NEWS ADSI FLASH
www.adsi.pro

Índice

Cena Anual de ADSI 2018

Jueves, 22 de noviembre, 20:00 horas.
Hotel Fairmont - Rey Juan Carlos I Barcelona

Un año más ADSI celebrará el evento de mayor relevancia de nuestra Asociación, la Cena Anual de ADSI.

Durante la misma se hará entrega de los premios ADSI.

Asociación de Directivos de Seguridad Integral
ADSI

Será un honor para esta Junta Directiva celebrar tan señalado evento acompañado de Socios, Patrocinadores y amigos de ADSI.

Nuestros Patrocinadores

Cena anual de ADSI 2018

Jueves, 22 de noviembre, 20:00 horas.
Hotel Fairmont - Rey Juan Carlos I Barcelona

Av. Diagonal, 661-671 Barcelona 08028

El jueves 22 de noviembre, un año más, **ADSI** celebrará el evento de mayor relevancia de nuestra Asociación, la **Cena Anual de ADSI**.

La **Cena Anual de ADSI** se constituye como el mayor punto de encuentro de **socios, patrocinadores** y amigos de nuestra Asociación.

En el transcurso de la Cena se efectuarán los siguientes actos:

- Entrega de los **Premios ADSI 2018**
- Discurso del **Presidente de ADSI, Don. Francisco Poley**

Durante la cena dispondremos de un espacio donde charlar relajadamente para comentar nuestras experiencias de este año y los planes de futuro para el siguiente.

Para evitar que el control de acceso al acto pueda retrasar el inicio de los mismos, os rogamos la máxima puntualidad. El mostrador de acreditaciones se abrirá a las 19:30 h, media hora antes del comienzo del aperitivo.

Precios de asistencia a la Cena Anual 2018:
- **Socio de ADSI 60,00 €**
- **No Socios de ADSI 85,00 €**

INSCRIPCION DE SOCIOS A LA CENA ANUAL

Rogamos a todos los socios de **ADSI** que deseéis asistir a este importante evento de nuestra Asociación, nos lo comuniquéis antes del **18 de NOVIEMBRE**.

Para ello pulse en INSCRIPCION y rellene el formulario que aparece:

INSCRIPCION

Seguidamente recibirán un mail de confirmación.

Como siempre, emitiremos el correspondiente cargo por el evento para facilitar los trámites a nuestros asociados.

INSCRIPCION DE NO SOCIOS Y EMPRESAS A LA CENA ANUAL

Aquellas personas, profesionales, amigos o acompañantes que no sean Socios de **ADSI**, así como empresas que deseen asistir a **la Cena Anual, pueden dirigir su petición de reserva de plaza, o de mesas por parte las empresas, hasta el 18 de NOVIEMBRE**, a los correos electrónicos:

Luis Gomez: secretario@adsi.pro
Elvira Marquez: tesorero@adsi.pro

Indicando en el asunto del correo *"Cena Anual ADSI 2018"* y adjuntando el correspondiente justificante del pago del importe de la cena.

El pago deberá realizarse a la siguiente cuenta bancaria de la Asociación:

CAIXA D'ENGINYERS ES56 3025 0004 3314 3323 5294

Indicando como referencia ***Inscripción cena Anual ADSI 2018***, haciendo constar nombre y apellidos de las personas inscritas, o bien el número total de plazas reservadas, cuando se trate de empresas que todavía no conozcan los datos de sus invitados.xxx

Crónica *"Martes con..."* Estrategias de Seguridad y retos de futuro

Junta Directiva ADSI

El pasado 06 de noviembre celebramos un *"martes con..."* en la Región Policial Metropolitana zona norte de Mossos d'Esquadra bajo el título Estrategias de Seguridad y retos de futuro llevada a cabo por la Jefa de la RPM **Cristina Manresa i Llop**.

Cristina Manresa tuvo el detalle de realizar la ponencia en la misma sala donde se reúnen los mandos de la RPM zona norte para coordinar los quehaceres diarios.

Un café con una botella de agua y un pequeño detalle dulce nos anunció lo que sin duda sería una más que agradable reunión.

Cristina se mostró en todo momento muy cercana, convirtiendo su ponendia en un debate en toda regla en torno al actual modelo de Seguridad pública/privada y a los retos a los que nos enfrentamos.

Nos ofreció datos sobre la Región Policial Metropolitana Norte de la que ella está al mando , indicandonos que tiene una población de más de dos millones de habitantes, una superficie de 1.750 km², 2.719 efectivos policiales de Mossos d'Esquadra, 2.678 efectivos de policías locales y está compuesta por 11 ABP y 9 CD.

Nos explicó como está estructurada la RPMN y los servicios de los que dispone, unidades regionales, áreas de investigación, unidades territoriales, unidades de recursos operativos, sala regional de mando, área regional de tránsito, sector de mobilidad, oficina de soporte regional, áreas básicas policiales y un largo etcetera que da la dimensión de la ingente labor que desarrolla diariamente.

También nos dio datos estadísticos de territorio, población, detenciones e incidentes con respecto al total del territorio catalán, nos citó los mayores riesgos que actualmente están tratando y cual es su evolución. Así mismo nos indicó las infraestructuras presentes en la RPMN, como hospitales, aeropuerto, circuito de Montmeló, centros de menores, UAB etc.

En la parte final de la ponencia nos habló de las estrategias de futuro haciendo especial incapié en la inteligencia policial, delitos en la red, ciberdelitos, etc. dejándonos tres premisas a seguir en la seguridad, como son, la prevención, la prospección y la visibilidad.

En definitiva la ponencia fue muy lucrativa, el debate generado durante el transcurso de la misma estuvo cargado de anecdotas e interesantísimas reflexiones, no solo de parte de Cristina sino de todos los allí presentes.

Cristina Manresa nos abrió las puertas de su casa y nos acogió con enorme cariño, desde **ADSI** queremos agradecerle este *"martes con..."* de tan alto nivel.

Inteligencia: Entender o Anticipar

Fuente: GESI
José Miguel Palacios
Coronel de Infantería y Doctor en Ciencia Política

Quizá las dos principales ambiciones de la inteligencia sean comprender el presente –en sentido amplio, incluyendo el pasado próximo– (podría asimilarse al popular concepto de situation awareness) y anticipar el futuro (warning). Distintos servicios, distintas comunidades de inteligencia, distintos países pueden dar más importancia a una o a otra de estas dos grandes líneas de trabajo, aunque, en mayor o menor medida ambas están siempre presentes.

La inteligencia americana, por ejemplo, se ha mostrado particularmente preocupada por evitar la sorpresa estratégica, quizá a causa de experiencias traumáticas como Pearl Harbour o el 11S, que tanta influencia han tenido en el desarrollo de la comunidad y de sus servicios componentes. Y siguiendo una orientación bastante distinta, los servicios británicos han estado en general más orientados hacia la comprensión de la situación y de sus factores (inteligencia explicativa).

