S2 GRUPO News

YOU ARE BEING WATCHED

ADEMÁS

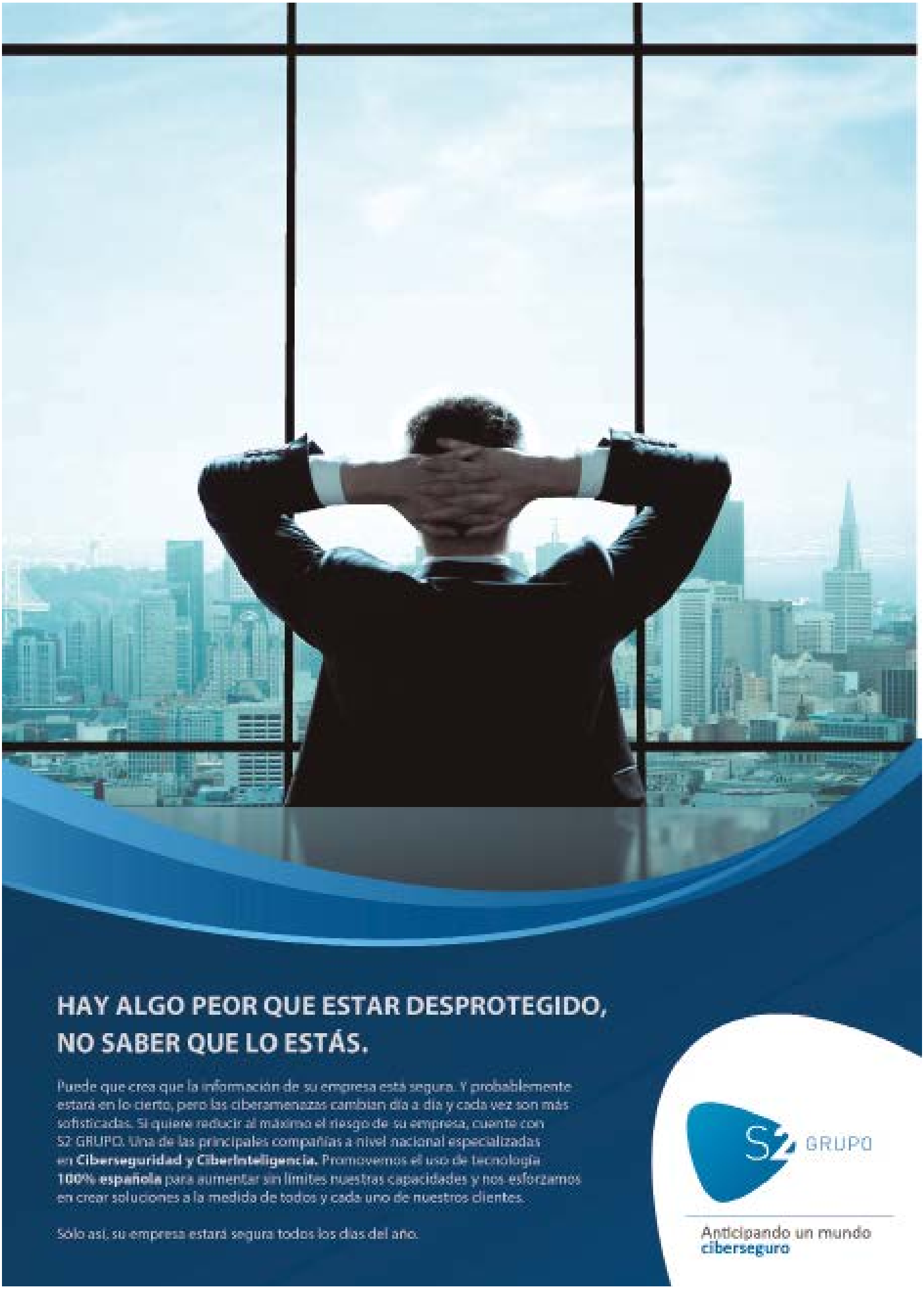
MATAR POR INTERNET

CIBERACOSO: UN CASO REAL CON FINAL LEGAL

CÓMO RECUPERAR CONVERSACIONES BORRADAS EN WHATSAPP

S2 GRUPO

Anticipando un mundo ciberseguro


HAY ALGO PEOR QUE ESTAR DESPROTEGIDO,
NO SABER QUE LO ESTÁS.
Puede que crea que la información de su empresa está segura. Y probablemente estará en lo cierto, pero las ciberamenazas cambian día a día y cada vez son más sofisticadas. Si quiere reducir al máximo el riesgo de su empresa, cuente con S2 GRUPO. Una de las principales compañías a nivel nacional especializadas en Ciberseguridad y CiberInteligencia. Promovemos el uso de tecnología 100% española para aumentar sin límites nuestras capacidades y nos esforzamos en crear soluciones a la medida de todos y cada uno de nuestros clientes.
Sólo así, su empresa estará segura todos los días del año.
S2 GRUPO
Anticipando un mundo ciberseguro

SUMARIO

6 / EDITORIAL

www.securityartwork.es

8 / SALUD, DINERO, AMOR Y... ¿CIBERSEGURIDAD?

12 / MATAR POR INTERNET

18 /CONFIANZA

20 / YOU ARE BEING WATCHED

24 / UN FACTOR CLAVE PARA PREVENIR PROBLEMAS DE SEGURIDAD

28 / UN NUEVO BLANCO FUTURO PARA CIBERATACANTES: "LAS CIUDADES INTELIGENTES"

34 / ORGANIZACIÓN DENTRO DEL MERCADO NEGRO

38 / ¿AUTOMÓVILES VULNERABLES A CIBERATAQUES?

42 / ECALL A PARTIR DE ABRIL DE 2018

44 / UN ARMA MUY PODEROSA DE CIBERATAQUE: CONOCIMIENTO IT + CONOCIMIENTO INDUSTRIAL

www.hijosdigitales.es

48 / CIBERACOSO: UN CASO REAL CON FINAL FELIZ (Y SOLUCIÓN LEGAL)

52 / ¿CÓMO PUEDO GRABAR LAS CONVERSACIONES QUE MANTENGO EN MI MÓVIL?

54 / CÓMO UTILIZAR WHATSAPP SIN QUE CAMBIE NUESTRA ÚLTIMA HORA DE CONEXIÓN

56 / HELLO BARBIE, EL CONFLICTO ENTRE LA PRIVACIDAD Y LOS AVANCES TECNOLÓGICOS

58 / ¿SÁBES QUE ES UNA CUENTA CONMEMORATIVA EN FACEBOOK?

60 / PUEDES UTILIZAR GOOGLE PLUS PARA CONOCER LA UBICACIÓN DE TUS HIJOS

64 / CÓMO ACTÚA UN DEPREDADOR SEXUAL DE MENORES EN INTERNET

68 / QUÉ DENUNCIAR EN FACEBOOK Y CÓMO HACERLO

72 / RAMSOMWARE: EL SECUESTRADOR DE NUESTROS ARCHIVOS

74 / NO TE FÍES DE LAS FALSAS APARIENCIAS

76 / CAMBIA EL USUARIO Y CONTRASEÑA POR DEFECTO DE TU CÁMARA IP

78 / ¿SOSPECHAS QUE HUSMEAN EN TU TELÉFONO?

EDITORIAL

PROTEGEMOS EL

Cuando nos embarcamos en este fantástico proyecto, S2 Grupo, no nos podíamos imaginar que conseguiríamos, en tan sólo unos años, ser un referente a nivel nacional en materia de CiberSeguridad y CiberInteligencia.

Nuestra premisa, dar un servicio integral de calidad a nuestros clientes, nos ha llevado a convertirnos no sólo en un prestigiado proveedor de CiberSeguridad, sino en un socio estratégico para muchas compañías nacionales e internacionales.

Somos conscientes de que la seguridad, en cualquier ámbito de la vida, es un activo fundamental y mucho más ahora en el entorno de hiperconectividad en el que nos encontramos. Por ello, hemos querido ir más allá en nuestra aportación a la sociedad y hemos puesto en marcha iniciativas que aporten valor y conocimiento a las personas.

"Protegemos el mundo en el que vives", es el principio bajo el que enunciamos nuestra aportación al bienestar general, puesto que nadie concibe, hoy, un mundo sin tecnología. Una de nuestras grandes aportaciones es el proyecto **ProtegITs®,** cuyo objetivos son, por una parte, **concienciar a la sociedad** de la necesidad de realizar un uso correcto de las

José M. Rosell y Miguel A. Juan. Socios directores.

MUNDO EN EL QUE VIVES

nuevas tecnologías y por otra, **proteger a colectivos vulnerables,** como son los niños, en la utilización de estas tecnologías. En este sentido, venimos ayudando desde 2009 a más de 5.000 niños y niñas. En la misma línea, nuestro **Blog Hijosdigitales.es,** con más de 10.000 visitas diarias de todo el mundo, se ha consolidado como un punto de encuentro de padres e hijos para fomentar el uso seguro de la tecnología.

Otra de nuestras aportaciones es **SecurityArtWork,** plataforma digital dirigida a profesionales del sector, que cuenta ya con miles de seguidores en el mundo. Un camino más para compartir conocimiento con un único fin: la ciberprotección de las personas.

Comprobar cómo el trabajo que estamos desarrollando comienza a formar parte de la realidad cotidiana, es para nosotros la mayor satisfacción de nuestro día a día y, a su vez, el motor que nos mueve para seguir mejorando y así, ofrecer las respuestas que la sociedad nos demanda para seguir creciendo.

SALUD, Y ...¿CIBER

Por Virginia García-Abad

Qué título tan pretencioso, ¿verdad? Algunos de vosotros ya habréis reflexionado sobre el tema que plantea este post, pero es posible que muchos de los lectores consideren que el título sugiere una situación exagerada y fatua. A continuación comparto con vosotros algunos datos recopilados durante la fase de investigación previa a escribir este artículo.

La ciberseguridad mueve cada vez más dinero a nivel mundial, para muestra las siguientes cifras (datos extraídos del informe realizado por el Center for Strategic and International Studies (CSIS) y McAfee , julio 2014):

> Impacto global de la ciberdelincuencia: aproximadamente 445.000 millones de dólares.
>
> Impacto económico de la ciberdelincuencia en las empresas: 400 millones de dólares
>
> Las pérdidas globales vinculadas a violaciones de "información personal" podrían llegar a 160.000 millones de dólares.

Por otro, lado el uso de las tecnologías para encontrar pareja es cada vez más frecuente ya que cada vez más relaciones de pareja comienzan con un contacto vía Internet:

DINERO, SEGURIDAD?

En España existen cerca de 10 millones de solteros y solteras mayores de 20 años, según datos del Instituto Nacional de Estadística (INE). La mitad de ellos, es decir unos 5 millones, utiliza Internet mensualmente como medio para encontrar una relación seria. Esta cifra aumenta un 7% cada año.

> En Estados Unidos casi el 75% de los solteros ha utilizado Internet por lo menos una vez para buscar una pareja.
>
> Del total de parejas que se casan cada año, el 17% se conoció en Internet.
>
> La gran mayoría de los portales más famosos para encontrar pareja en Internet no son gratuitos. Esta industria pasó de generar unos 700 millones de dólares en 2007 a 1900 millones de dólares en el 2012.

Nuestras relaciones personales forman parte de nuestra intimidad, y los aspectos relacionados con éstas se consideran de carácter confidencial. En este ámbito, cobra especial relevancia para la persona o personas involucradas el control de su privacidad. Algunas de estas cuestiones, como por ejemplo la orientación sexual, incluso están protegidas por la legislación vigente.
Parece claro que existen vínculos entre el dinero, el amor y la seguridad pero, ¿qué relación existe entre la salud de las personas y la ciberseguridad?
Si pensamos en la tecnología que soporta el funcionamiento de herramientas sanitarias, nos encontramos una gran variedad de entornos. Por ejemplo, los sistemas de información RISC (también conocidos como sistemas de gestión de imagen médica) que centralizan las imágenes médicas de diferentes orígenes y tipologías (radiologías, TAC, ecografías, RNMs,…), los implantes médicos (marcapasos, placas, implantes cocleares,…), las sondas (para el suministro de insulina, catéter, monitorización cardiovascular,…) y por supuesto las posibilidades de telecirugía o cirugía remota, que permite realizar operaciones quirúrgicas desde emplazamientos geográficamente distantes.
Parece claro que la dependencia actual entre la tecnología y la salud es, a día de hoy, relevante. Muchos de estos tratamientos ya disponen, o dispondrán en un futuro cercano, de opciones que permitan el uso de sus funcionalidades desde conexiones inalámbricas, siendo obvio la importancia de garantizar su seguridad. La tecnología favorece y condiciona la evolución de la medicina ofreciendo mejoras relacionadas con la rapidez, sencillez de obtención y fiabilidad de los resultados médicos. En la actualidad las universidades ya disponen de grados (Ingeniería de la Salud, Ingeniería Biomédica, etc.) y máster de varios tipos relacionados con la biomedicina.
También el mundo del celuloide ya ha mostrado o imaginado cómo se realizaría un ataque hacker a un marcapasos (no vamos a desvelar la serie donde

se puede ver esto) y líderes mundiales han tomado medidas de seguridad relacionadas con su salud (Cheney, el que fuera vicepresidente de EEUU con Bush, solicitó que le desactivaran las funcionalidades relacionadas con las comunicaciones inalámbricas de su marcapasos, para evitar posibles ataques hacker).

Nos encontramos pues en un momento significativo para las relaciones entre la tecnología y la salud.

Pero, ¿cómo nos preparamos los especialistas de la ciberseguridad? ¿Y los ciberatacantes? A día de hoy pocos dispositivos médicos incluyen medidas que permitan garantizar la seguridad de la tecnología que utilizan. Hasta ahora los fabricantes han priorizado otros aspectos como el uso de materiales compatibles con el cuerpo humano o crear soluciones de tamaño reducido, dejando de lado temas como la seguridad de los dispositivos médicos. No obstante, es ahora cuando tenemos que comenzar a buscar soluciones sólidas que garanticen la salud sin olvidar la seguridad.

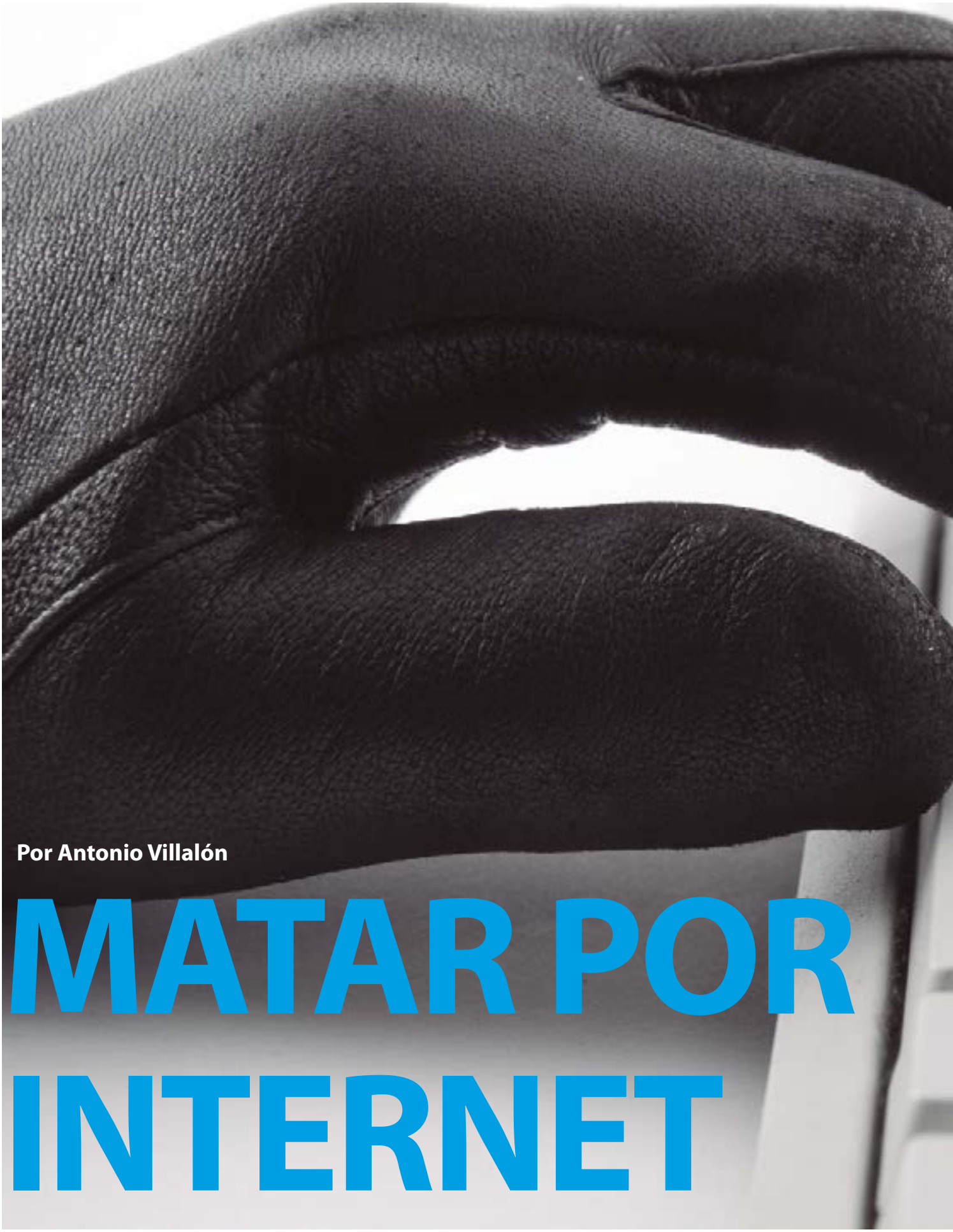
En este punto no puedo dejar de preguntarme como profesional de la ciberseguridad qué se considerará más importante: ¿los datos sensibles de un banco o los de un hospital? ¿Cuál sería el riesgo residual para un activo informático que contenga información crítica sobre la salud de los pacientes? ¿Cómo se definiría un plan de continuidad de negocio que tuviera que garantizar la contingencia de los implantes médicos? ¿Qué medidas técnicas se implantarán en los dispositivos médicos para garantizar su seguridad sin perjudicar su funcionalidad?

