CIBERSEGURIDAD : claves que deben aplicar los usuarios de internet para protegerse de ciberdelincuentes

CHEMA ALONSO | JOSEP ALBORS | MIRIAM GARCÍA
JESÚS RODRÍGUEZ | VICTOR MUNDILLA | MIGUEL GARRIDO
JUAN ANTONIO CALLES | EDUARDO SÁNCHEZ

AGRADECIMIENTOS

Aprovechamos este espacio para reconocer la participación de 7 profesionales expertos en seguridad informática quienes, compartiendo nuestra filosofía y objetivos, decidieron aportarnos valiosos contenidos que hemos recopilado para presentaros en este eBook al alcance de todos. El merecido agradecimiento a:

- **Josep Albors** - Communication Officer - Reserch & Awarenes Manager en ESET
- Miriam García López – Abogada del área de Ciberderecho de ECIX GROUP
- Jesús Rodríguez - CEO de Realsec
- Chema Alonso - CDO (Chief Data Officer) de Telefónica
- Victor Mundila - Cibersecurity Product Manager en ElevenPaths
- Miguel Garrido - SOC (Security Operation Center) en Prosegur
- Juan Antonio Calles - Cyber Security Senior Manager en KPMG España
- Eduardo Sánchez – Director de Marketing de RegaloOriginal.com

Sin todos ellos, este eBook no hubiese sido posible. ¡Muchas gracias!

ÍNDICE

INTRODUCCIÓN

En la actualidad la ciber-seguridad, también llamada seguridad en internet, va más allá de la informática y se ha convertido en el factor clave del empoderamiento de la Transformación Digital. Nuestro reto no es únicamente encargamos de asegurar la protección del mercado y las empresas, sino también el de los usuarios.

En este sentido, ASNEF PROTECCIÓN ha evolucionado convirtiéndose no sólo en la Asociación Nacional de Establecimientos Financieros de Crédito, sino que a su vez en un medio que promueve el freno del uso fraudulento por terceros de los datos personales de personas físicas y jurídicas de todo tipo de sector en perjuicio de su entidad, solvencia y patrimonio económico. Esto último gracias a nuestro producto: Fichero ASNEF PROTECCIÓN.

A través de este eBook gratuito, tenemos la intención de continuar promoviendo el debate, estudiando y evangelizando las inquietudes y retos de la ciberseguridad en función a las necesidades de nuestros asociados (empresas y personas particulares).

En dos capítulos, compartiremos las contribuciones de los influencers más importantes de la ciberseguridad que comparten nuestra filosofía y objetivos.

En el primer capítulo, Josep Albors nos contará cómo el Internet de las cosas viene revolucionado los paradigmas de los límites de la digitalización y pone en peligro la seguridad de hogares y hasta ciudades enteras. Y Miriam

García nos explica cómo nos hacemos cada vez más vulnerables, cuanto más conectamos nuestros dispositivos y nuestras vidas a la red.

En el segundo capítulo detallaremos medidas de seguridad sugeridas por expertos, como Jesús Rodríguez, Chema Alonso, Víctor Mundilla, Miguel Garrido, Juan Antonio Calles y Eduardo Sánchez, quienes explicarán de manera muy pedagógica el uso de instrumentos y buenas prácticas para proteger vuestras empresas y hogares de ciberdelincuentes.

CAPÍTULO 1

Los peligros de la evolución de la digitalización

Internet de las cosas

Cuando hablamos del Internet de las cosas a mucha gente se le llena la boca hablando de sus bondades y de los beneficios que traen consigo todos esos dispositivos conectados a Internet y/o entre sí. En los últimos años estamos viendo un incremento constante de estos dispositivos, algunos con funcionalidades más que dudosas pero que no hacen sino engrosar la lista de dispositivos a los que, solamente conectándolos a Internet, alguien ya pensó que podíamos considerarlos inteligentes.

Pero la historia del Internet de las cosas es larga y, a pesar de que podemos remontarnos varios años, vamos a centrarnos a partir de cuándo los usuarios empezaron a hacer un uso masivo de estos dispositivos. Tal vez, el primer dispositivo conectado a Internet que muchos usuarios conocieron y que no se trataba de un ordenador fue precisamente el encargado de darnos acceso a esta red.

Dispositivos cotidianos en la sala de estar

Estamos hablando, como no, del modem/router que el técnico de la operadora nos dejaba instalando y funcionando (aunque los más manitas nos lo configurábamos nosotros mismos) y que mientras funcionase de forma correcta, no había nada de lo que preocuparse. Pero aun a día de hoy, la gran mayoría de usuarios no se preocupa lo suficiente de ese dispositivo. Si acaso, alguno le cambia la contraseña por defecto de la WiFi pero cuando pasamos a preguntar por la actualización del firmware obtenemos el silencio como respuesta.

Y es que la máxima de "si funciona, no lo toques" sigue instaurada con plena vigencia en el pensamiento colectivo y más si hablamos de un dispositivo que, si deja de funcionar, tiene como consecuencia la pérdida del acceso a Internet. Así pues, no es de extrañar que otros dispositivos que aparecerían posteriormente como decodificadores para ver la televisión por

satélite/cable siguieran el mismo camino y se quedasen inmutables tal y como llegaron el primer día a nuestra casa.

Otro dispositivo que se ha popularizado en los últimos años han sido las cámaras IP de vigilancia. Siendo muy fáciles de configurar y permitiendo observar lo que ocurre dentro de su alcance ya sea en un circuito cerrado o a través de nuestro móvil, son ahora un dispositivo muy utilizado no solo en comercios sino también por padres preocupados por el sueño de sus retoños.

Pero estos tres dispositivos incorporan un pequeño ordenador en su interior del que nos deberíamos preocupar. Como mínimo deberíamos de cambiar las contraseñas que los fabricantes ponen por defecto y que se pueden sacar fácilmente, y preocuparnos de actualizar el sistema que gobierna ese dispositivo en el caso de que el fabricante saque una actualización.

En caso de no preocuparse por la seguridad de estos dispositivos nos podemos encontrar con que un atacante ha incorporado la señal de nuestra cámara IP a su colección y puede ver nuestra vida en directo como si de un reality show se tratase, peor aún si se ha hecho con el control de nuestro router, puesto que podrá obtener toda la información que pase a través de él y que incluye datos confidenciales como contraseñas, números de tarjeta de crédito o información confidencial.

Pero el Internet de las cosas no se quedó solo en esos dispositivos. Ha ido expandiendo sus tentáculos y, por ejemplo, a día de hoy ya es realmente difícil ir a comprar un televisor que no tenga la etiqueta Smart en el nombre. Estos dispositivos distan mucho de sus antecesores de tubo puesto que ya son más ordenadores que televisores convencionales y muchas de ellas ya permiten navegar, acceder a redes sociales o ver vídeo bajo demanda usando solo un dispositivo.

Teniendo un dispositivo así no es de extrañar que los delincuentes estén empezando a hacer sus pinitos en esto de controlar remotamente las televisiones, y no solamente para espiarnos a través de las cámaras que incorporan muchas de ellas. Ya se han dado casos de ransomware en algunos modelos de televisores y es que no hay nada peor que estar viendo tu programa favorito y que aparezca un mensaje en el televisor exigiendo un rescate si queremos volver a utilizarlo.

Cocinando los ataques AL iot

Del salón pasamos a otro espacio que ha visto como el desarrollo del Internet de las cosas ha afectado a muchos de los electrodomésticos que usamos en ese espacio. Uno de los primeros fueron las cafeteras, probablemente debido a que es el objeto más preciado cuando nos

levantamos muertos de sueño. Que mejor que tener un café calentito recién hecho sin tener siquiera que preocuparnos por encenderla, todo gracias a que la hemos programado mediante el móvil la noche anterior.

Pero claro, para que esto sea posible, la cafetera tiene que conectarse a alguna red y que mejor red que nuestra WiFi doméstica con nuestra contraseña super segura. Segura hasta que alguien se conecta directamente a la cafetera por bluetooth y averigua que guarda la contraseña de nuestra WiFi sin ningún tipo de cifrado y que, por ende, puede obtenerla y acceder a nuestra red doméstica para realizar todo tipo de maldades.

Otro electrodoméstico que encontramos en la cocina que ha sufrido una importante transformación en los últimos años es la nevera. Al principio alguien pensó que acoplar un pequeño monitor que mostrase noticias y datos del tiempo podría sernos útil mientras nos preparamos un vaso de leche con galletas o nos tomamos una cerveza bien fría. Sin embargo, la cosa ha ido evolucionando y ahora ya se permiten hacer pedidos al supermercado desde la propia nevera o incluso permitir que sea ella la que realice estos pedidos de forma automática cuando revise que tenemos pocas existencias de algún producto.

Pero claro, para hacer esos pedidos hace falta tener algún medio de pago almacenado en la nevera y es ahí donde comienzan los problemas. ¿De verdad le confiamos los datos de nuestra tarjeta de crédito a un

electrodoméstico? Un electrodoméstico que ya ha sido víctima de ataques y que incluso los delincuentes han utilizado para enviar spam en ocasiones anteriores.

Pero la revolución del Internet de las cosas en la cocina no se detiene ahí puesto que ya existen lavavajillas, lavadoras y secadoras "inteligentes" que incorporan muchas de las funcionalidades que acabamos de comentar.

Domótica y su seguridad

Una de las tecnologías que abrazó la interconexión de varios dispositivos desde sus orígenes es la de la domótica. Centrada en la automatización y en facilitar la gestión de varios aspectos de nuestro hogar, los avances realizados en los últimos años han conseguido que sea relativamente fácil y económicamente permisible controlar muchas de las tareas que realizamos en el hogar.

Esta implementación se está llevando a cabo tanto en entornos domésticos particulares como en varias cadenas hoteleras y, en muchos casos, permiten gestionar eficientemente todos los parámetros que hayamos estipulado desde nuestro smartphone o tableta.

Sin embargo, como suele suceder en demasiadas ocasiones, no es extraño ver sistemas domóticos en los que la seguridad es escasa o directamente

brilla por su ausencia. De esta forma, una atacante podría acceder a controlar aspectos tan cruciales como el sistema de vigilancia, las alarmas, la temperatura del aire acondicionado y el agua, las persianas, las luces o el hilo musical, por poner solo unos ejemplos.

En el caso de los fallos de seguridad aplicables a sistemas domóticos en hoteles estos podrían permitir obtener información confidencial de los huéspedes de las habitaciones, además de poderles causar otras molestias como programarle despertadores a horas intempestivas.

Jugando con fuego

La conexión de juguetes a Internet ha ido produciéndose de forma gradual, si bien catalogaremos juguetes en este punto solamente a aquellos considerados como tradicionales (principalmente muñecas, peluches y todos aquellos que no tenían un componente tecnológico en sus orígenes). A día de hoy ya no es extraño ver como fabricantes de juguetes incorporan la conexión a Internet como una característica importante y diferenciadora.

Los casos que más nos preocupan son aquellos que involucran a niños de corta edad y que, muchas veces tiene en su muñeca o peluche una especie de confidente. La posibilidad de que ese juguete no solo responda a sus preguntas, sino que sea capaz de entablar una conversación debería

preocuparnos aun sin tener en cuenta los problemas de seguridad informática existentes.

Esta comunicación no se realiza realmente con el juguete puesto que este aprovecha la red WiFi de la casa para conectarse a unos servidores gestionados por empresas que son los encargados de proporcionar esos "asistentes" de conversación. Serían algo como Siri o Cortana en los móviles, pero aplicados a la industria juguetera.

Como ya hemos visto, cualquier comunicación por WiFi es susceptible de ser interferida si no está debidamente fortificada y, siendo una de las partes un menor, deberíamos ser conscientes de los peligros que entraña una conversación con un delincuente que podría convencer al menor para que, por ejemplo, abriese la puerta de su casa o le dijese los números de la tarjeta de crédito de su padre o madre.

Coches conectados, ¿más seguros?

Además de todo lo expuesto hasta ahora, todas las mejoras electrónicas incorporadas a los automóviles desde hace décadas nos han llevado a un punto en el que se plantea seriamente el uso del coche autónomo como opción para conseguir disminuir los accidentes y convertir la conducción en

algo placentero en el que el conductor puede dedicar el tiempo del viaje a realizar otras tareas.