Los británicos, en cualquier caso, parecen estar en minoría. Todos los servicios que se inspiran en los modelos americanos (la mayoría de los occidentales) muestran un interés particular por la inteligencia predictiva (prospectiva o estimativa), en general bajo forma de "alerta temprana".

En el fondo, ambas orientaciones son menos distintas de lo que a primera vista parecen. Porque la buena comprensión de la situación es un requisito casi imprescindible para formular un buen pronóstico. Y aquellos que saben bien dónde están pueden prever, a menudo con un margen de error aceptable, dónde pueden encontrarse a corto o corto/medio plazo (los plazos largos son casi irrelevantes para la política real).

Si sabemos que a las 16.30 dos individuos han cometido un atentado terrorista en la Plaza de la Concordia de París y que han huido a pie del lugar del atentado no es difícil tener una idea aproximada de dónde pueden encontrarse a las 17.00. Y, sobre todo, de dónde no pueden encontrarse. Por ejemplo, es prácticamente imposible que hayan abandonado el país. Este conocimiento prospectivo, derivado de una exacta comprensión de la situación actual, es el que se utiliza en la práctica para poner en marcha 'operaciones jaula' tras sucesos de este tipo.

Tradicionalmente, la inteligencia prospectiva ha estado muy basada en la intuición de los analistas. En la actualidad, sin embargo, modelos matemáticos que hacen uso de la capacidad de computación de los ordenadores, permiten formular predicciones mucho más exactas, menos dependientes del talento (y de los sesgos) de los equipos analíticos. Sin embargo, esta mayor calidad técnica de la predicción puede no traducirse en absoluto en una mejor alerta que permita a los decisores políticos adoptar las medidas adecuadas antes de que las amenazas se materialicen.

El problema con las alertas es que su efectividad no depende únicamente del que las lanza, sino, sobre todo, del que las recibe. En 2007, la Comisión Europea organizó en Bruselas una conferencia bajo el lema "From early warning to early action - developing the EU's response to crisis and longer-term threats". Y el propio planteamiento inicial ya indicaba la idea fuerza que la Comisión deseaba transmitir: lo importante de

verdad es que las alertas den lugar a respuestas políticas eficientes, oportunas en tiempo y forma. De manera que la transmisión de la alerta y, sobre todo, su recepción pasan a tener una importancia capital. Y aquí surgen los problemas:

1. Los decisores políticos tienen una confianza limitada en la capacidad de la inteligencia (o de cualquier otro proveedor alternativo de conocimiento) para prever el futuro.
2. Aunque bastantes decisores puedan sentirse fascinados por el progreso científico y las posibilidades que las nuevas tecnologías ofrecen, es muy frecuente que confíen poco en instrumentos y metodologías cuyo funcionamiento no pueden entender. En 1975, poco después de la guerra del Yom Kippur (una sorpresa estratégica que Israel no había sido capaz de anticipar) el Ministro de Asuntos Exteriores israelí Ygael Alon encargó a un equipo formado por un conocido psicólogo (especializado en la psicología de la decisión) y a un analista de inteligencia que le prepararan un informe sobre cuáles serían las consecuencias de los posibles resultados de las negociaciones, entonces en curso, entre Israel y Egipto (con mediación norteamericana). El equipo planteó el proyecto desde el punto de vista de la Teoría del Análisis de Decisiones y llegó a unos resultados que fueron recibidos con indiferencia en el Ministerio: "The minister remarked politely that the probabilities were 'interesting'". Parece claro que los decisores no comprendían la base científica del informe que les presentaban y no creían, por ello, que los resultados que proporcionaba fueran correctos. O, si acaso, aceptaban que lo eran en la medida en que coincidían con su propio análisis, basado en la experiencia personal y/o grupal procesada con sentido común.
3. Finalmente, hay que tener en cuenta que cualquier medida política que se adopte tiene un precio, en términos de capital político. Cuando un gobierno toma una determinada medida en respuesta a una alerta, gasta capital político (porque la medida supondrá uso de recursos, que podrían emplearse con otros fines más populares, o puede entrañar la limitación de ciertos derechos o libertades), pero, como el público no conoce en detalle los motivos reales de alarma, puede entender que la respuesta es injustificada. Recuérdese el debate en España sobre el famoso 'comando Dixán'.

Una conclusión que quizá no compartan todos los lectores. En inteligencia la explicación del presente (en sentido amplio) es el objetivo fundamental que debemos intentar alcanzar. Si los decisores comprenden bien la situación, estarán en magníficas condiciones para tomar unas decisiones que no solo se aplicarán en un espacio futuro, sino que, en gran medida, contribuirán a conformarlo. En el terreno militar se ha dicho que "suele ser comparada la previsión de los grandes capitanes a la mirada del águila que, remontándose en pleno día a inmensa altura, ve mil secretos escondidos a los vulgares ojos". Es un talento que a menudo se denomina 'coup d'oeil' y que Clausewitz definió como "el hallar una verdad que se oculta a la mirada habitual de la inteligencia, o que solo se hace visible tras larga y reflexiva consideración". El gran capitán lo es por tomar decisiones correctas en medio de la incertidumbre (una incertidumbre en gran parte debida al carácter futuro de muchas de las amenazas a las que se va a enfrentar), y quizá baste con que comprenda bien la situación actual para estar en mejores condiciones de decidir con eficacia. Quizá no sea necesario que le digamos con antelación qué es lo que va a ocurrir.

Entre los gurús de la inteligencia moderna, Greg Treverton es uno de los que ha defendido este enfoque: "In the world looking to 2010 and beyond, the business of intelligence will be information defined as a high-quality understanding of the world using all sources, where secrets matter much less and where selection is the critical challenge". Incluso para un autor como Tom Fingar (otro de nuestros gurús), apasionado defensor de la inteligencia estimativa, el fin último de la inteligencia es (ayudar a) dar forma al futuro, no predecir cómo será.

Evolución de la agenda de ciberseguridad de la Unión Europea

Fuente: Real Instituto El Cano

Javier Alonso Lecuit

La agenda de ciberseguridad de la UE ha evolucionado significativamente desde el primer Plan Estratégico de Ciberseguridad en 2013 para incorporar nuevas medidas en defensa de la seguridad, prosperidad y libertades de los ciudadanos frente a las amenazas y vulnerabilidades disruptivas del ciberespacio.

La Red se ha convertido en un escenario de competición geopolítica y económica entre Estados donde se entremezclan ciberataques, ciberdelitos y desinformación con un propósito desestabilizador. En un primer estadio, la seguridad en la Red (ciberseguridad) se orientó a proteger la integridad, confidencialidad y disponibilidad de las redes y sistemas de información mediante medidas técnicas de seguridad perimetral. Para ello se utilizaron tecnologías orientadas a la detección rápida y la neutralización de las amenazas, el análisis dinámico de las vulnerabilidades de las redes y una respuesta eficaz ante ciberincidentes maximizando la capacidad de recuperación o resiliencia de los sistemas de información.