Desde mi punto de vista garantizar la salud de las personas debe estar por encima del fraude financiero y se me ocurren algunas soluciones a estas preguntas, pero de momento lo único que pretendo es levantar la mano en sentido figurado y proponer un tema de reflexión.

Si la evolución de las tecnologías y sus aplicaciones sigue creciendo al ritmo actual, es muy probable que en poco tiempo la seguridad de la información adquiera una posición crítica entre nuestras prioridades personales como un componente vital en la salud, el dinero y en el amor, quizá hasta formando parte de uno de nuestros deseos principales.

Espero que los profesionales de la biomedicina y de la seguridad sigamos un progreso alineado, que permita cubrir las necesidades de la salud sin olvidar la ciberseguridad, ofreciendo soluciones no sólo adecuadas desde el punto de vista sanitario sino también seguras.

14
12



Por Antonio Villalón

MATAR POR INTERNET

Hace unas semanas quedamos unos antiguos amigos para tomar unas cervezas en Madrid; viejos conocidos con los que en su momento compartí muchas noches conectado, y de los cuales algunos seguimos aún hoy trabajando en temas de seguridad. Con unas copas todo es más distendido, y hablando con Javi (nombre ficticio, of course) sobre cómo cambia todo con los años y las vueltas que da la vida, me estuvo contando cosas que, sinceramente, me dejaron un poco fuera de juego.

Y es que lo que estaba investigando en su trabajo (dirige la parte de seguridad de una empresa de automatización agrónoma) era cómo "ciberproteger" al ganado, porque matar animales por Internet es técnicamente posible aprovechando granjas conectadas a la red; esto lo habían investigado… y lo estaban probando. Por supuesto, le pedí que escribiera un post para nuestro blog, de forma anónima, y lo que me remitió me dejó más fuera de juego todavía que lo que me contó esa noche… Ahí va, juzguen ustedes mismos.

Matar a un animal en el ámbito físico es fácil, sobre todo los que no están sometidos a un control humano directo: si me acerco a un rebaño de ovejas con el pastor delante e intento degollar a una de ellas, seguramente el buen hombre o sus mastines acabarán conmigo. Si hago eso mismo en alta montaña, donde el ganado puede pasar días sin vigilancia humana —y si no están los mastines cerca, dicho sea de paso— la oveja no tiene nada que hacer. Es habitual, en zonas frías del norte de España (me vienen a la cabeza la zona oeste de Zamora y de León, el este de Galicia, la Cordillera Cantábrica…), dejar el ganado en las montañas durante días —semanas si la nieve impide subir a visitarlo—; aunque hace años los animales campaban a sus anchas, en la actualidad lo más normal es confinarlos en corrales donde, de manera automática, se les suministra agua y alimento, y además se les protege físicamente con cámaras y alarmas (el robo de ganado está a la orden del día). Evidentemente, estos sistemas de seguridad o de abastecimiento son completamente autónomos, e incluso se alimentan con energía solar para no depender de generadores de gasóleo. La duda que un técnico se plantea es: ¿habrá entornos de abastecimiento manejados por sistemas de control industrial y conectados a Internet? La respuesta es sí. Pero, ¿qué tiene que ver esto con la seguridad? Muy sencillo; hay animales que comen mientras tienen hambre, dejando de hacerlo una vez están saciados aunque tengan comida a su alrededor —por ejemplo, los gatos—, mientras que otros son capaces de comer

hasta reventar, como muchas razas de perro.
Un término medio son las vacas: el ganado vacuno pasta habitualmente de forma tranquila, pero si tiene hambre es capaz de hincharse demasiado (y eso sabemos que sienta mal). Si tenemos un rebaño sin comer ni beber durante un par de días y posteriormente les dejamos pastar, comerán mucho más de lo que deben. Y si ese alimento es grano, no hierba, y encima no les damos agua hasta que no han comido, sucede una cosa curiosa: la vaca comerá mucho grano porque tiene hambre, lo que incrementará su sed. Si cuando haya comido mucho grano, le dejamos beber agua, beberá mucha agua, que al mezclarse en el estómago del animal con la gran cantidad de grano producirá un efecto, digamos, curioso: el grano se hinchará y el estómago de la vaca reventará. ¿Y? Podemos intentar hacer esto de forma remota; para lograrlo sólo necesitamos unas cuantas cosas: un corral aislado sin presencia humana diaria, de esos del norte de España, con unas tolvas de grano y unos depósitos de agua controlados por SCADA y que ese mismo SCADA esté conectado a Internet. Lo primero que tenemos que hacer es averiguar si realmente hay sistemas SCADA que controlen la alimentación de explotaciones agropecuarias para, si existen, tratar de explotarlos. Utilizando nuestro buscador favorito, podemos darnos cuenta de que sí que hay sistemas de este tipo y es más, pueden conectarse a Internet, generalmente a través de GPRS o radio; estos sistemas controlan tanto el silo donde se almacena el grano como la bajada de pienso a los comederos, así como la dosificación de agua para las reses. Muchos fabricantes están metiéndose en este negocio, porque parece ser que es bastante rentable (sobre todo en Estados Unidos y Australia) y, dicho sea de paso, lo hacen con la misma alegría y despreocupación con la que se meten en otros negocios donde conectan todo a Internet sin mayores problemas.
Uno de estos fabricantes es Automatic Farm Systems (www.afsproducts.com), estadounidense, cómo no, y uno de sus productos estrella son los silos donde se almacena —y con válvulas se dispensa— el grano así como las trituradoras para para dárselo al ganado. Recordemos, tenemos que evitar que se triture el grano para hacer efectivo el ataque.
Pero al igual que muchos fabricantes industriales, Automatic Farm Systems no fabrica la parte de automatización de sus productos: otros lo hacen por él. En el caso que nos interesa, un integrador destacado es Wilson Groom (http://www.wilsongroom.com), que ha desarrollado software ad hoc que habla con

los productos de AFS, en concreto con los PLC de Allen-Bradley (Rockwell) que éstos incorporan, y que permiten el control de una explotación agropecuaria (¡oh, sorpresa!) desde Internet (literalmente, su publicidad indica que "it can be remotely accessed via any web browser, providing access from a wide variety of PC-based and smartphone platforms"). Vamos, que tenemos que buscar PLC de Rockwell, los usados por AFS, en España, y luego averiguar si se trata de una explotación o no. Resumiendo mucho este proceso, podemos empezar con Shodan buscando las firmas de estos PLC (hay varias, que no vamos a poner aquí, obviamente) y restringiendo nuestra búsqueda a España (country:ES); pero los PLC de Rockwell se usan para muchas cosas. ¿Cómo llegar a determinar que el PLC controla una explotación o no? Hay dos formas: la aproximada es usando Shodan; cuando el buscador es capaz de geolocalizar una IP hasta su ciudad, lo indica, mientras que si no es capaz, el campo está vacío.
Por supuesto, esto no es muy científico, pero bueno, es una primera aproximación. La segunda me gusta más: revisando las especificaciones técnicas de los productos de Wilson Groom (el integrador), disponibles en su web, vemos que esta gente utiliza una aplicación para mantenimiento remoto, contra sus propios sistemas desplegados en campo, que "por seguridad" no va a través del puerto 80, como va el acceso al sistema de control, sino que va por el puerto 9090/tcp, con usuario y contraseña.
Así, tenemos que buscar direccionamientos de PLC Rockwell en España, y que tengan el puerto 9090/tcp accesible. Volcamos la búsqueda de Shodan a un fichero, sacamos las direcciones IP y a partir de éstas buscamos direccionamientos con el 9090 abierto; una línea de script y obtenemos al menos diez dispositivos de control conectados a Internet que cumplen estas condiciones en España, de los cuales siete están sin geolocalización concreta (por debajo del país) en Shodan… estos serán nuestros objetivos principales (si alguno falla, iremos a por los geolocalizados).
La instalación de los PLC de Rockwell tiene, como tantos otros, un usuario web por defecto, con privilegios de control total sobre el sistema (de nuevo, no doy usuario y password, pero se puede obtener de listas de contraseñas públicas disponibles en Internet). Accedemos a uno de ellos que tiene esta configuración y que, aunque Shodan no geolocaliza, localizadores de IP —con la fiabilidad que éstos tienen, que es discutible— fijan en Asturias, fuera de las grandes ciudades y muy cerca del Parque Natural de Somiedo.
Bien, parece que nos vamos acercando. Con las credenciales por defecto accedemos a lo que es un interfaz de un sistema de control de una granja real. Pero, ¿cómo podemos saber que se trata de una granja de ganado vacuno y no de pollos, por ejemplo? Evidentemente, prueba y error. La verdad, no sabemos si aparte de unas vacas hemos perjudicado a gallinas, cerdos u ovejas, aunque creemos que no, porque estos animales no suelen ubicarse lejos de zonas urbanas: los cerdos o las gallinas no se dejan en el monte durante días y días, sino que están en granjas o corrales cerca de los municipios. En fin, es un proceso, como decimos, de prueba y error, pero confiamos en que nuestra granja sea vacuna.
Ahora toca buscar cómo cortar el grano y el agua que el sistema proporciona a los animales, cruzar los dedos y ver si funciona; en los PLC de Rockwell tenemos un usuario por defecto, "administrator", con una contraseña también por defecto, que no vamos a poner aquí pero todo el mundo conoce.

Como en muchas instalaciones, en la nuestra podemos probar si estas credenciales funcionan. Y sorpresa: ¡Sí que lo hacen! ¡Estamos dentro! Ahora tenemos que buscar dónde se controla la dispensación de agua y grano a los animales; para ir rápido, los manuales de la aplicación de control (como siempre, disponibles públicamente en la web del fabricante) nos son de gran utilidad; tenemos que llegar a la pantalla correspondiente:

En ella, en el menú superior del interfaz, tenemos todas las opciones de control de la alimentación; utilizaremos CLOSE tanto para la tolva de grano como para el depósito de agua (Ver esquema del procedimiento).

Vemos que se resalta en rojo el indicador, porque desde luego cortar agua y alimento a los animales, bueno, bueno, no parece a priori… ¿Qué queda ahora? Esperar. Cuarenta y ocho horas, para ser exactos. Trascurrido este tiempo, abrimos el dispensador de la tolva de grano. Esperamos un rato a que los animales coman lo suficiente para quedarse satisfechos… Eso sí, sin agua, y, por ejemplo seis horas después, abrimos el depósito, volviendo a la situación normal.

Ahora sólo queda esperar a que la naturaleza siga su curso. A priori, las vacas habrán comido mucho grano y ahora beberán agua en cantidad, con lo que teóricamente, llegamos al resultado que buscábamos. A los animales les reventará el estómago (esto lo he visto personalmente y no es lo más agradable de mundo, créanme).

Realmente, no podemos saber si hemos tenido éxito, es decir, si hemos matado por Internet. Pero como las noticias vuelan, y más en zonas donde la ganadería es un pilar fundamental de la economía, durante los días posteriores a nuestra prueba consultamos la prensa local de la zona. En el diario "La Nueva Asturias" nos llamó la atención el titular de una noticia: " Casi 100 reses muertas por un fallo mecánico". También nos llamó la atención la misma noticia en "El Cantábrico", un diario del norte.

¿Fallo en el sistema de alimentación? ¿Larga agonía? ¿Casualidad? No lo creo. Parece que hemos logrado nuestro objetivo: matar a través de Internet. Vacas, no personas, por supuesto. Evidentemente este artículo resume bastantes horas de trabajo —no todo sale a la primera, pero tampoco se trata de detallar todos los problemas técnicos o no técnicos que nos vamos a encontrar en el camino— y da una visión muy simplificada del proceso, pero creo que ilustra bien la situación actual. He tratado de ocultar detalles técnicos que faciliten a un tercero repetir el ataque, aunque cualquiera con algo de tiempo y unos conocimientos mínimos podría realizarlo o lo que es peor, automatizarlo por completo…

Es cierto que estas pruebas son un gran problema para el ganadero, al que tratamos siempre de localizar para compensarle anónimamente por nuestros análisis (lo que tiene el tema agropecuario es que somos cuatro gatos y nos conocemos todos), pero creo que la prueba de concepto ha valido la pena. También nos hemos puesto en contacto tanto con el fabricante de los PLC como con la empresa que ha desarrollado los SCADA para informarles de estos problemas, pero en fin, que aunque lo relatado sea solo ficción, si yo fuera ganadero, me preocuparía…

PASO 1

PASO 2

PASO 3

PASO 4

CONF

Por Gonzalo T.

Dice el dicho que 'la confianza da asco'. Esta frase, que se aplica normalmente en tono distendido para describir una característica propia de las relaciones humanas, cobra hoy especial significación en el mundo digital. Y es que la confianza ya no se limita a las relaciones interpersonales, sino que amplía su ámbito de aplicación a las relaciones persona-máquina e incluso máquina-máquina.

Con la llegada de la era digital, Internet y las nuevas formas de comunicación, se nos presentan cada día situaciones, de las cuales la confianza forma parte consustancial. Así pues, acciones cotidianas tales como abrir un email o acceder a una web determinada, implican un ejercicio de confianza que, en ocasiones, realizamos sin ni siquiera ser conscientes y que, lamentablemente pueden llegar a ocasionarnos perjuicios tales como el robo o pérdida de información, chantajes, daño a la imagen personal o corporativa… Aunque dado el perfil de nuestros lectores todo esto puede parecer trivial, casi todos conocemos algún caso, bien sea a través de terceros o de los medios de comunicación, en el cual la confianza mal entendida ha derivado en alguno de los quebrantos mencionados anteriormente.

La gestión de las relaciones de confianza resulta compleja dada su naturaleza, pues cumple en ocasiones las propiedades de asimetría (A confía en B pero B no confía en A) y transitividad (si A confía en B y B confía en C, entonces A confía en C). También cabe destacar que no es igual la gestión de la confianza en el ámbito personal, que se consolida con la cercanía y el tiempo, que en un entorno corporativo. En este último, se establece una relación de confianza entre la empresa y el trabajador, que viene impuesta por la naturaleza misma de la relación contractual entre ambos, y he aquí el problema.

Desde el momento en que damos a un usuario acceso a recursos corporativos, estamos haciendo un ejercicio implícito de confianza, por el cual asumimos el riesgo de que no se va a hacer un mal uso de dichos recursos. En este punto cabe destacar que la confianza puede verse amenazada, no solo por la mala intención de una de las partes, sino también por irresponsabilidad o ignorancia. No se trata de criminalizar al usuario.

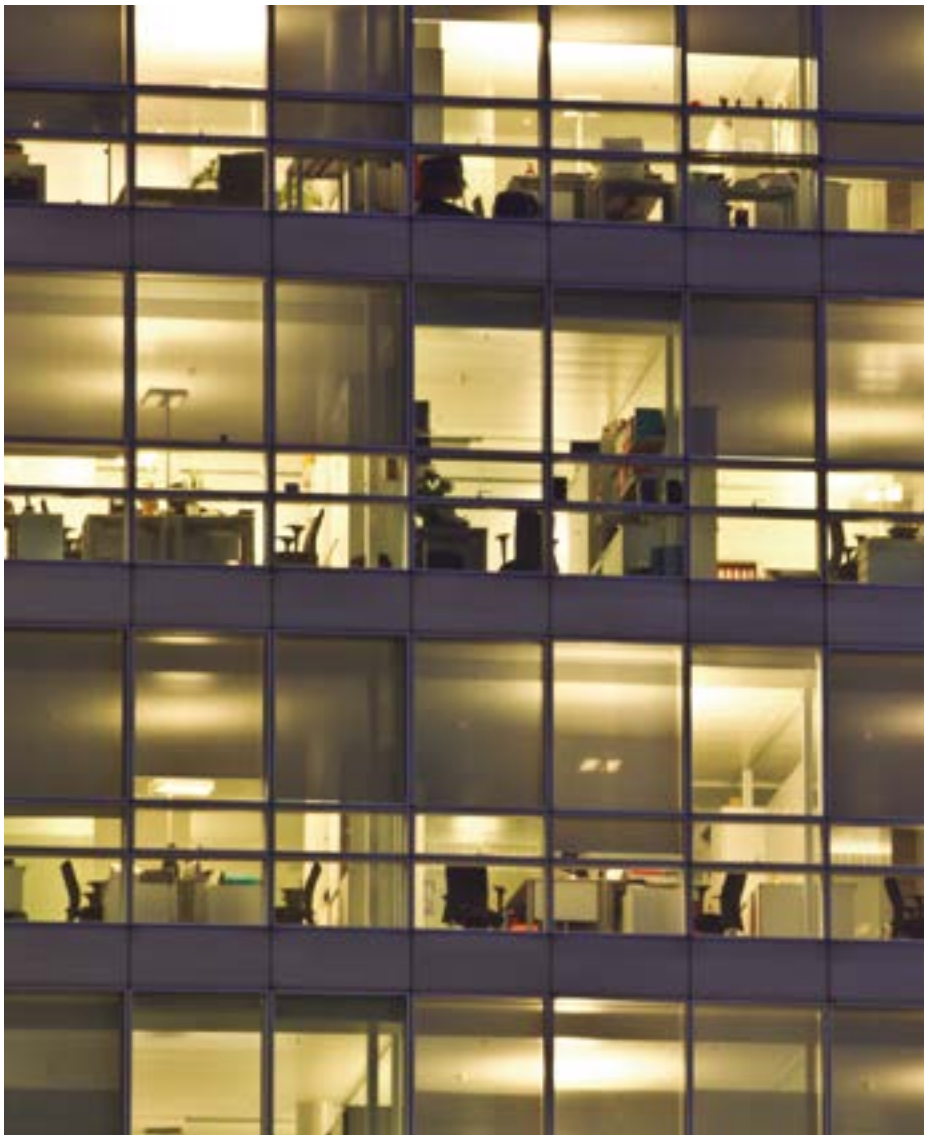
Pongamos por ejemplo, una empresa que proporciona acceso a sus empleados a uno de los servicios corporativos, permitiéndoles el acceso desde fuera de la red de la empresa. En general, los usuarios hacen un uso responsable del servicio en cuestión pero un usuario en particular, se conecta a través de una red insegura, exponiendo así sus accesos a dicho servicio a ataques de tipo Man in the Middle. Si bien no hay una intención expresa del usuario de poner en riesgo la seguridad del servicio, lo cierto es que la confianza implícita depositada en el usuario, se ve mermada por la ignorancia o irresponsabilidad de éste.