Buena parte de la culpa de estos logros la tienen los pequeños ordenadores que se han ido introduciendo poco a poco en los automóviles y que ahora facilitan mucho la conducción y permiten disfrutar de sistemas completos de entretenimiento. Incluso se han realizado pasos para usar nuestro smartphone como mecanismo de gestión de algunos parámetros de nuestro coche o directamente como alternativa a la llave de arranque.

Pero la incorporación de toda esta electrónica unido a la conexión de algunos modelos a redes telefónicas para poder disfrutar de un servicio de Internet para todos sus ocupantes ha supuesto también la existencia de agujeros de seguridad que podrían poner en peligro la seguridad o, como mínimo, el confort de los ocupantes.

Desde hace tiempo vienen saliendo a la luz numerosas investigaciones que muestran lo inseguro del diseño de algunos sistemas de conexión implementados por los fabricantes de vehículos. Algunos de ellos tienen incluso aplicaciones propias para smartphones que permiten modificar algunos parámetros como, por ejemplo, los valores del aire acondicionado para encontrarnos nuestro vehículo a la temperatura ideal cuando vayamos a cogerlo.

Un problema más grave es la posibilidad de controlar remotamente parámetros críticos como la conducción, los frenos o las luces. Si bien esto se creía improbable hasta hace poco, el estudio de varios investigadores ha demostrado que no solo es factible, sino que el número de coches afectados podría ser mayor del que se pensaba.

Smart cities

El siguiente paso, ya pensando en grande, es el que están realizando desde hace tiempo algunas ciudades que buscan implementar la tecnología para que les ayude a optimizar sus recursos y mejorar la vida de sus habitantes.

Sobre el papel todo es ideal, ya que, gracias a la interconexión constante entre dispositivos, los habitantes de las smartcities pueden estar informados de posibles atascos, retrasos en el transporte público, servicios básicos como la recogida de basura o incluso recibir alertas y notificaciones importantes.

Esto se ha venido realizando con mayor o menor éxito en diversas partes del mundo, existiendo ejemplos como el de la sociedad japonesa, en la que la utilización de dispositivos móviles para interactuar con información proporcionada por su ciudad o gobierno regional ha llegado hasta el nivel de avisar cuando se produce un terremoto el tiempo necesario para que los habitantes busquen refugio.

También existen ciudades como San Francisco, que anunció hace poco el lanzamiento de una nueva red inalámbrica especialmente diseñada para acoger e interactuar con todos los dispositivos del denominado Internet de las cosas. Un movimiento lógico, si pensamos que buena parte de la información relacionada con sus habitantes de la que se nutre una smartcity proviene de ese tipo de dispositivos.

El problema aparece cuando tanto los fabricantes de todo tipo de dispositivos conectados, como los que se encargan de su interacción con la smartcity, descuidan su seguridad. Para empeorar las cosas, tampoco se puede afirmar que los complejos sistemas utilizados en una ciudad para gestionar temas cruciales como el suministro eléctrico, el transporte público o la canalización de agua potable sean capaces de pasar una auditoría de seguridad estándar.

Si bien es cierto que estos sistemas se diseñaron pensando en su eficiencia y no tanto en su seguridad lógica, el panorama de riesgos ha cambiado mucho en los últimos años. Los encargados de controlar estos sistemas estarán acostumbrados a detectar averías y enviar equipos especializados a repararlas, pero no a que un atacante se infiltre en sus redes y comience a causar el caos.

En este punto, las smartcities son un objetivo perfecto para atacantes con oscuros intereses. Si hasta hace poco el control de los sistemas informáticos

que gestionan las ciudades eran, en su mayoría, sistemas aislados de las redes de comunicaciones públicas, el propio concepto de smartcity anima a que estos sistemas estén conectados a estas redes para poder recopilar la información de la que se nutren para mejorar su funcionamiento.

Y es en este punto donde aparecen los problemas de seguridad. Si la fortaleza de una cadena se basa en su eslabón más débil, la seguridad de una smartcity depende, en gran medida, de la seguridad de los dispositivos que conectemos a ella y de los sistemas utilizados para gestionarla.

Pongamos, por ejemplo, que una ciudad importante, con problemas de tráfico y contaminación, decide proponer el uso de transporte público o incluso fomentar el uso de un transporte ecológico como es la bicicleta. Para eso, se crea una serie de puntos donde los usuarios pueden alquilar temporalmente una bicicleta previo registro, el cual que se realiza online y a través de una aplicación para smartphones.

Aparentemente, todo son ventajas tanto para el ayuntamiento como para los usuarios, pero tan solo hace falta una mala implementación en el proceso de registro, un mal diseño de la aplicación móvil o utilizar un protocolo inseguro para enviar los datos para que la privacidad de miles de usuarios se vea comprometida, se puede acceder a otros servicios de la ciudad o se utilicen los puntos de recogida de bicicletas para mostrar imágenes no aptas para todos los públicos.

Este ejemplo no es algo hipotético. Ha pasado, y en España, concretamente en Madrid nada más implementar su sistema Bicimad, de alquiler de bicicletas (y no ha sido el único). Además, las posibilidades aumentan conforme se van conectando todo tipo de dispositivos como, por ejemplo, semáforos y señales de tráfico.

Varios investigadores han demostrado lo relativamente sencillo que resulta alterar el comportamiento de estos dispositivos tan críticos para el control del tráfico. Tan solo se necesita alguien con ciertos conocimientos y recursos para alterar su funcionamiento, ya sea de forma individual o para afectar a toda la red si consigue acceder al sistema que lo controla.

De hecho, el problema puede ser aún más grave si hablamos de servicios tan críticos como los de emergencias, puesto que los canales de comunicación utilizados tampoco son todo lo seguros que deberían y cuesta muy poco conseguir un dispositivo y modificarlo para escuchar e incluso emitir en sus frecuencias, siendo posible causar un caos considerable si algún atacante se lo propusiera.

Estos dos últimos ejemplos no están sacados de ninguna película de acción en las que un villano pone en peligro la vida de millones de habitantes de una ciudad controlando los sistemas que las gobiernan. Están sacados de una charla del investigador español Carlos García, ponencia que fue

presentada en la pasada edición del congreso de seguridad Navaja Negra en Albacete.

Como vemos, la idea de una ciudad inteligente y conectada es algo bueno y no dudamos en que será la tendencia a seguir por las urbes en años venideros. Sin embargo, también hemos de tener en cuenta que, a medida que se vayan conectando los sistemas que se encarguen de gestionar una smartcity, también aparecerán nuevos vectores de ataque.

Por eso mismo, es necesario que se tenga muy en cuenta todo lo relativo en seguridad a la hora de diseñar y proteger las smartcities conforme estás vayan creciendo y, ahora mismo, no estaría de más que en vez de denostar a hackers que nos ayudan a descubrir vulnerabilidades para poder solucionarlas, contemos con su ayuda para hacer de nuestras smartcities un lugar más seguro.

Josep Albors

Communication Officer and Reserch and Awarenes Manager

www.eset.es

Todo conectado, todos vulnerables

Poco a poco, el internet de las cosas – o Internet of Things (IOT)- se cuela en nuestras vidas, casi sin darnos cuenta: coches con sistemas de navegación con conexión a internet, smartphones, frigoríficos que permiten realizar la compra a través de una pantalla

interactiva incorporada, las llamadas SmartTvs o televisión inteligente, e incluso juguetes. Lo cierto es que cuanto más conectamos nuestros dispositivos y nuestras vidas a la red, más vulnerables somos frente aquellos que saben como explotar estas tecnologías a su favor en detrimento del resto de ciudadanos.

El Internet de las cosas es un concepto que nos ayuda a definir esa red de objetos cotidianos conectados a Internet y que está cambiando la relación entre los objetos y las personas. Sin embargo, ¿está la sociedad preparada para este cambio? ¿Somos los ciudadanos conscientes de todo lo que implica y conlleva esta tecnología?

Por lo general, todos somos muy conscientes de las ventajas, pero, si no valoramos los inconvenientes que pueden acarrearnos, no podremos adelantarnos a ellos. Debemos adelantarnos para tratar de mitigar y gestionar los riesgos del Internet de las cosas. Porque es posible.

En este sentido, es importante destacar que no podemos dejar que la responsabilidad sólo recaiga en la regulación llevada a cabo por los Estados, porque la tecnología siempre irá un paso por delante de la regulación. Por ello es importante que tomemos consciencia también los usuarios.

Y es que, realmente quienes tenemos la asignatura pendiente de tomarnos en serio este tema somos los ciudadanos, consumidores de esta tecnología: ¿Cuántos ciudadanos se preocupan de que esta tecnología respete sus derechos, o que se haya diseñado teniendo en cuenta la seguridad del sistema? ¿Cuántos usuarios se preguntan si sus datos estarán seguros, el propósito para el cual serán utilizados, o quienes podrán acceder en el futuro a ellos?

Todavía es habitual que el propio ciudadano sea el primero que menosprecia sus derechos con frase del tipo "no tengo nada que esconder". No es cuestión de esconder o no esconder, sino de ser conscientes de lo poderosa que es toda la información que generamos a través de los dispositivos conectados a internet, y lo fácil que será para las entidades analizarla y sacar conclusiones sobre nosotros en nuestro perjuicio.

Un wearable, como, por ejemplo, una pulsera de monitorización de actividad, puede recopilar gran cantidad de información personal, como la geolocalización de una persona en cualquier momento, sus datos de salud (como el ritmo cardiaco, la actividad física, o las medidas antropométricas), sus hábitos de vida, la cantidad de sueño, y así un largo etcétera.

Pero esto es lo que hace sólo una pulsera de monitorización de actividad, una casa con diversos dispositivos conectados a internet, como, por ejemplo,

las bombillas, el frigorífico o la televisión, puede generar información de todo tipo: desde el tiempo que se pasa en el domicilio, las franjas horarias en las que la casa permanecería deshabitada, hasta el tipo de alimentación que se lleva, el tipo de productos que se consumen, o las marcas que más se compran.

Lo anterior implica una pérdida o debilitación de los derechos a la intimidad y privacidad a favor de terceras entidades (empresas, entidades públicas, Estados...), que no siempre son conocidas por el usuario titular de esos derechos, ni éste conoce la finalidad real con la que se tratará su información.

Además, podría darse el supuesto que dicha información llegara a manos de delincuentes, -ya fuera porque la información se ha tratado sin diligencia o por la existencia de un fallo de seguridad en el sistema-, en cuyo caso, las implicaciones para nuestros derechos podrían llegar mucho más allá, pudiendo suponer un peligro incluso para nuestra integridad física –por ejemplo, si dicha información permite la monitorización y geolocalización, y se utiliza dicha información para atentar contra la vida de una persona-.

A nivel regulatorio, los Estados u organismos internacionales podrán establecer políticas de mínimos o estándares –normas no obligatorias-; pero

no podrán evitar con ellas que el usuario voluntariamente acepte determinados términos contractuales que debiliten sus derechos– como ocurre actualmente cuando se aceptan los términos y condiciones de una APP o un servicio de suscripción por internet-.

En cualquier caso, dos de los aspectos que sí deberían de ser reforzados del internet de las cosas son la seguridad del sistema y los derechos de los ciudadanos, y en especial, y como se ha puesto ya de relevancia, la privacidad.

En la actualidad, la mayor parte de las empresas que lanzan este tipo de dispositivos conectados a internet no apuestan por la seguridad como uno de los aspectos clave. Ello se puede deber a diversas razones: elevación de los costes de producción, se alarga el tiempo de puesta a disposición del dispositivo al mercado, la seguridad puede implicar en muchas ocasiones un sacrificio en la usabilidad...; pero la razón más importante, probablemente sea que el usuario, consumidor final, no da importancia a este aspecto, primando por encima de ésta la innovación o la tecnología utilizada.

En cuanto a la protección de los derechos de los ciudadanos, es preferible hablar de derechos en general, que centrarnos tan sólo en la privacidad o la intimidad. En un futuro no muy lejano, como ya se ha indicado, la utilización

de estos dispositivos podrá afectar a otros tipos de derechos como la integridad física de los ciudadanos, o la inviolabilidad de nuestros domicilios.

El problema no está en utilizar dispositivos conectados a internet, sino en cómo de seguro es el sistema y cómo se va a proteger la información generada. La solución incluye de manera importante al ciudadano consumidor de estos dispositivos, en quien ha de recaer la responsabilidad de exigir que se tengan en cuenta estos extremos por los fabricantes y por quienes venden estos productos.