Desde 2013, los tipos de amenazas e incidentes se han ampliado significativamente en número y gravedad, sin por ello disminuir el número de ciberataques dirigidos a terminales de usuarios, redes de comunicaciones y sistemas de información, con objetivos muy distintos. Entre otros, la obtención masiva de datos de carácter personal y de secretos comerciales; la manipulación de la opinión pública a través de redes sociales en procesos electorales; el uso de Internet para la preparación y consecución de ataques terroristas; ciberataques con motivaciones económicas a las corporaciones orquestados con el apoyo de los Estados, o la desestabilización política de los Estados democráticos mediante amenazas híbridas apalancadas en las capacidades de desinformación llevadas a cabo a través del ciberespacio. Esta dinámica se ve acentuada por varios factores que dificultan la gestión de estos nuevos riesgos, tales como la vertiginosa evolución tecnológica, la digitalización de todos los ámbitos de la sociedad y la economía o la inmaterialidad y ausencia de fronteras del ciberespacio.

Desde la perspectiva de las vulnerabilidades, la concienciación y formación de los usuarios sigue siendo el gran talón de Aquiles de la ciberseguridad. A pesar de los esfuerzos realizados por las empresas, instituciones privadas y organismos gubernamentales para impulsar la cultura de la ciberseguridad, el grado de vulnerabilidad aumenta a medida que se acelera la digitalización de la sociedad. Otra fuente de vulnerabilidades de carácter endémico es la dependencia tecnológica por parte de los Estados y las empresas europeas de un reducido número de fabricantes de tecnología avanzada en el diseño de circuitos integrados, equipamiento, firmware, sistemas operativos e incluso aplicaciones ofimáticas de uso generalizado, producidas por un número muy reducido de países y desplegadas en las nuevas redes de comunicaciones, los sistemas de información o los terminales, entre otros. Esta concentración del mercado de alta tecnología potencia la existencia de vulnerabilidades, en ocasiones intencionadas, de tipo zero-day y puertas traseras a disposición de los servicios de inteligencia de esos Estados, que, con el tiempo, acaban filtrándose y comercializándose para su uso por organizaciones criminales que operan en Internet.

Desde la perspectiva del cambio tecnológico, son conocidas las vulnerabilidades que plantean los dispositivos conectados (Internet de las Cosas, IoT por sus siglas en inglés) a los sistemas de información con los que se comunican debido a diseños que no tienen en cuenta los requisitos de ciberseguridad desde la fase inicial. También aparecen nuevos retos técnicos, y en ocasiones éticos, relacionados con el uso de la Inteligencia Artificial (IA). Las funciones de ciberseguridad a distancia (remotización) plantean asimismo a las compañías clientes y a los responsables del tratamiento de los datos nuevos retos en materia de confidencialidad y protección de datos. El uso por los ciberdelincuentes de algoritmos de IA para la identificación de objetivos y para la preparación y la ejecución de ciberataques probablemente desencadene un salto cualitativo tanto en la virulencia de estos como en los mecanismos para su rápida detección, neutralización y respuesta (hack-back). Por otro lado, la posibilidad de contar con ordenadores cuánticos en un futuro relativamente cercano, aunque todavía indeterminado, supondrá una discontinuidad en materia de ciberseguridad, ya que los actuales esquemas de cifrado robusto perderán su validez al poder ser descifrados con rapidez. De ahí que algunos Estados estén ya invirtiendo recursos en la investigación de algoritmos de cifrado poscuántico, es decir, resistentes a las capacidades de descifrado.

En este contexto, para hacer frente al imparable crecimiento de ciberincidentes, la Comisión Europea estableció en 2013 el Plan Estratégico de Ciberseguridad de la UE, por el que designaba nuevas autoridades y normativas para la criminalización y persecución de los delitos cometidos en la Red. Se incrementó la supervisión regulatoria a los proveedores de Internet, se elaboró legislación en apoyo de las fuerzas y cuerpos de seguridad y se definieron los instrumentos de respuesta en materia de ciberseguridad, ciberdiplomacia y ciberdefensa con el objetivo de reforzar la

protección y las capacidades de respuesta de personas y Estados.

La Comisión elaboró una directiva sobre la seguridad de las redes y sistemas de información (Directiva NIS) para establecer unas capacidades comunes de apoyo, coordinación y respuesta entre los Estados miembros ante ciberincidentes que afectaran a las redes y sistemas de información utilizados por los operadores de servicios esenciales para la seguridad y la economía nacionales. Posteriormente, en septiembre de 2017, ha revisado la Estrategia Europea de Ciberseguridad y ha aprobado un amplio conjunto de medidas que a continuación se enuncian (The Cybersecurity Package). La Comisión ha propuesto convertir ENISA en una Agencia Europea de Ciberseguridad con mandato permanente que se encargaría de definir un marco europeo de certificación y estandarización de ciberseguridad en productos y servicios con carácter voluntario para simplificar, reducir costes y barreras administrativas (un proceso de certificación por producto válido en la UE), fomentar la "seguridad por diseño" y mejorar la información facilitada a los usuarios de productos y servicios. La agencia funcionaría como secretaría de la red europea de CSIRT, apoyaría a los Estados en la implementación de la Directiva NIS y en la gestión de incidentes y colaboraría en el desarrollo de capacidades y en la concienciación para la prevención de incidentes.

Para reforzar la capacidad de respuesta de la UE y de sus Estados miembros, la Comisión ha propuesto un plan rector (Blue Print) y la creación de un centro europeo de investigación y competencias y de un fondo de respuesta para emergencias de ciberseguridad. También ha liderado una propuesta de cooperación diplomática internacional en materia de ciberseguridad (CyberDiplomacyToolbox) que propone endurecer la respuesta diplomática conjunta de la UE y ampliar el ámbito de estas cibercapacidades a terceros países. En materia de ciberdefensa, la Comisión desea financiar la investigación e innovación en el marco de la Política Común de Seguridad y Defensa (Fondo Europeo de Defensa) y la colaboración con la OTAN.

Medidas para luchar contra la desinformación en línea

En el curso de los procesos electorales de estos últimos años, al menos 18 países han demostrado la manipulación de su electorado a través de Internet. Desde septiembre de 2015 se han probado 3.900 casos de desinformación favorables a los intereses del Kremlin, es decir, informaciones traducidas a varios idiomas y repetidas diariamente que contradicen hechos constatables por la propia opinión pública. A pesar de que la desinformación es un mecanismo de influencia utilizado desde tiempo atrás, este fenómeno alcanza una nueva magnitud en Internet debido a la capacidad de propagación viral mediante las plataformas online y, en particular, las redes sociales para originar y distribuir información falsa con el objetivo de influir en determinados colectivos (la difusión de noticias falsas es un caso particular de desinformación).