Por todo ello, es importante tratar de reducir a su mínima expresión el papel que juega la confianza a la

IANZA

hora de establecer una política de seguridad en entornos corporativos. Aplicar el principio de mínimo privilegio, junto con campañas de formación y concienciación de los usuarios son medidas fundamentales para evitar incidentes que puedan comprometer la seguridad de nuestros sistemas y la información que contienen.

En definitiva, no se trata de desconfiar del usuario, sino de desconfiar de la confianza.



YOU ARE BEING WATCHED

"YOU ARE BEING WATCHED. THE GOVERNMENT HAS A SECRET SYSTEM: A MACHINE THAT SPIES TO YOU EVERY HOUR OF EVERY DAY."

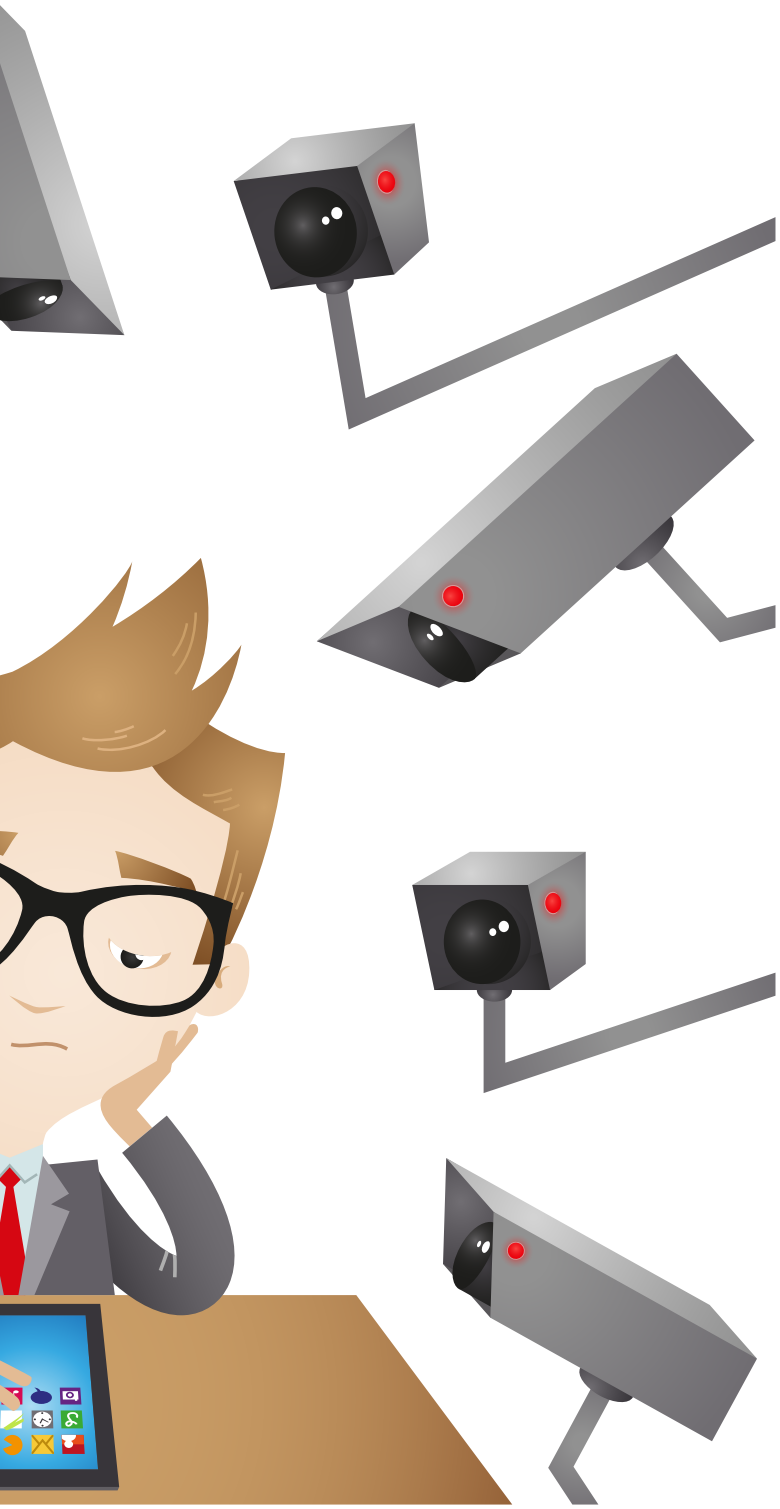
Por Armand Pascual

Un mundo donde estamos vigilados por un juez supremo que controla cada uno de nuestros movimientos. Podemos ser localizados en todo momento. Se puede predecir de manera estadística el futuro. Prevenir crímenes o actos terroristas es factible. Todo está controlado por una suerte de Gran Hermano, sólo que éste no es de carne y hueso. Es una máquina. Una máquina que recoge toda la información de internet, telefonía, imágenes de vigilancia, etc., la procesa y es capaz de entenderla y tomar decisiones. Hablamos de la historia que nos cuenta "Person of Interest" ("Vigilados" en su versión para España), una serie en emisión desde septiembre de 2011 producida por el conocido J.J. Abrams. Aunque el argumento principal es ficticio e introduce elementos que se podrían calificar de ornamentales para darle ritmo y hacerla más atractiva, la serie juega con componentes del mundo real que hacen verosímil la historia.

La filtración del programa de vigilancia PRISM de la NSA en 2013 hizo, si cabe, más realista la trama. No parece en absoluto descabellado imaginar un mundo en el que lo que la serie nos relata es completamente cierto. PRISM es sólo un ejemplo del interés y capacidad de gobiernos y empresas privadas para recopilar y analizar información. Más allá de la legitimidad de sus objetivos (cuestión que no pretendo tratar en este artículo), a nadie escapa ya que debemos ser cautos con aquello que compartimos.

Las tecnologías de la información y las comunicaciones no aparecen sólo en el ámbito privado, también lo hacen en el profesional. Hablo de su uso en oficinas y dispositivos corporativos, pero también en el mundo de la industria. Hoy en día, es difícil imaginar un proceso industrial en el que no intervengan en algún punto estas tecnologías. En la actualidad todo se mide, se controla, se monitoriza. Queremos tener datos en tiempo real de lo que ocurre en nuestras plantas, saber dónde se encuentra cada uno de los camiones de nuestra flota, o conocer el estado de nuestro proceso para poder actuar sobre él de manera remota en caso de que sea necesario. Para ello, la implantación y uso de redes de comunicaciones es imprescindible.

Las bonanzas que todos estos sistemas traen son notables. Incremento de la productividad, aumento de la flexibilidad de los procesos o reducción de costes asociados al control de los mismos pueden ser, entre muchos otros, algunos ejemplos. Por ello, igual que ocurre a nivel personal, la solución no puede pasar por vivir al margen. Eso está claro. Sin embargo, el uso



indiscriminado de todos estos avances trae consigo riesgos asociados para el sector industrial que no debemos pasar por alto.

Conocemos los resultados que puede tener el robo de información de nuestro PC. ¿Qué ocurre si lo extrapolamos al ámbito industrial? ¿Y si en vez obtener fotos de nuestro móvil estamos hablando de obtener secretos industriales estratégicos para nuestra compañía? ¿Y si borrar los datos de nuestro ordenador personal se convierte en detener un proceso crítico para una ciudad? ¿Y si conocer el historial de nuestro navegador se traduce en tener acceso al sistema de distribución de gas de una población? ¿Te parece imposible? Quizás hayas oído hablar de STUXNET…

Razones similares a las que nos obligan a ser prudentes en lo personal, nos deben obligar a serlo en el mundo industrial. ¿Qué motivos justifican que tu sistema esté conectado a la red? ¿Los beneficios que te aporta tienen más peso que los riesgos a los que te expone? Si así fuera, ¿has adoptado las medidas necesarias para reducir esos riesgos al máximo? ¿Estás absolutamente seguro de quién tiene acceso a tu sistema? ¿De qué medidas de control dispones? ¿Existe algún protocolo en caso de incidente? Si has decidido que tu sistema no debe ser accesible a través de la red quizá debas saber que los sistemas de control aislados no existen.

El modo en el que hoy interactuamos con la realidad es muy diferente al de hace apenas unos años. Eso también incluye los procesos industriales. Generamos una ingente cantidad de datos y una gran cantidad de acciones se puede realizar a través de la red. No se trata de caer en un estado de paranoia permanente (o quizá sí…), sino de ser conscientes de cuáles son los riesgos potenciales a los que estamos expuestos. Riesgos que nos afectan directamente como individuos pero también de manera indirecta a través de sistemas que pueden ser críticos para la sociedad en general o para nuestra compañía en particular.

Éste es el mundo en el que vivimos. Las posibilidades y beneficios que nos brinda la tecnología son inmensos. Hagamos uso de las mismas, pero un uso responsable. Conocer el estado de ciberseguridad de los sistemas industriales que nos afectan es, sin duda alguna, el primero de los pasos.

UN FACTOR PREVENIR DE SEG

Por Karina Coste

CLAVE PARA PROBLEMAS URIDAD

Entre una pareja, entre padres e hijos, entre los jefes y sus trabajadores; una buena comunicación es clave para prevenir problemas de seguridad en diferentes ámbitos, sobre todo en el empresarial, donde una de las principales causas de violaciones de datos son las acciones inconscientes e involuntarias de trabajadores de confianza, los también llamados Trusted insiders (inadvertent).
¿Cómo lograr que los trabajadores sean conscientes de que la seguridad de la información es una prioridad para la empresa y que de ellos depende en buen grado? Las campañas de concienciación y los programas de formación son muy importantes pero, ¿son suficientes? Una comunicación continua, de calidad, y bidireccional es el pilar fundamental para lograrlo.

Planificación y desarrollo continuo

No puedes pretender que tu hijo adolescente siga tus recomendaciones para no meterse en problemas si cuando era un niño no te preocupaste en cultivar una buena comunicación con él. Lo mismo aplica para el ámbito organizacional: no basta con enviar un e-mail con las normas de seguridad de la empresa cuando ocurre un incidente o realizar una campaña de concienciación por unos meses y olvidarse del tema.
Si se quiere que la seguridad de la información esté presente en la cultura corporativa, las campañas de concienciación deben formar parte de unas comunicaciones internas planificadas y desarrolladas de forma continua, que mantengan al trabajador informado y realmente comprometido con los intereses de la empresa en general, entre ellos la seguridad de la información. Por otra parte, las nuevas tecnologías avanzan muy rápido y con ellas surgen nuevos problemas de seguridad y medidas para enfrentarlos que deben ser comunicadas de manera constante, oportuna y comprensible a los trabajadores.

Variedad, claridad y gancho

Si quieres mucho a tu pareja pero no le dedicas tiempo ni haces nada divertido que rompa la rutina, corres el riesgo de que un "intruso" o "intrusa" se cuele en tu hogar. Lo mismo puede ocurrir en una organización si solo se utiliza el correo para enviar políticas de seguridad difíciles de digerir.
El correo es un buen canal de comunicación pero no es el único, ni siquiera el más eficiente. Las reuniones cara a cara, la intranet, los blogs, las redes sociales y últimamente las aplicaciones móviles, ofrecen una amplia variedad de opciones que deben aprovecharse al máximo para lograr una comunicación integral y eficiente entre la organización y sus trabajadores. Todos estos canales facilitan y enriquecen el desarrollo de campañas de concienciación y programas de formación en seguridad, sobre todo las redes sociales y aplicaciones móviles porque ofrecen la posibilidad de medir el consumo y la satisfacción de los trabajadores a través del registro de los links marcados, los "me gusta" y los comentarios.
Un título aburrido y una parrafada interminable y llena de términos técnicos complejos suelen espantar a cualquier trabajador, quien seguramente no les dedicará ni tres segundos de su atención, aunque tenga la obligación de leer dicho documento y tenerlo presente en su trabajo diario. Los contenidos que se comunican deben ser cercanos, comprensibles y sobre todo, tener gancho, si se quiere que sean entendidos y recordados. Noticias, twitters, posts, vídeos, recomendaciones, casos de la vida real, infografías y tutoriales con contenidos gráficamente atractivos, redactados de manera sencilla y creativa, son algunas de las herramientas de comunicación que se pueden utilizar para difundir las políticas de seguridad de una organización.

En ambos sentidos

Si quieres que tu hijo te preste atención y sea receptivo cuando le hablas sobre temas serios como su seguridad, tú también debes ser capaz de escucharlo y prestarle la misma atención que estás exigiendo cuando te hable a ti. Este principio también es básico en las comunicaciones internas de las empresas.
Si las comunicaciones solo se limitan a la transmisión unidireccional de mensajes por parte de la organización y no se fomenta ni se valora la participación de los trabajadores como emisores de información, la empresa seguramente no podrá evaluar correctamente la efectividad de sus comunicaciones y peor aún, es probable que no detecte a tiempo posibles problemas de seguridad.
Es importante que la comunicación fluya bidireccionalmente de forma vertical y horizontal en la jerarquía de la empresa. En este proceso es imprescindible que sean los líderes quienes promuevan y valoren el intercambio de información entre todos los trabajadores. Para ello contamos con nuevas tecnologías, como las Redes Sociales y las aplicaciones móviles, que amplían enormemente la interacción entre usuarios y que permiten compartir mucha información.

La comunicación entre los trabajadores de una empresa, es esencial para garantizar la seguridad de la información.

UN NUEVO BLANCO FUTURO PARA CIBER-ATACANTES: "LAS CIUDADES INTELIGENTES"

Por Servilio Alonso

Gran parte de las ciudades del mundo son cada vez más "inteligentes", lo cual se convierte en nuevos blancos para ciberatacantes. Las ciudades han ido incorporando nuevas tecnologías durante varios años, pero últimamente la tasa de tecnologización ha aumentado significativamente y muchas ciudades de todo el mundo son cada vez más inteligentes. Las nuevas tecnologías, junto con una conectividad más rápida y fácil, permiten a las ciudades optimizar recursos, ahorrar dinero y al mismo tiempo ofrecer mejores servicios a sus ciudadanos.
Una "ciudad inteligente" (Smart city en inglés) se puede definir como una ciudad que usa tecnología para automatizar y mejorar servicios de la comunidad, incrementando el nivel de vida de sus ciudadanos. En la ciudad inteligente del futuro todo estará conectado y automatizado. Esto todavía no es una realidad, pero mientras tanto, muchas ciudades ya están elaborando grandes presupuestos para poder ser más inteligentes en un futuro cercano.
Pero, ¿qué pasaría si uno o más servicios altamente dependientes de tecnología no funcionaran? ¿Cómo se verían afectados los desplazamientos dentro de la ciudad sin el funcionamiento de los sistemas de control de tráfico, sin semáforos o sin transporte público? ¿Cómo responderían los ciudadanos a un suministro inadecuado de agua o electricidad, a calles oscuras, o simplemente a una interrupción del servicio de recogida de basuras en verano con la consecuente proliferación de olores, insectos, ratas, patógenos, etc.?

¡La ciudad "inteligente" sería un CAOS si uno o más servicios altamente dependientes de tecnología dejaran de funciona"

Desafortunadamente esto podría ocurrir muy fácilmente debido a que muchas ciudades están implementando nuevas tecnologías sin tener en cuenta que estos estos sistemas son vulnerables desde el punto de vista de la ciberseguridad y por tanto están expuestos a ciberataques. Normalmente todos los aparatos y sistemas se someten a rigurosas pruebas de funcionalidad, resistencia a condiciones atmosféricas etc., pero prácticamente no se les somete a ningún test de intrusión en el que algún hacker pueda modificar y alterar sus condiciones de funcionamiento.
¿Qué hace que una ciudad sea más inteligente? ¿Qué tecnologías se usan? ¿Qué vulnerabilidades podrían presentar estas nuevas tecnologías desde el punto de vista de la ciberseguridad? Algunas de las tecnologías que podrían contribuir a incrementar la inteligencia de la ciudad y sus posibles vulnerabilidades serían:

•Control de tráfico inteligente: Semáforos y señales que se adaptan basándose en el volumen y las condiciones de tráfico actuales. Se detecta el tráfico actual y la información en tiempo real se utiliza para coordinar y mejorar el flujo en calles, carreteras, cuestas, etc.
Posible vulnerabilidad: Es posible introducir datos falsos en los sistemas de control de tráfico y configurarlos con opciones y tiempos incorrectos en los semáforos, señales de tráfico…, y así sucesivamente.