Miriam García López

Abogada del área de Ciberderecho de Ecix Group

www.ecixgroup.com

CAPÍTULO 2

Medidas de seguridad

sugeridas por expertos

La criptografía como instrumento para evitar el fraude y la suplantación de identidad

Estamos viviendo una auténtica revolución en nuestras vidas, una revolución propiciada por el desarrollo y evolución hacia un nuevo mundo: el mundo digital. Una revolución imparable que está trasformando nuestra economía, nuestra industria y nuestro comportamiento social, en digital.

Esta nueva revolución digital está cambiando el modo en que compramos y vendemos, la forma en que operamos con nuestros bancos y realizamos

tramites con la Administración, el modo en que accedemos a un nuevo puesto de trabajo y a nuestro propio centro de trabajo, incluso la forma social en que nos relacionamos con los demás.

Sin duda, se trata de un nuevo mundo lleno de oportunidades, pero también de riesgos y amenazas que es necesario identificar, prevenir y gestionar, si no queremos convertirnos en victimas del robo, la extorsión, el fraude o la suplantación de nuestra identidad en manos de los que hoy llamamos "ciberdelincuentes", de igual forma que a la seguridad la llamamos "ciberseguridad" y al delito "ciberdelito".

Ésta es la denominación que ahora utilizamos para mencionar a los delitos y a los delincuentes de este nuevo mundo.

La protección de pago y el uso de la criptografía

En términos generales, podemos decir que el fraude en los Medios de Pago se concentra, fundamentalmente, en: los activadores de tarjetas de crédito/debito, en los dispositivos móviles y en los canales web (comercio electrónico).

Con respecto a los primeros, podemos decir que cuando las empresas franquiciadoras de los Medios de Pago (VISA, MASTERCARD…) lanzaron al mercado las primeras tarjetas de banda magnética, de crédito y de débito,

éstas incorporaban una tecnología que, en principio, se consideraba capaz de proteger a los usuarios y proporcionar seguridad a las transacciones realizadas con dichas tarjetas en los cajeros y terminales punto de venta.

Con el paso del tiempo, surgieron bandas de delincuentes expertos en es esa tecnología que eran capaces de leer los datos de las tarjetas, apropiarse del código PIN e incluso clonar las tarjetas y extorsionar a los titulares de las mismas.

Esto, obligó a las empresas franquiciadoras de los Medios de Pago a definir un nuevo estándar de tarjeta de crédito/debito más seguro: La tarjeta con chip o Tarjeta EMV.

En los últimos años, los bancos han migrado las tarjetas de banda magnética de sus clientes a este nuevo modelo de tarjetas chip EMV, en las que la criptografía juega un papel clave en cuanto a la seguridad, al exigir la autenticación del titular en todas y cada una de las transacciones realizadas.

Un proceso de autenticación efectuado tanto para los pagos físicos como para la retirada de dinero en cajeros automáticos o las compras on line.

Las tarjetas EMV cuentan con un chip que almacena la información a través de algoritmos criptográficos de claves simétricas y asimétricas que cifran las comunicaciones, permitiendo así operar en un entorno confiable, extensible tanto a las propias tarjetas de crédito como a los terminales de pago (Cajeros y TPVs) y el propio Centro Autorizador de las transacciones.

Además, las empresas de Medios de Pago velan por la protección de los datos de los titulares de estas tarjetas y exigen, a todas las empresas de comercio y servicios con las que interactúan, la implementación de soluciones de cifrado para custodiar los datos de los titulares de la tarjeta, evitando así un posible riesgo por uso indebido de los mismos, a la vez que cumplen con los requerimientos de Certificación PCI/DSS.

Sin embargo, se está produciendo un gran cambio en el modo en el que realizamos nuestros pagos. Según un reciente informe, el 75% de los establecimientos en España aceptan el pago con Tarjetas Contacless, basadas en tecnología NFC. Una tecnología de comunicación inalámbrica de corto alcance que funciona por proximidad y que en los últimos años además de en las tarjetas de pago se ha integrado en los Smartphones y Tablets.

Se trata de una tecnología pensada que utiliza igualmente la criptografía para prevenir los riesgos de fraude y que está pensada para identificar y validar a otros dispositivos, ahorrando tiempo y dinero.

Para realizar, de manera segura, pagos con un Smartphone, éstos deben de estar vinculados a una tarjeta de crédito y la tarjeta SIM del Smartphone debe incluir una función más en el chip.

Usar esta tecnología requiere de la implicación de los Bancos, así como de las empresas franquiciadoras de los medios de Pago (VISA, MASTERCARD…) y de los operadores móviles.

Para garantizar que las transacciones realizadas en este entorno sean seguras y prevenir el riesgo de fraude, es recomendable que los Smartphones utilizados incorporen determinados niveles de seguridad: huella, tokenización y monitorización de software malicioso.

Administración electrónica confiable

Las gestiones on line con las Administración, tanto por parte de empresas como de ciudadanos, se han ido consolidando como un importante engranaje en el desarrollo de la sociedad digital.

La e-administración nos permite una relación más fluida, menos costosa y mucho más eficiente con las instituciones a la vez que se traduce en un ahorro de tiempo y costes.

Pero ¿Cómo podemos tener un sistema seguro de interacción de los ciudadanos y de las empresas con las Instituciones Públicas?

Pues gracias a la aplicación de la criptografía. Una tecnología que permite dotar a los procesos telemáticos de instrumentos de identificación y

autenticación confiables, a la vez que garantiza la no alteración e integridad de la información transmitida.

El uso de certificados digitales, basados en el algoritmo RSA (con clave pública y privada) y del cifrado asimétrico, identifican y autentican al ciudadano u empresa, permitiendo que éste pueda hacer uso de la firma digital, mediante la clave privada de un certificado emitido por una Entidad Certificadora confiable.

Podemos decir que fue en el año 2002, con la llegada del DNI electrónico, cuando realmente la criptografía se puso al servicio del ciudadano debido a que el chip de este documento es una tarjeta criptográfica, con la que poder identificarse y autenticarse de manera segura.

También el ámbito empresarial es cada día más consciente de los riesgos asociados al robo y suplantación de identidad y está apostando por la implementación de sistemas de cifrado para prevenir riesgos de suplantación de la identidad, proteger la propiedad industrial, evitar el robo o la extorsión.

Siendo el cifrado asimétrico, en particular, el que adquiere mayor protagonismo como algoritmo de protección de la información, las comunicaciones y la identidad corporativa.

En definitiva, podemos concluir diciendo que, aunque la seguridad en términos absolutos es una entelequia, la criptografía es una tecnología eficiente que contribuye a prevenir los riesgos de fraude, proteger nuestra identidad y evitar el robo o la extorsión de los ciberdelincuentes.

Jesús Rodríguez

CEO de REALSEC

www.realsec.com

Pentesting persitente

Ante la gran variedad y sofisticación en los ataques a los cuales se encuentran expuestas las organizaciones hoy en día, así como el incremento de la complejidad en sus infraestructuras y sistemas, es crítico para la organización identificar estas amenazas y adoptar contramedidas que permitan su prevención y detección, a través de una detección oportuna y gestión adecuada de las vulnerabilidades a las cuales se encuentra expuesto.

No sólo se trata de una ejecución aislada en la detección de vulnerabilidades, sino que, por el contrario, se busca una continuidad en el tiempo, instaurando para ello, un proceso integrado con el resto de los procesos, de forma que la organización sea capaz de mantener el nivel adecuado de seguridad en sus sistemas y servicios exigido por el entorno en el que se desenvuelve.

Muchas organizaciones realizan revisiones puntuales de seguridad, obteniendo como resultado más probable un informe con evidencias que demuestren que ha sido posible acceder a los sistemas de información y se aporte unas recomendaciones sobre como mitigar las vulnerabilidades detectadas. Además, casi siempre aparecen vulnerabilidades menores que ayudan a preparar ataques más importantes o fallos de configuración en el entorno que permiten finalmente acceder al sistema.

Estas revisiones puntuales van a seguir encontrando vulnerabilidades debido a que el tiempo que pasa entre un proceso de análisis y otro, un sistema informático sufrirá cientos de cambios provocados por actualizaciones del software de los servidores, el software de los clientes, toda la electrónica de red, etc. También habrá actualizaciones y cambios en el código de los sitios web realizadas por los desarrolladores.

Sin embargo, los ataques no se efectúan de este modo y la organización debe prepararse para poder revisar de forma continua el estado de seguridad de su infraestructura, huyendo del enfoque tradicional basado en la generación de un informe estático a la finalización de las pruebas de seguridad, debido a que el tiempo que existe entre la detección y el análisis del informe por parte de la organización, hace que el informe haya prescrito, pues no se puede asegurar que esos riesgos sigan presentes, ya que la infraestructura tecnológica probablemente habrá crecido en tamaño con la de adición de nuevos dispositivos, y se habrá modificado con el reemplazo de otros. ¿Cuál es la mejor forma de controlar la seguridad de un sistema teniendo en cuenta el entorno actual tan cambiante?

Unido a esto, hay que considerar que una empresa debe hacer frente a ataques maliciosos de individuos que intentan encontrar debilidades para ganar acceso a los sistemas de información. Estos ataques pueden ser llevados a cabo en cualquier momento y los atacantes se ven beneficiados por el entorno cambiante en que hoy en día se ven envueltos los sistemas

informáticos, pudiendo aprovechar cualquier fallo de seguridad para acceder a información valiosa o sistemas clave de las organizaciones. ¿Cómo se pueden preparar los sistemas para hacer frente a estos ataques?

La respuesta a estas dos preguntas es a través de la industrialización de estas revisiones hacia un proceso de detección continuo que denominamos "Pentesting Persistente" y asociándolo a unas herramientas que permitan de forma ágil la gestión de las vulnerabilidades detectadas.

En este proceso industrializado, la especialización requerida para detectar las amenazas da paso a que esta misión sea realizado por agentes especializados y la organización pueda centrarse en el proceso de corrección de las vulnerabilidades, gestionando el ciclo de vida de las vulnerabilidades: Desde que se detectan hasta que se valida que estas no son explotables.

Detección de vulnerabilidad. Pentesting persistente

Se basa en un enfoque recursivo de funcionamiento en las distintas fases que componen el proceso de Pentesting. Estas fases siguen la metodología basada en simular el proceso de ataque real:

Fase de Descubrimiento: Si analizamos como actuaría un atacante externo, este no parte de un número concreto de direcciones IP o nombres de servidores (FQDN), sino que generalmente lo único con lo que cuenta es el nombre de la empresa o dominios asociados, por lo que en primer lugar se

lleva a cabo a Fase de Descubrimiento orientada a obtener la visibilidad sobre todos los activos digitales del objetivo.

Una vez determinado los activos del objetivo, entra en la Fase de Análisis en la que trata de determinar las rutas que puede seguir para acceder a los activos, así como las técnicas usadas para poder lograr usar fallos, vulnerabilidades, malas configuraciones, recabar información sobre los objetivos, etc.

Por último, se pasa a la Fase de Explotación en la que emplea la información de contexto de las fases anteriores para tratar de explotar vulnerabilidades sobre los activos y configuraciones detectadas, incluso combinando varias vulnerabilidades de severidad menor en aras de obtener una vulnerabilidad de mayor severidad.

Para explicar este proceso de "Pentesting Persistente" utilizaremos la analogía de qué es, como si fuera un video, permitiendo acceder en tiempo de ejecución de los análisis, a los resultados de las vulnerabilidades e informaciones sensibles encontradas, en contraposición del enfoque basado en informe al finalizar las pruebas que sería como de fotos tomadas en diferentes momentos.

Si bien la gestión de las debilidades en el Pentesting Persistente puede realizarse en tiempo real, se debe dar la posibilidad de generar un informe con los resultados indicados y recomendaciones de mitigación y buenas

prácticas para corregir las malas configuraciones y vulnerabilidades, pues en ocasiones es necesario adjuntar este tipo de prueba, aunque no debe emplearse como el centro de la gestión de los riesgos detectados, pues las informaciones que aparecen en estos pueden haber prescrito.

Después de la ejecución de todas estas fases se descubren nuevos activos. Este descubrimiento de activos reinicializa el sistema y las mismas fases se ejecutan de forma recursiva, pero esta vez con pruebas adaptadas a la nueva información obtenida en la anterior ejecución.