En la actualidad, la desinformación a través de noticias falsas en Internet no es un acto penado por la legislación, aunque varios Estados miembros estudian la posibilidad de establecer medidas legislativas. En este sentido, la Comisión ha adoptado sucesivas medidas con creciente determinación desde que presentó en abril de 2018 una comunicación en la que propuso un plan de acción orientado a la protección de procesos democráticos basado en potenciar cuatro principios: la transparencia de las fuentes de información y su financiación, la diversidad de información disponible en Internet y offline, la existencia de mecanismos que faciliten verificar la credibilidad de la información y el compromiso duradero de todas las partes que intervienen en el proceso de (des)información. La Comisión solicitó a las plataformas en línea que tuvieran un comportamiento proactivo, proporcionado y responsable para proteger a los usuarios frente a la propagación de noticias falsas, sin incurrir en limitaciones a la libertad de expresión, un comportamiento que evaluará a finales de 2018 con el propósito de adoptar medidas más agresivas si lo considera necesario.

En España, la actual Estrategia de Seguridad Nacional, aprobada en diciembre de 2017, hace referencia a las campañas de desinformación como parte de una estrategia planificada de guerra híbrida que combina desde las fuerzas convencionales hasta la presión económica o los ciberataques. También hace alusión al fenómeno de la posverdad, que intenta movilizar las emociones desdeñando el rigor de los hechos y en la que "la manipulación de la información por parte de agentes externos ejerce de factor de influencia en la era de la posverdad, con efectos negativos en la cohesión social y la estabilidad política".

Medidas para garantizar la ciberseguridad de las elecciones europeas

La Comisión Europea ha mostrado una gran preocupación por proteger los procesos electorales, en particular las elecciones europeas en mayo de 2019, del riesgo que constituyen los ciberataques dirigidos a los sistemas de información utilizados por partidos políticos, candidatos o las propias administraciones públicas en las campañas y procesos electorales, ataques que pueden afectar a la integridad y la equidad del proceso electoral. El 12 de septiembre de 2018 la Comisión propuso un conjunto de medidas para garantizar unas elecciones europeas libres y justas frente a riesgos como el de campañas masivas de desinformación en línea que persiguen desacreditar y deslegitimar elecciones, tal como se ha visto en el punto anterior; el uso ilícito de los datos personales, y los ataques contra la infraestructura electoral y los sistemas de información de campaña, riesgos que constituyen en su conjunto amenazas híbridas habitualmente

orquestadas desde Estados externos a la UE con propósitos desestabilizadores.

La Comisión ha elaborado, junto con las administraciones nacionales responsables de la ciberseguridad y ENISA, orientaciones específicas sobre las amenazas a la ciberseguridad, una comunicación con el fin de potenciar las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de ciberseguridad y la lucha contra las campañas de desinformación, así como orientaciones sobre la aplicación del Reglamento General de Protección de Datos de la UE y una enmienda legislativa que hace más rigurosas las normas sobre la financiación de los partidos políticos europeos. La Comisión insta a las autoridades nacionales, los partidos políticos y los medios de comunicación a que también adopten medidas para proteger sus redes y sistemas de información de amenazas de ciberseguridad.

Por su parte, el Grupo de Cooperación de la Directiva NIS, compuesto por un representante de cada Estado miembro y representantes de la Comisión y de ENISA, emitió en julio de 2018 un informe orientado a facilitar directrices de ciberseguridad y de gestión de incidentes, así como potenciar la cooperación estratégica entre los Estados, en relación con la seguridad de las redes y sistemas de información utilizados en las elecciones. Acompañando este conjunto de recomendaciones, la Comisión ha propuesto un reglamento para poner en común recursos y conocimientos técnicos en tecnologías de ciberseguridad. La Comisión plantea crear una Red de Centros de Competencia en Ciberseguridad con el fin de canalizar y coordinar mejor la financiación disponible para la cooperación, investigación e innovación en materia de ciberseguridad. Un nuevo Centro Europeo de Competencia en Ciberseguridad gestionará la ayuda económica con cargo al presupuesto de la UE destinado a ciberseguridad, lo que fomentará la inversión conjunta de la Unión, los Estados miembros y empresas del sector para fortalecer la industria de ciberseguridad de la UE y asegurar que los sistemas de defensa incorporen las técnicas más avanzadas.

La prevención de la difusión de contenidos terroristas en línea

La Comisión Europea incluyó en el paquete de medidas en materia de ciberseguridad presentado en septiembre de 2017 una comunicación con un conjunto de directrices y principios encaminados a potenciar la proactividad de las plataformas en línea a la hora de prevenir, detectar y eliminar contenidos ilícitos en la Red que inciten al odio, la violencia o el terrorismo. Esta comunicación era el primer paso de un proceso por el que iba a monitorizar la proactividad y el progreso experimentado en las plataformas de Internet durante los próximos meses para evaluar la posible necesidad de adoptar medidas adicionales que garanticen una rápida detección y eliminación de contenidos ilícitos en línea, incluyendo posibles medidas legislativas.

A tenor de los resultados obtenidos, la Comisión emitió en marzo de 2018 una recomendación para la adopción de un conjunto de medidas operativas más estrictas; entre otras, la adopción por los proveedores de procedimientos más claros de «notificación y acción» a fin de evitar que se retiren de forma accidental contenidos que no sean ilícitos; instrumentos proactivos para detectar y retirar los contenidos ilícitos, en particular contenidos terroristas o aquellos que no necesiten contextualización para considerarse ilícitos (por ejemplo, el material relacionado con abusos sexuales a menores o las mercancías falsificadas); salvaguardias más sólidas para garantizar los derechos fundamentales, y, en particular, la supervisión y verificación por humanos de mecanismos automatizados de detección y retirada de contenidos. La Comisión hizo un llamamiento a la cooperación más estrecha entre las distintas autoridades y a compartir las mejores prácticas en beneficio de las plataformas de menor tamaño, que habitualmente cuentan con unos recursos y unos conocimientos técnicos más limitados.

Asimismo, la Comisión propuso en septiembre de 2018 la adopción de un reglamento para la prevención de la difusión de contenidos terroristas en línea que establece como medida central la obligación de todas las empresas online a retirarlos, como norma general, en el plazo de una hora desde su notificación. Además, las empresas de Internet deberán introducir medidas proactivas, principalmente basadas en la detección automatizada, para retirar los contenidos terroristas o inhabilitar el acceso a ellos de manera eficaz y rápida y evitar que vuelvan a aparecer una vez hayan sido retirados. A fin de ayudar a las plataformas más pequeñas, las empresas han de compartir y optimizar los instrumentos informáticos adecuados y poner en marcha acuerdos de colaboración que favorezcan una mayor cooperación con las autoridades pertinentes, en particular con Europol. El reglamento insta a los Estados miembros a introducir nuevos procedimientos para tramitar las notificaciones con la mayor rapidez posible y asegurarse de disponer de las capacidades y los recursos necesarios para detectar, identificar y notificar los contenidos terroristas.