•Estacionamiento Inteligente: Los ciudadanos pueden utilizar una aplicación de estacionamiento para encontrar plazas de aparcamiento disponibles, revisión de precios y sus cambios según la hora del día, la disponibilidad, la ubicación, etc.
Posible vulnerabilidad: Vulnerar esta aplicación podría generar un colapso en un parking concreto, desviando todos los conductores a dicho parking, o incluso haciendo que siempre acudieran a cierto parking con mayor frecuencia de forma que sus propietarios percibieran mayores beneficios.

•Alumbrado público inteligente y Gestión de energía inteligente (Smart Grid): El alumbrado público inteligente se gestiona de forma centralizada. Las luces de la calle se pueden adaptar a las condiciones climáticas, pueden reportar problemas, o se pueden automatizar por hora del día. Las luces de la calle se pueden incluso apagar y encender dependiendo de la detección de vehículos y personas en movimiento. Por otro lado, una red inteligente (Smart Grid) puede entregar energía dependiendo de las necesidades. Los contadores inteligentes pueden comunicarse con la red inteligente para programar un suministro de energía a una hora específica con un menor coste económico. La red inteligente puede incluso apagar el calentador de agua de nuestra casa durante las horas pico, en las que la electricidad es más cara. Los edificios inteligentes utilizan el mismo principio para conservar energía y comprar electricidad cuando las tasas son "low cost".

Posible vulnerabilidad: Muchos proveedores permiten que se dé acceso privilegiado para cualquier persona a un dispositivo o sistema conectado a una red local, ya que asumen que la red interna es segura. Normalmente muchos implementan sistemas inalámbricos y protocolos de comunicación por cable con poca o sin seguridad. La mayoría de los nuevos dispositivos son inalámbricos (como los contadores inteligentes, las farolas, sensores, semáforos, tuberías inteligentes, cámaras de tráfico y vigilancia etc.), lo que hace que sean fáciles de implementar, pero también fáciles de hackear si la comunicación no está debidamente encriptada. Por otra parte, las conexiones vía cable requieren acceso físico y eso hace que sean más difíciles de hackear, pero algunos de estos sistemas cableados como PLC (Power Line Communication) están más expuestos y es más fácil acceder a ellos. Un atacante tan solo tiene que conectarse a la red eléctrica para obtener acceso y tener todos estos dispositivos a su merced.

•Transporte público inteligente: Se proporciona a los ciudadanos la información en tiempo real acerca de los horarios (bus, tren y metro) y posibles retrasos. Los pagos sin contacto físico permiten a los ciudadanos pagar con facilidad, incluso utilizando un teléfono inteligente.
Posible vulnerabilidad: Con solo mostrar información incorrecta mediante la manipulación de los sistemas de información de transporte público, es posible influir en el comportamiento de las personas para causar retrasos, hacinamiento, y así sucesivamente. Por ejemplo, falsificando un retraso en una línea de metro, los atacantes pueden provocar que la gente se concentre en otra línea provocando una avalancha de personal. También un atacante podría alterar los sistemas de pago. Si los sistemas de pago no funcionan, la gente podría viajar gratis o incluso miles de personas podrían saturar con quejas los mostradores de atención al cliente o las líneas telefónicas.

•Gestión inteligente del agua: Las tuberías inteligentes miden la calidad del agua, detectan fugas, distribuyen el agua y detectan problemas. Técnicas similares se utilizan para gasoductos y oleoductos.
Posible vulnerabilidad: Los ataques sobre los sensores inalámbricos de las tuberías y el envío de datos falsos a la central tendría graves consecuencias en cuanto a medidas tan importantes como la calidad del agua. Cualquier filtración o contaminación no sería detectada e implicaría suministrar agua en mal estado a los ciudadanos, con las consecuencias en la salud de estos.

•Gestión de residuos inteligente: Los sensores en los contenedores de residuos detectan el volumen de basura, el olor y así sucesivamente. La recogida de basura puede ser más eficiente si se descartan previamente los contenedores vacíos y se detiene con anterioridad solo delante de los contenedores que huelen.
Posible vulnerabilidad: Los ataques sobre los sensores inalámbricos de los contenedores y el envío de datos falsos a la central tendría graves consecuencias en cuanto a la recogida de basuras. La basura podría llegar a acumularse en ciertas zonas de la ciudad, con su consecuente impacto sobre la salud de los ciudadanos y sobre el medio ambiente.

•Seguridad ciudadana: Cámaras de vigilancia, sensores de detección de bala y otros dispositivos de seguridad proporcionan información en tiempo real sobre lo que está pasando y dónde. Tecnología de "conteo" de personas, tales como el seguimiento de los teléfonos móviles o comunicación (como WiFi o Bluetooth) se utiliza para determinar el número de personas en un área determinada como una calle, un parque o un edificio.
Posible vulnerabilidad: Las cámaras de tráfico y vigilancia son los ojos de la ciudad y al atacarlos, los atacantes pueden provocarle ceguera a las ciudades inteligentes. No siempre es posible

reiniciar remotamente las cámaras. Además, los ataques de denegación de servicio se pueden hacer persistentes mediante la modificación de firmware. La ciudad se quedaría sin vigilancia. Estas tecnologías están respaldadas por:

•Sistemas de gestión de la ciudad: Estos sistemas ayudan a automatizar diferentes tareas de administración de la ciudad.
Posible vulnerabilidad: Un atacante podría manipular la información del mapa de localización y las órdenes de trabajo para enviar trabajadores públicos o de alguna contrata para hacer una intervención sobre canalizaciones de gas, agua o cables de comunicación, con la intención de dañar esas instalaciones.
•M2M (Machine to Machine): Con el fin de hacer una ciudad más inteligente, se necesitan dispositivos (máquinas) que hablen entre sí, de forma que se tomen decisiones de forma automática.
Posible vulnerabilidad: Las nuevas tecnologías están siendo integradas dentro de las viejas tecnologías, las cuales son más vulnerables. Algunos sistemas antiguos requieren de tecnología en medio que haga de traductora de protocolos de comunicación con los nuevos sistemas. Como algunos sistemas no funcionan en los nuevos (los cuales poseen sistemas operativos más seguros), se

utilizan sistemas operativos más viejos y vulnerables. Esto añade complejidad, aumenta la superficie de ataque, y ralentiza la incorporación de nuevas tecnologías. Un claro ejemplo sería el edificio inteligente Burj Khalifa, el edificio más alto y más inteligente del mundo. Los sistemas principales del edifico se ejecutan con el sistema operativo Windows XP, que es viejo, anticuado y menos seguro que los nuevos sistemas operativos. Esto convierte Burj Khalifa en un blanco fácil para posibles ataques cibernéticos.

•Sensores: Usados para todo, los sensores (a menudo sin cable) suministran datos de forma continua a las ciudades inteligentes. Ejemplos: Sensores de tiempo (detectan las condiciones climáticas y envían alertas), sensores sísmicos (situados en puentes y bajo tierra, detectan daños en túneles y en infraestructuras causados por terremotos, envejecimiento u otros problemas), sensores de niveles de polución (detectan e informan sobre niveles de polución en diferentes partes de la ciudad), sensores de olor (para la basura, gas natural…detectan posibles problemas), sensores de inundaciones, sensores de sonido (pueden detectar disparos, alarmas, actividad….etc.).
Posible vulnerabilidad: La mayoría de los sensores utilizan tecnologías inalámbricas fácilmente accesibles. Los ataques que impliquen comprometer sensores y enviar datos falsos pueden afectar directamente a los sistemas, ya que las decisiones y acciones que estos tomen dependerán de datos falsos. Esto podría tener un gran impacto en función de cómo los sistemas afectados utilizan los datos e interactúan con otros sistemas.

•Datos de dominio público: Los gobiernos comparten datos (a veces en tiempo real) para que las personas puedan desarrollar aplicaciones.
Posible vulnerabilidad: Los datos públicos (open data) están disponibles para los atacantes, a veces en tiempo real. Estos datos pueden ayudar a determinar el mejor momento para los ataques, ataques de horario, crear disparadores de ataque, coordinar ataques, y así sucesivamente. Con esto los atacantes no necesitan actuar a ciegas. Pueden actuar de forma precisa basándose en datos reales.

•Aplicaciones móviles: En un ecosistema de ciudad inteligente, las aplicaciones móviles fomentan la interacción entre los ciudadanos y la ciudad. Los ciudadanos pueden obtener información de los sistemas de la ciudad, sensores, y así sucesivamente a través de aplicaciones móviles, y con ello tomar decisiones en función de la información que reciben.
Posible vulnerabilidad: Los atacantes podrían dirigirse a empresas de desarrollo de aplicaciones móviles o simplemente modificar los datos con los que se nutren las aplicaciones. Las aplicaciones móviles son un objetivo importante, ya que los ciudadanos van a tomar decisiones y actuar en base a la información suministrada por esas aplicaciones. Hackear aplicaciones móviles tiene un impacto directo en el comportamiento de los ciudadanos. Por ejemplo, si la aplicación de transporte público está mostrando un retraso en un autobús, un ciudadano puede optar por viajar a trabajar en coche; si la misma decisión es tomada por cientos de personas en una zona de alta densidad poblacional, el resultado es un atasco de tráfico. También muchos servicios están basados en la localización, lo que significa que la suplantación de GPS y otros ataques son posibles. Las personas perciben la información de localización en tiempo real, y si la ubicación es incorrecta, entonces la gente va a tomar decisiones basadas en información incorrecta. La naturaleza del impacto es función de la medida en que una ciudad depende de los servicios afectados.

CONCLUSIÓN

Cuanta más tecnología utiliza una ciudad, más vulnerable a los ataques cibernéticos es, por lo que las ciudades más inteligentes tienen los mayores riesgos. Las tecnologías utilizadas por las ciudades deben ser correctamente auditadas antes de su implementación desde el punto de vista de la ciberseguridad. Cuando a una ciudad inteligente se le suministran datos fácilmente manipulables en los que confía ciegamente, y además esta tiene sistemas fácilmente hackeables y problemas de seguridad por doquier, entonces pasa rápidamente de ser una "ciudad inteligente" a ser una "ciudad estúpida". Esperemos que los responsables tengan todos estos problemas de seguridad en mente.

ORGANIZACIÓN MERCADO

Por Yolanda Olmedo

Cuando se habla de un delito informático, se tiende a pensar en una persona al otro extremo de la red con altos conocimientos técnicos que está intentando lucrarse ilícitamente. Pero lo cierto es que detrás de estos delitos no suele haber una única persona, sino organizaciones complejas con diferentes roles y actores que gestionan, administran y ejecutan sus acciones.

El fraude a través de la red ha tenido una gran evolución, lo que ha ocasionado una sofisticación mayor en la manera de cometer los ciberdelitos utilizando infraestructuras cada vez más complejas. Este aumento en el grado de complejidad implica que los propios delincuentes no pueden abarcar todo el funcionamiento y métodos de ataque sobre una infraestructura u organización.

Al igual que hay en el mundo mercantil desarrollo de software, operaciones de compra/venta, colaboraciones, rivalidades, etc., lo mismo ocurre en el mundo mercantil "negro" de forma paralela. Sin embargo, en esta ocasión hablamos de desarrollo de exploits, compra/venta de exploits y vulnerabilidades, colaboraciones entre organizaciones criminales, etc.

De la misma forma, existe una segregación de tareas definida en la que podemos identificar varios roles claramente, en función de la tarea que realizan en la cadena criminal:

Roles técnicos

En esta categoría están incluidas todas aquellas personas que se encargan de la creación y mantenimiento de los recursos utilizados para cometer las acciones delictivas. Son los encargados de crear las herramientas que se utilizarán para una campaña de fraude. Pueden, por ejemplo, realizar tareas de modificación de un malware, tomando una muestra existente de malware y adaptarla para algún otro objetivo o también desarrollar malware a medida. En esta línea, Kaspersky Lab descubrió que existen escuelas para cibercriminales, donde se ofertan cursos para enseñar a todo aquel que quiera desenvolverse en el mundo criminal. Entre los cursos ofertados, los hay según el tipo de delito del que se trate, destacando "How to be a Hacker", "Kit Spammer" o "How to be a Defacer".

Una variante que está surgiendo del software a medida es la generación de malware genérico personalizable, de modo que la persona o entidad que adquiere el malware tiene la posibilidad de modificarlo y crear tantos binarios como desee, adaptándolo a sus requeri-

DENTRO DEL NEGRO

mientos.
Dentro del grupo de los desarrolladores, podemos separarlos según el tipo que software que se trate:
Malware: son los encargados de la creación y modificación de troyanos, herramientas para propagar infecciones, envío de spam, realizar ataques DDoS (llamados ddosers o flooders), Keyloggers y stealers, encargados de los delitos de robo de credenciales. Dentro de esta categoría, también están incluidos los desarrollos de software de sistemas anti-detección. Consiste en un software malicioso que es capaz de pasar desapercibido entre los sistemas de protección e identificación de intrusos para no ser detectado o dificultar su análisis. Son los denominados packers. Algunas de las técnicas que se utilizan es el cifrado de ciertas partes del software dificultando la obtención de cadenas, detección de ejecución bajo un depurador, detección de herramientas de ingeniería inversa o evitar la ejecución en entornos virtualizados.
Exploits: se encargan de la elaboración de software que se aprovecha de las vulnerabilidades de otras aplicaciones y sistemas. Además, los exploits se pueden vender en packs donde se incluyen varios, cada uno de ellos enfocado a una vulnerabilidad distinta. Entre las distintas vulnerabilidades, se encuentran las de zero-day, que son aquellas para las cuales todavía el fabricante no ha sacado una solución, ya que aún no ha sido detectadas.
Phishing: estos desarrolladores se encargan de la creación de sitios que son una imitación exacta de sitios legítimos (bueno, a veces no son exactas, pero la intención es lo que cuenta).
Paneles de control: son un tipo de software específico cuya tarea consiste en centralizar en una única aplicación la gestión y administración de un cometido delictivo. Por ejemplo, una botnet compuesta por cientos de ordenadores se puede gestionar desde un solo punto con un panel de control.

Roles comerciales

Dentro de la cadena del delito, este rol sería el segundo eslabón. Cobra mayor sentido en los delitos bancarios donde se realizan robos de las credenciales y tarjetas bancarias. Una vez se está en posesión de dicha información, los comerciales son los encargados de transformar los datos bancarios en beneficios. Para ello participan dos actores:
Cashiers: son los encargados de mover las ganancias económicas entre diferentes cuentas. Si la operación es compleja en cuanto a infraestructura, el cashier suele utilizar otro actor para que desempeñe esta función, que son los denominados muleros.
Mulero: son aquellas personas cuya función principal es la del blanqueo de capital. Actúan de intermediarios en la cadena del fraude, llevándose a cambio un porcentaje del beneficio. Un caso muy común son las ofertas de trabajo suculentas para ganar dinero fácil. La oferta de trabajo consiste en recibir una cantidad de dinero en su cuenta bancaria, donde el destinatario se queda con una comisión de un tanto por ciento y el resto lo ingresa en otra cuenta bancaria distinta.
El lado negativo es que los muleros en la mayoría de ocasiones son personas inocentes cuya intención no era la comisión de un delito, sino ganar un dinero extra, por lo que de una manera involuntaria se convierte en engañado y delincuente al mismo tiempo. La finalidad del uso de muleros es complicar y dificultar la investigación del verdadero origen del dinero.

"LA ORGANIZACIÓN, ESTRUCTURA E INFRAESTRUCTURA DE LOS CIBERDELINCUENTES" ES CADA VEZ MÁS COMPLEJA, NO SE TRATA COMO VEMOS EN LAS PELÍCULAS DE UN ÚNICO "HACKER" QUE REALIZA TODAS LAS ACCIONES ILEGÍTIMAS."

Roles de gestión

En la jerarquía nos encontramos en la parte más alta al rol de gestión, al igual que ocurre en las compañías legítimas. Este rol es el encargado de coordinar, dirigir, decidir las contrataciones de las personas o grupos y supervisar las operaciones. El rol de gestión está condicionado al tamaño del grupo de ciberdelincuentes que componga la organización. En organizaciones más pequeñas, este rol puede estar mezclado junto con el rol de comercial, llevando a cabo las operaciones de comercial y gestión la misma persona o grupo de personas.
La finalidad de este post ha sido poner en situación cada una de las partes que hay detrás de un delito informático, y dar una visión general de este tipo de organizaciones. Como se ha visto, la organización, estructura e infraestructura es cada vez más compleja, no se trata como vemos en las películas de un único "hacker" que realiza todas las acciones ilegítimas. Hay grandes organizaciones detrás, un mercado donde se mueven grandes cantidades de dinero y una distribución geográfica que puede estar repartida por diferentes países del mundo.

¿AUTOMÓVILES VULNERABLES A CIBERATAQUES?

