre si es o no suficientemente seguro conectarse a

una red WiFi pública para utilizar la aplicación móvil de su cuenta en banca electrónica con almacenamiento de datos bancarios y tarjetas de crédito; a cualquiera le pueden robar o puede perder su dispositivo móvil en el que recibe los correos de sus clientes con información sensible que debemos proteger; e incluso, y sin la más mínima mala intención, cualquiera puede haber entrado en un sitio malicioso o descargarse un virus de forma inadvertida a través del uso de un pen drive o dispositivo extraíble e incluso haciendo clic en un enlace contenido en un correo procedente de una entidad aparentemente fiable.

Es suficiente con que un dispositivo USB o el móvil sea afectado por un maleware para que, con técnicas de propagación sencillas para los ciberdelincuentes, se consiga infectar toda la red de datos de nuestro despacho poniendo en evidente peligro no sólo el normal funcionamiento de nuestra actividad y nuestra reputación, sino nuestros compromisos con clientes y nuestro deber de confidencialidad, secreto y protección de datos.

Cada vez se está convirtiendo en más común que compartamos documentos digitales que pueden contener información confidencial entre compañeros y con clientes, enviándolos como adjuntos por correo electrónico; vía FTP; copiados en dispositivos USB o mediante el alojamiento en la nube. Sin embargo, lo que todavía no es nada común es que tengamos la precaución de proteger dichos archivos de documentos, ni tan siquiera mediante el sencillo uso de contraseñas en las opciones

generales de guardado. Y esto supone una importante brecha de seguridad así sea porque en el momento en que el documento sale de nuestra cuenta no tenemos ningún tipo de control sobre quien pueda acceder al mismo y de qué otras formas pueda estar siendo compartido.

Llegados a este punto, el objetivo de esta publicación es hablar un poco sobre la seguridad de la información que manejamos, qué responsabilidad legal tenemos en relación a la misma y qué podemos hacer para minimizar posibles riesgos de brechas de seguridad o fugas de datos en nuestra actividad.

La seguridad informática total parece ser inexistente, sin embargo y frente a dejar prácticamente la puerta abierta a nuestros datos y a los de terceros, tenemos opciones para al menos poner un poco más difícil el acceso a la ciberdelincuencia.

Según el último estudio sobre ciberseguridad en España del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es, junto con el Instituto Nacional de Ciberseguridad (INCIBE):

> — Más del 40% de los usuarios no utilizan medidas de seguridad activas (antivirus, firewall, etc.) porque dicen que no son necesarias.
>
> — El 54% de los usuarios no utiliza contraseñas para proteger el equipo y los documentos.
>
> — Un 12,5% de los usuarios no tiene su red WIFI protegida o

desconoce si lo está.

— Sólo un 8,2% de los usuarios utiliza un sistema de cifrado en su terminal para evitar que, en caso de robo o pérdida, la información que contiene sea accesible.

— Un 59,9 % no utiliza antivirus a sus dispositivos móviles.

— Un 48,5 % de los usuarios no tiene anotado su IMEI. (Se trata del código que debemos indicar a la operadora para el bloqueo y en la denuncia en comisaría en caso de robo del terminal móvil).

— Un 36,4% no realiza copias de seguridad periódica. En caso de pérdida, robo o avería del terminal carecer de copia de seguridad conlleva la pérdida de todos los datos.

— Un 43,9 % no tiene activado el bloqueo con contraseña tras un período de inactividad en su móvil.

— El 26,4% de los usuarios de redes sociales tienen su perfil público, por lo que cualquiera puede acceder a su información personal y a sus publicaciones. El 4,6% desconoce el nivel de privacidad de sus perfiles en las redes sociales.

— El 36,8% de los usuarios se conecta a redes WiFs públicas y lo hace siempre que lo necesita y en cualquier lugar, sin tener en cuenta que al hacerlo está exponiendo sus

datos a terceros pudiendo usar estos para fines maliciosos.

Implicaciones jurídicas de un ciberataque

El aparentemente sencillo hecho de hacer clic en un enlace insertado entre el contenido de un correo electrónico malicioso puede llevarnos a la producción de daños propios y a terceros.