Medidas para la regulación del acceso a pruebas electrónicas

Las investigaciones policiales y judiciales de la UE se desarrollan en un contexto en el que más del 50% de las investigaciones penales incluyen —al menos— una solicitud transfronteriza para la obtención de pruebas electrónicas que obran en poder de prestadores de servicios establecidos en otro Estado miembro o externo a la UE. Casi dos terceras

partes de los delitos cuyas pruebas electrónicas se encuentran en otro país no pueden ser debidamente investigados o enjuiciados debido al tiempo necesario para recabar tales pruebas o debido a la fragmentación del marco jurídico, en el que la cooperación público-privada entre proveedores y autoridades es ineficiente, no existe un marco legal para la cooperación voluntaria trasfronteriza y no hay suficiente certeza legal sobre el uso de pruebas electrónicas en investigaciones transfronterizas. Para contrarrestar ese entorno tan perjudicial para las investigaciones, la CE propuso en abril de 2018 dos normas para facilitar a las autoridades policiales y judiciales la obtención de pruebas electrónicas necesarias para investigar, enjuiciar y condenar a delincuentes y organizaciones terroristas: un reglamento para el acceso transfronterizo a pruebas electrónicas (e-evidence) y una directiva que lo complementa con el propósito de armonizar la designación de los representantes legales de las compañías en línea.

El reglamento establece una orden de producción europea para la entrega de pruebas electrónicas en investigaciones transfronterizas que permitirá a la autoridad judicial de un Estado miembro solicitarlas directamente al prestador de servicios establecido en otro Estado de la Unión, con independencia de la ubicación de los datos. El prestador habrá de responder en 10 días máximo o en 6 horas en casos excepcionales. Asimismo, prevé una orden de producción de ámbito europeo para la conservación de las pruebas electrónicas en el curso de una investigación que impida el borrado de los datos. El reglamento se dirige a aquellos prestadores de servicios de información cuyo elemento definitorio del servicio que ofrecen sea el almacenamiento de datos. Incluye, entre otros, a proveedores de comunicaciones electrónicas, hosting y almacenamiento en la nube, redes de distribución de contenidos, plataformas de redes sociales, mercados online orientados a consumidores finales y negocios, comunicaciones vocales y proveedores de infraestructuras de Internet. El reglamento obliga a designar un representante legal en la UE, incluye garantías procesales y vías de recurso para la protección de los derechos fundamentales y ofrece seguridad jurídica tanto para las autoridades como para los prestadores de servicios.

Conclusiones

En un contexto creciente de amenazas y vulnerabilidades en el que la seguridad del ciberespacio excede actualmente el mero ámbito de la ciberseguridad de redes y sistemas de información, las autoridades europeas y nacionales amplían las iniciativas estratégicas y legales para hacer frente a este escenario cada vez mayor de ciberamenazas, lo que muestra la necesidad de supervisar y regular en determinadas situaciones a los proveedores de Internet. En este sentido, la Directiva NIS instaba a la revisión de las estrategias de ciberseguridad de los Estados para adaptarlas al nuevo escenario.

Las estrategias de ciberseguridad ofrecen un enfoque de seguridad nacional del ciberespacio centrado en la obligación del Estado de asegurar el funcionamiento de los servicios públicos, las infraestructuras críticas, las redes y sistemas y la privacidad y los derechos digitales del ciudadano. Sin embargo, son las empresas privadas las encargadas de proteger las redes y sistemas de información utilizados para ofrecer servicios esenciales. Por ello, resulta vital fortalecer los mecanismos de colaboración entre las instituciones y el sector privado.

El gobierno español aprobó en agosto de 2018 un Acuerdo del Consejo de Seguridad Nacional por el que se aprueba el procedimiento para la revisión de la Estrategia de Ciberseguridad Nacional de 2013. En él se considera la participación de un comité de expertos independientes en la fase de revisión del borrador elaborado por un Comité Técnico de la Administración. Este procedimiento de doble instancia agiliza la tramitación, pero no garantiza que el texto final responda a una visión compartida por el sector público y el privado respecto a los riesgos de ciberseguridad conocidos y emergentes que se han mencionado.

El CNI, preocupado por la fuerza de Anonymous en España: ¿tiene razones?

Fuente: eldiario.es
David Sarabia / Carlos del Castillo

Cuando "la cúpula de Anonymous" (en palabras de la Policía) fue detenida en junio de 2011, la carcajada en Internet fue generalizada. Más aún cuando cinco años después los tres hombres que integraban ese teórico aparato fueron absueltos, a pesar de que la Fiscalía pidiese cinco años de prisión para ellos.

¿Era realmente Anonymous una estructura jerarquizada desmantelada aquella mañana de julio? ¿O nunca ha dejado de ser más bien una idea, una inspiración para pequeños grupos de hackers que actúan por su cuenta? Para el Centro Criptológico Nacional (CCN), un organismo encargado de la ciberseguridad en España y dependiente del Centro Nacional de Inteligencia (CNI), Anonymous representa aún una amenaza para "infraestructuras críticas o las instituciones públicas españolas".

El CNI asegura que durante 2017 se produjeron 75 ataques a instituciones públicas que tuvieron "cinco o seis réplicas" durante el año y que se prolongaron una media de 10 días en el tiempo. Según el organismo de inteligencia especializado en ciberseguridad, los ataques partieron desde "núcleos de hackers bajo la bandera de Anonymous vinculados al procés de Catalunya". A su vez, también anuncian que "la geolocalización de los ataques no se da en España" aunque sea un dato "que no dice nada".

El CNI también explicó que estos 75 ataques están contenidos dentro de los 38.000 ciberincidentes que el CCN gestionó exitosamente el año pasado. Solo un 2,7% de esos ataques (1.026) los califica como "de peligrosidad alta". Restan importancia a los objetivos institucionales que según ellos se fijó Anonymous, ya que la mayoría fueron atacados a través de DDoS (ataque de denegación de servicio que consiste en tumbar una página web inundando de peticiones el servidor, haciendo que colapse).

España: ¿Último bastión del movimiento?

Anonymous es un movimiento internacional. "Londres ahí está, Italia, USA, Grecia, Guatemala, Nicaragua, Venezuela (aunque no acabemos de comulgar con sus piedras de molino)...", explica a eldiario.es una de las cuentas de Anonymous España en Twitter. "Con el tema de la independencia de Catalunya han surgido o se han mostrado algunos sectores con más fuerza que anteriormente y da la sensación de que en España estamos muy activos", continúan.

No esconden que "en general, el movimiento ha perdido fuerza a nivel internacional", pero no consideran que Anonymous esté desactivado. "¿Que somos los últimos en los que está vivo el movimiento...?", preguntan irónicamente.

