Secure &MAGAZINE

Número 3 | Enero 2018

ENTREVISTA

Luis Villafranca

IT Manager de Azkoyen S.A.

PREVISIONES DE CIBERSEGURIDAD PARA 2018

Sanción a Facebook: LOPD vs. RGPD

HACKER ÉTICO

¿Por qué hay que añadir un adjetivo a esta profesión?

Secure&h4x

La marca de *hacking* ético de **Secure&IT**

IoT
La inteligencia del secador de pelo

Manuel Martínez (RNE)

EL *RANSOMWARE* Y OTROS MALES

Ángel Pablo Avilés "Angelucho"

Secure&IT
www.secureit.es

Editorial

Estimados lectores,

Aunque en el número anterior de ***Secure&Magazine*** publicamos un especial sobre protección de datos (con motivo de nuestra Jornada de Ciberseguridad), también quisimos hacer hincapié en una de las amenazas más peligrosas para usuarios y empresas, el *ransomware*. Este tipo de *malware* solo representa una pequeña parte de las ciberamenazas a las que nos enfrentamos todos los días, pero lo cierto es que WannaCry o Petya coparon muchos de los titulares de prensa del momento (no olvidemos que pusieron en jaque a países enteros). Lamentablemente, y como pronosticábamos en ediciones anteriores de nuestra publicación, el *ransomware* sigue siendo noticia (después de WannaCry y Petya, llegó Bad Rabbit) y seguirá su línea creciente (sobre todo aumentará su efecto destructivo). **Nos vamos a enfrentar a ataques más agresivos y que evitan las defensas de seguridad.** Irán, sobre todo, destinados al robo de información o dinero. Y, como era de esperar, con el auge del Internet de las Cosas (IoT, por sus siglas en inglés), llegará el incremento de los ciberataques dirigidos a esta tecnología.

De nuevo, **la formación y la concienciación de empleados y usuarios será clave para evitar los efectos de los ataques**. No nos cansamos de decir que nadie está exento de ser víctima del cibercrimen. No importa qué tamaño tengan las empresas; una pyme corre los mismos riesgos que una gran compañía (incluso más, porque suelen tener menos medidas de protección). Por este motivo, es necesario invertir no solo en tecnología para evitar (o mitigar) los ataques, sino también en formación y concienciación de los empleados.

Uno de los problemas sigue siendo que se percibe la ciberseguridad como un gasto y no como una inversión. Es cierto que cada vez hay más conciencia sobre la importancia de la gestión de la seguridad de la información, pero falta mucho por hacer. Los responsables de las compañías deben entender que existen más amenazas dentro (errores humanos, empleados descontentos, falta de medidas técnicas, formación insuficiente o inexistente, incumplimiento legal, etc.), que fuera (los temidos ciberdelincuentes). Por cierto, vamos a aprovechar estas líneas para hacer una aclaración: **no debemos confundir a los delincuentes con los *hackers***. Para evitar el error, hablamos de este tema en uno de los artículos de este tercer número de ***Secure&Magazine*** (donde también aprovechamos para presentaros la imagen de nuestra marca de hacking ético)**.** Pero, Ángel Pablo Avilés (Angelucho) lo resume perfectamente en esta frase: **"*Un hacker es un experto en seguridad. El que comete el delito es delincuente, no hacker*".**

Otra de las grandes preocupaciones de las empresas es cómo cumplir con el nuevo Reglamento General de Protección de Datos (RGPD o GDPR, por sus siglas en inglés). En la edición anterior hablábamos de la falta de preparación de las empresas para abordar el RGPD. Seguimos con la misma incertidumbre en materia de protección de datos. ¿Y cuál es el mayor problema? El 25 de mayo, fecha en la que la nueva normativa será de obligado cumplimiento, se acerca a toda velocidad y muchas compañías todavía no se han puesto en marcha; no han empezado a adaptar su forma de trabajar a los requisitos del nuevo Reglamento. Por este motivo, **dedicaremos la cuarta edición de nuestra Jornada de Ciberseguridad (que se celebra en mayo) al Reglamento General de Protección de Datos.** Por supuesto, os iremos informando a través de nuestra web y redes sociales de la fecha, el lugar y los contenidos. ¡Nos encantaría contar con vuestra presencia!

En este número contamos con la participación de varios colaboradores a los que queremos agradecer su dedicación; sin sus aportaciones esta revista no sería lo mismo: Ángel Pablo Avilés (Angelucho), Horatiu Bandoiu (Bitdefender), Manuel Martínez (Radio Nacional de España), Óscar Maire-Richard (Prot-On) y Pablo García Pérez (Fortinet).

El equipo de Secure&IT

Sumario

4 Entrevista

Luis Villafranca, IT Manager de Azkoyen, S.A.

7 Previsiones para 2018

Los ciberataques serán más agresivos y sofisticados en 2018

8 *Hacker* ético

La necesidad de añadir el adjetivo "ético" a esta profesión

12 El *ransomware* y otros males

Ángel Pablo Avilés, "Angelucho", editor de *El Blog de Angelucho*

16 Ciberseguridad pasada y futura, lo que nos deparará 2018

Pablo García, Senior Telco/Carrier Systems Engineer en Fortinet Iberia

18 La inteligencia del secador de pelo

Manuel Martínez, director del programa 5.0 de RNE

20 Tecnología IRM y cumplimiento GDPR

Óscar Maire-Richard, Prot-On Founder & Product Manager

22 La inteligencia artificial y el *machine learning* en seguridad informática

Horatiu Bandoiu, ISO 27001 LA y Channel Marketing Manager de Bitdefender

24 Sanción a Facebook: LOPD vs. RGPD

Luis Villafranca

"En ciberseguridad, la preocupación siempre es muy alta y la atención debe ser constante "

Luis Villafranca empezó a trabajar para el Grupo Azkoyen en el año 1989 y, en la actualidad, ocupa el cargo de IT Manager de la corporación. Lleva casi 30 años dedicado a una compañía con una alta complejidad interna (debido a sus diferentes líneas de negocio y a su presencia en varios países), que ha vivido cambios organizativos muy importantes y con un fuerte impacto en los sistemas de información. El departamento de Tecnologías de la Información de Azkoyen, S.A., del que Luis es responsable, es corporativo y está centralizado en su sede de Peralta (Navarra). Desde allí, se da servicio a once empresas del grupo que están situadas en Colombia, EEUU, Portugal, Francia, Alemania, Italia, Reino Unido y España. De ellas, tres son centros de fabricación (Colombia, Italia y Reino Unido) y, el resto, sedes comerciales.

Llevas casi 30 años trabajando en Azkoyen, ¿cómo ha sido el proceso de transformación digital en la empresa?

En Azkoyen ha habido una gran transformación. Por ponerte un ejemplo, desde que yo llegué hasta el año 2003, cada empresa del grupo era independiente del resto (teníamos 3 departamentos de IT diferentes). Pero, en aquel momento, en el que yo era responsable de Tecnologías de la Información de una de las empresas del grupo, la informática –entre otros departamentos– pasó a gestionarse de manera corporativa y me ofrecieron ocuparme de ese nuevo departamento de IT. Poco a poco, hemos ido integrándolo todo y, a día de hoy, podemos decir que todos los servicios que prestamos desde el área son únicos para todo el grupo.

Pero, tenemos un nuevo reto. Hasta ahora, el departamento de IT se encargaba de lo que llamamos "IT de negocio", es decir, dar soporte a todos los sistemas que necesita la empresa para gestionar el negocio (correo electrónico, ficheros, bases de datos, sistemas de seguridad, etc.). Pero, Azkoyen –que es una compañía que siempre ha fabricado y vendido máquinas– está transformando su negocio. Vamos a empezar a comercializar *software* y una serie de servicios, con el modelo de pago por uso. Hablamos de telemetría de las máquinas, monederos virtuales, etc.

Ya no solo vamos a fabricar máquinas; ahora, se abre ante nosotros un escenario novedoso e interesante, que va acompañado de nuevos desafíos tecnológicos y de seguridad. De aquí en adelante, nos encargaremos no solo de la "IT de Negocio" sino también de la "IT de Producto", que es donde estamos depositando muchos de nuestros esfuerzos.

Algunos informes revelan que casi el 30% de las empresas industriales se ha enfrentado en los últimos 12 meses a ataques dirigidos y que El 'fraude del CEO' crecerá un 70% este año. Esto es definitivo para que muchas empresas se planteen invertir en seguridad de la información. ¿En qué momento decidisteis vosotros abordar la ciberseguridad como algo necesario para la compañía?