Imaginemos que, de pronto, aparece una ventana en nuestra pantalla que nos dice que todos nuestros datos han sido cifrados y que para poder acceder a la clave para su recuperación debemos pagar como rescate una cantidad suficientemente elevada como para desestabilizarnos. De repente también nos vemos imposibilitados para el normal funcionamiento de nuestra actividad, para cumplir con las obligaciones judiciales, contractuales, laborales y fiscales de aplicación, lo que a priori nos sitúa en un escenario de retrasos, gastos añadidos seguramente no previstos y desconfianza; y ello sin descuidar las posibles exigencias de responsabilidad por parte de clientes o terceros ante posibles incumplimientos de nuestras obligaciones contractuales o extracontractuales, e incluso por no haber tomado las medidas de seguridad legalmente previstas o no haber actuado con la debida diligencia o agilidad que haya podido llevar a que la información personal de terceros haya sido expuesta y accesible, además del perjuicio propio de haber sido víctimas de extorsión.

A su vez, el acceso a datos de nuestra titularidad o que se

encuentran bajo nuestra custodia puede derivar en esa solicitud de dinero para descifrar los archivos de la que hablábamos antes, así como en posibles delitos de estafa y coacciones; o como modo para acceder a la venta de datos en el mercado ilegal de datos; o como base para el blanqueo de capitales sirviendo para la compra artículos a bajo coste con cargo a tarjetas de crédito cuyos datos han sido robados para después para revenderlos, y un largo etcétera de supuestos.

Un paso importante en nuestra propia concienciación en materia de seguridad de la información puede ser tener cierto interés por conocer, así sea a nivel básico, cómo actúan y qué objetivos tienen algunos tipos de «virus» que pueden situarnos en el escenario antes comentado.

Algunos tipos de maleware y sus efectos más comunes

Llamamos malware, software malicioso o comúnmente mal denominados «virus» a un inmenso y variado catálogo de programas malignos que pueden atacar nuestros equipos y que constituyen las herramientas de las que se valen los cibercriminales [(2)] .

Existen miles de programas maliciosos clasificados según su origen, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se esconden, los daños que causan, etc. Es común a todos ellos, y esto es importante, que a ninguno de estos programas maliciosos les gusta que mantengamos al día las actualizaciones de seguridad y del antivirus, así como que seamos usuarios cautelosos y precavidos en

nuestra navegación online.

Vamos a enunciar algunos de los que podemos estar oyendo hablar habitualmente y, si es posible adivinar qué es lo que más les molesta de nosotros:

El **Troyano** se esconde en un programa aparentemente inofensivo que, al instalarlo o ejecutarlo, instala otro programa —el troyano en sí— que permite el control en remoto del equipo desde otro equipo, captando datos confidenciales como por ejemplo contraseñas, que envía a otros y/o eliminando ficheros o destruyendo información del disco duro.

Este tipo de maleware lo que realmente le molesta es que tengamos actualizados nuestros antivirus y antitroyanos; que no nos fiemos de adjuntos sospechosos, o que no utilicemos software pirata ya que le dificultamos su actuación.

El **gusano** se instala en la memoria del equipo y se caracteriza por propagarse en ella, haciendo copias de sí mismos a mucha velocidad sin tocar ni dañar ficheros, pero consumiendo banda ancha o memoria del sistema. Las infecciones producidas por estos virus casi siempre se realizan a través del correo electrónico y canales de Chat o mensajería de Internet.

Lo que más les molesta a los gusanos es que tengamos instalado y actualizados los parámetros de nuestro cortafuegos (firewall) y antivirus ya que le dificulta esa propagación en la red, así como que seamos usuarios de redes y chats con cierto cumplimiento de parámetros de seguridad.

El **programa espía (Spyware)** es

un software que recopila información de un ordenador y después la transmite a un equipo externo sin el conocimiento ni consentimiento del propietario del ordenador. Este tipo de software malicioso puede ocasionar una importante pérdida de rendimiento del sistema, así como problemas de estabilidad por ralentización; dificultades de conexión a Internet e incluso extraer información del equipo del usuario.

Suele proceder de adjuntos recibidos en correos electrónicos o acompañando a programas gratuitos o ilegítimos/no oficiales. Le molesta que mantengamos el antivirus de nuestra web y correo electrónico, las puntuales actualizaciones de los navegadores web y sus complementos de seguridad.