También advierten sobre la cuenta de Twitter @ANONYMUS_ES, un perfil mercenario para inflar el impacto de la ultraderecha en España: "Utilizan nuestro nombre y nuestra imagen. Por cierto, nos han bloqueado pero seguimos viendo su actividad en redes", continúan desde la cuenta oficial del movimiento.

El grupo hacktivista se despide dejando un mensaje al CNI: "Hay temas y grupos en Internet bastante más importantes y peligrosos de los que deberían preocuparse y a los que prestar bastante más atención". Anonymous no está muerto pero ha perdido cadencia: ni siquiera los expertos les dan por desaparecidos, al menos en España. Todo lo contrario.

"La Nueve paró y eso les permitió regresar"

Hay al menos dos claves para que Anonymous siga siendo un actor relevante en nuestro país. Las señaló en conversación con este medio Gabriella Coleman, antropóloga que pasó seis años en los foros que la comunidad hacker utilizaba para organizarse, usando sus herramientas y empleando su lenguaje. Su nick, "Biella".

"España es un sitio bastante único en lo referente a la cultura hacker y la organización de protestas a través de las redes. Ha habido un movimiento muy potente de hackers progresistas que se han integrado muy bien en varios movimientos sociales. Lo hicieron en el 15M llevando la tecnología a las plazas, pero también han estado muy presentes en el independentismo catalán", afirma Coleman, cuya investigación sobre Anonymous se convirtió en una de las principales referencias para conocer los códigos de esta identidad colectiva.

El segundo motivo que apunta la investigadora es que las fuerzas de seguridad no llegaron a cazar a los hacktivistas españoles, aunque lo intentaron. "Hubo arrestos en el norte de España que la Policía quiso relacionar con Anonymous, pero en realidad ninguno de los grandes hackers fue detenido. Eso es importante, porque cuando los hackers importantes son arrestados todo el movimiento tiende a colapsar".

Por último, la investigadora indica una última carta que los hackers españoles que se han valido de la careta de Guy Fawkes jugaron para no acabar en prisión. Menciona directamente a La Nueve, una rama española de Anonymous que fue muy activa: "Supieron parar. Tiene sentido hacer eso, porque no es sostenible hackear todo el tiempo. Primero porque al final te terminarían cogiendo y después porque técnicamente es complicado continuar sin parar. La Nueve era muy activa hace unos años y pararon, dieron un paso atrás. Eso les ha permitido regresar".

Se triplica la identificación de menores no acompañados

Fuente: La Razón

La fiscalía acusa la progresiva y creciente llegada de jóvenes extranjeros sin tutelar

La Fiscalía de Menores de Barcelona dictó en 2017 un total de 815 decretos de determinación de minoría de edad de menores no acompañados, casi triplicando la cifra del año anterior, en la que decretó 277 identificaciones de menores, según la Memoria de ese año.

En total, en 2017 se incoaron 1.455 expedientes, un elevado número de expedientes, según el fiscal, que son consecuencia «de la progresiva y creciente llegada a la provincia de Barcelona de menores extranjeros no acompañados», que comportó un incremento considerable en el trabajo de la Fiscalía de guardia.

Concretamente, se dictaron 815 decretos de determinación de minoría de edad, 145 decretos de mayoría y 156 de archivo provisional, y en coordinación con el Instituto de Medicina Legal (Imelec) para dar una respuesta «lo más ágil posible».

En su informe, la Fiscalía constata que la Generalitat, que gestiona los centros de acogida, se ha visto «desbordada» por el aumento de la llegada de menores que requieren atención, si bien considera que en 2017 la actuación protectora de la administración puede calificarse en términos generales positiva y que funciona el servicio de asistencia inmediata en caso de riesgo.

Sin embargo, puntualiza que hubo «muchos problemas para poder dar una respuesta rápida» a la hora de otorgar con la celeridad necesaria la plaza en centros de acogida, por lo que muchos menores permanecieron en dependencias del área de custodia policial del edificio de Fiscalía un tiempo excesivo, de más de 48 horas.

Para el fiscal, ello fue «incompatible con la atención y el trato que deben recibir desde la administración protectora», una situación que cambió después de que la Sala de Gobierno del Tribunal Superior de Justicia de Cataluña (TSJC) dictara un acuerdo el 24 de octubre del año pasado prohibiendo la pernocta en dependencias judiciales.

Para la Fiscalía, corresponde a la dirección general de Atención a la Infancia y la Adolescencia (Dgaia) adoptar las medidas necesarias para asignar de forma inmediata y «con carácter urgente» la plaza en centro de protección para que los jóvenes estén el tiempo mínimo y estrictamente necesario en la sala de espera del edificio judicial.

Este 2018, en el que se ha mantenido la elevada afluencia de llegada de menores –la Fiscalía no ofreció datos actualizados–, la problemática se ha desplazado a las comisarías de los Mossos d'Esquadra, como la de la plaza de España.

El mercado de Seguridad Privada alcanzará los 4.500 millones este año

Fuente: Interempresas

Las compañías de seguridad generaron en 2017 un volumen de negocio de 4.315 millones de euros, lo que supuso cerca de un 5% más respecto al año anterior. Frente al alto grado de madurez que muestran los servicios de vigilancia, el principal motor de crecimiento del sector es el área de sistemas electrónicos de seguridad. La facturación sectorial continuará creciendo a corto y medio plazo, si bien con una progresiva tendencia a la desaceleración, estimándose una cifra de 4.500 millones de euros al cierre de 2018. Estas son algunas conclusiones del estudio Sectores 'Compañías de Seguridad' publicado recientemente por el Observatorio Sectorial DBK de Informa (filial de CESCE), referente en el suministro de Información Comercial, Financiera, Sectorial y de Marketing en España y Portugal.

Según el Observatorio Sectorial DBK de Informa, la positiva coyuntura económica, reflejada en el mejor comportamiento de la demanda, tanto de clientes profesionales como residenciales, favoreció en 2017 un nuevo crecimiento en el mercado de seguridad privada.

Así, el volumen de negocio generado por las compañías de seguridad en España alcanzó los 4.315 millones de euros en ese año, lo que supuso un crecimiento del 4,9%, muy similar al contabilizado en 2016.

Los servicios de vigilancia se mantienen como la principal área de actividad, si bien tienden a perder peso en el negocio global. Con un valor de 2.570 millones de euros en 2017, concentraron el 59,6% del mercado total.

El principal motor de crecimiento del negocio sigue siendo la actividad de instalación, mantenimiento y conexión a CRA de sistemas electrónicos, cuyo valor de mercado alcanzó en ese año los 1.424 millones de euros, un 33% del total.

Por su parte, en un contexto de mayor actividad comercial, el mercado de transporte de fondos generó unos ingresos de 321 millones de euros, representando el 7,4% del mercado total.