Por Servilio Alonso

Todavía recuerdo el tiempo que pasé trabajando en Nissan (Barcelona) como ingeniero de calibración de motores de combustión interna. Básicamente los ingenieros modificábamos y mejorábamos parámetros en calibraciones (variables calibrables) con la finalidad de obtener una respuesta o resultado en el funcionamiento del motor y de la conducción del coche en general. Digamos que modificábamos las "neuronas del cerebro" del vehículo para optimizar su sistema de locomoción, así como mejorar sus prestaciones. Los coches utilizan cada vez más componentes electrónicos pensados para mejorar el rendimiento, la seguridad y la comodidad de los usuarios. La mayoría de dichas funcionalidades implica procesar distintos tipos de señales del vehículo y coordinarlas en tiempo real, por lo que es necesario disponer de sensores que proporcionen los datos, unidades que se encarguen de procesarlos (Electronic Control Units o ECUs, "cerebros") y una forma de comunicación entre todas ellas (a través de uno o varios buses de datos mediante el Standard Controller Area Network o CAN). Un coche actual tiene docenas de ECUs, dependiendo del modelo, fabricante y versión. Cuando era ingeniero de calibración en Nissan, utilizaba un cable "Diag 3" con puerto USB con el que me conectaba desde mi portátil a la ECU (normalmente llamada ETK en el sector de la automoción) de un coche de pruebas. Lógicamente, esta ECU era "abierta" (reprogramable, con conexión adicional para pruebas e instrumentación). Para reprogramarla utilizaba una aplicación suministrada por Bosch (famoso fabricante de ECU's), y para conectarme y hacer cambios en la calibración en tiempo real, un programa desarrollado por el grupo ETAS llamado INCA (famoso gestor de calibraciones). Como anécdota para los informáticos os contaré que cuando yo estaba en Nissan, INCA solo funcionaba con el sistema operativo Windows XP, y con todas sus vulnerabilidades. Estos industriales y sus equipos expuestos a ciberataques.

¿Pero qué es eso de la calibración? ¿Y por qué os cuento todo esto? Os hago una pequeña síntesis para que os hagáis una idea:

Cuando tú reprogramas una ECU tienes dos archivos a introducir: el software y la calibración. El software comprende la lógica de control y todas las estrategias destinadas a controlar el funcionamiento del coche. Cada ECU y versión de motor tiene su versión de software desarrollada por los ingenieros informáticos de la correspondiente firma automovilística. La calibración es la base de datos (constantes, mapas de motor, etc.) de la cual se sirve el software para ejecutar su acción de control de una forma sensata y eficiente. Estos datos son ajustables, es decir, su valor se puede modificar (son calibrables). De esta forma, los

ingenieros de calibración pueden cargar diferentes calibraciones, con sus correspondientes cambios personalizados, en el mismo software.

Luego la ECU es tan solo una caja negra que recibe variables medidas por sensores (inputs), las procesa de forma eficiente gracias a una lógica de control y variables calibrables y a continuación genera una serie de variables de salida (outputs) que serán enviadas a los actuadores para que provoquen una respuesta que coincida con la demanda del usuario (conductor del coche).

Cuando hacía los ensayos, me conectaba con el programa INCA y podía hacer lo que quisiera: cortar la inyección, limitar la velocidad según el par motor y las revoluciones, modificar parámetros de funcionamiento del turbocompresor, el catalizador, la trampa de partículas, etc. Evidentemente los ingenieros hacíamos pruebas con las variables de la lógica de control que íbamos a modificar previamente estudiadas; se trataba de ensayos coherentes con los que poder investigar, hacer grabaciones y analizar el comportamiento del vehículo después de cada cambio. Pero, ¿qué pasaría si un hacker de algún modo cualquiera fuera capaz de acceder al "cerebro" con la finalidad de hacer cambios incoherentes en la calibración? Después de lo que os he contado podéis imaginar que las consecuencias serían nefastas.

Las ECUs se comunican mediante paquetes CAN.
La comunicación a través de CAN es "broadcast" y, aunque existen algunas redes segmentadas, cada ECU decide si un paquete de datos está destinado a él o no. No existe ningún tipo de autenticación ni identificación de la fuente de un paquete. En caso de tener acceso a los buses de comunicación CAN, es posible capturar el tráfico entre las distintas ECUs. No sólo eso, también es posible inyectar paquetes que interactúen con los distintas ECUs del vehículo. Esto puede proporcionar un control total, incluyendo el sistema de frenos, motor, luces y cualquier otra funcionalidad que incorpore el vehículo. Durante los últimos años, han surgido diversos estudios que demuestran que es posible interferir con todos estos sistemas del vehículo, como podrían ser los frenos. ¡Qué desastre, nos quedamos sin frenos! ¡Frenos rotos, coches locos!

Por ello, un punto clave se centra en si es posible o no obtener acceso a dicha comunicación. ¿Podrían ser la conexión a Internet o mediante smartphone (bluetooth) posibles vías de acceso a dicha comunicación….? Eso es lo que vamos a ver en este artículo.

Además de todas estas funcionalidades que implementan los coches, existen también las relacionadas con la comunicación y servicios derivados de Internet que se incluyen en la nueva generación de coches "conectados". No me refiero a la asistencia al aparcamiento, sino de acceso a redes sociales, correo electrónico, conectividad con el smartphone, cálculo de rutas, aplicaciones que se ejecutan en el coche, etc.
La conexión coche-Internet se puede realizar de dos modos:

A partir de la tarjeta SIM del vehículo. Esta conexión es la que se utiliza en los servicios/aplicaciones: In Car Browser Apps por ejemplo.

•A partir del smartphone del usuario (vía bluetooth). Modalidad utilizada en los servicios In Car Smarphones Apps.

Audi ha sido pionero en este campo cuando en 2005 puso en marcha proyectos conjuntos con Google y Nvidia para desarrollar software y hardware, y en 2009 la marca de los cuatro aros ofreció por primera vez conexión a Internet en un automóvil. El sistema Audi Connect se ofrece en casi todos los modelos de la marca, incluido el A1. Los ocupantes de cualquier vehículo Audi equipado con este sistema pueden navegar y acceder al correo electrónico en todo momento, así como utilizar un gran número de servicios online de Google mediante el acceso a Internet.
La conexión se realiza a través de una tarjeta SIM vinculada a una línea de datos, aunque como alternativa se puede acoplar el móvil al equipo del coche vía Bluetooth. Otra función es el punto de acceso inalámbrico WLAN, con la que el teléfono del automóvil permite que el acompañante y los ocupantes de las plazas traseras puedan conectar vía Wi-Fi y de forma simultánea hasta ocho dispositivos diferentes (ordenadores portátiles, iPads, etc) para navegar por Internet, consultar el correo o incluso jugar online, independientemente de sus sistemas operativos. Todo el control de este teléfono se realiza a través del mando del MMI Navigation Plus de Audi, utilizando el volante multifunción, mediante la pantalla táctil con reconocimiento de escritura que se ofrece en algunos modelos, o incluso mediante control por voz.
La inclusión de estas nuevas tecnologías implica una serie de nuevos riesgos a los que el usuario nunca antes había tenido que afrontar. El mundo sigue evolucionando y los riesgos con él.

ECALL A PARTIR DE ABRIL DE 2018

Por Hilario Miró

La Unión Europea, después de muchos años y tras varios intentos fallidos, ha conseguido incorporar el dispositivo de emergencias eCall en los nuevos vehículos. Finalmente se ha aprobado una ley para que sea obligatorio en todos los modelos nuevos de coches y furgonetas ligeras a partir de abril del 2018.
La Comisión de Mercado Interior y Protección de los Consumidores del Parlamento Europeo ha dictaminado que, a partir del 31 de marzo del año 2018, todos los coches y furgonetas ligeras nuevas deberán ir equipados con el sistema automático de llamada a los servicios de emergencia en caso de siniestro, denominado eCall La verdad es que esta medida no es nueva, sino que se lleva hablando de ella desde hace varios años; en un principio el 2015 era el año en el que debía ser obligatorio, pero diversos motivos legales la han ido retrasando hasta el 2018. Este retraso al menos servirá para instalar la infraestructura necesaria para garantizar que el sistema funciona correctamente.
La mayor parte de los retrasos que ha acumulado el proyecto se deben principalmente a temas relacionados con la privacidad y a la protección de los datos de los usuarios. En ese sentido, los europarlamentarios han ido corrigiendo el texto legal para que la privacidad no quedara en entredicho. Básicamente han

reforzado la cláusula sobre protección de datos para impedir que se rastreen los vehículos equipados con el nuevo dispositivo antes de un accidente.
Según la nueva normativa, la llamada automática de emergencia solo facilitará datos básicos, como el tipo de vehículo, el combustible utilizado, la hora del accidente, la localización exacta y el número de pasajeros. Además, también establece que ningún dato será transferido a terceros sin el consentimiento explícito de la persona, y que los fabricantes garanticen el borrado completo y permanente de los datos almacenados.
Pero, ¿cómo funciona este sistema? El sistema eCall utiliza la tecnología del número 112 para avisar automáticamente a los servicios de emergencia en caso de un accidente grave. Así pueden decidir inmediatamente el operativo de asistencia necesaria. Además, los estudios demuestran que gran parte de las víctimas mortales y de las lesiones graves son causadas por la ausencia de asistencia médica inmediata. Con la incorporación de este dispositivo se espera reducir entre un 50 y un 60% el tiempo de respuesta ante un accidente, y con ello el número de víctimas mortales.
En caso de accidente, eCall realiza una llamada inmediata al 112, quienes responderán a la llamada y tratarán de ponerse en contacto con los ocupantes del vehículo para confirmar su estado y por otro lado, advertir en caso necesario, si el accidente no reviste gravedad. De no contestar nadie, se activará inmediatamente un protocolo de emergencia para que acudan al lugar del accidente ambulancias, policías y bomberos. Para ello, el dispositivo transmitirá la marca y el modelo del coche, el titular del vehículo, el tipo de combustible, la hora del accidente, la localización exacta y el número de ocupantes. (Fuente: DGT)
Aunque de momento no es obligatoria su instalación en los coches nuevos, muchas marcas ya lo han incorporado en muchos de sus modelos. Por ejemplo Mercedes, BMW, Citroën, Ford y Opel ya lo hacen. El sistema se suele ofrecer como equipamiento opcional, incluyendo su uso por un determinado periodo de tiempo, que posteriormente requiere de una suscripción con la correspondiente cuota anual. No obstante, también los hay que no conlleva ningún coste ni suscripción por parte de los conductores.
A partir de la fecha límite, este dispositivo tendrá que ser de serie en todos los vehículos y se supone que no conllevará ningún coste añadido, ni ninguna tarifa de suscripción para los servicios básicos obligatorios, ni ningún problema de privacidad… Aunque esto, como se imaginan, está todavía por ver.

UN ARMA MUY PODEROSA DE CIBERATAQUE: CONOCIMIENTO IT + CONOCIMIENTO INDUSTRIAL

Por Servilio Alonso

Cada vez son más frecuentes los ciberataques producidos por equipos multidisciplinares en los cuales sus integrantes disponen de conocimientos IT y conocimientos del funcionamiento del sistema industrial al cual pretenden atentar. Esto se ha convertido en un arma muy poderosa, ya que los atacantes no solo son capaces de acceder al sistema de control industrial, sino que pueden identificar qué parte del proceso industrial es crítica y delicada y que sabotean-do su sistema de control, pueden producir graves daños que afecten tanto a la producción de la planta como a la propia instalación.
Todos recordamos el caso del malware Stuxnet que en 2010 atacó una instalación industrial dañando más de 3000 centrifugadoras en Irán. Recientemente, según un informe de la oficina federal alemana para la seguridad de la información, una planta de acero sufrió un ciberataque a sus sistemas de control industrial ocasionando graves daños. Según un informe anual publicado por la oficina federal alemana para la seguridad de la información, conocida como BSI (Bundesamt für Sicherheit in der Informationstechnik), existe evidencia de un ataque cibernético dirigido a los sistemas de control en una acería alemana

que resultaron en daños "masivos" a un alto horno.
El informe BSI describe las destrezas técnicas de los atacantes como "muy avanzadas". Tenían "know-how avanzado no sólo de la seguridad IT convencional, sino también el conocimiento técnico detallado de los sistemas de control industrial y procesos de producción de la planta". Diferentes sistemas internos y componentes industriales fueron comprometidos. El informe describe el ataque a la acería, pero no identifica a la empresa afectada ni revela cuando se produjo el ataque.
La planta fue atacada combinando un ataque "spear phishing" y la ingeniería social para acceder a la red de oficinas de la institución. A partir de ahí, el ataque continuó su camino a través de la red de producción causando un gran daño en un alto horno.
Tácticas del Atacante, Técnicas y Procedimientos (TTPs). Descripción.
El informe original alemán no proporcionaba detalles sobre el atacante ni sus TTPs, pero debemos tener en cuenta la evaluación de los conocimientos del atacante respecto al ICS.
Atacante – La BSI describe el incidente como un "APT-Attack". Probablemente podemos pensar en un atacante que utiliza tácticas y herramientas APT tradicionales, sin embargo, su objetivo final va más allá de la propiedad intelectual.
Técnica – La técnica utilizada para infiltrarse en la red corporativa de la instalación fue un correo electrónico de phishing.
El informe del BSI describió este vector de ataque

Los ciberataques industriales pueden provocar cuantiosas pérdidas a las empresas.

como un ataque de "ingeniería social avanzada" que varios atacantes utilizan para obtener acceso a la red corporativa. Después se abrieron camino en las redes de producción industrial (ICS).
A partir del análisis previo de los incidentes relacionados con el spear-phishing dentro de los ICS, es muy probable que el correo electrónico tuviera un documento PDF que al abrirse ejecutara código malicioso en el equipo, que a su vez abrió una conexión de red para el atacante(s) sin que el personal de planta se diera cuenta. No se ha proporcionado información sobre cómo el atacante penetró dentro de la red de producción industrial, pero el análisis de estudios de casos similares nos indica que probablemente lo hiciera a través de zonas y conexiones de confianza entre la red corporativa y la red industrial.
Oportunidad – Las redes corporativas son un objetivo muy valioso para los atacantes interesados en ICS, ya que tienen a menudo conexiones con la red ICS que los atacantes pretenden atacar. Muchas de estas redes de proceso fueron construidas como sistemas aislados que permitían solo comunicaciones necesarias con redes de proceso de nivel superior para realizar determinadas operaciones de mantenimiento o control, pero como ya hemos visto en otras ocasiones, los nuevos tiempos de negocio requieren visibilidad adicional, órdenes, programación y soporte remoto, lo cual requiere comunicaciones adicionales entre las redes tradicionales de TI y las redes de control de procesos industriales.
Muchos grupos de atacantes han demostrado habilidad para pivotar desde las redes de nivel superior a las redes de operación industrial a través de estos canales de comunicación de confianza. En el caso de que estas redes no estén conectadas entre sí, la información contenida en las redes corporativas sigue siendo muy útil para los atacantes, ya que puede contener especificaciones o diagramas de los ICS así como datos personales: correos electrónicos e información de la red que puede ser usada para utilizar otros vectores de ataque.
Motivación – No se ha publicado la motivación del atacante. Se pueden extraer múltiples teorías que incluyen el sabotaje industrial por parte de la competencia, intereses nacionales, extremistas medioambientales, o alguna persona o grupo probando sus capacidades y tácticas para ver si se producía daño físico o no.
Es poco probable que el atacante fuera un empleado descontento dado que el vector de ataque inicial era

un correo electrónico de phishing. Una amenaza interna hubiera tenido medios más accesibles y no hubiese estado interesada en principio en causar estragos en la red. Sin embargo, llegado a este punto muy pocas teorías se pueden descartar. La motivación se convierte en un aspecto muy interesante, dado que el ataque tuvo daños físicos sobre la planta y los procesos industriales.

Otro aspectos que debemos considerar y que se valora adecuadamente en el informe es que los atacantes tenían un avanzado "know-how" en ICS y conocimiento del proceso, y lo más importante, fueron capaces de lograr un daño masivo en éste. La descripción dada por el informe BSI acompañada del conocimiento de los incidentes del proceso, lleva a los autores a creer que el daño provocado en el proceso industrial fue intencionado.

Conclusión

Al revisar todos los datos del incidente, da la impresión de que los "malos" sabían con detalle qué elemento de la producción industrial era crítico y vulnerable, en este caso el alto horno de la acería alemana.

Sabían cómo funciona, cómo se controlaba y qué elementos de su sistema de control debían adulterar o desestabilizar para producir un daño físico importante, suficiente para parar la producción de acero y provocar grandes pérdidas económicas (sin olvidar que con este tipo de ataques también se ponen en riesgo vidas humanas).

Aparentemente el acceso a la información y los controles se produjo aprovechando las conexiones de confianza entre la red industrial y la red corporativa, a la cual accedieron mediante un correo electrónico infectado.

De una forma tan "sencilla", podemos ver el desastre que puede provocar un simple correo electrónico "desconocido" que un día cualquiera, un empleado cualquiera abre de forma inocente sin pensarlo dos veces.

L1
L2
L3
L1
L2
L3

CIBERACOSO: SOLUCIÓN

Por JMPÉREZ

UN CASO REAL Y LEGAL

Muy interesante el post que nos hace llegar un padre tras vivir una dramática experiencia de ciberacoso con su propia hija. Por suerte, para este padre anónimo y para su familia, el problema se ha solucionado con un final feliz.
¡Gracias por transmitirnos tu experiencia y sobre todo por compartir con nosotros lo que podríamos denominar 'la solución'!

La verdad es que no se cómo empezar la historia, pero espero de verdad que la experiencia, horrible por otra parte, sirva a más padres.

Todo comienza con el Whatsapp, comienza con un grupo que tu hija y sus amigas crean. En principio lo usan para quedar, comentar sus cosas, preguntar cosas sobre los deberes etc..

Parece una herramienta inocente, pero la matona del grupo, que siempre las ha habido y siempre las habrá (recordad que para haber héroes, tienen que haber villanos), ve en sus manos la herramienta perfecta para cometer sus fechorías, (no hace falta estar cara a cara, ni dejar marcas físicas) además de ser la herramienta perfecta para incitar a otras niñas a que colaboren.