"Se abre ante nosotros un escenario novedoso e interesante, que va acompañado de nuevos desafíos tecnológicos y de seguridad"

En todo el proceso de integración que hemos vivido en Azkoyen desde 2003, el tema de la seguridad no había sido nunca el prioritario. Habíamos trabajado en la implantación de SAP, renovación y unificación de infraestructuras, integración de las empresas que se iban adquiriendo, etc. Nosotros teníamos nuestros *firewalls* y nuestro *software* antivirus; sabíamos que la seguridad es mucho más que eso, pero siempre había proyectos más prioritarios para el negocio. En el año 2014, decidimos finalmente "coger el toro por los cuernos" y afrontar todos los problemas relacionados con la seguridad.

Después de un proceso de selección con diferentes proveedores, **Secure&IT** fue el que más nos interesó porque contaba con un servicio de seguridad 360 grados.

El primer paso era claro: debíamos hacer una auditoría completa, no solo en temas de ciberseguridad, sino también en temas de cumplimiento y de procedimientos. El resultado de la auditoría fue un plan de acción que hemos ido ejecutando a lo largo de estos años.

Con carácter general, el aumento de los incidentes de seguridad en estos últimos meses ha sido muy grande. En términos de seguridad, nunca puedes tener la certeza de estar completamente protegido, pero no me cabe ninguna duda que Azkoyen está ahora mucho mejor preparada para convivir con esta nueva situación que antes. Pese a todo, la preocupación siempre es muy alta y la atención debe ser constante.

¿Cómo ha evolucionado el Grupo Azkoyen en lo que a seguridad de la información se refiere?

Nosotros decidimos apostar por la seguridad como una inversión de futuro. En un primer momento, en los inicios del proyecto, creíamos entender la importancia de lo que nos contaban (amenazas, riesgos, formación y concienciación, etc.), pero en realidad veíamos los ataques como algo lejano, algo que nunca nos iba a suceder a nosotros. En este periodo han sucedido varias cosas que nos han hecho comprender, de verdad, la relevancia de este tema. Una de ellas es que hemos sufrido ataques (y los hemos gestionado bien). Pero, añadiría que existe una gran presión legislativa y el hecho de que los medios de comunicación le estén dando mayor visibilidad a la ciberseguridad. Por eso, aunque antes creíamos que lo entendíamos, es ahora cuando podemos decir que estamos concienciados y sensibilizados. De hecho, la exigencia que nos hacemos en este ámbito es cada vez mayor.

La mayor parte de los peligros no están fuera, sino dentro de la propia empresa y, uno de los más importantes son los errores humanos. Los datos hablan por sí solos: el 85% de los trabajadores desconoce las políticas de ciberseguridad de su empresa. ¿Qué importancia le dais a la formación y concienciación en Azkoyen?

"Nuestro objetivo es que los trabajadores del Grupo Azkoyen apliquen la seguridad no solo en el ámbito laboral, sino también en el personal "

Nosotros siempre hemos apostado por mantener informados a nuestros trabajadores. Cuando se ha producido algún evento de seguridad importante (como lo sucedido con Wannacry, Petya, etc.), lo hemos notificado a todos nuestros empleados. Esa labor ha existido siempre. Pero, además, desde hace un tiempo contamos con los consejos de seguridad que semanalmente nos hace llegar **Secure&IT**, y que han conseguido una mayor concienciación y aprendizaje por parte de los trabajadores. Diría que la labor de los medios de comunicación en este sentido también es importante; el hecho de ver los ataques en la televisión nos influye. Y, con el paso del tiempo, la evolución es notoria. Antes, ningún empleado nos hacía consultas relacionadas con la seguridad, ahora, ante cualquier duda o cualquier cosa extraña, preguntan.

En definitiva, nuestro objetivo es que los trabajadores del Grupo Azkoyen apliquen la seguridad no solo en el ámbito laboral, sino también en el personal (en su casa, con sus hijos, etc.). De esta forma, todos salimos beneficiados.

Venimos de un año en el que Wannacry, Petya y, después, Bad Rabbit han puesto la ciberseguridad en boca de todo el mundo. Aunque el *ransomware* es solo una pequeña parte de las amenazas a las que nos enfrentamos día a día, ¿qué grado de preocupación genera esto a un IT Manager?

De entrada, cualquier ataque, aunque no te afecte directamente, genera preocupación e interés (saber qué ha pasado, por qué se ha producido, si se podía haber evitado, etc.). Por supuesto, estos eventos hacen que incrementes la aplicación de medidas preventivas. Te obliga a estar más encima. En nuestro caso, nos ofrece mucha tranquilidad el hecho de contar con un SOC (Centro de Operaciones de Seguridad, en inglés, Security Operations Center) como el de **Secure&IT**, en el que se monitorizan todos nuestros eventos de seguridad, con un servicio 24x7. Eso, más el trabajo constante de actualización de sistemas y de formación y concienciación de los empleados, nos permite estar más "tranquilos".

"Cualquier ataque, aunque no te afecte directamente, genera preocupación e interés "

Otra de las grandes "preocupaciones" para las empresas en 2018 es el nuevo RGPD. Ya ha entrado en vigor, pero a finales de mayo será de obligado cumplimiento. ¿Un nuevo reto?

Efectivamente, es un nuevo reto y de gran importancia para nosotros. Hasta ahora, en Azkoyen teníamos que cumplir con la legislación nacional de protección de datos en cada uno de los países europeos donde tenemos presencia propia. La nueva legislación nos permite resolver el problema de forma corporativa y, desde España, vamos a asegurar el cumplimiento de la normativa en todas nuestras empresas. Además, el proyecto de adaptación al GDPR no nos lo hemos tomado como una nueva obligación legal, sino que hemos decidido implantar un Sistema de Gestión de Seguridad de la Información que nos permita el cumplimiento normativo y, sobre todo, aportar una mayor seguridad a la información de la compañía. Adicionalmente, se hace una labor continua en *compliance* y estamos inmersos en un proyecto de prevención del delito, a raíz de los cambios que se produjeron en el Código Penal.

¿Qué papel juegan en vuestro trabajo empresas como Secure&IT?

Para nosotros no hay ninguna duda, en materia de IT consideramos que es mejor externalizar los servicios con empresas y profesionales especialistas. Si nos centramos en el ámbito de la seguridad (y también del cumplimiento) el trabajo de **Secure&IT** es fundamental para nuestra empresa y nos ofrece una cobertura completa: se realiza un seguimiento constante; contamos con un plan de actuación; nos aseguramos de cumplir con la normativa; disponemos de asesoramiento en la implantación de medidas tecnológicas y, además, recibimos formación.

AZKOYEN GROUP

Desde su fundación en 1945, la compañía se ha caracterizado por la apuesta tecnológica, la investigación y el desarrollo de nuevos productos.

- **Medios de Pago: diseño, fabricación y comercialización de mecanismos y sistemas de selección, devolución y control de medios de pago para los sectores de recreativo, *vending*, kioscos, banca, telefonía, *retail*, transporte y parking.**
- **Sistemas de Seguridad y Control de Acceso: fabricación, comercialización e implantación de sistemas innovadores de *software* y *hardware* para el control de accesos, el control de presencia y sistemas integrados de seguridad.**
- **Máquinas Expendedoras – Máquinas *Vending*: diseño, fabricación y comercialización a nivel global de máquinas expendedoras de tabaco, café y otras bebidas calientes, bebidas frías, snacks y otras soluciones *vending*.**

Los ciberataques serán más agresivos y sofisticados en 2018

Para mirar hacia adelante, primero hay que echar la vista atrás y analizar qué ha sucedido este 2017. En la Evaluación de Amenazas del Crimen Organizado en Internet (en inglés, *Internet Organised Crime Threat Assessment* –IOCTA-), elaborada por Europol, destacan del año pasado aspectos como el *ransomware*, el Internet de las Cosas (IoT), el fraude *online* o los ataques a redes bancarias.

Lo cierto es que, aunque solo son una pequeña muestra de las ciberamenazas a las que nos enfrentamos, **los ataques de *ransomware* han eclipsado este 2017 al resto**. WannaCry o Petya han conseguido poner la ciberseguridad en boca de todo el mundo, debido a su impacto y a su gran capacidad de propagación.