Los **falsos antivirus (Rogueware)** son programas fraudulentos que simulan un análisis de seguridad en el sistema reportando infecciones de seguridad inexistentes para asustar al usuario e invitarle a que compre licencias de su presunto e inservible antivirus, cuando en realidad lo que buscan es desactivar el administrador de tareas del sistema operativo, bloquear la ejecución de programas instalados y cambiar la configuración para poder iniciarse automáticamente al arrancar el sistema, lanzando programas maliciosos adicionales, sustrayendo datos personales y dañando archivos almacenados. Pagar por un antivirus falso supone, además de tirar el dinero ya que son inútiles para el destino para el que lo pretendíamos contratar, la cesión de datos bancarios a los ciberdelincuentes, lo que suele conllevar cargos adicionales en la tarjeta de crédito.

Este tipo de maleware suele

proceder de descargas ilegales, en algunos casos de programas gratuitos, webs infectadas o páginas de dudosa reputación. Le molesta que mantengamos el antivirus de los sistemas y de nuestra web y correo electrónico, las puntuales actualizaciones de los sistemas operativos, navegadores web y sus complementos de seguridad, y más concretamente los usuarios que se informan y buscan la confianza online antes de comprar en la red.

Los **KeyLogger** o registradores de teclas son un software o hardware instalado en un ordenador que tiene la capacidad de registrar y memorizar todo lo que se teclee en el teclado unido al equipo, capturando datos como contraseñas, cuentas bancarias e información confidencial que envían a otro destino de forma manual y ajena al consentimiento del dueño del equipo.

Puede venir integrado en un programa troyano, como anexo o ejecutable en un email e incluso en un dispositivo USB.A los keylogger les molestamos los usuarios que mantenemos vigilados y bajo control nuestros equipos y dispositivos y los antivirus en general.

En los **Ransomware** o secuestradores de datos o criptovirus me voy a detener un poco más porque este virus parece destinado a quienes todavía siguen pensando que sus datos y los datos que almacenan y/o tratan no tienen un valor en el mercado tal como para ser víctimas de un ciberataque.

Pero ¿Y si llegamos un día al despacho y al encender los equipos nos encontramos con un aviso de Ransomware diciéndonos que todos

nuestros datos, archivos e información del sistema han sido cifrados por un virus y que para poderlos recuperar nos piden pagar un rescate de 10.000 euros en 48 horas, o de lo contrario, nunca permitirán el acceso a los datos cifrados y, además, publicarán en Internet datos de nuestros clientes?

Los cibercriminales tienen claro que si los datos no tienen valor en el mercado, lo tienen para nosotros, ya que su recuperación no sólo puede costarnos dinero, pérdida de tiempo en el normal funcionamiento de nuestros despachos, sino responsabilidades evidentes frente a nuestros clientes cuyos datos debemos proteger.

El ransomware un software malicioso que capacita al ciberdelincuente para bloquearlo desde una ubicación remota cifrando nuestros archivos y quitándonos el control de toda la información y datos almacenados, ya que para desbloquearlo el virus lanza una ventana emergente en la que nos pide el pago de un rescate y suele incorporar una cuenta atrás en la que indica que de no pagarse la cantidad requerida borrarán el contenido del disco duro.

Se suele camuflar dentro de otro archivo o programa que invite a hacer clic al usuario, bien por lo apetecible del archivo o por la confianza de la entidad suplantada que aparentemente envía el correo electrónico (son los casos de phishing que últimamente tanto nos rodean y conoceremos como el de la Policía, Hacienda (TAPE), Correos, el de Paypal). En ocasiones, y para dar mayor sensación de temor, en el mensaje emergente suelen hacer aparecer la IP del usuario, datos de la operadora WiFi e incluso alguna

foto del usuario captada con la webcam.

Suelen proceder de enlaces o adjuntos en correos electrónicos, de troyanos y gusanos en forma de programas gratuitos o piratas. Como al resto de maleware le molesta si mantenemos actualizados nuestros sistemas, versiones y antivirus así como los usuarios precavidos y desconfiados.

Mucho mejor que tratar de recuperarnos de un incidente de seguridad es prevenirlo controlando los activos frente a posibles riesgos, definiendo los procedimientos a seguir en caso de infección, implementando los controles para asegurar el cumplimiento de las políticas de seguridad, concienciando a todos los miembros de nuestros equipos, realizando auditorías periódicas, etc.