De repente ves que algo a lo que no has dado importancia empieza a tomar forma, y esa forma se vuelve monstruosa cuando hay comentarios hirientes, chicas y chicos del grupo que se suman a esos comentarios, y parece que haya una competición para ver cual es más gracioso (es decir más hiriente), y el pitidito del Whatsapp se convierte en una pesadilla porque no deja de sonar.

Las 10, las 11, las 12… las 2, las 3, y el maldito pitido sigue sonando, y con cada sonido tu hija cada vez está más deprimida, y te ves impotente ante la situación porque no sabes cómo pararlo.

Evidentemente tu hija se borra del grupo, pero el acoso sigue por lo privado: la maquinaria se ha puesto en marcha y no hay quien la pare.

La siguiente fase son las amenazas, por ejemplo le "insinúan" que en el viaje fin de curso no será bienvenida (te vamos a dar por todos lados, asquerosa…). Así pues tu hija hace el viaje con la otra clase, pero eso tampoco está bien porque como no ha ido el viaje de autobús les ha salido un euro más caro, así que "se va a enterar cuando le pillemos", y empiezan a quedar por Whatsapp para pillarla.

Al final, ante esa situación decides acudir a la Guardia Civil, pero su respuesta te deja anonadado:

"...Mire usted, los niños de 13 años son INIMPUTABLES, con lo cual el juez seguro que archiva el caso, nosotros no podemos hacer nada,… ¿por qué no prueba a hablar con los padres?".

Los padres no te hacen caso ya que "son cosas de niños", y el patético resultado con los niños es éste.

Ciberbullying con final feliz

Viniendo de una niña de "familia bien" choca que usar el diálogo para

encontrar una solución, solo provoque que tu hija les "de más asco y rabia".

O sea que lo que tenemos que hacer es dejar que la maten, o se mate ella, o cambiarla de colegio, o contratar a SVETOSLAV, un ruso que no cabe por la puerta para que les haga una visita. En realidad no sabes qué hacer, y os juro que es desesperante.

Esto no mejoró hasta que un día recordé un artículo del semanal de El País que hablaba de los chats, donde se comentaba el ejemplo de que si estas chateando con Claudia Schiffer nadie te garantiza que no estás chateando con su perro y que lo único que está claro es que se habla desde la IP de Claudia Schiffer (bendita sea la IP).

Así pues, igual que los niños son inimputables por tener 13 años, tampoco pueden tener un contrato de teléfono a su nombre, así que optamos por hacernos la gran pregunta: ¿cómo puedes asegurar que la amenaza la ha hecho un niño?, ¿y si es el padre el que está amenazando? Es similar a lo que sucede cuando se multa a un conductor conduciendo a 200 por hora en una autopista con una foto y se envía la multa al dueño del coche para que, si él no es el conductor, lo identifique.

Basándose en esta idea nuestro abogado puso la denuncia como amenazas desde un número de teléfono, no directamente a una persona, y que fuese la Guardia Civil quien identificase al dueño y éste al autor.

Con lo cual dejas al padre de los otros niños en la situación de que si no identifica a su hijo delante del juez, carga con la culpa, y si lo identifica, queda como un cobarde delante de su hijo (que al fin y al cabo es lo que es).

Os aseguro que el bálsamo fue inmediato. Al segundo padre que la Guardia Civil llevó a declarar ante el juez, las amenazas cesaron, los mensajes cesaron e incluso algunos padres y niños nos pidieron perdón.

Aunque con franqueza he de decir que no puedo perdonarles, mi hija es carne de mi carne y sangre de mi sangre. Hay un tiempo para el perdón, – pero yo todavía no lo he encontrado-, hay un tiempo para callar y un tiempo para hablar – muchos padres ya hemos callado demasiado tiempo, es hora de que hablemos-, un tiempo para amar y un tiempo para odiar, un tiempo de guerra y un tiempo de paz.- Espero que nuestro tiempo de paz haya llegado-. Eclesiastés capítulo 3.

¿CÓMO PUEDO CONVERSAC MANTENGO

Por JMPÉREZ

¿Alguna vez has echado de menos la posibilidad de grabar una conversación telefónica?

Puede haber muchas razones para querer grabar nuestras llamadas de teléfono. Quizá simplemente para recordar a los seres queridos mediante conversaciones mantenidas en el pasado.

O desde el punto de vista profesional, conservando un registro de todas las conversaciones con los clientes, pudiendo comprobar, siempre que queramos, aquel pedido que pudimos apuntar. Otros fines pueden ser más 'oscuros', pero no por ello menos interesantes, como la grabación de aquellas conversaciones que mantenemos cuando contratamos algún servicio por teléfono y que luego no cumplen como nos habían prometido.

Y la finalidad mas 'dura' sería la extorsión o chantaje que se puede hacer por medio de una conversación grabada con contenido comprometedor.

Es importante por tanto, conocer que actualmente podemos grabar las conversaciones mantenidas con nuestro Smartphone pero asimismo debemos ser conscientes de que también cualquier persona puede estar grabándonos cuando conversamos con ella.

Cuidemos lo que decimos por teléfono, es probable que nuestro interlocutor nos esté grabando.

¿EN QUÉ TELÉFONOS PUEDO GRABAR MIS CONVERSACIONES?

•Android. Sistema operativo que cuenta con más aplicaciones para esta finalidad. Se encuentran de pago y gratuitas. No todas funcionan con todos los modelos, por lo que si realmente te interesa, quizá tengas que probar con más de una. Una de las que mejor puntuación presenta es Record my Call y a mí me ha funcionado perfectamente. Está en inglés, pero solo hay que ir a los ajustes e indicarle que se active. A partir de ese momento grabará todas las conversaciones, tanto las entrantes como las salientes.

•BlackBerry. Puedes probar con Call Recorder que, aunque algunos comentarios dicen haber tenido problemas, la mayoría la puntúan de forma excelente. Aporta alguna ventaja respecto a la privacidad, como la protección con contraseña o el cifrado de los archivos

GRABAR LAS IONES QUE EN MI MÓVIL?

guardados para que nadie más los pueda escuchar.

•Windows Phone. También se llama Call Recorder y está pensada para grabar las conversaciones y para almacenarlas en el espacio virtual que ofrece Windows, Skydrive. Realmente, lo que hace es activar la grabadora de sonidos en el momento que se hace la llamada, por lo que necesita que conectemos el 'manos libres' para que la grabadora capte el sonido de nuestro interlocutor.

•iPhone. No he encontrado ninguna aplicación que permita esta función para este tipo de teléfonos.

Piénsalo bien antes de conservar determinadas conversaciones en tu móvil. Existe el riesgo de que éstas lleguen a manos de personas mal intencionadas. Podemos perder el móvil, prestarlo por un momento o podemos ser víctimas de algún robo de archivos por medio de algún 'malware'.
Conversaciones de índole íntimo o con información sensible como direcciones, teléfonos u otros datos personales tuyos o de terceras personas podrían quedar sin protección y ocasionar problemas si llegan a manos indeseadas.

Si la utilizas, quizá sería buena idea que emplearas algún medio de bloqueo por contraseña de la aplicación.

CÓMO UTILIZAR WHATSAPP SIN QUE CAMBIE NUESTRA ÚLTIMA HORA DE CONEXIÓN

Por JMPÉREZ

Casi todos los que utilizamos Whatsapp hemos "vigilado" alguna vez la última hora en la que se conectó alguien a quien habíamos enviado un mensaje para saber si ya lo había leído. A veces necesitamos conocer si esa persona se ha enterado o no de nuestro mensaje y comprobar este dato puede ser "orientativo".
La información que proporciona la "última vez" y el hecho de que se pueda ocultar despierta todo tipo de suspicacias y de comportamientos obsesivos de vigilancia. Preguntas como ¿me habrá bloqueado? ¿por qué no me contesta? ¿me habrá borrado de la agenda? y otras relacionadas con la privacidad de la aplicación son continuas en los comentarios que dejan nuestros lectores.
Si por ejemplo enviamos un mensaje a alguien a las 12:00 pm y diez minutos más tarde vemos que la última vez que se conectó fue a las 12:02 pm, podemos sospechar con bastante fundamento que lo leyó. A todo esto hay que añadir la posibilidad de ocultar la notificación de lectura con el doble check azul que dispone Android y la configuración de privacidad que cada usuario puede elegir, lo que llega a complicar bastante conocer con seguridad si alguien ha leído o no nuestro mensaje. Veremos cómo podemos confundir a nuestros contactos leyendo mensajes sin alterar nuestra última conexión.

Hay una forma de despistar a quien nos vigila. Podemos leer e incluso escribir mensajes sin mostrar cuándo es la última hora real en la que nos conectamos y sin necesidad de ocultarla. Es decir, podemos utilizar Whatsapp sin modificar la última conexión.

Es una medida que podemos utilizar, por ejemplo, si somos objeto de vigilancia por parte de alguno de nuestros contactos. Nos permitirá leer sus mensajes y utilizar la aplicación sin alterar ni ocultar la última hora de conexión. Funciona si somos usuarios de un teléfono Android o Windows, pero no si se trata de iPhone.

¿Cómo lo conseguimos?

•Debemos desactivar la notificación de lectura que encontramos en la sección 'Ajustes > Cuenta > Privacidad (Android). Esto hará que no les aparezcan las marcas de color azul a nuestros contactos tras leer los mensajes, aunque debemos saber que también a nosotros se nos ocultarán.

Nuestro contacto ve que hemos leído el mensaje por el color azul de las marcas pero aparentemente nuestra última conexión es anterior al envío.

•Modo avión. Para evitar que la aplicación actualice nuestra última hora de conexión debemos abrirla cuando el teléfono carece de conexión a Internet. El modo más sencillo de anular la conexión en un teléfono móvil es utilizar la función "avión", que desconecta instantáneamente cualquier conexión inalámbrica.

El mismo efecto tendría la desactivación de la conexión wifi y la red telefónica de Internet, pero resulta más rápido y cómodo utilizar esta función del "modo avión".

•Ahora podemos abrir Whatsapp, leer todos los mensajes que nos han llegado hasta el momento e incluso escribir nuevos mensajes respondiendo a las conversaciones, aunque no tengamos conexión a Internet.

•Al finalizar, debemos cerrar Whatsapp y después recuperar las conexiones, desactivando el modo avión.

•Nuestros mensajes saldrán en cuanto recuperemos la conexión aunque tengamos la aplicación cerrada, pero la hora de "última vez" no se verá modificada.

Existen incluso aplicaciones, como Whatsapp Ghost o Shh para Android, que realizan estas tareas de forma automática siempre que vamos a utilizar Whatsapp, permitiendo un uso "casi normal" de éste pero asegurándonos que se mantiene invariable el dato de nuestra última conexión.

A partir de ahora, si sigues estos consejos, tendrás más libertad utilizando el Whatsapp.

HELLO BARBIE, EL CONFLICTO ENTRE LA PRIVACIDAD Y LOS AVANCES TECNOLÓGICOS

Por JMPÉREZ

Mattel, el fabricante de la archiconocida muñeca Barbie, ha decidido incorporar a su creación un avance tecnológico que está causando una gran polémica. El nuevo modelo de Barbie hablará con los niños gracias a su micrófono, su altavoz y su conexión a Internet vía Wifi.
La muñeca aún no ha salido al mercado, se espera para finales de año, pero en su presentación ya explican que el juguete dispondrá de un botón en la cintura que los niños podrán pulsar para hablar y la muñeca les contestará de forma personalizada.

Hello Barbie fue presentada por Mattel en la pasada Feria Internacional del Juguete de los Estados Unidos

La gran innovación presentada es que esta muñeca podrá conversar con los niños gracias a un sistema inteligente que reconocerá el lenguaje, lo procesará y responderá según sus peticiones. Además, será capaz de memorizar los gustos y aficiones de diferentes niños y adaptar sus respuestas según las necesidades. Es decir, una muñeca que "habla y conversa de verdad".

La polémica surge porque todo este sistema funciona a través de Internet, con lo que ello supone para la privacidad del menor. Las conversaciones quedarán grabadas en los ordenadores de la compañía tecnológica que ha desarrollado el sistema, en principio para adaptar las respuestas de la muñeca, pero sin duda será una información muy valiosa que puede ser utilizada en el futuro para otros fines, por ejemplo, para algo tan codiciado por las empresas como la publicidad dirigida. Pero son muchas más las razones que podrían preocuparnos si un juguete así se incorpora en la vida cotidiana de nuestros niños. Por ejemplo:

• Qué medidas adoptará la compañía para garantizar la seguridad de los datos almacenados y que no puedan ser robados por hackers.

• Cómo de seguro será el dispositivo para que no sea vulne-

rable al ataque exterior y por ejemplo, pueda grabar conversaciones sin que el niño se percate, como ocurre con las webcams.

• Cómo podremos estar seguros de que los niños no comparten información privada sensible o simplemente queda grabada involuntariamente porque la recoge del sonido ambiente.

• La información viajará de forma segura o podría ser interceptada por hackers.

Ante tan osada invención de Mattel, ya ha surgido en USA una plataforma que se opone al lanzamiento y que califica la muñeca de "espeluznante". El fabricante se defiende argumentando que el sistema es equivalente a, por ejemplo, el asistente de información Siri que incorporan el iPhone o iPad. Seguramente es cierto, pero la diferencia principal es que la muñeca va dirigida a niños que, como es lógico, carecen de todo el sentido de la privacidad.

Quizá lo más preocupante del caso no sea la muñeca en sí, sino lo que este hecho viene a anunciar. El "internet de las cosas" parece imparable, es cuestión de tiempo que "todo" esté conectado a la Red y los juguetes no van a ser una excepción. Televisores, frigoríficos, vehículos, pulseras, relojes, etc. estarán conectados y ofrecerán nuestros datos a sistemas inteligentes que interactuarán y nos facilitarán la vida, pero inevitablemente pagaremos un alto precio con nuestra privacidad.

En mi opinión es algo que resulta inevitable, si no es ésta la compañía de juguetes o no es éste el modelo que finalmente incorpora conexión a Internet, terminará haciéndolo otro fabricante y con el tiempo será habitual que los juguetes se conecten incluso entre ellos mismos e interactúen.

La privacidad y los avances tecnológicos parecen incompatibles y a estos últimos no hay quien los detenga.

¿REGALARÍAS UNA MUÑECA ASÍ A TUS NIÑ@S?

¿SABES QUÉ ES CONMEMORATI FACEBOOK?

Por JMPÉREZ

UNA CUENTA VA EN

Si alguna persona próxima a nosotros, como un familiar o un amigo ha fallecido y tenía cuenta en Facebook, podemos solicitar a la red social que convierta su cuenta en conmemorativa.

Las cuentas en redes sociales de Internet están pensadas para los vivos, pero en el caso de Facebook encontramos una excepción. Podemos convertir la cuenta de alguien que ya ha desaparecido en un tipo de cuenta muy especial, lo que llaman cuenta conmemorativa. La cuenta seguirá mostrándose en la red social pero con algunas diferencias importantes, como por ejemplo, ya no aparecerá como sugerencia de nueva amistad a nadie.

Desde hace algún tiempo, los usuarios ubicados en EE.UU pueden escoger en su configuración a algún "contacto de legado" para que administre su cuenta cuando ya no la puedan utilizar, algo similar a lo que ofrece Google para sus cuentas inactivas. Pero de momento, lo único que podemos hacer en nuestro país es solicitar que la conviertan en conmemorativa.

¿Para qué sirve?

Las cuentas conmemorativas proporcionan un lugar para que amigos y familiares se reúnan y compartan recuerdos de un ser querido que haya fallecido. Convertir una cuenta en conmemorativa ayuda a protegerla, ya que nadie puede iniciar sesión en ella. Tienen las siguientes características:

- Aparecerá la expresión "En memoria" junto al nombre de la persona en su perfil.

- Los perfiles conmemorativos no aparecen en espacios públicos como las sugerencias de "Personas que quizá conozcas", los recordatorios de cumpleaños o los anuncios.

- En función de la configuración de la privacidad de la cuenta, los amigos pueden compartir recuerdos en la biografía conmemorativa.

- El contenido que haya compartido el usuario (por ejemplo, fotos, publicaciones, etc.) permanece en Facebook y está visible para el público con el que se compartió.

- Nadie puede iniciar sesión en una cuenta conmemorativa.
- Los grupos con un administrador cuya cuenta se haya convertido en conmemorativa podrán elegir a un nuevo administrador.

- Las páginas con un único administrador cuya cuenta se haya convertido en conmemorativa se eliminarán de Facebook.

Además, los familiares pueden solicitar que se elimine la cuenta de Facebook.

¿Cómo se solicita?

En el servicio de ayuda de Facebook explican cómo solicitar la conversión de una cuenta en conmemorativa.

En realidad nos dirigen a dos posibles sitios donde hacer la petición:

- En el primero – solicitud de cuenta conmemorativa – nos piden mucha menos información y parece más directo. Desconozco si es suficiente con rellenar esos pocos datos. La única prueba que exigen es un simple enlace de internet a un obituario u otro tipo de documento.

- En otra sección, encontramos el formulario "Solicitud especial para la cuenta de una persona fallecida", donde nos piden más información y además de la solicitud anterior, también podemos pedirles que eliminen una cuenta o alguna otra petición.

No es un tema muy agradable de tratar, pero con seguridad todos vamos a tener algún caso próximo antes o después y con la presencia que hoy tiene Facebook en la sociedad, creo que todos debemos conocer esta opción y utilizarla llegado el momento.