La falta de medidas técnicas que ayuden a proteger datos de carácter personal han favorecido, de nuevo, la difusión de enormes cantidades de datos (se han filtrado unos 2 millones de registros que afectan a ciudadanos de la UE). Y, en este sentido, hacemos alusión, como posible medida correctora, al cumplimiento del nuevo Reglamento Europeo de Protección de Datos (GDPR por sus siglas en ingles).

En 2017 se han producido, además, los primeros ataques serios a dispositivos del Internet de las Cosas (IoT); y hemos visto cómo emergen aquellos dirigidos a redes bancarias, con el objetivo de manipular saldos de tarjetas, controlar cajeros automáticos o hacer transferencias; o las intrusiones producidas en vehículos, contadores e suministro eléctrico, y otros dispositivos.

Además, el fraude *online* se extiende como la pólvora, afectando a todas las industrias. Incluso, algunos sectores son atacados para facilitar otros delitos como el tráfico de personas, de armas o de drogas. Y, por cierto, la *Darknet* sigue siendo fundamental en todo esto.

Europol también apunta que los ciberataques seguirán creciendo y, sobre todo, evolucionando de aquí en adelante. No es una novedad. El CCN-CERT asegura que los ciberataques contra el sector público y empresas estratégicas de nuestro país aumentarán casi un 27% (una tendencia que se puede extrapolar al resto de compañías y organizaciones).

Y, ¿hacia dónde vamos en 2018?

- **Ataques menos crecientes en número, pero mucho más agresivos.**

No será necesario que aumente en mucho el número de ciberataques porque, si su efecto es mucho más destructivo, conseguirán su propósito. ¿Qué supone esto? Las empresas y las administraciones deben tener especial cuidado, además, tendrán que asumir que las consecuencias serán cada vez más graves.

- **Nuevos ataques que evitan las defensas de seguridad**

Las amenazas son cada vez más sofisticadas. Eso significa que ni las mejores defensas, ni los mejores motores de antivirus e IPS (*Intrusion Prevention Sistem*; en español, Sistema de Prevención de Intrusos) serán capaces de detectar o mitigar algunas de las nuevas amenazas. ¿Cuáles son? Llegarán en forma de amenazas "*fileless*" o sin fichero asociado, incorporadas a componentes hardware y, sobre todo, a través de técnicas de ingeniería social (se obtiene la información de forma directa, simplemente engañando a los usuarios o empleados).

Por ello, no nos cansamos de decir que **dos de los aspectos fundamentales en ciberseguridad son la formación y la sensibilización**, que deben ser continuas.

La mayor parte de los problemas de seguridad de la información no se producen por ataques externos llevados a cabo por ciberdelincuentes, sino por fallos internos. Debes recordar que las personas son el eslabón más débil de la cadena de ciberseguridad, por eso tienen que estar formadas.

- **Ataques orientados a robo de información o dinero**

Los ataques van a estar muy orientados al robo de información y dinero. Llegarán en forma de coacciones y chantajes (por ejemplo, amenazando a las víctimas con publicar la información robada). Además, seguirá jugando un papel fundamental el conocido como "fraude al CEO", que se basa en la suplantación de identidad de una persona con alto poder de decisión en la empresa. Puede realizarse a través de un correo electrónico que parezca proceder de un directivo, mediante una llamada falsa o alguna técnica similar. El objetivo es el robo de dinero y, aunque el modo de proceder parece sencillo, no lo es. Preparar este tipo de estafa puede llevar a los ciberdelincuentes meses e, incluso, años.

- **Crecen las amenazas dirigidas al Internet de las Cosas (IoT) y a dispositivos móviles**

Con el auge del Internet de las Cosas, llega el auge de los ciberataques dirigidos a esta tecnología. Gracias al IoT, elementos cotidianos de nuestra vida (como los vehículos, la televisión, el aspirador o la nevera) están conectados a Internet y, por tanto, pueden ser atacados por los ciberdelincuentes. También van a crecer los ataques a dispositivos móviles, especialmente a aquellos que tengan el sistema operativo Android.

A pesar de que la ciberseguridad va cobrando importancia dentro del sector TI, es necesario que empresas y usuarios hagan los deberes y se pongan al día, en lo que se refiere a seguridad de la información. Este puede ser un buen propósito para el año 2018.

Hacker ético: ¿por qué hay que añadir un adjetivo a esta profesión?

Antes de empezar con el artículo, nos gustaría que te plantees un par de cosas: ¿Qué te sugiere la palabra "*hacker*"? ¿Le das una connotación positiva o negativa?

En general, se suele pensar que los *hackers* son gente oscura, encapuchados de los que conviene protegerse. Aunque, la tendencia está cambiando. Es gracias a la fama de algunos de estos profesionales ya que, incluso, existen programas de televisión dedicados a esta temática.

Alrededor de la definición de este término hay un gran debate. Si consultamos la palabra *hacker* en el Diccionario de la Real Academia de la Lengua (DRAE) nos remite directamente a este significado:

Pirata informático, ca

> 1. m. y f. Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta.

La Wikipedia, por su parte, nos ofrece varios significados: el primero habla de todo individuo que se dedica a programar con entusiasmo y que considera la información un bien preciado, que hay que poner al alcance de todo el mundo. La segunda definición nos remite a la visión de Eric Raymond, también conocido como ESR, que consiguió la fama como historiador de la cultura *hacker*. Según él, el reconocimiento de sus iguales es el motivo principal por el que los *hackers* crean software para distribuirlo de forma gratuita. En tercer lugar, nos informan de que este término nació en la segunda mitad del siglo XX y de que su nacimiento está ligado a los laboratorios del *Massachusetts Institute of Technology* (MIT).

Pero, lo cierto es que no todas las definiciones que se dan son tan "benevolentes". Por este motivo, hemos querido consultar con nuestros expertos y les hemos pedido que nos dieran su visión sobre este tema.

Nos comentan que desde hace años se criminaliza al *hacker*. De hecho, por un delito informático, la acusación es de terrorismo. Pero, además, nos dicen que se produce una paradoja: "*Llevas muchos años actuando en segundo plano, evitando que te vean. Y, cuando ya tienes un cierto nivel técnico, son las propias empresas, organizaciones o administraciones (de las que te escondías porque te querían denunciar), las que te ponen un contrato delante*".

"Ser hacker es algo meritorio, no es un calificativo que se da uno mismo"

Comentan, además, que se les suele adjudicar una personalidad muy concreta: "*la gente tiene la versión del hacker que ha dado Hollywood y que, al final, supone un desprestigio*". De hecho, recuerdan que un *hacker* no tiene por qué ser alguien que se dedican a la informática, simplemente son personas de cualquier ámbito a las que les apasiona lo que hacen: "*Un día te das cuenta de que un ordenador es mucho más y, a partir de ahí, no existen las horas, ni los días. Es un vicio que se disfruta. Y, en general, ni siquiera es por dinero (aunque lógicamente hay que comer), se hace por superación y reconocimiento*". Además, para ellos ser *hacker* es algo meritorio: "*Es el entorno el que te atribuye esa virtud, no es un calificativo que se da uno mismo*".

Angelucho: "Un hacker es un experto en seguridad. El que comete el delito es delincuente, no hacker".

Evidentemente, no todos los *hackers* son "buenos", igual que no lo son todos los abogados, electricistas o carniceros. Pero, si al resto de profesionales no los metemos en un mismo saco, ¿por qué en este caso sí?

En este sentido, Ángel Pabo Avilés "Angelucho", miembro del Grupo de Delitos Telemáticos de la Guardia Civil y creador de X1RedMásSegura, aclara: ***"Un hacker es un experto en seguridad. El que comete el delito es delincuente, no hacker".***

Lo cierto es que parece imprescindible explicar que los *hackers* no son delincuentes, que no son el enemigo, porque socialmente se ha dado por supuesto que hay que tener cuidado con ellos. De hecho, se venden soluciones para protegerse de los *hackers* o se establece una defensa contra ellos. Pero, no nos damos cuenta que utilizamos ese término, cuando de lo que en realidad hablamos es de delincuentes. Quizás de ahí viene la necesidad de añadir el adjetivo calificativo "ético" a la profesión *hacker*.