Además de estar familiarizados con este tipo de cuestiones, es conveniente tener en cuenta algunos **hábitos de seguridad mínimos para prevenir el impacto de un ciberataque sobre nuestra información:**

- **Contraseñas.** Todos los años la compañía de software de administración de contraseñas SplashData publica una lista de las contraseñas más usadas en el mundo, precisamente procurando concienciar de la importancia de contar con contraseñas fuertes. Como anécdota curiosa, en los últimos años la contraseña más usada a nivel mundial era «password», que en 2014 dejó de ser la

más usada siendo desbancada por «123456».

La seguridad nunca es comodidad. Igual que es menos cómodo cerrar la puerta de casa con llave que si ella pero desde luego es algo más seguro; las contraseñas débiles son tan fáciles de recordar como vulnerables.

Veamos algunas **recomendaciones** para nuestras contraseñas:

- Modificar las contraseñas generadas por defecto por los sistemas y acostumbrarnos a desactivar el recordatorio de contraseñas por defecto.
- Utilizar contraseñas fuertes, es decir entre 6, 8 o más caracteres, que difícilmente puede ser adivinada o

averigua
da
gracias a
la
ingenierí
a social;
a ser
posible
alfanumé
ricas, con
mayúscul
as y
minúscul
as y
algún
símbolo.
Si
queremo
s que sí
tenga
una base
en la
realidad,
podemos
usar con
cierta
creativid
ad una
palabra
que
recordem
os
fácilment
e, pero
con
caractere
s
especiale
s. Así, en
lugar de
«casa»
podríamo
s usar
«c4$a»
(no
utilicemo
s justo
los
ejemplos
de
contrase
ñas que
damos
en las
publicaci
ones,
son sólo

ejemplos pero muy conocidos). Procuremos evitar que sean fechas de cumpleaños, el nombre del perro o de los hijos.

— No utilizar para todas las cuentas la misma contraseña, cambiarlas asiduamente y no llevarlas escritas en la cartera o móvil, ni en un post-it frente a la pantalla del ordenador. Esta es la parte que a todos resulta más difícil. Si no podemos acordarnos de todas nuestras —ahora diversas— contraseñas podemos

recurrir a un gestor de contraseñas para poder administrarlas de forma segura y cifrada, procurando minimizar el riesgo de comprometerlas.

— Las contraseñas no se deben compartir. Si compartimos nuestra contraseña de acceso al equipo, o al correo electrónico u otras cuentas en redes o páginas webs, debemos saber que estamos dando el acceso a esa persona para que pueda leer nuestros correos, mensajes privados y demás informaci

ón propia y de terceros. Además, le estaremos dando la llave de acceso para cambiar nuestra configuración de privacidad y seguridad, a utilizar nuestra cuenta de correo electrónico para acceder a otros servicios online que utilizamos habitualmente (como nuestra cuenta bancaria o cuentas en webs de compras habituales); e incluso a utilizarla haciéndose pasar por nosotros. Incluso cuando compartimos nuestra contrase

ña con alguien en quien confiamos, es recomendable que esa confianza alcance a su grado de información en esta materia hasta el punto de que estemos seguros de que, a su vez, no la va a compartir con nadie más así sea por descuido o accidentalmente, y aun en este caso hemos de ser conscientes de que escapará de nuestro control.

- **Cifrar** los **documentos confidenciales** con contraseña en las opciones generales de guardado. En los casos en los que ciframos documentos confidenciales con contraseña y debemos comunicarla a nuestro

interlocutor para poderle facilitar su apertura, casi es mejor indicarla verbalmente que enviarla por mail y menos aún por sistemas de mensajería instantánea del tipo whatsapp.

- Instalar y mantener actualizados los **antivirus** de nuestros equipos y dispositivos móviles.

- Mantener los sistemas operativos y aplicaciones **actualizados.** Cada vez que se nos envía una actualización del sistema operativo, antivirus o aplicación suelen traer consigo mejoras de seguridad que pretenden corregir vulnerabilidades que hayan podido detectarse, por lo que conviene estar al día en las actualizaciones.

- **Cifrar los equipos y dispositivos móviles.** Estos software de cifrado requieren una contraseña de acceso previa al encendido del sistema operativo que no queda registrada de ningún modo, ni puede solicitarse su recordatorio o recuperación. Tras ello requerirá la contraseña de acceso al sistema como siempre a cada usuario, significando una doble puerta con llave de acceso frente a nada.