Fase de Descubrimiento

El desarrollo/adquisición de nuevos servicios o aplicaciones y la mejora de los existentes para responder a las necesidades del negocio de forma rápida y eficiente, prácticas habituales en un entorno tan cambiante, pueden ser causas de cambios en la infraestructura tecnológica de los clientes. Estos cambios provocan que el inventario de sus activos se encuentre desactualizado y sin información precisa para ser consultado en cualquier momento, impidiendo tener una visión global de la dimensión y extensión de su compañía. Existen en el mercado herramientas que proporcionan un inventario preliminar de la organización, pero mantenerlo actualizado es una tarea dinámica que conlleva una gran cantidad de recursos técnicos y procedimentales.

También pueden producirse cambios no autorizados en la infraestructura como la instalación de servidores, sistemas operativos o paquetes de software en puertos específicos que no son comunicados inmediatamente a los grupos responsables de la organización por falta de coordinación o compromiso entre los procesos implicados. Estos cambios no suelen cumplir la política de seguridad de la compañía, que especifica qué elementos están autorizados para ser instalados, y no cuentan con las configuraciones correctas ni con las últimas versiones de paquetes de software o actualizaciones de seguridad.

En ocasiones las organizaciones pueden tener activos que se encuentran descuidados y no están siendo gestionados o de los que ha olvidado su existencia que no cubren ninguna necesidad del negocio, pero, al estar expuestos en internet, introducen un nuevo vector de ataque a la organización.

Otro reto al que enfrentarse es Shadow IT: En el mundo de la empresa cada vez los empleados hacen más uso de lo que llamamos Shadow IT, o lo que es lo mismo, de su propia infraestructura IT para hacer su trabajo. Del BYOD donde los usuarios tienen su propio dispositivo móvil, hemos pasado al BYOIT (Bring Your Own IT), donde ya no solo traen su propio smartphone, sino que además traen sus propias cuentas de servicios de vídeo-conferencia, correo electrónico, transmisión de ficheros, conexión a Internet por medio de sistemas de tethering para evadir los controles de firewalls o

proxy, sus propios sistemas de almacenamiento de documentos - que pueden crear hidden links en las redes - , tienen sus propios sitios webs e incluso sus propios servidores en la nube, que a veces usan para hacer sus propias webs de recursos, pequeñas campañas de marketing, gestor documentales o simplemente pruebas.

Los equipos de administración IT y seguridad en las empresas cada vez tienen menos control del IT que usan sus empleados. Y ese Shadow IT crece y crece cada día siendo un vector de ataque a la organización al no contar con el mismo grado de seguridad que el aplicado en el resto de sistemas gestionados por los departamentos de TI.

No solo existe un gran incremento del número de activos controlados por IT, sino que también existe un subconjunto muy peculiar, que son los dispositivos IoT. A veces son dispositivos "Plug & Play" que se auto-configuran, o sistemas autónomos con conexión que se conectan a una red y hacen todo el trabajo ellos. Pueden ser impresoras, vídeo proyectores, teléfonos VoIP, controles de puertas, etcétera.

Por si esta situación no fuera lo suficientemente compleja, los ecosistemas IoT añaden más entropía a la ecuación para la gestión de riesgos, derivado por el hecho que en muchos casos estos dispositivos son muy sencillos e incluso muchos de ellos se auto-configuran utilizando servicios externos, pasando inadvertidos para los departamentos de TI.

Todos estos dispositivos, como Webcams, NAS, Smart printers, routers, WirelessAccessPoints, TVs o teléfonos IP están conectados, configurados y manipulados muchas veces por empleados con mayor o menor conocimiento técnico, se convierten en un punto importante del Shadow IT o Shadow IoT en el contexto de "Internet de las cosas". Las herramientas tradicionales de escaneo de vulnerabilidades no los buscan en sus sistemas de discovery y escaneo de vulnerabilidades a diferencia de las técnicas empleadas en el Pentesting Persistente.

Los atacantes no se limitarán a lanzar ataques contra activos IT tradicionales, sino que buscan cualquier punto de entrada y todos esos pequeños sistemas IoT pueden abrir un gran fallo de seguridad en una organización, siendo necesario dotar de capacidades de autodiscovery de estos dispositivos IoT conectados a la empresa, con el objetivo de categorizarlos y lanzar una serie de ataques específicos en la capa de aplicación, detectando no solo vulnerabilidades a nivel de red (falta de cifrado, cifrado débiles, servicios inseguros, ...) sino también a nivel de aplicación como (autenticación/autorización insuficiente, credenciales conocidas, ataques de inyección, reutilización de mensajes, ...)

Tener el conocimiento de los activos de la organización es una práctica vital para una gestión efectiva de las fuentes de posibles problemas, ya que a diario se publican multitud de vulnerabilidades y el cliente no puede proteger aquello que desconoce su existencia. Los atacantes continuamente

buscan servidores y dispositivos obsoletos y versiones de software sin actualizar que puedan ser explotados de forma remota y ganar acceso a la organización, por eso es importante conocer qué elementos (servidores, dispositivos, sistemas operativos, paquetes de software) forman parte de la infraestructura de la organización y en qué estado de actualización se encuentran.

Implementación de Descubrimiento

Para lograr tal objetivo se recomienda adoptar un enfoque de análisis como el que se realiza en el "Pentesting Persistente" el cual parte de un nombre de dominio y empleando fuentes OSINT (Open Source INTelligence) usadas habitualmente por pentesters y atacantes (buscadores web como google o bing, metadatos, consultas a DNS, servicios como Shodan, Robtext o Archive.org entre otros) de forma continua determina el conjunto de activos de una empresa accesibles desde Internet.

Esto realmente imita el comportamiento que los atacantes realizan previo a la explotación. Ellos se apoyan en buscadores que indexan información sobre una compañía y obtienen una visión de los activos que son accesibles desde internet.

Veamos como el enfoque de Pentesting Persistente ayuda a controlar el Shadow IT:

Supongamos que se realiza una campaña de marketing para la empresa ACME (nombre de dominio principal acme.com), y el subdominio de la campaña (technology-event.acme.com) se aloja en una dirección IP que pertenece a la empresa encargada de la campaña de marketing. Esto es una práctica insegura que puede ser realizada para cumplir con compromisos temporales adquiridos: la empresa acme.com tiene implementado un proceso de QA (Quality Assurance) exhaustivo que podría retrasar la publicación de la página web de la campaña de marketing. Por ello, se decide alojar la página web y sus contenidos dentro de los rangos de direcciones IP de la empresa encargada de la campaña de marketing.

En este caso, se desconoce el nivel de seguridad de la página web, y además tampoco se dispone de información que certifique la seguridad de los sistemas, aplicaciones y hosts de la empresa de marketing.

En estas páginas de marketing suelen existir formularios que piden información de carácter personal. Supongamos que existe una implementación insegura de la validación de las entradas para la consulta a la base de datos de la empresa responsable de la campaña de marketing. Si un usuario malicioso pudiera realizar inyección de código (por ejemplo, SQL), accedería a este tipo de información de carácter personal y podría poner en riesgo la reputación de la empresa unido a sanciones económicas por el tratamiento inseguro de información de carácter personal. Por otro lado, debemos tener en cuenta que muchos de los usuarios que visitarán

technlology-event.acme.com serán empleados de la empresa acme.com que podrán entrar a la página desde dispositivos corporativos. Si un usuario malicioso lograra insertar un código persistente en esta página en apariencia confiable estaría posiblemente logrando infectar a empleados de acme.com mediante un envenenamiento de la fuente, pudiendo acceder a información delicada que condujera (usuarios, claves, etc.) a la entrada en los sistemas de información de esta empresa.

Debido a la fase de descubrimiento que realizada en el Pentesting Persistente va a ser capaz de encontrar el subdominio technology-event.acme.com a diferencia de otras soluciones de Pentesting Web o Web Application Security Scanners limitadas de entrada por rangos de direcciones IP o URL de Aplicaciones Web concretas, el Pentesting Persistente no sesga la imagen digital de la empresa ACME ya que se orienta a dar la visión global de una organización descubriendo todos los activos accesibles desde Internet.

Es importante destacar la necesidad de que, en esta fase inicial de descubrimiento, se empleen técnicas para determinar los diferentes Virtual Hosts configurados en una dirección IP, de modo que revisaría todas las aplicaciones accesibles desde Internet, y que ayuda a controlar el control de las aplicaciones obsoletas:

La empresa InGen hace uso de Virtual Hosting en un servidor dimensionado para soportar tres aplicaciones web:

- *http://jobs.ingen.com ->10X.XX.231.5*
- *http://test.ingen.com -> 10X.XX.231.5*
- *http://sales.ingen.com -> 10X.XX.231.5*

Desde hace un mes están experimentando problemas de lentitud en el funcionamiento de las aplicaciones. La ejecución de un escáner del servicio de Pentesting Persistente arroja los siguientes resultados relativos al servidor mencionado. En primer lugar, ha sido capaz de descubrir una cuarta aplicación http://old.ingen.com corriendo en el mismo servidor haciendo reversing de la dirección IP para comprobar los nombres de dominio que apuntaban a la dirección IP del servidor. Para ello, se hace uso de la opción del buscador Bing que permite verificar los dominios públicos que comparten una misma IP.

Se debe tener en cuenta que la cuarta aplicación descubierta se encuentra obsoleta y fuera del control de la organización. No figura en el inventario actual de activos y tampoco está sujeta a actualizaciones ni parcheado. En este caso también es una aplicación que está corriendo consumiendo recursos del servidor compartido con otras tres aplicaciones.

Con la implementación que realiza el resto de herramientas de Pentesting en la fase de discovery, se usa la dirección IP para contactar al sistema, y el navegador web enviará la dirección IP como nombre de host. El servidor web recibirá como cabecera Host la propia dirección IP y el servidor responderá con el primer Virtual Host o uno por defecto, que normalmente no coincide con la página web que el usuario esperaba.

Esto no sucede en el caso de un Pentesting Persistente al ser capaz obtener los virtual host configurados para cada servicio HTTP encontrado de las empresas. De este modo el análisis posterior es mucho más profundo no dejando nada fuera por una orientación puramente de direcciones IP, puesto que, en tal caso, sólo se analizaría el primer virtual host o el de por defecto que devuelva el servidor web.

Un atacante va a implementar estas mismas técnicas para buscar puntos de entrada para detectar aplicaciones obsoletas o que escapan al control de la organización. Estas aplicaciones suelen tener un nivel de seguridad menor que el resto de los activos, ya que no se tiene consciencia de su existencia, y por ende tampoco entran dentro de actualizaciones o procedimiento de parcheado.

Fase de Análisis

En la fase de análisis se trata de determinar las rutas que puede seguir para en la siguiente fase atacar a los objetivos. Estas rutas, son los servicios generalmente expuestos en Internet, que entre otros se trata de evaluar:

- Configuraciones inseguras de servicios expuesto en internet: SSH, DNS, HTTP,
- Evaluación de certificados y protocolos SSL.
- Análisis de cabeceras HTTP.
- Identificación y análisis de versiones detectadas en la infraestructura.
- Evaluación de sistemas de gestión contenidos (Wordpress, Joomla, Drupal).
- Ficheros sensibles, Metadatos, configuraciones inseguras, etc.
- Accesos sin autenticación.
- Obtención de información para realizar ingeniería social.

Cabe destacar la capacidad del proceso de "Pentesting Persistente" de combinar distintas técnicas propias de una atacante simulando de forma real su comportamiento. Ejemplo de esto sería la descargar de los distintos tipos de ficheros jugosos (juicy files) que previamente han sido descubiertos en la fase de Discovery con el enfoque recursivo. A diferencia de una herramienta de Análisis de Vulnerabilidades que sólo indicaría la existencia de estos archivos, en el "Pentesting Persistente" los descarga para posteriormente analizar el contenido de estos ficheros en busca de información relevante en

un proceso de pentesting: rutas a ficheros locales, rutas no indexadas en buscadores, metadatos, información generada por desarrolladores, usuarios, contraseña, ficheros ocultos o perdidos, fugas de datos y de código, etc.