Esto no es algo nuevo. En su manifiesto *The Conscience of Hacker*, escrito en el año 1986, The Mentor profundizaba en la personalidad de estos profesionales. En este documento, que perfectamente podía haber sido escrito hoy, hablaba de lo que es ser especial, de sentirse incomprendido desde pequeño y descubrir, gracias a los ordenadores, un lugar al que pertenecer. En su necesidad de defenderse concluyó su manifiesto con estas palabras:

"*Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike*".

Se reconocía criminal, sí, pero aseguraba que su crimen es la curiosidad; en el hecho de juzgar a las personas por lo que dicen o piensan, no por su apariencia; y de tener una inteligencia superior al resto.

El *hacker* en la empresa

Puede ser difícil para el común de los mortales, pero quizá deberíamos empezar a pensar en ellos como gente que, simplemente, cuenta con unas capacidades especiales y que dedica mucho tiempo (es su obsesión) a resolver las dudas que rondan por su cabeza. Pero, el hecho de contar con esas capacidades y de poder poner en un brete a empresas y administraciones, no les convierte en delincuentes *per se*; no les hace ni buenos ni malos.

Lo cierto es que los *hackers* son importantes para las empresas. ¿Has pensado los beneficios que puede aportarte poner sus capacidades al servicio de tu compañía? ¿Por qué crees que las grandes organizaciones contratan *hackers*?

Hay casos muy conocidos. ¿Te suena Nicholas Allegra, más conocido como "Comex"? Quizá por el nombre no, pero si te decimos que creó la solución *JailbreakMe* para liberar los dispositivos de Apple, puede que te sea familiar. Lo curioso es que terminó trabajando para ellos. ¿Y GeoHot? Él consiguió romper la seguridad de PlayStation, y después acabó siendo fichado por Facebook. En definitiva, estos casos revelan la necesidad que tienen las grandes empresas de contar con estos profesionales.

¿Cómo te puede ayudar un *hacker* (ético)?

Realizar auditorías de seguridad periódicas se está convirtiendo en un imprescindible para las compañías. El *hacking* ético permite a las empresas identificar vulnerabilidades en los sistemas de información y comunicaciones, conocer el riesgo que implican y aplicar una contramedida para subsanarlas.

Te podemos dar varias razones por las que realizar una auditoría de *hacking* ético o un *pentesting* puede ser importantísimo para tu empresa. En primer lugar te permite conocer el nivel de seguridad que tienes y, por ende, los riesgos a los que te enfrentas (así sabrás si la inversión en ciberseguridad y continuidad de negocio que haces es la adecuada). Además, llevar a cabo auditorías de forma cíclica te permitirá estar siempre al día y adaptar tus recursos a las necesidades del momento. En definitiva, es una forma de asegurarte de que haces las cosas bien y poder minimizar los riesgos.

Puedes encontrar más información sobre hacking ético en nuestra web. ¿Necesitas más datos? No dudes en contactar con nosotros.

Por cierto, estamos encantados de presentarte **Secure&h4x**, la marca de *hacking* ético de **Secure&IT**.

Secure&h4x

La marca de *hacking* ético de **Secure&IT**

El *ransomware* y otros males

En el artículo "*El secuestro digital de la información – el ransomware*" del primer número de **Secure&Magazine** ya hablamos de la ciberamenaza protagonista de los últimos años; un hecho que hemos podido corroborar durante todo el pasado año 2017.

El *ransomware* o "Virus Mortadelo", como lo bauticé en mi blog allá por el 2013, ha seguido cambiando de disfraz en el último año (incluso después de la publicación del nº 1 de esta revista). No solo los usuarios finales, sino también las pequeñas empresas se han visto amenazados. Pero, dando una vuelta más de tuerca, nuestro "Mortadelo" se ha atrevido, incluso, con grandes empresas del mundo tecnológico. Y, como ya anticipábamos, cada vez con mayor agresividad.

Durante 2017, el *ransomware* ha sido (desgraciadamente) noticia, debido a diversos ataques con nuevas variantes o mutaciones.

A todos los lectores les vendrá rápido a la memoria el mediático WannaCry, una evolución del *malware,* que aprovechaba una vulnerabilidad del Sistema Operativo Windows de Microsoft. Su misión no era el robo de información o la inhabilitación de las máquinas que se vieron afectadas en más de cien países sino, como ya venían haciendo sus antecesores, el cifrado de los archivos ofimáticos (.doc, .jpg, .pdf, etc.). El objetivo: que, una vez cifrados, fuera posible pedir un rescate en *bitcoins* para poder recuperarlos.

La agresividad de esta nueva variante llegó hasta el punto de tener capacidad no solo de afectar a los archivos locales de la máquina, sino también de propagarse por la red interna, en la que se encontraba el dispositivo víctima, y replicarse en todos los dispositivos conectados. De esta forma, se cifraba toda la información importante de la organización, sin que los usuarios tuvieran la menor oportunidad de mitigar el problema del secuestro de la información.

No terminó el año con este ataque, posteriormente conocimos la existencia de otras evoluciones, como Petya, que se servía igualmente de una vulnerabilidad en el protocolo de red de los equipos Windows afectados.

Estas dos variantes, como ya hemos explicado, utilizaban vulnerabilidades de sistemas operativos Windows relativas al protocolo SMB (*Server Message Block*), que permite la comunicación entre los dispositivos de una red Windows. Estas vulnerabilidades fueron solucionadas mediante actualizaciones de la propia compañía Microsoft y parcheadas por los usuarios y empresas.

Luego llegó el Bad Rabbit, un suma y sigue de *ransomware* que, en esta ocasión utilizaba la vulnerabilidad en otro tipo de software. Durante la navegación por una página comprometida, la víctima veía como en su navegador aparecía una ventana informativa "*pop-up*" anunciando la desactualización del Adobe Flash Player. Al pulsar en la opción de "actualizar" se instalaba en el dispositivo el código malicioso. Aunque esta variante no era tan agresiva como las anteriores, sí tenía la capacidad de acceder a las contraseñas que se guardaban en la memoria del ordenador.

En este 2018 recién estrenado, **el *ransomware* continuará en la misma línea creciente**, de "suma y sigue", en cuanto a los ataques se refiere. Por supuesto, continuarán presentándose con distintas mutaciones que serán, sin ningún lugar a duda, más elaboradas, complejas y agresivas.

La mayoría de las nuevas amenazas tendrán como denominador común el usuario final que, una vez más, será el eslabón más débil (ya sea doméstico o empleado de una empresa). De nuevo, el usuario será protagonista indiscutible en caso de infección del dispositivo que gestione.

Por ello, todas las empresas (incluso las más pequeñas) deben invertir, además de en tecnología para evitar estos ciberataques, en concienciación y formación de sus empleados. **La falta de cultura de ciberseguridad convierte a los trabajadores en una puerta abierta de par en par para los ciberdelincuentes.** Siguen siendo vulnerables a las viejas técnicas de *phishing* o de ingeniería social, trasladadas mediante campañas de correos electrónicos no deseados (*spam* – correo electrónico tradicional) e, incluso, mensajería instantánea (*spim*- WhatsApp, Telegram, etc.). Y no debemos olvidar las técnicas de *smishing* (*spam* mediante mensaje de texto SMS), mensajes que nuevamente parecen emerger de sus cenizas.

"La falta de cultura de ciberseguridad convierte a los trabajadores en una puerta abierta para los ciberdelincuentes"

Este año, muchos de estos mensajes fraudulentos de *spam, spim* o *smishing*, llevarán como título "MUNDIAL DE RUSIA". Al ser un acontecimiento deportivo a nivel mundial (y de seguimiento masivo), se convierte en un gran atractivo para ser utilizado como temática de enganche para los internautas menos precavidos, que serán víctimas de estafas, robos de identidad (*phishing*), o infección de dispositivos.

Estas vulnerabilidades "humanas", se verán también incrementadas con la cada vez más utilizada tendencia del *Bring Your Own Device* (BYOD). Con el BYOD, las empresas permiten a sus trabajadores utilizar sus propios dispositivos portátiles en el trabajo, teniendo también la posibilidad de conectarse a la red y recursos corporativos desde fuera de la empresa. Esta tendencia se convierte en peligrosa desde el momento en que la política de seguridad, en la utilización del BYOD, sea inadecuada o inexistente. La seguridad corporativa de la red de empresa (y, por consiguiente, la información confidencial o privada de la compañía) puede estar expuesta por la simple pérdida o sustracción de un dispositivo personal carente de medidas de protección y seguridad adecuadas (cifrado, acceso al borrado remoto, etc.).