Un paso más podrán ser las herramientas de cifrado y gestión de acceso a los documentos que nos

permiten definir diversos permisos (lectura, edición, impresión, cambio de clasificación, eliminar protección, modificación de usuarios autorizados, impresión de pantalla y copiar y pegar, y monitorizar el acceso al documento y su historial de uso).

- Realizar periódicamente **copias de seguridad de equipos y dispositivos móviles** manteniéndolas en soportes cifrados. Es vital. En caso de pérdida, robo o, en el peor de los escenarios, en caso de un ataque Ransomware podremos recuperar nuestra información sin necesidad de percibirnos como víctimas de extorsión.
- Concienciar al personal del despacho en la **implicación de todos en materia de seguridad de la información.** Recordemos que somos el eslabón más débil y establezcamos pautas o alertas, algunas de las cuales podrían ser:

o Sospechar, no responder, ni rellenar formulario de los mensajes, correos electrónicos o sitios que invitan a hacer clic en un vínculo para ver una foto, un artículo o un video; o que directamente o dirigiéndonos a una página web desconocida piden datos personales tales como nombres de usuario, contraseñas, números de seguridad

social, números de cuentas bancarias, PIN (números de identificación personal), números completos de tarjetas de crédito, fecha de nacimiento, etcétera. Ningún sitio web oficial y legítimo pedirá que enviemos nuestras contraseñas por correo electrónico o cualquier otro sistema de mensajería.

En la mayoría de los casos de phishing la apariencia del correo es totalmente inocua y de empresas comúnmente conocidas que no nos llevan a sospecha inicial si no nos detenemos un rato a analizar que la dirección el correo no parece oficial o incluso que el lenguaje utilizado parece una mala traducción al castellano. Generalmente se trata de cuentas suplantadas o vulneradas

o Nunca acceder o introducir nuestra contraseña en un sitio al que somos dirigidos a través de un enlace recibido por correo electrónico o en un chat que no resulten de confianza real. Tengamos en cuenta que Correos, Hacienda y PayPal pueden ser empresas o proveedores de confianza para muchos de nosotros y, sin embargo, recientemente han sido víctimas de ataques que han servido para una enorme propagación, valiéndose los atacantes precisamente de esa apariencia de confianza. En tales casos, es mejor incluso ir al sitio web de la entidad que nos dirige la comunicación a través de la barra de navegación del buscador y verificar si ese es su correo electrónico habitual u oficial o no.

o Es importante acostumbrarnos a verificar si la dirección web comienza con https://, sobre todo en fases de pago en operaciones online, ya que la «s» implica un compromiso de

conexión encriptada y una mayor protección contra intromisiones. Algunos navegadores incluyen el ícono de un candado en la barra de direcciones junto a https:// para indicar claramente ese compromiso de conexión segura.

¡Al rescate!

¿Qué **acciones** debemos tomar frente a una brecha de seguridad o fuga de datos para superar una situación en la que los recursos de la organización puedan verse comprometidos?.

1.- Determinar el alcance de la infección: En estos casos la rapidez de reacción es muy importante sin apresurarnos a realizar suposiciones o estimaciones que puedan desviar las decisiones correctas. Es preciso que, si nosotros mismos nos tenemos conocimiento técnico en seguridad de la información podamos contar con los servicios externos a quienes demos el parte del ataque para que valoren mediante una auditoría analítica el verdadero impacto de la infección, como único modo de recopilar indicios que conduzcan a las respuestas adecuadas.

Con este tipo de análisis nos informarán qué sistemas se han visto comprometidos y hasta qué punto (un único equipo o toda la red, con o sin repercusión en cuanto al robo de datos, con o sin repercusión a terceros a quienes debamos avisar del suceso, con o sin filtración de datos sensibles de empleados y/o clientes o corporativos, etc.).

2.- Asegurar la continuidad del servicio: En el caso de que hayan resultado comprometidos datos de empleados o clientes deberemos generar una alerta sobre la posible

brecha de seguridad, aconsejándoles que estén al tanto de posibles correos maliciosos que puedan ser enviados utilizando nuestras listas de contactos o bases de datos, así como que mantengan actualizados sus firewall, antivirus y copias de seguridad.