Este comportamiento se lleva a cabo por ejemplo en el descubrimiento de un fichero SVN Entries. Si desarrollas aplicaciones web, es muy cómodo tener el repositorio en el mismo servidor donde estás publicándola, pero eso puede ser un craso error, pues de este fichero se obtiene información sobre los últimos updates que se han realizado en un proyecto de desarrollo que utiliza SVN como gestor de código y que ofrece información lo suficientemente sensible como para bloquear su acceso.

La información contenida en los metadatos, contenidos en archivos públicamente accesibles de la organización, debe ser analizada pues puede contener información que nos permita montar un ataque más sofisticado. El análisis de metadatos permite obtener datos sobre usuarios concretos y sus direcciones de correo; información del mapa de red para la generación de enlaces en apariencia confiables desde emails de usuarios de la empresa y además, se consigue identificar servidores concretos con la información asociada a ellos para poder diseñar malware específico. Todo orientado a aumentar las posibilidades de éxito de la campaña de phishing por ejemplo.

Las herramientas tradicionales de escaneo de vulnerabilidades no realizan este análisis y por tanto no identifican riesgos de seguridad asociados a los metadatos:

- Encontrar relaciones ocultas entre compañías o personas.
- Se puede detectar casos de piratería de SW, al descubrir que un documento de una empresa se ha generado con un SW del que no se ha adquirido la licencia.
- Puede localizarse información táctica para estudiar posibles objetivos de ataques y adquirir conocimiento interno de una compañía.
- Se pueden trazar eventos, posicionándolos tanto en tiempo como en espacio.

Si durante la ejecución de esta fase de análisis se descubrieran nuevos activos (p.e. URL contenida en un fichero analizado) reinicializa el sistema y las mismas fases se ejecutan de forma recursiva, pero esta vez con pruebas adaptadas a la nueva información obtenida.

Fase de Explotación

La última fase consiste en realizar las pruebas pertinentes de explotación, en base a la información obtenida en la fase de análisis. En esta fase se realiza una explotación controlada de las vulnerabilidades conocidas de los activos

y elementos pertenecientes al dominio auditado. Básicamente se pretende simular la acción de un intruso sobre un activo, reproduciendo entre otras las siguientes técnicas de ataque:

- Inyecciones de contenido.
- Ataques en la parte cliente.
- Inclusión de ficheros local y/o remota.
- Ataques específicos de protocolos (SMTP, DNS Xfer, DRP, SSH, …)

De los ataques exitosos, se debe generar una evidencia con el detalle suficiente para conocer donde se encuentra el problema identificado e información que permita reproducir el ataque.

A continuación, se muestra un ejemplo de evidencia, en la indica que se ha realizado una inyección de tipo QueryString, al ser una petición HTTP GET, sobre el parámetro fecha.

Como resultado de esta inyección se produce la ejecución de una instrucción SQL que está siendo ejecutada por el motor de Bases de datos, produciéndose lo que se conoce como SQL-Injection.

"Description": "There is a difference of 9,1169821 seconds between the first and second request, using the following true\/false injections on parameter 'fecha'.",

"InjectedParameter": "fecha",

"InjectionType": “QueryString”,

"InjectionValue": "20160531'\/*.*\/&&\/*.*\/BENCHMARK({time},MD5(0x41))\/*\u000d\u000a20160531'\/*.*\/&&\/*.*\/BENCHMARK(0,MD5(0x41))\/*",

"RequestsAndResponses": {

"HttpMethod": GET,

"Protocol": HTTP,

"Request": "GET /inforeserva.html?fecha=20160531%27%2F%2A.%2A%2F%26%26%2F%2A.%2A%2FBENCHMARK%281000000%2CMD5%280x41%29%29%2F%2A HTTP/1.1\u000d\u000aUser-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0\u000d\u000aAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8e\u000d\u000aHost: demofaast.e-paths.com:9002\u000d\u000aConnection: Close\u000d\u000a\u000d\u000a",

"Response": "HTTP/1.1 200 OK\u000d\u000aConnection: close\u000d\u000aContent-Length: 389\u000d\u000aContent-Type: text/html\u000d\u000aDate: Fri, 29 Apr 2016 04:00:12 GMT\u000d\u000aServer: Apache/2.4.10 OpenSSL/1.0.1i PHP/5.5.15\u000d\u000aX-Powered-By: PHP/5.5.15\u000d\u000a\u000d\u000a\u000d\u000a<html>\u000d\u000arandom link\u000d\u000a

\u000d\u000aContent: \u000d\u000acb02cce59df9e0bcdc119314599f9dc9

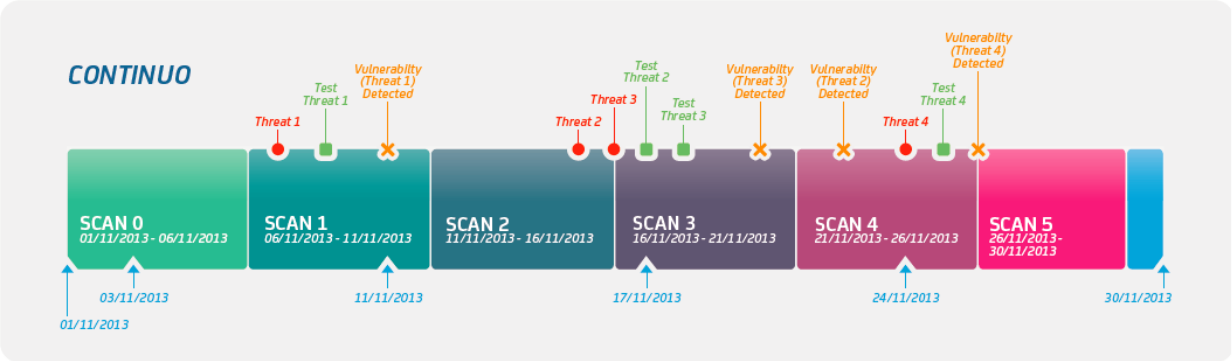
\u000d\u000aLeak:
\u000aWarning: md5() expects at least 1 parameter, 0 given in /home/webapp/inforeserva.html on line 14
\u000a

\u000d\u000aXSS: 20160531'/*.*/&&/*.*/BENCHMARK(1000000,MD5(0x41))/*</html>" }

Continuidad en el Tiempo

Al concluir todas las fases del análisis del Pentesting Persistente, es necesario reiniciar el proceso en la fase de descubrimiento iniciando un nuevo análisis con el objetivo de detectar nuevamente vulnerabilidades y/o fallos de configuración provocados por actualizaciones del software de los servidores, actualizaciones y cambios en el código de las aplicaciones realizadas por los desarrolladores.

Se muestra el ejemplo que ilustra a la perfección el concepto de pentesting continuo que posibilita la reducción del tiempo de exposición de los sistemas a vulnerabilidades:



El servicio de Pentesting Persistente viene soportado por la idea de que el pentesting no debería ser un proceso puntual que se contrata, sino un servicio de seguridad 24x7 durante todo el ciclo de vida de un sistema.

Mediante la implementación de un pentesting continuo:

- permite en un entorno tan cambiante favorecer el conocimiento y control de una infraestructura TI accesible desde el exterior, brindando una visión actualizada de la seguridad de todos los activos accesibles desde Internet, independientemente del tamaño de la compañía y,
- prepara los sistemas ante ataques reduciendo el tiempo que sus sistemas están expuestos a vulnerabilidades.

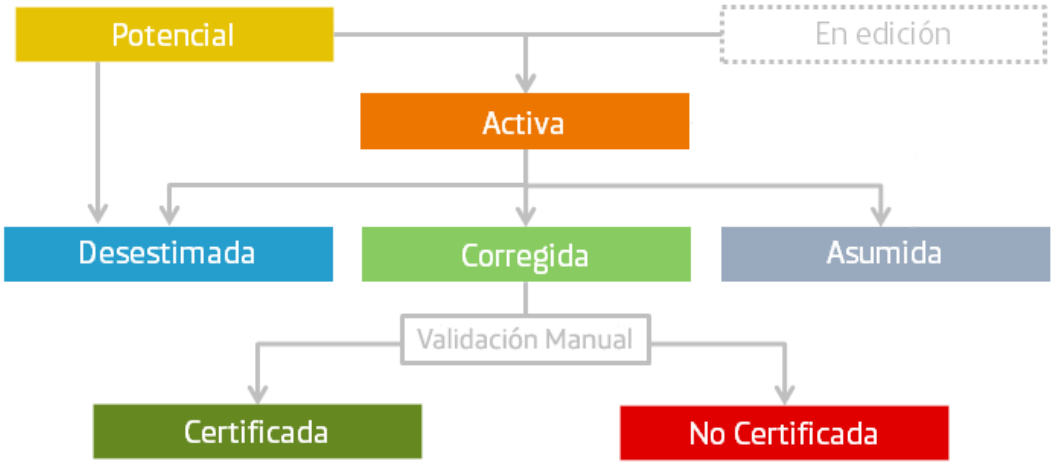
De este modo se hace necesario un control del diseño de los sistemas desde sus primeras fases y la aplicación de Pentesting by Design contemplando un dimensionamiento de recursos en cuanto a la capacidad de procesamiento,

almacenamiento y el ancho de banda de la línea de comunicaciones para brindar una QoS a los usuarios, más un porcentaje que tenga en cuenta los ataques maliciosos y más el porcentaje necesario para que el sistema puede someterse a un proceso de Pentesting Continuo.

Gestión de vulnerabilidad

Como ya vimos, en la industrialización del proceso no acaba con la detección de las vulnerabilidades, sino que continúa con la gestión del ciclo de vida de las vulnerabilidades detectadas. Como ya indicamos, esta gestión debe comenzar tan pronto son detectadas, huyendo del enfoque tradicional basado en la generación de un informe estático a la finalización de las pruebas de seguridad y finaliza cuando una vulnerabilidad se valida que ya no es explotable.

Este seguimiento de estados puede modelarse atendiendo al siguiente "workflow" de estados, garantizando la trazabilidad de las acciones realizadas para determinar si una vulnerabilidad se encuentra mitigada.



Dado que el proceso es continuado en el tiempo, en el que se lanzan varios scans se debe analizar las diferencias entre las distintas ejecuciones de los tests. En este diferencial, existirán nuevas vulnerabilidades y otras que han cambiado el de estado de las mismas, de modo que si una vulnerabilidad no ha vuelto a ser detectada podría identificarse como corregida y por el contrario vulnerabilidades que se pensaban mitigadas, ante una nueva detección se consideraría que en realidad no está corregida.

Un punto a tener en cuenta en la gestión, es la priorización de los esfuerzos para la mitigación puesto en algunos casos esta tarea puede ser compleja cuando se detectan un número muy elevado de vulnerabilidades, o dicho de otra forma, "¿Por dónde debería comenzar a corregir?"

Entre los factores para realizar esta priorización se encontrarían:

La severidad o gravedad de la vulnerabilidad detectada, junto a la facilidad de explotación de la vulnerabilidad (privilegios necesarios, existencia de exploit, …)

Activos afectados, no es lo mismo una vulnerabilidad muy grave en un activo de desarrollo que en un entorno de producción, o con un alto valor para el negocio.

La combinación de ambos factores, nos proporciona un valor de criticidad y urgencia para la corrección de la misma expresado en términos de negocio, ya que, aunque se detectara una vulnerabilidad muy severa, p.e. SQL Injection, pero se trata de un sistema a de desarrollo aislado la criticidad y la urgencia para la organización no es la misma que si se detectara sobre un sistema de producción.

Por tanto, para lograr el éxito de este proceso de gestión de vulnerabilidades, la organización debe aplicar una clasificación y categorización de los activos analizados tanto en términos de ubicación física/lógica (Producción, Preproducción, DMZ Transaccional, DMZ Informacional, Proveedores, etc.), como en términos de negocio (Ventas, CRM, SAP, Critico para el negocio, etc.). Generalmente casi todas las organizaciones cuentan con una CMDB donde se inventarían los activos con cierto grado de categorización de los mismos, sin embargo, no suele

disponer de un detalle concreto en cuanto a versiones de software instalado, servicios de red ofrecidos entre otros.

Para lograr una Gestión de Vulnerabilidades eficaz debe ser capaz de combinar la información contenida en la CMDB de la organización junto a la recogida por las herramientas de análisis de seguridad facilitando de este modo establecer una priorización de acuerdo a términos de negocio.