Entre los objetivos principales de los ciberdelincuentes para este 2018 se encontrarán, posiblemente, las infraestructuras críticas; los cada vez más presentes dispositivos con Internet de las Cosas (en inglés, Internet of Things, abreviado IoT); y, sin lugar a duda, los dispositivos móviles, que son los nuevos ordenadores de bolsillo.

En cuanto a esta forma de conexión "de las cosas" nos enfrentamos a una inexistente seguridad por defecto (o de origen por parte los fabricantes) y totalmente inexistente por parte del usuario. Por este motivo, durante el pasado año, la falta de seguridad en estos dispositivos propició la aparición de "redes zombi" (BOTNET) compuestas por dispositivos IoT, controlados en remoto por ciberdelincuentes, con la capacidad de llegar a colapsar servicios mediante ataques masivos de Denegación de Servicios (DDoS).

ALERTA DE
SEGURIDAD

Actualmente el IoT va mucho más allá de un electrodoméstico conectado que nos hará la vida más fácil. Hoy en día, disponemos de implantes médicos, como un marca pasos, conectado y controlado desde Internet; de vehículos controlados desde la red; e, incluso, de vehículos creados para la conducción sin participación humana. Por este motivo, las posibilidades de ataque con las que cuenta un ciberdelincuente se pueden multiplicar por mil (y cada vez tiene una mayor "oferta" para lanzar sus ataques).

Para evitar la problemática que hoy os hemos detallado, nos reiteramos una vez más en la actualización, tanto de los dispositivos como del distinto *software* utilizado (no hay que confiar en el simple uso de un antivirus, puesto que no nos garantizará el 100% nuestra seguridad ante una infección).

Realizar copias de seguridad, de forma periódica, debería estar entre nuestras prioridades a la hora de pensar en la recuperación de nuestra información ante cualquier tipo de eventualidad que origine su pérdida (especialmente cuando hablamos de *ransomware*).

Si eres responsable de una empresa, una recomendación: conciénciate en materia de ciberseguridad e implementa en tu empresa las medidas tecnológicas adecuadas para que tu pyme disfrute de "aceptable salud digital". Recuerda que tus empleados son el eslabón más débil de la cadena de ciberseguridad y que está en tu mano reforzar ese eslabón, implementando también actividades en materia de ciberseguridad, para lograr concienciar y formar a tus empleados de todos los niveles. El objetivo es que hagan un uso seguro de la tecnología que utilizan y sean conocedores de las políticas de seguridad que se acuerden, tanto dentro como fuera del ámbito empresarial.

Y, cuando les aparezca el mensaje "Instala… Descarga… Ejecuta… Usuario/Contraseña…", se les encienda la bombilla roja con el mensaje: "En Internet nosotros somos nuestra mayor vulnerabilidad, pero también somos nuestro mejor antivirus."

Nos vemos en la red.

Ángel-Pablo Avilés – "Angelucho"

Editor de *El Blog de Angelucho*

Ciberseguridad pasada
deparará

La historia nos ha demostrado que aquellos que no aprenden de ella están condenados a repetirla. Otra máxima que también es cierta es que, para predecir el futuro, simplemente hay que mirar el pasado. Partiendo de ambos pensamientos, es importante hacer un análisis rápido del estado actual de la ciberseguridad, qué es lo que ya podemos atisbar en el horizonte y cómo pueden las organizaciones proteger sus redes frente a lo que se avecina.

Las medianas empresas y su disyuntiva con la *cloud*

Las medianas empresas se encuentran, en determinados momentos, entre Escila y Caribdis con respecto a la nube. Por un lado, ofrece enormes beneficios para el negocio, pero también conlleva importantes riesgos. Los estudios demuestran que las empresas medianas han registrado las tasas más altas de infección por *botnets*, lo que revela que estas firmas tienen más problemas de seguridad de los que les corresponden. Es posible que los ciberdelincuentes consideren a las organizaciones medianas como un "objetivo perfecto" ya que no suelen tener el mismo nivel de recursos y tecnologías de seguridad que las grandes empresas, pero sí disponen de activos de datos valiosos. Al mismo tiempo, la superficie de ataque para las empresas medianas está creciendo a un ritmo más rápido que la de las empresas más grandes, debido a que las tasas de adopción de la nube también son más rápidas.

La nube continúa siendo un punto vulnerable porque sus servicios están centralizados. Sus redes complejas e hiperconectadas pueden suponer un punto de error. En lugar de piratear una docena de empresas, los delincuentes pueden *hackear* un único entorno de nube y potencialmente tener acceso a los datos de docenas o cientos de organizaciones, o incluso acabar con un servicio concreto con un solo ataque. Este es el escenario que permitió la extensión del *botnet* Mirai a través del proveedor de hosting DNS.

El éxito de los *botnets* de IoT como Mirai, Hajime y Reaper confirma que los cibercriminales seguirán utilizando inteligencia artificial (AI) para detectar una debilidad y, posteriormente, aprovecharla para paralizar un servicio (que genera millones de dólares al día para el proveedor, a la vez que interrumpe el servicio para potencialmente cientos o miles de negocios y decenas de miles o millones de sus clientes).

La problemática de los *botnets*

En el último trimestre, muchas empresas fueron infectadas por el mismo *botnet* varias veces. Esto podría deberse a una de estas dos razones. O bien la organización no entendió completamente el alcance total de la brecha y la *botnet* quedó en estado latente para atacar de nuevo una vez se reanudaran las operaciones normales, o nunca encontraron la raíz del problema o "paciente cero".

A medida que los dispositivos IoT no seguros son más sofisticados y las metodologías de ataque se vuelven más inteligentes, existe el riesgo potencial de crear enjambres de dispositivos de IoT comprometidos que podrían atacar indiscriminadamente, como si de una colmena de abejas enojadas se tratara. Es muy probable que los ciberdelincuentes reemplacen las *botnets* con grupos inteligentes de dispositivos comprometidos construidos alrededor de la tecnología de enjambre para crear vectores de ataque más efectivos, que requieren una mínima supervisión mínima, o -incluso- pueden operar de forma autónoma.

Esto se convertiría en un *hivenet*, un ejército de dispositivos comprometidos, en lugar de una red de *bots*, el cual sería capaz de utilizar el autoaprendizaje para dirigir de manera efectiva los ataques a los sistemas vulnerables previamente detectados. Los *hivenets* podrá usar enjambres de dispositivos comprometidos para identificar y abordar diferentes vectores de ataque a la vez. A medida que identifica y compromete más dispositivos, el *hivenet* podría crecer exponencialmente, ampliando su capacidad para atacar simultáneamente a múltiples víctimas.

y futura, lo que nos 2018

Defensas inteligentes

Estas amenazas de seguridad requieren nuevas estrategias y tecnologías, pero sin dejar de lado la ciberseguridad tradicional. Ni el mejor equipo del planeta puede asegurar una puerta que se haya dejado abierta. Por lo tanto, el primer objetivo es identificar todos nuestros activos autorizados y no autorizados dentro de nuestro entorno. Es fundamental tener información sobre qué debemos proteger.