Las previsiones de evolución del sector de seguridad privada a corto y medio plazo apuntan a una prolongación de la tendencia de ascenso de la demanda, en un contexto de aumento del consumo privado y la inversión, y desarrollo de nuevos productos y servicios.

Es previsible, no obstante, una progresiva moderación del ritmo de crecimiento del negocio, el cual cerrará 2018 con una cifra de en torno a 4.500 millones de euros, un 4,3% más que en el año anterior.

Se aprecia una notable y creciente concentración de la oferta en el grupo de compañías líderes. De esta forma, los cinco primeros operadores reunieron en 2017 de forma conjunta el 58% del valor total del mercado.

Número de empresas autorizadas [a]	1.391
Número de vigilantes de seguridad habilitados	248.820
Mercado (mill. euros)	4.315
• Vigilancia	2.570
• Sistemas	1.424
• Transporte de fondos	321
Concentración (cuota de mercado conjunta en valor)	
• Cinco primeras empresas (%)	57,9
• Diez primeras empresas (%)	70,5
Crecimiento del mercado en valor (% var. 2017/2016)	+4,9
Previsión de evolución del mercado en valor (% var. 2018/2017)	+4,3
Previsión de evolución del mercado en valor (% var. 2019/2018)	+3,8

[a] por el Ministerio del Interior y las Administraciones autonómicas. Fuente: Observatorio Sectorial DBK de Informa. Estudio Sectores 'Compañías de Seguridad'

Se constituye el Comité Estatal de Coordinación sobre Vialidad Invernal ante el inicio de la Campaña 2018-2019

Fuente: Ministerio del Interior

El Ministerio de Fomento dispone de 1.350 máquinas quitanieves de empuje, 34 quitanieves dinámicas, además de 349 almacenes de fundentes y 538 silos con capacidad de almacenamiento para más de 243.000 toneladas de fundentes. La Unidad Militar de Emergencias despliega 1.400 efectivos en 31 secciones, con 15 quitanieves y más de 100 vehículos especialmente adaptados para trabajar en condiciones adversas.

La subsecretaria del Ministerio del Interior, Isabel Goicoechea, acompañada por el director general de Protección Civil y Emergencias, Alberto Herrera, ha presidido hoy la reunión constitutiva del Comité Estatal de Coordinación sobre Vialidad Invernal ante nevadas y otras situaciones meteorológicas extremas para la Campaña 2018-2019.

En la reunión han estado presentes los directores generales de Tráfico, Pere Navarro, y de Carreteras, Javier Herrero, junto con otros representantes de los distintos organismos del Estado implicados como el Departamento de Seguridad Nacional, Guardia Civil, Policía, Dirección General de Política de Defensa y Unidad Militar de Emergencias o la Agencia Estatal de Meteorología.

Durante el encuentro, se ha hecho balance de la Campaña del año anterior y se han expuesto las líneas generales de actuación para el próximo invierno de manera que se pueda garantizar que los ciudadanos transiten siempre en las mejores condiciones por las carreteras estatales y en los accesos a las grandes ciudades, tal y como contempla el Protocolo vigente.

Los miembros del Comité han recalcado la importancia de activar las alertas tempranas para coordinar de manera más eficaz la respuesta ante estos fenómenos adversos, e implementar con la debida antelación las medidas correspondientes en cuanto a la circulación de vehículos y autoprotección de los ciudadanos.

Balance de la Campaña 2017-2018

La Campaña 2017-2018 comenzó en diciembre con episodios esporádicos y poco intensos, que fueron superiores a lo habitual a partir de enero-febrero en toda la mitad norte y, en especial, en la Meseta norte, Cantábrico y zona centro.

- Incidencia en carreteras: En 89 ocasiones se precisó el corte de vía, y en 642 tramos fue necesario el uso de cadenas. Además, en 1.226 ocasiones fue preciso restringir el tráfico de vehículos pesados.

  El Ministerio de Fomento, que gestiona los más de 26.000 km. de la red de carreteras del Estado, distribuyó más de 266.000 toneladas de sal y 544 de cloruro cálcico, así como 162.000 litros de salmuera, cantidades sensiblemente superiores a las de la Campaña anterior.

- Consecuencias sobre personas y bienes. A efectos de Protección Civil, el número de sucesos con consecuencias sobre la población ascendió a 45. En 24 de ellos hubo que atender a personas aisladas o atrapadas, que en algunos casos tuvieron que ser rescatadas y evacuadas a zonas de albergue. Por otro lado, hay que lamentar el fallecimiento de dos personas y seis resultaron heridas.

  La Unidad Militar de Emergencias tuvo que intervenir en una ocasión, en la A- 6, coincidiendo con el regreso del puente de Reyes.

- Incidencias en la red de ferrocarriles, red eléctrica y transporte aéreo. Por lo que se refiere al servicio ferroviario, hay que destacar que se produjeron 7 incidencias de este tipo, el mismo número que por cortes en la red eléctrica. Por otro lado, el 5 de enero, 42 vuelos tuvieron que ser cancelados como consecuencia de la lluvia engelante.

Medios disponibles durante la Campaña 2018-2019

- El Ministerio de Fomento dispone de 1.350 máquinas quitanieves de empuje, 34 quitanieves dinámicas, además de 349 almacenes de fundentes y 538 silos con capacidad de almacenamiento para más de 243.000 toneladas de fundentes. Por otro lado, dispone de 33 aparcamientos de emergencia localizados en puntos estratégicos de la red de carreteras. El coste estimado de la Campaña es de 64,6 millones de euros.

  Al igual que en campañas anteriores, Fomento realiza un gran esfuerzo por optimizar recursos y mejorar la gestión, con el fin de informar con antelación de las posibles dificultades en la red de carreteras, minimizar las perturbaciones al tráfico provocado por las nevadas y evitar la formación de placas de hielo en las vías.

- La Dirección General de Tráfico mantiene la difusión de información a través mensajes lanzados en los medios de comunicación y las redes sociales, así como en los paneles luminosos de las carreteras. Además, atiende las llamadas de los ciudadanos en su servicio 011 y facilita información actualizada en su aplicación gratuita.
- Por su parte, la Unidad Militar de Emergencias (UME) del Ministerio de Defensa aporta 15 quitanieves y más de 100 vehículos, especialmente preparados para actuar en situaciones adversas (TOA, VEMPAR, góndolas, palas cargadoras o Dozer de cadenas). La UME mantiene un despliegue territorial en 31 secciones con 1.400 militares disponibles.
- La Agencia Estatal de Meteorología (AEMET) proporciona información de distintas variables meteorológicas (lluvia, nieve, viento, temperaturas bajas) y su evolución temporal. Este año va a probar un sistema denominado AEMET Vialidad invernal para UVR (Unidad de Valoración de Riesgo), que puede aportar información muy valiosa a los organismos encargados de gestionar las posibles emergencias.