En los casos en los que algún equipo físico resulta gravemente comprometido suelen ponerse en marcha procesos de activación de recursos de respaldo que debe seguirse simultáneamente con el procedimiento debidamente definido para este suceso en nuestra organización.

3.- Contener la infección: Básicamente se procede al aislamiento de los equipos comprometidos interrumpiendo su conexión con el atacante para el robo de la información y suspendiendo los segmentos de red de los que dichos equipos formen parte estos equipos, para evitar que la infección continúe propagándose a través de la red corporativa.

En los casos en que el tráfico generado por el maleware se encuentra cifrado, nuestros servicios externos en seguridad y analítica iniciarán el proceso de ingeniería inversa del mismo para intentar descifrar las claves criptográficas.

Todo este análisis suele llevarnos a descubrir nuevos equipos infectados, lo que a su vez servirá para establecer nuevas reglas de firewall que sirvan de barrera de defensa. Se suele recomendar también el cambio de contraseñas de cuentas y de la red corporativa para evitar que el atacante pueda utilizar la información robada suplantando nuestra identidad mediante el uso de

las que hubiera podido obtener.

4.- Mitigar la infección y eliminar el vector de ataque: En caso de que el malware no hubiera sido detectado por el antivirus, o éste no hubiera estado actualizado debidamente, los técnicos analizarán al detalle el código con el fin de comprender el funcionamiento del malware. Asimismo, se procederá a eliminar del sistema el vector de ataque o falla que permitió la entrada del maleware.

Es por esto que resulta de vital importancia mantener estos sistemas de respaldo actualizados en nuestros planes de mantenimiento activo de la seguridad de nuestra información, ya que esto nos permite una desinfección más rápida y automática en el tiempo de respuesta.

En algunas ocasiones se consigue saber si la infección fue como consecuencia de un descuido de cualquiera de nuestros compañeros de despacho, o bien si se trata de un ataque dirigido contra nuestra organización. En este último caso, nos tocará intentar descubrir quién está detrás del ataque y prever que puede ser sólo el primero.

5.- Denunciar. Si sufrimos un ataque con robo, fraude o extorsión acudamos inmediatamente a denunciarlo a la Comisaría más próxima.

6.- Protegernos más. La supresión de vulnerabilidades que ignorábamos teníamos y la identificación de puntos de acceso débiles a nuestros sistemas nos ayuda a fortalecer nuestras pautas de seguridad y a realizar pruebas para conocer dónde puede estar fallando el plan de seguridad que hasta entonces

seguíamos.

(1) Especialista en Derecho Digital y Seguridad IT, Marketing y Comunicación y gestión de procesos de innovación y management empresarial. Coordinadora de la Comisión de Comunicación. Miembro de junta fundadora de ANPHACKET (Asociación nacional de profesionales del hacking ético constituida por técnicos IT, juristas y miembros de seguridad del estado). Colaborador experto en la Red de Conocimiento de Computer World. www.susanagonzalez.es (@SusanaCyZ). @CyZabogados www.cyzabogados.com –

Ver Texto

---

(2) Termino este artículo con un guiño a la comunidad Hacker o hackers éticos distinguiéndoles radicalmente de los ciberdelincuentes. Los hackers son necesarios en tanto que «auditores técnicos en seguridad» cuyo objetivo no es otro que el de mejorar los sistemas informáticos, detectando y avisando de posibles vulnerabilidades y solucionando posibles problemas en los sistemas. Todo lo contrario que un ciberdelincuente, que aprovecha las vulnerabilidades que encuentra en un sistema para su propio beneficio y generalmente mediante o para la comisión de algún ilícito.

Ver Texto

Opinar (0)

Queremos saber tu opinión

Nombre

ZARIURIS, S.L.

E-mail (no será publicado)

cyz@cyzabogados.com

Comentario

Conozco y acepto las condiciones sobre protección de datos ☐

LA LEY no se hace responsable de las opiniones vertidas en los comentarios. Los comentarios en esta página están moderados, no aparecerán inmediatamente en la página al ser enviados. Evita, por favor, las descalificaciones personales, los comentarios maleducados, los ataques directos o ridiculizaciones personales, o los calificativos insultantes de cualquier tipo, sean dirigidos al autor de la página o a cualquier otro comentarista.

Introduce el código que aparece en la imagen

Enviar