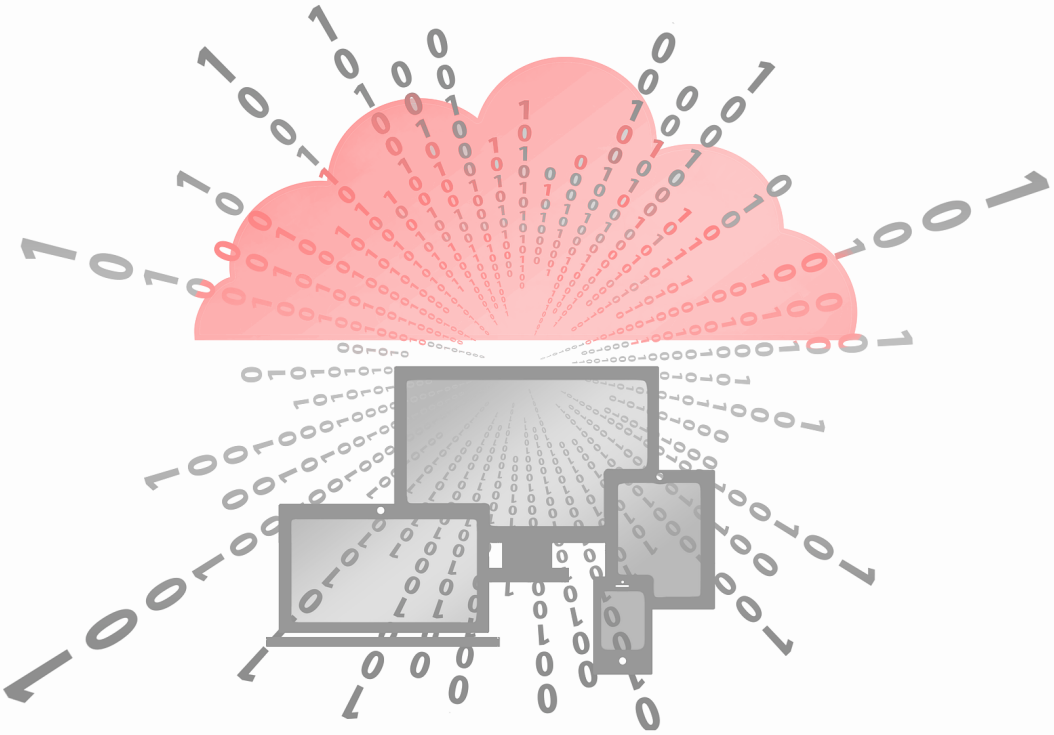
También es importante limitar los privilegios del usuario; está claro que no todos nuestros empleados necesitarán permisos de administrador. Además, se deben mantener los activos actualizados y parcheados, y limitar las aplicaciones solo a aquellas personas que lo necesiten. El uso de aplicaciones innecesarias amplía la superficie de ataque y aumenta la complejidad de proteger el entorno de red.

En cuanto a las brechas de seguridad, elaborar un plan documentado de cómo detectar, analizar, responder y recuperarse ante ellas, es determinante. Debemos asegurarnos de centrarnos en identificar correctamente el alcance completo de la violación y el análisis forense para determinar de dónde procedió la amenaza.

Hacia la seguridad integrada

Por último, la mejor defensa contra las amenazas inteligentes y automáticas de hoy en día es una estructura de seguridad integrada, colaborativa y altamente adaptable. Si podemos disponer de una arquitectura de seguridad Security Fabric, que utiliza aplicaciones de Inteligencia Artificial como el aprendizaje automático (*machine learning*), tendremos el sistema de defensa de seguridad por excelencia, y podremos sobrevivir tanto a las amenazas de este año como a las que vendrán el año que viene.

Pablo García
Senior Telco/Carrier Systems Engineer en Fortinet Iberia



La inteligenci
de p

El sector de las nuevas tecnologías se ha convertido, seguramente por haber caído en los mullidos y acogedores brazos del *marketing*, en un auténtico generador de etiquetas, tendencias y modas. Las empresas de este gremio se rigen por la innovación (es lógico) pero también por la necesidad imperiosa de vender, porque para eso desarrollan productos y servicios que generalmente mejoran la vida de todos.

Lo que ocurre es que en esa carrera constante por ser los más innovadores cada año hay una palabra, una tendencia o una categoría de producto que alguien coloca primero en el mercado y que con posterioridad el resto de fabricantes replican con ligeras modificaciones. Unos le añaden al nombre una sigla de su propia cosecha, otros tunean ligeramente el chasis del objeto en cuestión, otros se atreven con colores innovadores, pero la esencia es la misma.

Después de recorrer muchas ferias internacionales, se refuerza en mí la sensación de que el sector no para de innovar, pero siempre más pendientes de lo que hace el vecino que de las ideas propias. Un fabricante de teléfonos considera que tu móvil debe llevar dos cámaras en lugar de una, y a los pocos meses todos llevan dos cámaras. Una firma sugiere lo importante que es para el ser humano monitorizar los pasos que da cada día y medir el ritmo cardíaco de un oficinista de manera constante y en un breve lapso de tiempo, toda la competencia lanza su propia banda cuantificadora y hasta tu suegra luce una en la muñeca.

¿Son muchos de los avances sugeridos por la industria tecnológica respuestas a las necesidades de los usuarios o meros reclamos vestidos de modernidad? Me lo planteo cada vez con más frecuencia.

La palabra más repetida que he escuchado en las ruedas de prensa, presentaciones y entrevistas que he realizado durante el pasado año es "smart", en inglés que mola más que decir inteligente. Y junto a ella unas siglas (también en inglés, claro) que forman el acrónimo de moda, el IoT.

No seré yo, ni por profesión ni por convicción, quien no esté encantado con el desarrollo del internet de las cosas. Me gusta, creo en ello y estoy seguro de que una vida conectada puede ser una vida mejor para todos.

a del secador
pelo

Lo que ocurre es que un término, a fuerza de repetirse y por el simple hecho de ir en letras con gran tipografía en la caja de un producto, puede perder la esencia de su valor original. Tan cierto es que la miniaturización de los chips y los transistores y los esfuerzos de los técnicos en los laboratorios han conseguido que cualquier cosa pueda conectarse a la red, como que, seguramente, no todo debe estar conectado por obligación.

Un televisor conectado permite acceder a contenidos que no podría ver de otra forma, un coche conectado puede ser más seguro y puede buscar en tiempo real los trayectos más eficientes, un termostato conectado puede permitirme manejar la calefacción de casa desde el móvil y ahorrar energía,... pero, ¿un secador de pelo, un aspirador o un microondas doméstico deben estar conectados a Internet?

El otro día, antes de ver una película en el cine, durante el cuartito de hora de publicidad que pagas con la entrada a precio de oro, vi el anuncio de un secador de pelo que sus creadores definían como "inteligente" y "conectado". No dudo que fuera un ingenio técnico sobresaliente y que te dejara la melena con un moldeado increíble, pero si dudo de la utilidad de que mi secador se conecte a la red. Puede ser innovador, moderno, espectacular... pero no lo veo necesario.

El hecho de que un objeto cotidiano esté conectado sirve también para generar datos (útiles o no para terceros, pero seguramente tan personales como hábitos de uso que no queremos revelar) y lo convierte también en algo susceptible de ser atacado desde la red. Porque existe otra cara menos amable del internet de las cosas que debería, al menos, llevarnos a la reflexión de si merece la pena que todo se conecte a la red porque lo diga la moda. Por cierto, no me he comprado el secador inteligente, pero sí una afeitadora conectada que me envía una alerta al móvil cuando cree que ya ha pasado demasiado tiempo sin que me afeite y me ha cambiado la vida, no se cómo lo hacía antes, si alguien quiere, le doy la referencia.

Manuel Martínez

Director del programa 5.0 de Radio Nacional de España

Tecnología IRM y cumplimiento GDPR

El Reglamento General de Protección de Datos, más conocido por sus siglas en inglés GDPR, comenzará a aplicarse el 25 de mayo de 2018. Hasta ese momento las empresas y organizaciones que tratan datos deben establecer medidas técnicas y organizativas que les permitan el cumplimiento en el momento en que el Reglamento sea aplicable.

El cumplimiento del GDPR requiere una fuerte **implicación de la alta dirección** de las empresas para **impulsar políticas y procesos de seguridad de la información**, como son la realización de evaluaciones de impacto, la certificación de procesos, y la clasificación de la seguridad de la información. La implantación de estas políticas, y los cambios necesarios en los procesos de tratamiento de la información, debe ir acompañada de las **herramientas necesarias que faciliten su adopción** a los empleados responsables de generar y tratar con la información sujeta al cumplimiento normativo. Afortunadamente, y a diferencia de lo que ocurría hace unos años, hoy estos empleados están concienciados respecto a las amenazas sobre la seguridad de la información, y sobre el impacto que una fuga de información puede tener, tanto a nivel de reputación de marca como de sanciones por incumplimiento normativo.

El GDPR no específica que herramientas deben utilizarse para el cumplimiento de la norma, sin embargo, en su artículo 25 sí especifica que las empresas deberán establecer las medidas técnicas necesarias para la **protección de datos desde el diseño y por defecto**.

Entre estas medidas técnicas tres de las más relevantes son las funciones fundamentales de la tecnología IRM (*Information Rights Management*):

- Cifrado de la información
- Gestión de permisos y control de acceso
- Registro de la actividad sobre la información

Estas tres medidas técnicas repercuten directamente en mitigar los riesgos identificados en las evaluaciones de impacto, así como en facilitar la auditoría y certificación de los procesos.