Generalmente, las organizaciones llevan a cabo de forma más o menos industrializados ciertos procesos de revisión de seguridad de sus activos mediante subscripciones de servicios de alertas, uso de escáneres de seguridad, pentesting manuales realizados y que proporciona información de forma disgregada, siendo necesario emplear mucho tiempo para realizar el seguimiento de las amenazas detectadas, pues en muchas ocasiones es totalmente manual, basado en hojas Excel, imposibilitando tener una visión del estado actualizada en toda la organización.

El proceso de gestión de vulnerabilidades debe poder responder de forma ágil a la sencilla pregunta que todos nos haríamos "¿Cuántas vulnerabilidades me afectan y cuál es el estado de las mismas?"

Por tanto, es importante disponer de un cuadro de mando que permita visualizar de forma unificada y basada en estándares como CVE u OWASP las amenazas detectadas en todos los análisis de seguridad realizados y que la organización pueda visualizar en tiempo real los diferentes tipos de

vulnerabilidades que afectan a sus sistemas, pudiendo conocer el origen y determinar la causa en aras de relacionarlo con los controles más adecuados.

El proceso de gestión de vulnerabilidades debe ser continuo y por tanto el tratamiento de las amenazas detectadas deberá ser llevado a cabo en base a la información en tiempo real que se tiene sobre las vulnerabilidades detectadas en lugar de analizar informes estáticos del resultado de un proyecto.

Si este no fuera el caso, es posible que se estén empleando recursos para la mitigación de vulnerabilidades que pudieran haber desaparecido en detrimento de otras nuevas vulnerabilidades que pudieran tener una urgencia mayor para la organización.

Esto no quiere decir que el proceso de gestión de vulnerabilidades no deba contar con informes en el que se recojan los hallazgos, sino que estos informes deben ser generados bajo demanda por la organización con la información actualizada desde la BBDD.

Como indicábamos al principio de este artículo, este proceso de gestión de Vulnerabilidades no debe verse como un proceso aislado con los existentes en la organización y por tanto debe contar con un interfaz que permita la integración con otros sistemas ya que en las organizaciones generalmente

para poder realizar una acción que mitiguen una vulnerabilidad suele ser necesario abrir una solicitud en el sistema de ticketing de la organización.

Este proceso es laborioso y por tanto es altamente recomendable acometer una integración bidireccional con el sistema de ticketing, que aumentaría la eficiencia al disponer de un cuadro de mando de seguridad y que permitiría gestionar y comprobar la mitigación de las vulnerabilidades detectadas.

Por último y no por ello menos importante, mientras se está aplicando las medidas mitigadoras indicadas en el ticket de soporte y con el objetivo de poder reducir el tiempo de exposición de las debilidades detectadas, se puede emplear una estrategia de Virtual Patching. Para ello es necesario colocar delante de nuestras aplicaciones web un sistema Web Application Firewall, capaz de analizar las peticiones que reciben las aplicaciones e interceptar el tráfico malicioso, bloqueando los intentos de la explotación de vulnerabilidades. De este modo se consigue reducir la exposición de las vulnerabilidades ya que mientras que el código fuente o la configuración de la aplicación no han sido modificados, la mitigación de la vulnerabilidad está siendo realizada.

Chema Alonso

CDO (Chief Data Officer)

www.Telefónica.com

Victor Mundila

Cibersecurity Product Manager

www.elevenpaths.com

Control parental

Hoy en día, los ordenadores, móviles e Internet son herramientas cotidianas en nuestro mundo. Tenemos la necesidad de usarlas constantemente, sin embargo, ¿todo el mundo es consciente del peligro que existe al navegar por Internet? La respuesta a esta pregunta es…sí y no. Existen todo tipo de personas, hay gente que lo sabe, pero le resulta indiferente, otras que ponen límites o barreras de seguridad y otras que simplemente lo desconocen. Los más desprotegidos son los pertenecientes a este grupo final, pero ¿quiénes podrían ser estos últimos? Pues principalmente los menores o adolescentes, los cuales tienen unos intereses concretos.

Por norma general, cualquier niño o joven usa internet para revisar sus redes sociales, entretenimiento u ocio. Ante ellos se abre un campo de posibilidades tan enorme que nadie puede decir con seguridad qué tipo de información llegan a buscar (por ejemplo, pueden encontrar y/o buscar contenido no apto para su edad o pueden enfrentarse a cualquier tipo de amenaza informática sin saberlo, ni estar preparado para ello).

En este tema, al que hemos denominado "Control Parental", analizaremos, explicaremos e informaremos de las aplicaciones que nos pueden ayudar a enfrentarnos a todas estas posibilidades.

¿Qué es un control parental?

Se llama Control Parental a cualquier herramienta que permita a los padres o tutores controlar y/o limitar el contenido al que un menor puede tener acceso cuando navega por internet.

¿Es legal?

La pregunta parece simple pero no es así, ¿tienen los padres derecho a espiar a sus hijos?

Los niños, y menores de edad, en general, son titulares de derechos desde el nacimiento. Así lo reconoce el Código Civil, en su artículo 30:

"La personalidad se adquiere en el momento del nacimiento con vida [...]"

Otra cuestión distinta es que, como son menores, no tienen todavía la capacidad de obrar ni de discernir lo conveniente o no de sus actos, por lo que esta carencia debería ser suplida por los padres o tutores. Tenemos que tener en cuenta además que los menores tienen derecho a la intimidad en toda la extensión posible que otorga el artículo 18 de la Constitución.

"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."

Así, además se garantiza en la LO 1/1996 de protección jurídica del menor,

> *"1. Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones."*

vía artículo 4:

Pero por otro lado, y este es el punto de discusión, los padres como

> *"La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y con respeto a su integridad física y psicológica.*

titulares de la patria potestad deben practicar (art. 154 Código Civil)

Esta potestad comprende los siguientes deberes y facultades:

1. Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral.
2. Representarlos y administrar sus bienes."

Por lo tanto, los padres deben velar por ellos, educarlos y procurarles una educación integral, y para poder desarrollar este amplio campo, ¿hasta dónde pueden inmiscuirse en la vida del hijo?

Sistemas de control parental

Existen distintos sistemas de control, dependiendo del tipo de vigilancia que los padres ejerzan sobre sus hijos:

Sistemas de filtrado de contenidos

Desde mi punto de vista, sería legal la instalación de sistemas de filtrado de contenidos, pues como reconoce el artículo 5 de la LO 1/1996:

"1. Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo."

"2. Los padres o tutores y los poderes públicos velarán porque la información que

Y ello a pesar de que el propio artículo 2 de la LO 1/1996 establece que:

"Las limitaciones a la capacidad de obrar de los menores se interpretarán de forma restrictiva."

Así entiendo que tiene sentido limitar el acceso de los menores a ciertos contenidos de la red en base a los principios expuestos, con el fin de velar por los derechos reconocidos. Este control es similar al que se desarrolla habitualmente fuera de internet, donde los padres o tutores limitan el acceso de sus hijos a contenido pornográfico o violento (cine, televisión, publicidad, locales…).

Sistemas de geolocalización

Son aplicaciones que usan la geolocalización del teléfono (GPS). De esta manera se podría ubicar al menor en un punto concreto cuando fuera necesario.

En este caso, la afectación de la intimidad puede ser mayor, para evitarlo habrá que tener cuidado para que esta localización no suponga además una intrusión también en el secreto de las comunicaciones.

A mi juicio, entiendo que sería conveniente que el menor tuviera conocimiento previo de la intención de la instalación por parte de los padres de este tipo de sistemas, además de la posibilidad de deshabilitarlo.

Revisión de url de contenido

El lugar donde podríamos recoger la mayor parte de la información, seria en la revisión de las URLs visitadas y que podemos encontrar en el historial del navegador. Esto puede dar una idea de los sitios y la información visitada.

A mi entender los padres sí podrían revisar el historial de navegación siempre que se haga desde un usuario abierto y sin contraseña. Es decir, que el menor use un usuario compartido con los padres, etc. Al contrario, si usáramos un perfil de administrador o con privilegios suficientes para poder entrometernos en la cuenta del menor, no se vería admitido y violaría la intimidad.

Acceso a perfiles de redes sociales

Si el menor propaga su propia información en internet no habría violación a su intimidad. El padre o tutor podrían acceder al perfil de la red social, siempre y cuando esta tuviera una configuración pública.

Si la red estuviese cerrada o no fuera accesible desde una URL a usuarios sin registrar, los padres no deberían poder acceder a la misma. A menos que el menor lo consienta, bien cediendo sus contraseñas o bien admitiendo a los padres en el círculo de confianza.

Tampoco sería legítimo, crear un perfil falso o suplantar una identidad para que dicho menor acepte una invitación y por lo tanto entrase en el círculo de confianza y así dar acceso a sus contenidos compartidos.

"[...] el concepto de intimidad personal [...], compuesto por datos y actividades que conforman la particular vida existencial de cada persona y autoriza a preservarla de las injerencias extrañas, salvo que medie autorización libremente practicada, en cuyo supuesto el circulo se abre y la intimidad se comunica, y como es lógico no es la misma para todos, ya que cada persona tiene su propia

El Tribunal Supremo, ha admitido que:

Teniendo en cuenta estas cuestiones, los padres no podrán entrometerse en comunicaciones del menor o invadir su intimidad usando estas herramientas, siempre y cuando estas vulneren los derechos reconocidos para la protección del menor.

¿Es necesario?

Antes de realizar una instalación de algún programa de esta categoría, deberíamos de analizar si realmente es necesario. Considerando la

posibilidad antes de nada de ofrecer una educación apropiada informando de los riesgos. Esta formación es realmente es un pilar muy importante, pero en última instancia, estas herramientas nos ayudarán y podrían evitarán sorpresas desagradables.

¿Cómo funcionan?

Se trata de utilidades que en su versión más completa permiten bloquear, controlar y registrar el uso que se hace desde cualquier dispositivo con conexión. Y no solo se trata de impedir el acceso a contenidos indebidos, sino también de poder evitar situaciones que a día de hoy son muy comunes en las redes sociales, por ejemplo, si son víctimas de ataques de compañeros cyberbullying (ciberacoso) o de personas con malas intenciones, o si, simplemente, pasan demasiado tiempo delante del ordenador o móvil en lugar de estudiar. Por ello, un programa de control parental bien configurado puede ayudar enormemente a los padres.

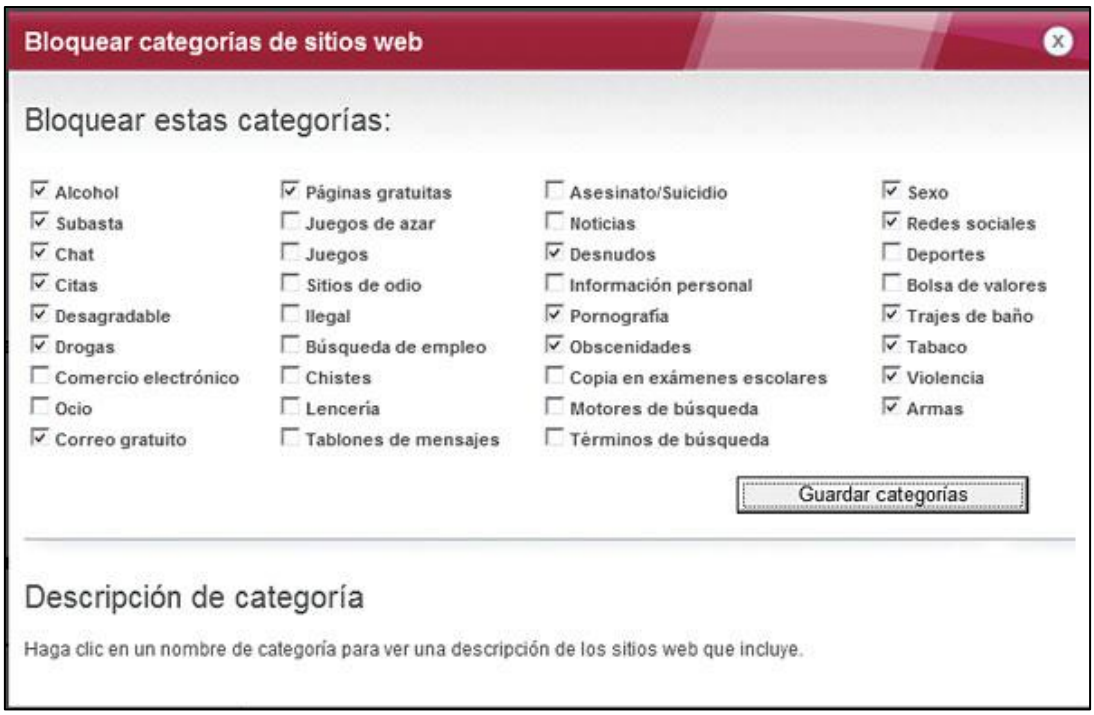
A nivel técnico funcionan como un antivirus, con una serie de procesos cargados en la memoria que controlan numerosos aspectos.