PUEDES UTILIZAR GOOGLE PLUS PARA CONOCER LA UBICACIÓN DE TUS HIJOS

Por JMPÉREZ

Muchos padres deciden regalar a sus hijos móviles de última generación aún siendo niños. Hoy es difícil encontrar chicos o chicas a partir de los 12 años que no dispongan de un smartphone conectado a Internet. Lo que se preguntan muchos padres es si podrían utilizar alguna de sus funciones para conocer dónde se encuentran sus hijos en un momento determinado.

La respuesta es claramente sí, es muy sencillo y está disponible en una aplicación tan conocida como Google+.

Ya sabemos que existen aplicaciones espía que instaladas en un teléfono nos pueden indicar su localización y mucha más información, incluso de forma "silenciosa". Pero no es esto lo que tratamos de explicar aquí.

Lo que Google nos proporciona con su aplicación es un modo de compartir la posición a tiempo real con tantas personas como se quiera, siempre que todos ellos hayan dado permisos y configurado la opción para que así sea. Cada uno de ellos podrá ver la posición de los otros sobre los mapas de Google de forma precisa y cuando quiera. Google+ (Google plus) es esencialmente una red social, pero ofrece esta función añadida entre otras muchas que puede llegar a ser muy útil en el entorno familiar.

Veamos qué debemos configurar y cómo se utiliza esta herramienta de localización.

Requisitos del teléfono

De momento, esta función solo la encontraremos en la aplicación Google plus que podemos instalar en los dispositivos móviles Android o iPhone. Otras versiones, como la Web o la de teléfonos Windows, de momento no disponen de esta herramienta.

1.Instalar Google +. La mayoría de los teléfonos Android ya vienen con ella de fábrica. Si no la tenemos, solo debemos dirigirnos a la tienda oficial correspondiente e instalarla de forma gratuita.

Deben instalarla todos los componentes del grupo que quieran compartir la ubicación, y será necesario que cada uno acceda con su propia cuenta de Google.

2.Permitir Ubicación. Debemos dar permisos a nuestro teléfono para que utilice los sistemas de auto localización por GPS. En Android podemos encontrar estas opciones en 'Ajuntes > Ubicación > Modo > Máxima precisión. Esta ruta puede cambiar ligeramente según la versión del sistema operativo. De este modo, siempre que sea posible, el teléfono compartirá su ubicación con las aplicaciones que se lo soliciten de la manera más precisa posible.
En el iPhone, los permisos para la localización del teléfono los encontramos en 'Ajustes > Privacidad > Localización'. Allí deberemos activarla y asegurarnos que Google + tiene permisos concedidos.

3.Activar historial de ubicaciones. Hay que dar permiso a Google para que utilice nuestro historial de ubicaciones. En Android encontramos esta opción en la aplicación 'Ajustes de Google' en el apartado 'Historial de ubicaciones de Google'. Desde allí podremos activar o no este historial, borrarlo hasta el momento actual y gestionar otros dispositivos que pudiéramos tener bajo nuestra misma cuenta. en iPhone podemos verlo en las opciones de configuración y ajustes de la propia sección 'Ubicaciones' de Google+.

Configurar Google plus

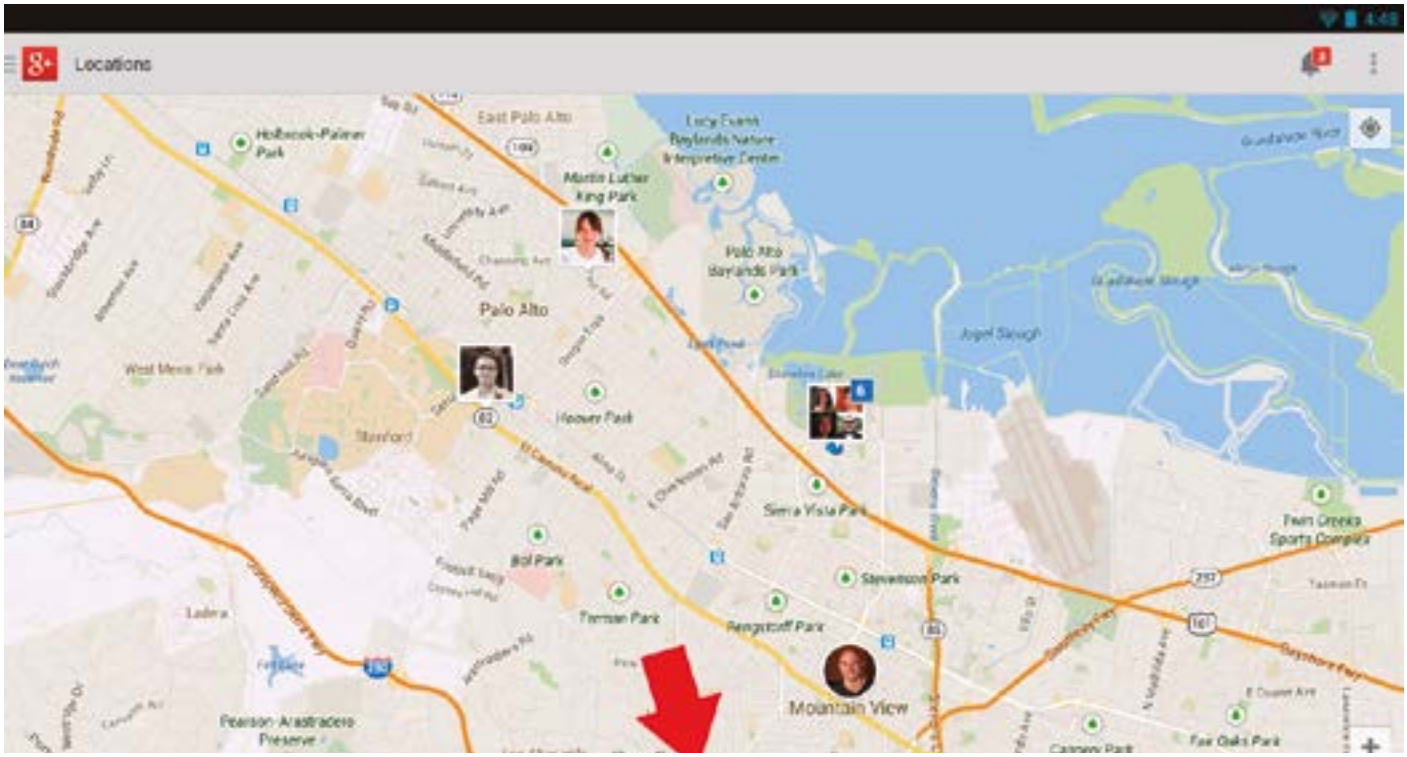
1.Amigos en la red social. Para que podamos compartir la ubicación con otra persona por este medio, es imprescindible que ambos utilicemos la red social y que seamos 'amigos' en ella. Si queremos utilizarla, por ejemplo con nuestra familia, podemos agregar a cada uno de los miembros a un círculo llamado 'familia' o como queramos. El icono que señalamos es el que nos permite buscar y añadir nuevos amigos.

2.Compartir la ubicación. Debemos escoger con

quién queremos compartir nuestra posición geográfica, siempre de entre nuestros amigos. Para ello, dentro de la aplicación Google + buscaremos el apartado 'Ubicaciones'. En iPhone aparece en el menú lateral izquierdo, pero en Android debemos pulsar sobre la pequeña flecha de la parte superior o 'Inicio'. El apartado aparece en la parte inferior.
Una vez en el apartado ubicaciones, accederemos al menú de opciones, y pulsaremos sobre 'Ajustes de la ubicación'. ('Ajustes' en iPhone)
En la pantalla siguiente, podremos elegir a las personas con quien compartir la localización. Encontramos dos modos de hacerlo, mostrando nuestra posición deforma exacta o solo la ciudad donde nos encontramos. Según el nivel de precisión que queramos proporcionar a una persona elegiremos incluirla en una sección u otra.

Las personas que elijamos podrán ver nuestra posición en el mapa desde ese momento. Para que esa persona nos muestre la suya, ella deberá hacer lo mismo, pero compartiendo la ubicación con nosotros.

Tocando sobre la imagen de una de ellas, nos aparecerá información sobre su ubicación en la parte inferior, como la dirección aproximada y el momento en que se encontraba allí. El icono central nos muestra la lista de todas las personas con las que compartimos nuestra ubicación y también nos proporciona la posibilidad de invitar a alguno de nuestros contactos a utilizar esta función mediante un correo electrónico.



Para ver a las posiciones en el mapa, solo tenemos que acceder al apartado 'Ubicaciones' como hemos descrito antes y sobre el mapa se situarán pequeños iconos señalizando a las personas que hemos incluido y a nosotros mismos.

CÓMO UN DEP SEXUAL DE EN INT

Por JMPÉREZ

Una vez más es noticia la detención de una persona que utilizaba Internet y en especial las Redes Sociales para extorsionar a menores y con ello obtener favores sexuales.
El último caso publicado por los medios, hace solo un par de días, es el de un joven de 25 años, maestro y catequista en la localidad de Chipiona, Cádiz. Aunque realmente joven, ha sido calificado por la Policía como un auténtico "depredador sexual" ya que ha sido detenido en dos ocasiones anteriores y cuenta con un importante historial delictivo anterior.
En esta ocasión parece que utilizaba como medio de contacto con sus víctimas la conocida red social basada en fotografías Instagram. Contactaba con antiguos alumnos con los que además había tenido alguna otra relación en actividades extraescolares, de edades comprendidas entre los 12 y 13 años y siempre varones, ganándose inicialmente su confianza y tejiendo poco a poco una trama de extorsión.
Tras las primeras conversaciones de índole sexual que intercambiaban a través de mensajes electrónicos, el pederasta comenzaba con el chantaje, amenazándoles con publicarlas en las redes sociales y obligándoles al envío de imágenes y vídeos de desnudos. Una vez conseguidas las imágenes, las amenazas subían de nivel y las peticiones exigían encuentros sexuales en persona. Todo este mecanismo de extorsión para conseguir favores sexuales de menores se conoce con el término "grooming".

Y es que se demuestra una vez más que Internet es un medio propicio para las "sextorsiones", donde los pederastas aprovechan la ingenuidad y eldesconocimiento de los menores para aprovecharse de ellos y hacerles actuar a su voluntad.
Quizá lo más importante que podemos hacer para prevenirlo sea enseñarles que "estas cosas pasan", tanto a chicas como a chicos y que la previsión es la mejor manera de combatirlo. Utilizar Internet con sentido común y no hacer allí lo que no haríamos en persona es fundamental para mantenerse al

ACTÚA REDADOR MENORES ERNET

margen de muchos problemas.

Consejos para prevenir el chantaje sexual en menores:

•La educación es fundamental. Los padres y profesores tenemos la labor de adelantarnos a este peligro advirtiendo a los menores de las consecuencias tan dramáticas que pueden llegar a tener algunos actos, aparentemente inofensivos, cuando se realizan por Internet.

•Nunca establecer contacto en Redes Sociales con desconocidos. Desconfiar de quien contacta con nosotros, especialmente si somos menores, tal y como lo haríamos en las relaciones reales o en persona.

•No enviar imágenes con contenido sexual bajo ningún concepto. Ni siquiera a amig@s o novi@s en los que confie-

mos ciegamente. El sexting es uno de los fenómenos que traen situaciones más dramáticas y puede volverse en nuestra contra en cualquier momento.

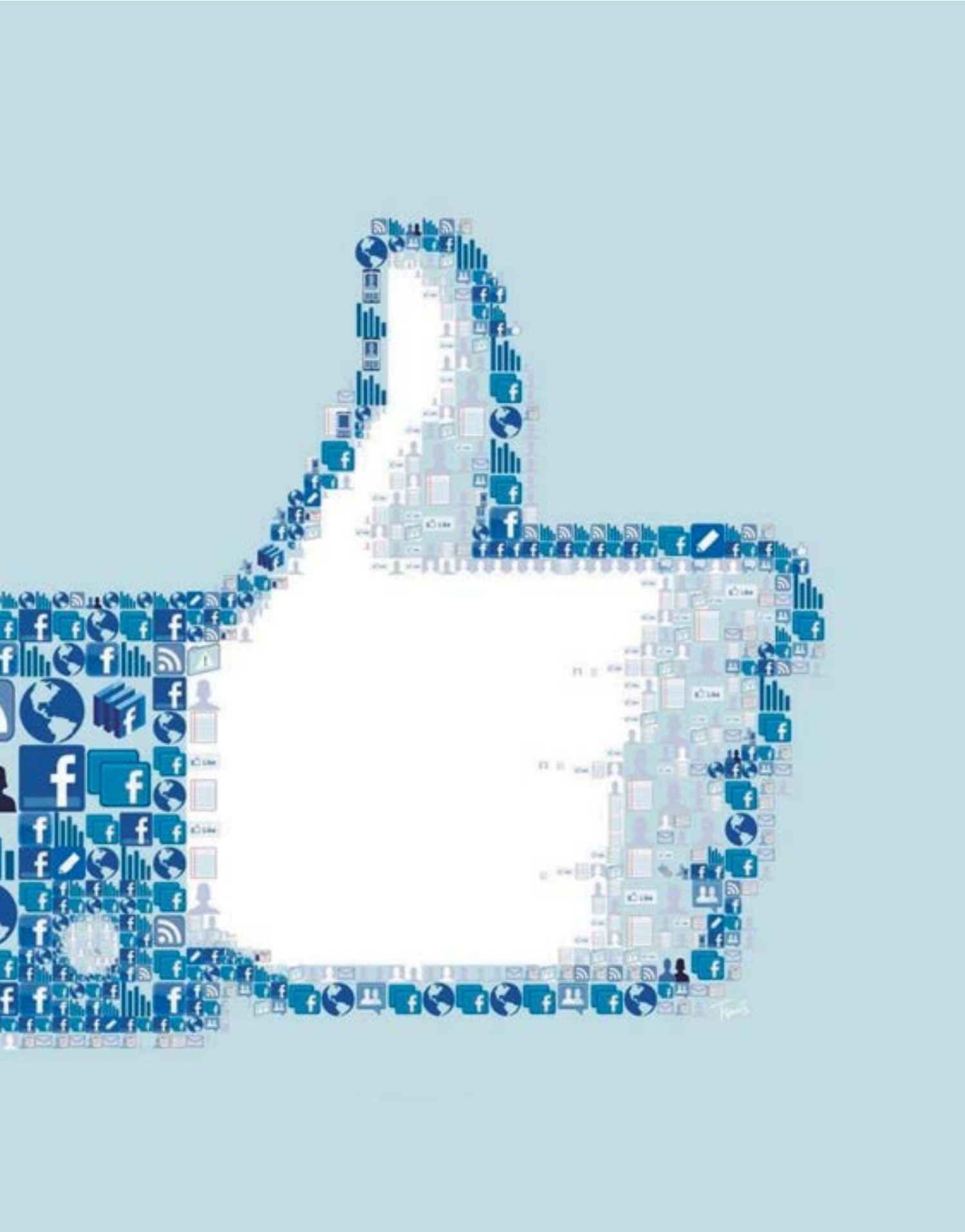
•Lo mejor es no hacer ese tipo de fotos. Es importante saber que las fotos, igual que otros archivos, pueden caer en manos de personas con malas intenciones de muchas maneras, como por la pérdida o robo de un teléfono u otro equipo, el efecto de un virus informático, el mal uso de un familiar o amigo al que le prestamos nuestro dispositivo o un simple un despiste con nuestra privacidad. Indudablemente, si queremos mantenernos a salvo del riesgo de perder nuestras fotos de desnudos, lo más efectivo será no hacerlas nunca.

•Convencer a los menores de que lo pueden contar. Exponiéndoles el problema a la edad adecuada, con seriedad pero de forma abierta y sin tapujos, conseguiremos que lo identifiquen como un tema del cual "se puede hablar". El objetivo sería convencerles de que deben compartir con sus padres o algún adulto de confianza cualquier situación extraña que les pueda preocupar con respecto a los contactos sexuales por Internet.

•Denunciar si cae alguna en sus manos. Si alguna vez reciben alguna imagen o vídeo con contenido sexual de alguien conocido y especialmente si se trata de un menor, nunca compartirlo, pero sí deben avisar a sus padres y denunciar el hecho a la Policía.

QUÉ DENUNCIAR EN FACEBOOK Y CÓMO HACERLO.

Por JMPÉREZ



Facebook, la red social utilizada por más de 1.300 millones de personas en el mundo, se ha convertido en una "sociedad paralela", en la que las personas conviven y se relacionan y donde, cómo no, surgen conflictos, riñas, insultos y otros problemas cotidianos.
Como en la vida real, si somos molestados o somos testigos de que algo no cumple con la Ley, podemos, incluso debemos denunciarlo. En esta enorme red social también tenemos mecanismos para denunciar las conductas que no cumplen con las normas impuestas por los administradores. En principio están pensadas para procurar la seguridad de las personas y conseguir que todos podamos sentirnos cómodos independientemente de nuestros orígenes o creencias. Por nuestra seguridad y por una convivencia más cordial, debemos hacer uso de esta herramienta de denuncia siempre que sea necesario. Pero en realidad, no todos los usuarios conocemos los comportamientos clasificados como "denunciables" para Facebook. Podemos sentirnos molestos por algún comentario o imagen desagradable, pero quizá no infrinjan las normas del juego y por tanto sería inútil denunciarlas.
Y lo que es más importante, conociendo estas normas comunitarias, aprenderemos a reconocer qué podemos compartir y qué debemos evitar si queremos mantenernos a salvo de problemas.

¿Qué podemos denunciar?