Hay que destacar que, si bien el GDPR se refiere explícitamente a la protección de datos estructurados (como son las bases de datos), la información estructurada puede estar constituida por unidades de información no estructurada como pueden ser documentos de identidad escaneados, alocuciones, vídeos, etc. Además, como parte del tratamiento de la información es frecuente que se generen informes y hojas de cálculo a partir de la información estructurada.

Por tanto, debemos considerar varios escenarios en la aplicación de medidas técnicas como el cifrado, la gestión de accesos y el registro de actividad:

1. Previamente al almacenamiento estructurado de los datos.
2. En el acceso a la información estructurada.
3. Al extraer información consolidada para su tratamiento.

Previamente al almacenamiento estructurado, y en el contexto de la protección de datos desde el diseño y por defecto que nos exige el reglamento, debemos tener bien definidos los procesos de captación y almacenamiento seguro de la información. Si la información la va a almacenar un **sistema de gestión de base de datos (SGBD)**, deberemos ver qué medidas de seguridad podemos implantar en dicho sistema, que típicamente nos podrá aportar las medidas técnicas necesarias.

“El cumplimiento de GDPR requiere la involucración de la alta dirección de las empresas para impulsar políticas de seguridad de la información y transformación de procesos, que deben ir acompañados de herramientas que completen el conjunto de medidas técnicas y organizativas que posibiliten el cumplimiento”.

Pero si parte de la información va a almacenarse fuera del control del SGBD, probablemente la mejor aproximación para garantizar cifrado, gestión de permisos y control de acceso, y registro del uso de la información, sea implantar una **solución IRM**. En esta fase, además, las **herramientas de clasificación de la seguridad de la información** toman especial relevancia.

Así cuando accedemos a la información ya estructurada, dependiendo de la naturaleza de los datos tendremos diferentes mecanismos de control y protección, bien proporcionados por el SGBD bien por el IRM.

Finalmente, cuando extraemos información consolidada para su tratamiento, es frecuente que manejemos los datos ya fuera del control del SGBD, por lo que en esta fase el IRM toma especial relevancia, ya que facilita el cumplimiento de los requisitos que el GDPR impone explícitamente al responsable o el encargado del tratamiento:

- Mantener registro de las actividades de tratamiento de los datos.
- Implantar medidas técnicas como el cifrado para mitigar riesgos.

Complementando estos dos requisitos que impone el reglamento, un IRM además nos garantiza que solo las personas autorizadas para ello podrán acceder al contenido de la información, independientemente de dónde esté el archivo. Esto cobra especial importancia en esta fase ya que es habitual que el tratamiento de los datos esté externalizado a empresas proveedoras de servicios, que consumirán la información fuera del perímetro más controlado de nuestra empresa. En este contexto, es importante recordar que tanto el propietario de los datos, como los encargados de su tratamiento, tienen responsabilidad directa sobre la seguridad de dicha información y del cumplimiento del GDPR.

En resumen, el cumplimiento del GDPR requiere la involucración de la alta dirección de las empresas para impulsar políticas de seguridad de la información y transformación de procesos, que deben ir acompañados de herramientas que completen el conjunto de medidas técnicas y organizativas que posibiliten el cumplimiento. Entre estas herramientas, el IRM es una pieza fundamental especialmente para la protección de información que no se almacena directamente en base de datos, y, sobre todo, para permitir el tratamiento de los datos de forma segura y con la trazabilidad requerida. Dentro de este tipo de tecnologías Prot-On es una solución IRM que además aporta funcionalidades de clasificación de la información, prevención de fuga de datos y control de versiones e integridad de los archivos protegidos.

Óscar Maire-Richard
Prot-On Founder & Product Manager

Prot-On
Protect what you share

La inteligencia artificial y el *machine learning* en seguridad informática

Aunque en los últimos dos o tres años se ha hablado mucho de estos dos conceptos, en realidad la investigación y el uso de la inteligencia artificial (AI por sus siglas en inglés) y el *machine learning* (ML) es anterior al mismo Internet. Estas tecnologías han tenido varios picos de interés e inversión. El primero se produjo a finales de los años 50. Pero, también produjeron un gran interés a finales de los 80, los últimos años de los 90 y, sobre todo, después de 2007.

La inteligencia artificial es un concepto muy amplio, que incluye cualquier forma de inteligencia que no sea humana y que esté relacionada con las máquinas. Durante años, la AI se ha organizado en varios campos de trabajo: pensamiento, conocimiento, aprendizaje, planificación, reconocimiento del lenguaje, percepción, interacción y la posibilidad de llevar a cabo acciones. El aprendizaje automático (ML) es solo un campo de la inteligencia artificial, que se refiere a la posibilidad de las máquinas de desarrollar algoritmos, clasificar y extraer inteligencia de grandes bases de datos, sin ser programadas previamente y específicamente para unos resultados concretos.

La inteligencia artificial y el aprendizaje automático se han usado para conseguir progresos importantes en varios ámbitos. Últimamente, debido a la gran cantidad de información que estamos generando, con tecnologías cada vez más potentes, el IoT e Internet, se ha incrementado drásticamente el uso de la AI y ML para trabajar en el *big data*, extraer inteligencia y emprender acciones en función de estas conclusiones.

El uso de la inteligencia artificial y el *machine learning* en seguridad

Con la avalancha de los ciberataques y el tsunami del *malware* (más de 500.000 nuevas variantes aparecen cada día), el hecho de usar la inteligencia artificial para hacer frente a estos fenómenos era una evolución natural. La automatización del *malware* fue probablemente el factor decisivo que forzó el empleo del aprendizaje automático en la clasificación, prevención y detección del *malware*, y las acciones para solucionarlo. Y la industria de la seguridad informática no ha tardado en investigar, emplear y promocionar el uso del *machine learning* como respuesta a los retos actuales (y posiblemente futuros).

Pero, aunque es verdad que todos los coches tienen cuatro ruedas, no se puede decir que todos son iguales. Hay mucho ruido en el mercado de la seguridad acerca del *machine learning* (y casi todas las marcas importantes tienen un proyecto y una solución basada en ello), pero la diversidad es grande. Esto hace que la toma de decisiones sea más difícil para los potenciales clientes. Nuestra intención es aportar un poco más de luz en este proceso: explicaremos cómo funcionan estas tecnologías, qué se puede esperar de ellas y cuáles serían los posibles criterios de diferenciación.

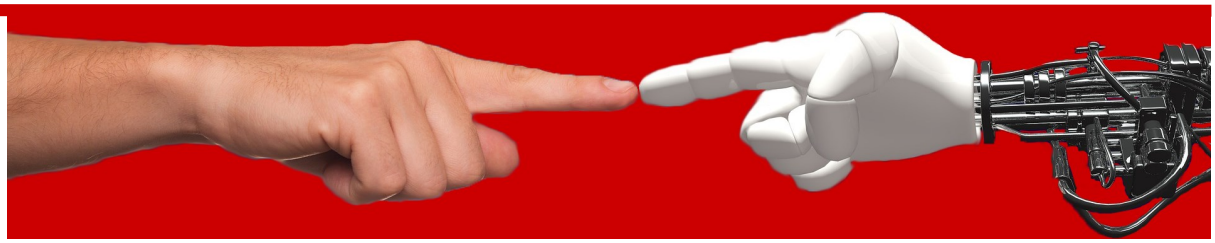
Para aprender, cualquier módulo de *machine learning* necesita dos cosas fundamentales:

- Grandes bases de datos (cuanto más grandes, mayor precisión).

- Tiempo para aprender y entrenarse. Esto se traduce en ciclos de investigación y desarrollo de algoritmos, tanto de representación como de interpretación de los datos.

La inteligencia artificial ha intentado imitar el modo de pensamiento humano, pero se ha encontrado con retos importantes. Por un lado, la simplificación (los humanos simplificamos la representación de los conceptos para poder extraer conclusiones aplicables), lo que conlleva el riesgo de pasar por encima de algunos aspectos importantes. Y, por otro lado, los "atajos" que usamos debido a nuestra intuición (estos atajos, con más o menos precisión, nos ayudan a ser rápidos en la toma de decisiones, sin hacer el análisis de todos los datos disponibles), con el riesgo de tomar decisiones equivocadas.