Estas herramientas pueden ser automatizadas o no. Las herramientas automatizadas son aquellas que permiten trabajar en dos niveles de seguridad: la prevención y el control. Ninguna de estas herramientas es 100% efectiva por lo que también debemos destacar la valía de las

herramientas no automatizadas: la educación y la concienciación. El diálogo con los menores es la mejor herramienta de prevención para los riesgos que existen en la web.

Contenidos bajo control

La función más básica de un control parental debe ser filtrar los contenidos. Los más básicos utilizan simplemente listas blancas y negras de URLs, que



podríamos completar y personalizar en función de nuestras necesidades.

Otra opción similar la de utilizar un sistema de categorías que filtrarían el acceso en función de la base de datos que tenga el fabricante. Así, las webs catalogadas en una categoría no autorizada, simplemente se bloquearán, y aquellas que estén dentro de las categorías autorizadas se podrán visitar sin problemas.

Otra variante es la basada en keywords (palabras clave) que permite filtrar por palabras y si quisiéramos restringir más las búsquedas deberíamos añadir cada palabra clave en diversos idiomas. Así, el control parental analiza todo el tráfico y, tan pronto como detecta una determinada palabra en una URL, título o contenido de página web, bloquea el acceso a la misma. El problema principal que existe en esta configuración seria que en una web de confianza, existiera alguna de las palabras clave que queríamos filtrar.

Las comunicaciones e internet

Otra área cada vez más importante es la que atañe a las redes sociales, el chat, el correo y otros recursos que los menores tienen a su alcance para comunicarse a través de Internet. Como ya hemos comentado, no dejan de aparecer en prensa casos de cyberbullying (ciberacoso), y las redes sociales son un lugar idóneo para los que realizan estas prácticas. Controlar lo que

ocurre en los canales sociales o cuentas de comunicación que maneja el menor es muy importante.

Para ello muchos controles parentales permiten desde simplemente bloquear el acceso a sesiones de chat, correo, Facebook, Twitter y otros métodos de comunicación, hasta registrar toda la actividad en dichas redes o herramientas para entregársela a los padres o tutores de manera periódica. Los más avanzados permiten, incluso, registrar amigos, fotografías y datos en torno a los círculos en los que se mueve el menor on-line. De esta forma, en el caso de que éste utilice las redes sociales, siempre podremos detectar cualquier problema antes de que sea grave.

El control del software

La siguiente área que debería administrar todo buen sistema de control parental es el software que se ejecuta en el dispositivo. Muchos de ellos permiten controlar especialmente los juegos que se ejecutan en el ordenador mediante un sistema de clasificación por edades. En Europa el estándar es PEGI (Pan European Game Information), que clasifica los juegos utilizando una serie de rangos de edad (entre 3 y 18 años). De esta manera, si nuestro software de control parental permite controlar la ejecución de

juegos con clasificación por edad, podemos restringir el uso de los mismos, por su violencia o contenido explícito, o bien por que estén recomendados para una edad superior a la del niño. Aunque esto depende del desarrollador y es opcional, por lo tanto, podemos encontrarnos con muchos juegos sin clasificar y no sea recomendable el uso de los mismos por parte de los menores.

A favor del uso responsable

Además de controlar lo que pueden y no pueden hacer los menores en un PC, también es muy importante vigilar durante cuánto tiempo lo hacen. Normalmente son muchos los padres que intentan marcar unas determinadas horas al día para evitar el uso excesivo de la tecnología, pero es muy difícil de conseguir, ya que los menores aprovecharan cualquier despiste.

Muchas aplicaciones de control parental incluyen un apartado que nos permite controlar el tiempo que un determinado usuario tiene abierto el PC al día o la semana, e, incluso, los intervalos horarios en los que puede utilizarlo. De esta manera, es muy sencillo asegurarse de que no se pasa demasiado tiempo delante del dispositivo.

Local también en la nube

Es importante conocer que hay dos tipos de software de control parental: los instalados en nuestros equipos y los alojados en Internet. En el primer caso se trata de una aplicación instalada y gestionada desde nuestro dispositivo, muchas veces imperceptibles (sin icono en Inicio o Agregar/Quitar programas), y que tenemos que configurar o consultar directamente en el propio PC en el que está instalado. La otra opción es que esté alojado en Internet, de manera que localmente solo cargue un servicio, y que todos los ajustes, informes y control, se realicen desde la web del fabricante y empleando cualquier equipo con conexión a Internet. Este último formato es el más habitual en los productos de última generación, y también el más práctico a la hora de gestionar el control, incluso, si estamos fuera de casa o en el trabajo.

Lo más importante es educar

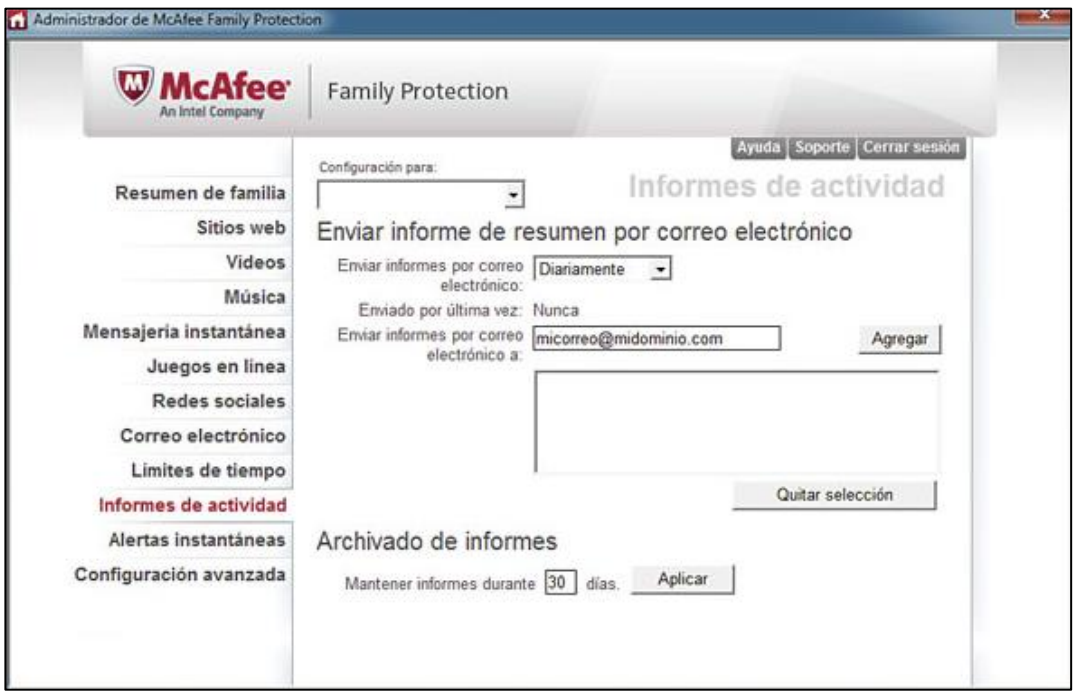
A la hora de instalar un control parental en el equipo de casa, es importante tener claros nuestros objetivos y, sobre todo, la edad del menor a controlar. Con niños pequeños quizá baste instalar el control parental y limitar su acceso a todo lo que consideremos oportuno. Si el niño no puede entrar en una página o arrancar un juego, lo normal es que no tenga mayores consecuencias. El problema viene en la adolescencia (la más delicada en el uso de Internet), sobre todo si otros amigos no tienen limitaciones en sus casas. Por ello, es muy recomendable optar por una estrategia de supervisión más que de bloqueo, y siempre educar al menor para el uso Internet, haciéndole ver los riesgos y peligros, e instándole a conocer que el software de control parental está instalado y que es por su propia seguridad.

Aplicaciones

A día de hoy existen numerosas aplicaciones que realicen este tipo de actividades. Todas estas ofrecen la compatibilidad con los móviles. En función del fabricante se ofrecen versiones gratuitas y/o de pago. A continuación, detallaremos algunas de las aplicaciones más conocidas:

MCAFEE FAMILY PROTECTION

McAfee Family Protection ofrece a sus hijos libertad para descubrir Internet de forma segura. El control parental avanzado, puede proteger a los hijos para que no queden expuestos a contenidos inadecuados, a los riesgos de las redes sociales, a personas desconocidas ni a otras amenazas online.



NORTON ONLINE FAMILY

Esta alternativa destaca por ser uno de los primeros controles parentales que se apoyó en la Nube para permitir el control y la configuración de cada uno de los equipos de la familia. Tan solo requiere la instalación de un sencillo cliente software en cada equipo y vincularlo con nuestra cuenta de Online Family.

QUSTODIO

Permite, una vez instalado, la creación de cuentas de los usuarios, así como el ajuste de las preferencias. Permite controlar la navegación por categorías y listas blancas o negras, el tiempo de uso y las horas autorizadas, con opción de bloquear el PC o solo Internet.

Miguel Garrido

SOC (Security Operation Center)

www.prosegur.es

10 Consejos de Ciberseguridad

En las siguientes líneas se brindarán 10 ciber-consejos de recomendado cumplimiento si se desea contar con las medidas básicas de seguridad para poder navegar tranquilo en Internet, libres de todo tipo de estafas, sustracciones de datos, acosadores, etc.

Ciber-consejo I

Actualiza el sistema operativo (Windows, Linux, Mac OS, etc.) y todos tus programas (Java, Flash, Adobe, etc.). De forma regular, los fabricantes de software lanzan nuevas actualizaciones, normalmente gratuitas, para solventar diversos fallos de seguridad que se van localizando a lo largo del tiempo. Si estas actualizaciones, también conocidas como parches de seguridad, no son aplicadas, estos softwares se convierten en puertas de acceso a nuestros equipos informáticos, permitiendo a potenciales delincuentes tomar acceso remoto y secuestrar nuestra información. Por ello, es vital aplicar siempre todas las actualizaciones que nos recomiendan nuestros sistemas operativos y nuestros programas instalados.

Ciber-consejo II

Instala un buen software Antivirus, y por supuesto utiliza mejor uno gratuito, antes que uno pirata que probablemente se encuentre infectado por otro malware (virus). Los softwares antivirus no son la panacea, pero son capaces de bloquear la mitad del malware existente en el mundo cibernético. Sin ellos, las posibilidades de que un ciberataque tenga éxito se multiplican por 2.

Ciber-consejo III

Cuidado con el SPAM. No publiques tu email en web públicas y no abras, ni descargues nada de remitentes desconocidos. ¿Recibes mucho spam en tu email? Eso es debido a que en alguna ocasión colocaste tu email en algún foro, blog, sitio web, o te registraste con él en alguna web de dudosa confiabilidad. Si es así poco puedes hacer, más que confiar en el filtro anti-spam de tu servicio de email, o cambiar de cuenta de correo. Es vital no compartir nuestra cuenta de email en Internet, porque es un lucrativo negocio para empresas que comercializan sus productos mediante spam (generalmente productos ilegales, como los estupefacientes o medicamentos sin receta).

Ciber-consejo IV

Cuidado con las toolbars (barras de navegador), en muchas ocasiones tienen objetivos maliciosos, por lo que verifica su autenticidad antes de instalarlas. Cuando descargamos un software de dudosa procedencia, no tenemos garantías de que su negocio no seamos nosotros mismos, e intenten instalarnos segundos programas ocultos para extraernos información, engañarnos para adquirir determinados productos, o incluso suscribirnos a determinados servicios Premium. Por ello debemos evitar siempre que sea

posible el hacer uso de estas toolbars, que no vienen de fabricantes de reconocido prestigio.