La lista es bastante larga, tanto que Facebook ha creado una página donde nos explica qué conductas podemos denunciar y las razones por las que cree que debe prohibirlas y las agrupa en cuatro grandes apartados:

1. Ayudar a mantenernos a salvo, donde encontramos comportamientos como:

- Fomentar el suicidio y las autolesiones, incluidos los trastornos alimentarios. Estos temas se pueden tratar siempre que no sea para fomentarlos.
- Cualquier contenido que trate sobre explotación sexual, incluidas las simples peticiones de material sexual y las ofertas de estos servicios.
- El acoso, como insultos, imágenes con la finalidad de avergonzar a alguien modificadas o no, información compartida para chantajear, incluso el envío reiterado de solicitudes de amistad a quien no quiere recibirlas.
- Aunque permiten debates sobre personajes públicos, debemos evitar las amenazas y los mensajes que inciten al odio de esas personas.

2. Fomentar un comportamiento respetuoso

- Están prohibidos los desnudos, aunque con una gran cantidad de matices que limitan lo que podemos y no podemos mostrar y las relaciones sexuales, incluidas las descritas solo con texto.
- No permitirán cualquier contenido que incite al odio o pretenda discriminar por cualquier razón, como raza, religión, discapacidades, orientación sexual…
- Eliminaran imágenes sobre violencia, especialmente las relacionadas con ataque terroristas y que se comparten por sadismo.

3. Proteger tu cuenta e información personal

- Teóricamente, todos los perfiles personales deben corresponder al nombre real y eliminarán el perfil si detectan que se trata de una suplantación de identidad.
- No podemos tener más que un perfil por persona.
- Podemos utilizar las páginas para crear presencia en Facebook de mascotas, organizaciones, personajes fantásticos, etc.
- Los fines comerciales no son consentidos, a menos que pagues por los anuncios, claro.

4. Proteger tu propiedad intelectual

- Para publicar algo, debemos tener la propiedad o los derechos para hacerlo. Eliminarán contenido compartido con derechos de autor, las marcas comerciales y cualquier otro derecho de propiedad intelectual.

Si te interesa ampliar información, no dejes de visitar su página que encontrarás en correcto español titulada Normas Comunitarias.

¿Cómo denunciar?

Ahora que ya sabemos qué tipo de información presente en Facebook podemos denunciar, veamos cómo hacer uso de las herramientas que nos lo permiten.
En realidad, aquí Facebook ha hecho una gran labor. Encontramos la posibilidad de denunciar prácticamente todo lo que allí vemos. Perfiles, comentarios, páginas, fotos, anuncios, etc. Incluso pone a disposición del público un formulario para denunciar contenido que no podemos ver, pensado para que la denuncia la formulen incluso personas que no tienen cuenta en la red social.
Explicar cómo formular la denuncia en cada uno de los lugares posibles sería demasiado extenso, pues éstos son muchos y variados: perfiles, publicaciones, publicaciones de la biografía, fotos y vídeos, mensajes, páginas, grupos, anuncios, eventos y preguntas.
Solo hay que agudizar un poco nuestra observación y buscar algún elemento desplegable o menú de opciones relacionado con el contenido publicado. A modo de ejemplo, veamos dónde encontrarlo para:

Denunciar una publicación. Abrir el desplegable que encontramos en la esquina superior derecha de cada publicación.

Denunciar un perfil. Desde el botón con tres puntos que encontramos en su foto de portada, situado en la esquina inferior derecha.

Denunciar una foto. Cuando vemos la foto en el visor de imágenes, la posibilidad la encontramos en el apartado 'Opciones'.

Si no sabes cómo denunciar algún elemento en Facebook, consulta su página de ayuda relacionada.
Defiéndete de los que infringen las normas de convivencia, no lo dejes pasar.

RANSOMWARE: EL SECUESTRADOR DE NUESTROS ARCHIVOS.

Por Patricia B

De un tiempo a esta parte, tenemos un nuevo campeón indiscutible dominando en el universo del malware. En un principio, parecía que sería como cualquier otro virus o troyano a los que ya estamos acostumbrados, pero hemos ido viendo como su poder y popularidad ha ido creciendo de manera exponencial con el paso del tiempo. Hablamos del ya famoso ransomware. Fíjense si es famoso que hasta tiene un papel muy relevante en un capítulo de la última temporada de una conocida serie de televisión (y no vamos a decir más).

Todos aquellos que trabajamos dentro el ámbito de la seguridad de la información, ya conocemos a este espécimen, pero por si hay alguien que aún no tiene claro de lo que estoy hablando, explico brevemente al tipo de malware al que me refiero.

Conocemos como ransomware a todo aquel malware que nos bloquea el acceso a (parte o toda) la información almacenada en el dispositivo comprometido, mediante el cifrado de ésta con una clave que desconocemos, y que pide un rescate económico a cambio de recuperar el acceso a dicha información.

Dos ejemplos a nivel nacional que se han propagado ampliamente han sido el Virus de la Policía y la campaña de Cryptolocker que suplanta a Correos mediante un email. Ambos han tenido gravísimas consecuencias para mucha gente a nivel personal. Incluso a nivel corporativo ha habido múltiples casos de empresas cuyos procesos de negocio se han visto afectados de forma crítica como consecuencia de una infección con ransomware.

De hecho, el Virus de la Policía vuelve a estar activo. La última versión está enfocada a dispositivos Android y aunque parece

que no cifra la información almacenada, sigue siendo un incordio. Así que ya sabéis, sed precavidos y tened cuidado con las apps que descargáis.

El problema de este tipo de malware es que en algunos casos, ni pagando el rescate se ha conseguido recobrar el acceso a la información. Ha habido víctimas que después de pagar el rescate no han podido descifrar la información bloqueada o que incluso no han encontrado forma de pagarlo.

Lo cierto es que la Policía recomienda no pagar el rescate que se pide, ya que haciéndolo estamos fomentando que se continúe con la propagación del ransomware y de su chantaje asociado.

Son muchas las variantes que circulan ahora mismo y aunque las medidas preventivas a aplicar pueden parecernos básicas e incluso triviales, nunca está de más recordar aquello de:

- Sé precavido con los enlaces que recibes en los correos electrónicos.
- Los adjuntos también deben tratarse con delicadeza, por si acaso.
- Evita reenviar correos innecesarios, aunque el gatito del adjunto sea adorable.
- Mantén tus dispositivos y aplicaciones actualizados.
- Ten instalado y actualizado un antivirus en todos tus dispositivos.
- Haz copias de seguridad de tu información de manera periódica.

Este tipo de malware se ha extendido y diversificado tanto que el CCN-CERT publicó un documento oficial en el mes de Abril en el que hablaba de las principales variantes [PDF] y cómo desinfectar o recuperar los archivos cifrados, en caso de que se pudiera.

Un caso curioso es el del autor del ransomware Locker (CryptolockerV) que ha pedido perdón por las consecuencias de su software, se ha compadecido de las víctimas y parece que ha publicado las claves para descifrar la información secuestrada. No se ha confirmado que haya publicado todas ellas ni tampoco se sabe con certeza si todos los afectados por este ransomware han conseguido recuperar el acceso a su información.
A veces no somos conscientes del valor de la información que manejamos hasta que viene alguien y nos la quita, o nos quita el acceso a ella como en este caso.

"PROTECT YOUR INFORMATION AND DEVICES, AND LET IT RAIN."

NO TE FÍES FALSAS AP

Por Lupe

Soy Lupe, una joven de 18 años que ya he colaborado en alguna otra ocasión en este blog y hoy comparto una historia real que me ha ocurrido a mí misma. Aunque no soy la víctima, he sido testigo de un caso que me ha parecido interesante contar por si a alguien le puede servir de ayuda y le "abre los ojos" ante situaciones parecidas que ocurren continuamente en Internet.

Lo que cuento es completamente real y me ha sucedido hace solo una semana. Solo he cambiado los nombres de las personas implicadas para mantener su privacidad.

Hace unos días fui la intermediaria de uno de tantos problemas que se dan a raíz de las Redes Sociales. Es un problema que se da mucho pero no le das importancia hasta que no te pasa a ti mismo/a. Se trata de la suplantación de identidad y posterior intento de acoso.

Me habló una chica de otra ciudad de España a través de mensajes privados de Instagram, quería preguntarme algo muy importante y me dio su número de Whatsapp. Yo no quise dárselo hasta que no me adelantara de qué trataba eso tan importante.

En cuanto me nombró a uno de mis mejores amigos y me dijo que eso tan importante estaba relacionado con él, le hablé por Whatsapp. Le dije que me contara qué es lo que pasaba y me contestó que hace 4 meses conoció a un chico por Instagram que supuestamente se llamaba "Andrés García".

Irene, la chica que me habló, y "Andrés" estuvieron conociéndose hasta que él consiguió gustarle a ella, sin haberse visto nunca en persona. Hablaban por Facebook ya que él se suponía que no tenía Whatsapp, en cambio sí Instagram, Facebook y Twitter.

Hace unos días, "Andrés" le pasó una captura de pantalla del Instagram de mi amigo Carlos y le dijo a Irene que denunciara esa cuenta porque se estaba haciendo pasar por él subiendo fotos suyas (supongo que para provocar que Instagram bloqueara la cuenta de Carlos y éste no se diera cuenta de que le estaban suplantando su identidad).

A Irene le pareció muy raro y estuvo husmeando esa cuenta de Carlos. Gracias a los comentarios de las amigas en la cuenta de Carlos, consiguió dar con mi Instagram y preguntarme por privado si yo conocía a Carlos. Yo le contesté que él es mi amigo y de la ciudad de donde somos. Finalmente ella se dio cuenta de todo lo que le estaba sucediendo, y me lo explicó.

Alguien que se hacía llamar Andrés, se hizo pasar por mi amigo Carlos subiendo fotos suyas tanto en Instagram como en Twitter y en Facebook. "Andrés" le había hecho pensar a Irene que ya eran novios y le pidió que le pasara fotos calientes. Ella confiada le hizo caso y ahora que se ha dado cuenta que nadie conoce a esa persona, se arrepiente de haber confiado en alguien que sólo conoce a través de redes sociales. Irene tiene solo 15 años.

Además "Andrés" lo hizo todo más creíble ya que falsificó otras cuentas de amigas de Carlos para hacerle ver a Irene que son sus primas, amigas etc. De este modo, también suplantó la identidad de una amiga en común de Carlos y mía. Utilizó sus fotos en otro perfil falso y se hizo pasar por una supuesta prima de "Andrés" con la que simulaba una relación normal.

DE LAS ARIENCIAS

Ahora estas cuentas falsas han sido denunciadas a la Policía por mis dos amigos y menos mal que el supuesto "Andrés" no ha conseguido hacerle, todavía, una amenaza usando las fotos calientes que Irene la pasó. Espero que lo pillen antes que pueda hacerlo.

Espero que mi historia sirva para que no confiéis en personas que solo conocéis en Internet ya que no es posible saber quién está detrás de los perfiles de las Redes Sociales.

La suplantación en Internet cada vez es más frecuente en las Redes Sociales.

CAMBIA EL USUARIO Y CONTRASEÑA POR DEFECTO DE TU CÁMARA IP

Por JMPÉREZ

En el mercado abundan las cámaras que podemos conectar a nuestra red Wifi y nos permiten observar a distancia y a tiempo real lo que deseemos. Son conocidas genéricamente como cámaras IP y hoy resultan fácilmente asequibles para cualquiera por su reducido precio.

Encontramos una enorme gama a poco que busquemos por Internet. Además de las disponibles en tiendas físicas, la oferta online es interminable. Hay tiendas especializadas en la venta de estos dispositivos en Internet, pero también es un artículo que se vende extensamente en tiendas genéricas internacionales como Ebay o Amazon.

Sus impresionantes posibilidades y especialmente su bajada de precio hacen que sea un artículo con gran éxito de ventas y que está extendiéndose por muchos hogares. Las cámaras IP procedentes de China están disponibles desde escasamente 40 euros y nos ofrecen posibilidades tan llamativas como las siguientes:

•Se conectan a Internet por cable o por Wifi.
•Visión remota desde un teléfono u ordenador conectado a Internet. La mayoría disponen de su propia aplicación para Android o iPhone.
•Movimiento de la cámara motorizado desde remoto.
•Visión nocturna gracias a una serie de leds que emiten luz infrarroja y que se conectan automáticamente en la oscuridad.
•Posibilidad de emitir alarmas que nos llegan a nuestro dispositivo si detectan movimiento o sonido, incluso con imágenes por correo electrónico.
•Disponen de altavoz y micrófono.

Estos dispositivos no son nuevos, ya hace algunos

años que aparecieron en el merado, pero conforme avanza el tiempo resultan cada vez más accesibles. Son conocidos los problemas de privacidad que han ocasionado, sobre todo las primeras versiones que aparecieron con importantes fallos de seguridad, lo que ocasionó que miles de cámaras que en principio debieron ser privadas, acabaran siendo disponibles para todo aquel curioso que investigara un poco por Internet.

Con el tiempo, los principales fabricantes han corregido sus brechas de seguridad y mejorado los sistemas para evitar la acción de los hackers, pero de nada servirán estas mejoras si como usuarios no tomamos un mínimo de medidas para garantizar nuestra privacidad.

Consejos a usuarios de cámaras IP

El primero y más importante es:

1.¡Cambia el usuario y contraseña!
Las cámaras necesitan unas credenciales para que podamos efectuar la conexión inalámbrica, simplemente un nombre de usuario y una contraseña. Los fabricantes, normalmente, proporcionan sus dispositivos con unas credenciales estándar y conocidas, como "admin, admin" y a menudo la contraseña ni existe, como el caso de la siguiente imagen correspondiente a una etiqueta de identificación de la base de una cámara IP convencional.

No cambiar estos datos es como dejar nuestra cámara disponible a los ojos de cualquier curioso de Internet. Debemos configurar estos datos para que sean diferentes a los de fábrica y que no puedan ser adivinados por sistemas automáticos. El modo de hacerlo será diferente para cada modelo, pero deberemos buscar algún menú de opciones similar al siguiente tras conectarnos inicialmente con las credenciales de origen.

- La contraseña que registremos debe ser robusta, es decir, debe ser muy larga, mayor de 12 caracteres preferiblemente y estar formada por números, minúsculas, mayúsculas y símbolos y a ser posible que carezca de significado.
- No debemos utilizar la misma contraseña para otros lugares.
- Debemos cambiarla regularmente para una mayor seguridad.

2.Actualizaciones del firmware. Las actualizaciones que los fabricantes lanzan tanto para el sistema de la propia cámara como para las aplicaciones que las gestionan suelen tener como objetivo solucionar problemas conocidos de seguridad. Debemos consultar el manual de la cámara o el servicio al cliente para conocer si existe esa posibilidad y el modo de llevarla a cabo.

3.Configurar la seguridad del router Wifi. Para evitar la conexión a nuestra red inalámbrica que facilitaría el espionaje de la cámara por vecinos próximos, debemos configurar nuestro router wifi con la mejor protección disponible, WPA2.

4.Cuidado con la protección de datos. La Agencia Española de Protección de Datos (AEPD) insiste en la necesidad de proteger adecuadamente el acceso a este tipo de cámaras y recuerda que su uso como dispositivos de vigilancia de seguridad solo pueden llevarlo a cabo las empresas debidamente autorizadas. No obstante, podemos utilizarlas siempre que sea en un entorno privado y familiar.

Por tanto, cuidado con instalar estas cámaras en lugares donde pudieran aparecer personas ajenas a la familia y que pudieran reconocerse.

¿SOSPECHAS QUE HUSMEAN EN TU TELÉFONO?

¡HAZ UNA FOTO SECRETA A LA CARA DE QUIEN LO INTENTE!

POR JMPÉREZ

Si tienes confianza suficiente con ciertas personas para dejarles el móvil, pero no tanta como para que lean conversaciones o vean fotos personales, CM Security es la aplicación que necesitas. CM Security es una aplicación para móviles y tablets Android que, entre otras cosas, permite bloquear el acceso a cualquier aplicación de nuestro dispositivo mediante el uso de un patrón de pantalla. Además, cuenta con funciones tan variadas como la limpieza de archivos "basura", de elementos sensibles a la privacidad, detección de posibles amenazas instaladas, localización a distancia o borrado remoto de la memoria.
Hasta aquí nada nuevo, pero lo que hace de esta herramienta algo destacado es que podemos programarla para que si alguien intenta el desbloqueo de una aplicación y no lo consigue, la cámara frontal le haga una foto y la guarde, incluso que nos la envíe inmediatamente por correo electrónico, todo de forma silenciosa.

Las funciones que anuncia esta App son tan interesantes como las siguientes:

- AppLock, bloquea tus fotos, galería y mensajes de ojos y amigos curiosos o impide que tus hijos compren aplicaciones y juegos no deseados.
- Limpieza u optimización del dispositivo.
- Localiza tu teléfono en un mapa a través de su web. Requiere registro inicial.
- Hazlo sonar al máximo para encontrarlo.
- Escanea aplicaciones y sistema para detectar aplicaciones pre-instaladas e instalados y el sistema de archivos para mantener el teléfono a salvo de virus, troyanos, malware y spyware.
- Escanea profundamente las tarjetas SD, detectando y eliminando amenazas.
- Previene el daño en su dispositivo con el análisis en tiempo real de las nuevas aplicaciones y actualizaciones.
- Previene el acoso mediante el bloqueo de llamadas entrantes no deseadas.
- Navegación y phishing: bloquea los sitios web maliciosos y protege contra los sitios web que pueden suplantar la identidad con notificaciones de alerta instantánea.

La confianza tiene unos límites y esta App se encarga de recordárnoslo.

S2 GRUPO

Anticipando un mundo
ciberseguro