Cuando aplicamos el aprendizaje automático al mundo de la seguridad informática, estos retos toman mucha relevancia: si simplificamos se nos pueden escapar eventos de seguridad importantes o los mismos virus, y si "tomamos atajos" podemos llegar a muchas conclusiones equivocadas, como los falsos positivos.



Por esto son importantes tanto el tamaño de las bases de datos, como la "experiencia" adquirida por el ML en hacer (mejor o peor) las siguientes tareas:

- colección y normalización de los datos;

- análisis y extracción de las características comunes y de las diferencias relevantes;

- aprendizaje y auto-perfeccionamiento de los propios algoritmos;

- clasificación de los elementos analizados (ficheros, procesos, técnicas de ataque, código) en benignos y malignos.

En la actualidad, varios fabricantes (Bitdefender incluido) están proponiendo tecnologías de nueva generación bastante avanzadas y "entrenadas". En Bitdefender nos enorgullecemos de haber anticipado esa necesidad hace más de 8 años, llegando a desarrollar una arquitectura innovadora que aprende de más de 12 mil millones de eventos al año. En este momento, usamos el *machine learning* a nivel del *threat intelligence* global (el cerebro en el *cloud*, que potencia nuestras soluciones) y a nivel local (aprendiendo tanto de los procesos y comportamientos legítimos de uso, como de las anomalías y excepciones).

Además, hemos implementado varios mecanismos de ajuste y corrección: a través de modelos estadísticos y probabilísticos, la predicción de tendencias y la validación de los resultados contra la misma base de datos en varios niveles de aprendizaje (lo que incrementa la precisión y reduce el nivel de falsos positivos). Algunas voces de la industria llaman este tipo de tecnología "*Deep Learning*" y la consideran el futuro. En el caso de Bitdefender, este proceso se sustenta en varias patentes registradas, y es algo muy similar al comportamiento humano: aprendemos de las interacciones, de los errores y de las experiencias positivas.

Los resultados conseguidos en los últimos años nos han dado muchos motivos para creer que estamos en el buen camino: WannaCry, NotPetya, BadRabbit y todo el *ransomware* moderno no han constituido una amenaza real para nuestros clientes; nuestro *machine learning* ha sido capaz de detenerlos en la fase de pre ejecución.

Pero, a pesar del uso de la inteligencia artificial en seguridad informática, sigue habiendo vida para los "malos". Podemos anticipar (porque, de hecho, ya se han empezado a usar) un crecimiento de técnicas de evasión especialmente diseñadas contra estas tecnologías. Hablamos de un incremento de la ofuscación del código maligno; de cambios en los *packers*; de un aumento de la fragmentación de los ataques; y de la intención de usar herramientas populares entre los usuarios, que tengan posibilidad de ser *whitelisted* (lo hemos visto ya con Bad Rabbit). También se usa más la técnica de esconder el código detrás de objetos web (en sitios populares) o de extensiones de navegador.

Somos conscientes de que el uso de las tecnologías de AI y ML no es la respuesta definitiva a los problemas. Nosotros nos hemos diferenciado por el uso de una arquitectura adaptativa y multinivel (o multicapa), que pone frente a los ciberdelincuentes varios tipos de barreras, obstáculos y "señuelos" durante el ciclo de vida de un ataque, tanto en la fase de pre-ejecución (con las tecnologías predictivas y de detección correlativa y la inteligencia colectiva en la nube) como en la fase de post-ejecución (con nuestro EDR, la inspección de procesos y las tecnologías de solución). Y, aunque sabemos que contamos con una propuesta compleja y completa, que cubre todo tipo de *endpoints* y *data centers*, somos conscientes de que el éxito pasa por mantener la vigilancia y estar siempre un paso por delante de los atacantes.

En conclusión, podemos decir que la inteligencia artificial ayuda mucho, pero no es la respuesta definitiva. Tenemos que entender los fallos y preparar controles compensatorios para mitigar los riesgos.

Horatiu Bandoiu,
ISO 27001 LA
Channel Marketing Manager de Bitdefender

Bitdefender

Sanción a Facebook: LOPD vs. RGPD

Después de los cambios que llevó a cabo Facebook en sus términos y condiciones de uso en el año 2015, la Agencia Española de Protección de Datos (junto con las autoridades de Protección de Datos de Bélgica, Francia, Alemania y Países Bajos) llevó a cabo una investigación que se saldó con una sanción de 1.200.000 euros al gigante americano. Se acusa a la red social de incurrir en dos infracciones graves y una muy grave de la Ley Orgánica de Protección de Datos y, por ello, se le imponen 300.000 de sanción por cada una de las infracciones graves y 600.000 por la considerada muy grave.

En la investigación se analizó si los tratamientos de datos realizados por Facebook se adecuaban a la normativa. **La AEPD comprobó que se estaban recabando datos sobre ideología, sexo, creencias religiosas o navegación, sin informar claramente al usuario del uso y finalidad que se da a esa información.** De hecho, se ha demostrado que Facebook trató datos especialmente protegidos de los usuarios con, entre otros, fines publicitarios y sin el consentimiento expreso que exige la normativa (esto supone una infracción muy grave de la LOPD).

En cuanto a las infracciones graves, en primer lugar, la Agencia ha estimado que Facebook no obtiene correctamente el consentimiento de sus usuarios (tampoco de aquellos que no son usuarios –y cuyos datos también trata–). Los motivos son los siguientes:

- **No se informa a los usuarios de forma clara y exhaustiva sobre los datos que se recopilan y el tratamiento que se hace de ellos.** Se recogen datos, procedentes de la actividad que los usuarios llevan a cabo en la red social y en sitios de terceros, sin indicar debidamente la información que se está recabando, ni la finalidad con la que se va a utilizar.
- **Los usuarios no son conscientes de que se trata su información mediante el uso de cookies, cuando navegan en páginas que no son de Facebook y que contienen el botón "Me gusta".** También pasa esto con internautas que ni siquiera son miembros de la red social, pero han visitado alguna vez sus páginas; y cuando aquellos que sí están registrados navegan en páginas de terceros (aunque no hayan iniciado sesión en Facebook).

LOPD	
Grave 300.000€	Tratar datos de carácter perso sentimiento de las personas c mismo sea nec
Grave 300.000€	Tratar datos de carácter perso mente con conculcación de tías establecidos, puesto que de los usuarios no son cancelo cuando han dejado de ser ú por el que fueron recogidos ni plícitamente solicitó su
Muy grave 600.000€	Tratamiento de datos especial fines de publicidad, entre otro sentimiento expreso d

* Del volumen de negocio total anua

- **La política de privacidad de Facebook contiene expresiones genéricas y poco claras y, además, obliga a pinchar en muchos enlaces para conocerla completa.** Esto provoca que un usuario de la red social, con un conocimiento medio de las nuevas tecnologías, no sea consciente de la recogida de datos, su uso, almacenamiento o tratamiento. Pero, además, **los internautas que no están registrados ni siquiera saben que Facebook está almacenando sus datos de navegación**.

La segunda infracción grave se impone porque **la AEPD considera que los datos personales de los usuarios no se eliminan acorde a las exigencias de la Ley Orgánica de Protección de Datos**. En este sentido, la Agencia ha constatado que **la red social no elimina la información que obtiene a partir de los hábitos de navegación de los usuarios** (la guarda y la reutiliza después, asociada al mismo usuario). Además, se ha demostrado que, cuando un miembro de Facebook elimina su cuenta y solicita el borrado de información, la red social recoge y trata información -durante casi año y medio- a través de una *cookie* de la cuenta que se ha eliminado.

La pregunta es: si esto hubiese ocurrido después del 25 de mayo de este año, cuando sea de obligado cumplimiento el nuevo Reglamento General de Protección de Datos, ¿a qué multas se enfrentaría Facebook? La siguiente tabla responde a esa cuestión:

RGPD	
nal sin recabar el con- afectadas, cuando el esario.	**10.000.000 € como máximo o 2%* (mayor cuantía)** **Art. 8 y 83.4.a)**
onal o usarlos posterior- los principios y garan- los datos personales ados en su totalidad ni tiles para el propósito cuando el usuario ex- u eliminación.	**20.000.000 € como máximo o 4%* (mayor cuantía)** **Art. 6 y 83.5.a) y b)**
mente protegidos con os, sin obtener el con- e los usuarios.	**20.000.000 € como máximo o 4%* (mayor cuantía)** **Art. 9 y 83.5.a)**

l global del ejercicio financiero anterior.

Secure&IT

www.secureit.es