Ciber-consejo V

Activa el cortafuegos (firewall) del sistema operativo. Nuestro equipo cuenta con numerosas puertas, denominadas puertos, prediseñadas para que distintos servicios puedan comunicarse con nuestro set de aplicaciones. Estos puertos pueden abrirse y cerrarse a través del cortafuegos. Debemos mantener en todo momento el cortafuegos habilitado, siguiendo las instrucciones indicadas por el fabricante (Microsoft en el caso de Windows generalmente). Si tenemos instalado un software antivirus, es habitual que estos programas gestionen y configuren de la mejor manera posible el firewall de forma automática. Por lo que, en este caso concreto, podemos delegar en ellos la tarea.

Ciber-consejo VI

Utiliza contraseñas seguras, cámbialas regularmente, utiliza contraseñas distintas en cada servicio, y a ser posible, utiliza un doble factor de autenticación. Últimamente se están produciendo robos de contraseñas en servicios muy extendidos, como por ejemplo el reciente caso de LinkedIn.

Si utilizamos la misma contraseña para todas nuestras aplicaciones, ya nos habremos convertido en un blanco fácil para cualquier persona que, con intenciones maliciosas, quiera secuestrar por ejemplo nuestras identidades digitales. Por ello, se recomienda contar con una contraseña distinta para cada servicio.

Un ejemplo de contraseña segura podría ser "Epdsrntrprrslhc.65" (El perro de san roque no tiene rabo porque Ramón Ramírez se lo ha cortado + SIMBOLO + AÑO). Y para utilizar esta contraseña para distintos servicios podríamos añadir la primera letra del nombre de este servicio en algún lugar de la contraseña, por ejemplo, para Facebook podríamos utilizar "Epdsrntrprrslhc.F65", para Twitter "Epdsrntrprrslhc.T65".

Ciber-consejo VII

Asegura tus redes Wireless. Utiliza sistemas fuertes de cifrado como WPA2 (WEP está obsoleto).

Y no realices compras,ni gestiones bancarias desde Wireless que no c ontroles (bibliotecas, centros comerciales, etc.), porque podría haber otra persona esnifando (escuchando) todo el tráfico de datos que circula por esa red, y, por tanto, viendo todas tus contraseñas, números de tarjeta de

crédito, etc. Por ello, todo este tipo de transacciones deberemos hacerlas desde nuestra propia conexión de Internet, o desde lugares de máxima confianza.

Ciber-consejo VIII

Protege tus redes sociales. Haz tu perfil siempre privado y cierra los círculos de amistad a tus verdaderos amigos. Tu nº de amigos cercanos debería ser igual a las personas que invitarías a tu boda. ¿De verdad invitarías a 1.500 personas a tu boda?

Ciber-consejo IX

Siempre que sea posible, utiliza HTTPS para navegar a un sitio web. Esto posibilitará que los datos que viajan desde nuestros ordenadores y móviles hasta el servidor donde se encuentra alojada la aplicación que deseamos utilizar, vayan cifrados. Y por tanto, si fuesen secuestrados por un atacante, tendría que intentar descifrarlos, lo que le dificultaría enormemente esta labor.

Ciber-consejo X

Nuestro último ciber-consejo es el más sencillo de comprender, pero probablemente el más complejo de aplicar, y es el sentido común. Y por poner un sencillo ejemplo, si nunca hemos jugado en ninguna lotería por Internet, ¿por qué alguien nos va a enviar un cheque a nuestro email?

Juan Antonio Calles

Cyber Security Senior Manager en KPMG España

home.kpmg.com

Ciberseguridad en eCommerce

"¡Todo el mundo gana dinero en internet menos yo!" y "¡Eso lo hace cualquiera!" son dos de los pensamientos más típicos por los que surge un eCommerce. Y es que la teoría parece sencilla, pero el proceso tiene demasiadas áreas como para resultar sencillo. No es necesario tener grandes conocimientos técnicos, tampoco ser un experto en leyes, pero es importante tener, al menos, una ligera idea sobre el negocio que quieres montar, su funcionamiento y mercado, no se puede ir a ciegas y, aunque efectivamente no es como montar una tienda física, tienes que darte de alta en la Seguridad Social y en Hacienda.

En este artículo no se va a hacer una guía de cómo montar un eCommerce, sino que se va a abordar uno de los aspectos más importantes del comercio online: la ciberseguridad. Y no se va a hacer desde un prisma ultra técnico incomprensible para el gran público, sino desde una visión más amplia que ayude a quien quiera montar un eCommerce, a quien ya lo tenga o simplemente a usuarios que quieran saber más sobre la seguridad en los sitios a los que compran.

La ciberseguridad es rentable

Vamos a empezar hablando desde el punto de vista teórico, incluso comercial. Pueden parecer conceptos poco relacionados, pero ciberseguridad y rentabilidad son dos caras de una misma moneda.

Según el último informe Total Retail de la consultora PwC, España es un país muy atrasado en materia de comercio electrónico: mucha menos población compra por Internet que en países europeos y no digamos ya en Estados Unidos. Sigue habiendo recelos entre una tienda física, a la que se puede acudir en caso de problema, y lo etéreo que parece el comercio online. Tanto es así que sólo la mitad de los españoles reconoce haber adquirido algún producto por medio de Internet, y de ellos sólo el 7% lo hace de forma frecuente.

Por eso, transmitir que tu comercio es seguro es un punto fuerte para el cliente. Si consigues que la ciberseguridad sea una de tus señas de identidad, ninguna venta se perderá por miedo a introducir tu tarjeta.

Otra obviedad: ciberseguridad es fortaleza, fortaleza es continuidad. Dicho de otro modo: ¿os imagináis un comercio electrónico que deja de vender en Navidad porque un ciberataque consigue echarlo abajo? Si tu tienda online es robusta, podrás operar sin problema los 365 días del año. Pero si no has prestado atención a la seguridad, puedes quedarte fuera de servicio en el momento de mayor facturación.

Hacer las cosas bien en materia de ciberseguridad desde el día uno, te permitirá dedicarle muy poquito tiempo a tu día a día como gestor de una tienda online y de este modo poder centrarte en lo que realmente sabes: vender el producto. Por eso, una vez más, ciberseguridad es rentabilidad.

Y, sin querer vender las soluciones de nadie, hay que poner esta parcela en valor. Igual que normalmente la gente acude a un gestor para que le haga el papeleo, no estaría de más acudir a una empresa especializada en ciberseguridad para una auditoría de vez en cuando.

Formas de montar un ecommerce

Siendo muy muy escuetos y simplificando al máximo, se puede montar una tienda online de dos maneras: apostando por un desarrollo propio o por una solución ya existente.

Un desarrollo propio posee numerosas ventajas desde el punto de vista de la flexibilidad, tendremos absoluta libertad y, en este sentido, podremos hacer prácticamente lo que queramos. Mejor dicho, lo que sepamos (en caso de desarrollar nosotros) o lo que podamos pagar (en caso de contratar a una empresa).

Las soluciones existentes se pueden dividir, a su vez, en dos opciones: los proyectos open-source y los de pago. Los primeros, denominados de código fuente abierto, son los que más volumen presentan a día de hoy, siendo las empresas Prestashop y Magento las que lideran el mercado. Por su parte,

los de pago, también tienen representantes muy poderosos, un buen ejemplo es Shopify, una plataforma utilizada, entre otras marcas, por Hawker.

Pero, ¿cuál de las dos alternativas es más segura? El debate es amplio e interesante. Un desarrollo propio pudiera parecer que tenga más garantías para el usuario medio, ya que al no depender de otros tienes la salvaguarda de que nadie te dejará una ventana abierta.

Sin embargo, hay dos problemas de base. El primero es que la ciberseguridad no siempre se mete en el ciclo de vida de desarrollo de software: si has encargado un proyecto con un determinado plazo de entrega, el objetivo será tenerlo en esa fecha, no que sea seguro en esa fecha.

En segundo lugar, un desarrollo propio es sinónimo de soledad: tus problemas no siempre los tendrá otra persona, dependerás de tu desarrollador, puede haber errores humanos sin testear…

¿Eso significa que ir a proyectos ya existentes es más seguro? Tampoco. Los proyectos open-source, por ejemplo, tienen comunidades de usuarios detrás apoyando, que hacen avanzar al proyecto y lo hacen más sólido. Estas circunstancias permiten una rápida resolución de los problemas de vulnerabilidad detectadas, aunque al mismo tiempo, también hace que sean más atractivos a ojos de cibercriminales: si consigues vulnerar Prestashop,

consigues acceder a millones de comercios electrónicos de una sentada. Exactamente lo mismo para proyectos de pago. Hay noticias casi cada semana de vulnerabilidades en las principales plataformas de eCommerce.

En definitiva, no hay una solución ideal. Pero esto no es algo propio del comercio online, también ocurre con el comercio tradicional. Una verja de metal o una alarma electrónica no te garantizan la ausencia de robos.

Alojamiento

Otro punto muy importante de la ciberseguridad en comercios electrónicos es dónde se aloja el proyecto. Nuevamente hacemos una simplificación de la realidad y debatimos entre alojamiento en un tercero o alojamiento in-house.

La opción de alojamiento externalizado es la más habitual y "comprar un 1-and-1" ya forma parte del acervo popular. Esto supone confiar en la fortaleza de la empresa que escojamos. Eso está bien, te planteas, porque si sufren un hackeo la pérdida de prestigio y dinero será de ellos... ¡Mentira! Tus clientes lo único que verán es que tu tienda online ha sido hackeada, con lo cual las iras y la mala imagen serán para ti.

Alojar la web en servidores propios puede parecer poco viable de primeras, pero si el volumen de la tienda online crece puede ser recomendable. Eso sí, recomendable únicamente si tienes conocimientos suficientes de ciberseguridad o si confías en una empresa que te ayude a montar la estructura. Los mismos problemas de un desarrollo específico son achacables a un servidor propio.

No solo ciberseguridad para tiendas online

Hay que pensar que la ciberseguridad para eCommerce no tiene demasiadas cosas ajenas a la ciberseguridad que aplicaríamos en nuestros lugares de trabajo o en nuestros hogares.

No vamos a ir a cosas básicas como tener un password del módem robusta o no dejar las contraseñas escritas en post-it, que este eBook está lleno de aportaciones de grandes personalidades de la ciberseguridad y ellos son los que tienen que dar los buenos consejos. Sin embargo, hay que tener en mente que aquí, en el comercio online, algunos problemas se magnifican. Como muestra un botón: utilizar un procesador de textos crackeado puede ser la puerta a malware, software malicioso que podría acabar afectando a

tus usuarios. O no instalar las actualizaciones recomendadas, por ejemplo, puede ser otro vector de riesgo.

Módulos de pago: el kit de la cuestión

Hay un apartado muy muy concreto pero que, por su importancia, es necesario incidir en él. Es lo que vamos a llamar "la teoría del champú": se puede ahorrar en todo, menos en champú.

Pues bien, el champú de la ciberseguridad en eCommerce es el módulo de pago. Existen cientos de módulos de pago para todas las plataformas de comercio electrónico que se han visto, además de los módulos desarrollados para software propio. Se puede ahorrar en formularios de contacto, en plugins para redes sociales y cosas así, pero jamás conviene ahorrar en la parte de la plataforma que gestiona el pago.

Si no tenemos seguridad en el apartado más crítico de la operación, que no es otro que cuando el cliente confía sus datos bancarios en nosotros, no tenemos seguridad en nada. Y ojo, que no es cuestión de que por tener un módulo inseguro nos vayan a robar al momento: pueden estar obteniéndose datos durante meses o años y producirse un ataque cuando la cantidad de información sea gigante.

Conclusiones

Siempre se apela al sentido común, cosa obvia, pero en este caso el artículo va a concluir haciendo referencia al sentido 1.0. Es decir, si quieres que tu eCommerce sea seguro, empieza por aplicar todas aquellas cosas que funcionarían en un comercio de toda la vida.

Es indudable que no existe tienda física en el mundo en la que un empleado cualquiera tenga acceso a absolutamente todo, incluyendo nuestras cuentas o la caja fuerte. Tampoco parece seguro dejar a la vista los datos de tus clientes, utilizar una cerradura muy barata o dejar las ventanas abiertas por las noches, por poner tres ejemplos.

Pues bien, lo mismo con un eCommerce. Si nuestra tienda online es fuerte en materia de seguridad, tendremos mucho terreno ganado.

Eduardo Sánchez

Director de Marketing de RegaloOriginal.com

Blogger en www.eduyeriviajes.com

www.asnefproteccion.com