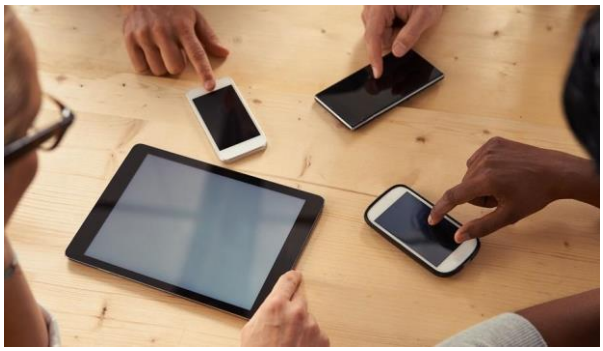
Bondades y riesgos del BYOD

Instituto Nacional de Ciberseguridad

INSTITUTO NACIONAL DE CIBERSEGURIDAD

La proliferación de dispositivos móviles y la mejora considerable en las especificaciones de software y hardware o el aumento del ancho de banda en las conexiones inalámbricas, han conseguido que consideremos a los smartphones, tablets y ordenadores portátiles como herramientas indispensables para desarrollar nuestro trabajo. En algunas organizaciones se sigue la política «trae tu propio dispositivo» o por sus siglas en inglés BYOD «Bring Your Own Device». Así, nos encontramos ante el aumento del número de dispositivos móviles de uso personal en el ámbito laboral.

El BYOD es una política que fomenta esta práctica, aportando ventajas como la reducción de costes por parte de la empresa, el aumento del teletrabajo o de la productividad y eficiencia por parte del empleado. Pero, como sucede en la mayoría de las ocasiones, estos beneficios están ligados a posibles riesgos que se deben tener en cuenta antes de decidirse a implantar esta política.



Riesgos del BYOD

Los principales riesgos asociados al uso del BYOD son:

- Robo, extravío o daño del dispositivo. El ser dispositivos móviles, con un tamaño cada vez más reducido y de un valor económico relativamente alto, los convierte en elementos muy susceptibles de sufrir alguna de estas posibilidades.

- Falta de actualizaciones de seguridad. Cuando un dispositivo no cuenta con la última versión de sistema operativo y aplicaciones, es vulnerable ante fallos de seguridad que sean conocidos.

- Ausencia de controles de seguridad en el sistema operativo. Algunos usuarios eliminan los controles que trae el dispositivo por defecto ya que desean añadir ciertas funcionalidades que en un estado de fábrica no son posibles. Rootear dispositivos Android o hacer un jailbreak en dispositivos Apple puede poner en riesgo la seguridad del dispositivo.

- Conexiones inalámbricas inseguras. Utilizar redes wifi inseguras puede poner en riesgo tanto al dispositivo como a la información que gestiona. Un atacante podría acceder a toda la información que envía o recibe en caso de no encontrarse cifrada o contar con un cifrado débil. Otras tecnologías inalámbricas, como bluetooth o NFC, también pueden suponer un riesgo, ya que cualquier atacante que se encuentre dentro de su rango de acción podría aprovecharse de vulnerabilidades o de una mala configuración.

- Falta de cifrado. La ausencia de cifrado en uno de estos dispositivos supone un riesgo. Un atacante que consiguiera acceder podría conseguir toda la información que en él se aloje. Actualmente los sistemas operativos Android e iOS cuentan con cifrado por defecto pero otros sistemas operativos, como Windows o OS X, no lo tienen. El cifrado debe extenderse también a los dispositivos de almacenamiento extraíbles.

- Ausencia de controles de seguridad para acceder al dispositivo. No tener implantados mecanismos de control de acceso robustos o utilizar mecanismos laxos, como el patrón de desbloqueo, supone un riesgo.

- Instalación de aplicaciones no confiables. Instalar aplicaciones de repositorios o fuente no confiables supone un riesgo ya que éstas pueden solicitar acceso a demasiada información del dispositivo o llevar consigo funcionalidades “extra”.

- Ceder el dispositivo conscientemente. Al tratarse de dispositivos que se usan conjuntamente, tanto en la vida laboral como en la personal, podría darse el caso que se ceda el dispositivo conscientemente a otra persona que a su vez accediera a información confidencial de la empresa.

- Empleados que han terminado su relación laboral. Al ser dispositivos personales, puede que hayan descargado en ellos información confidencial y que al terminar su relación laboral hagan un uso inadecuado de ella.

Recomendaciones de seguridad en BYOD

Ante estos riesgos asociados, las organizaciones que decidan implantar una política de BYOD deberán llevar a cabo una serie buenas prácticas para que se haga un uso seguro de estos dispositivos. Está en juego la información confidencial de la empresa.

- Crear una normativa clara que regule el uso del BYOD y dársela a conocer a todos los miembros de la organización. Se elaborará un listado de dispositivos autorizados, en qué condiciones se permite su uso, cómo se accede a la información, qué configuraciones de seguridad serán necesarias para poder utilizarlos, etc.

- Se implantará una política de concienciación y formación para todos aquellos empleados que hagan uso del BYOD. Ésta es la mejor herramienta para evitar incidentes de seguridad.

- Ante la posibilidad de robo o pérdida, se establecerán medidas que permitan su localización por medio del GPS. Además, se habilitará la posibilidad de realizar un borrado remoto del dispositivo. Como medida de seguridad adicional, todos los dispositivos y los medios de almacenamiento externos, como tarjetas SD o memorias USB, siempre estarán cifrados.

- Tanto el dispositivo como las aplicaciones que tenga instaladas estarán actualizados a la última versión disponible. De esta forma, contará con los últimos parches de seguridad.

- Se prohibirá el uso de dispositivo que hayan sido rooteados o cuenten con un jailbreak. Se elaborarán dos listas con aplicaciones permitidas junto aquellas cuyo uso queda totalmente prohibido.

- Se evitará el uso de redes wifi abiertas o aquellas que no sean confiables y se fomentará el uso de las redes 3G o 4G. En caso de que el dispositivo no tenga conectividad con estas redes, se usará un modem USB o se compartirá la conexión de datos del dispositivo móvil. Cuando se tenga que utilizar una red considerada poco segura, como la red wifi de un establecimiento público, se usará siempre por medio de canales seguros donde la información viaje cifrada, como una VPN.

- Todos los dispositivos deben contar con mecanismos que eviten accesos no autorizados por medio de contraseñas robustas o mecanismos de control biométricos, como touch-id. También se recomienda establecer un tiempo máximo de inactividad para que el dispositivo se bloquee automáticamente.

- Se evitará ceder el dispositivo de forma voluntaria a otras personas y se mantendrá siempre bajo custodia.

Implantar una política de BYOD en una organización es una tarea que no debe tomarse a la ligera, ya que conlleva un gran número de riesgos para la empresa. Pero su correcta adopción, siguiendo las recomendaciones anteriores, puede mejorar considerablemente la productividad de la organización.

RECORDATORIO

Próximo 22 de noviembre de 2018, en Hotel Fairmont-Rey Juan Carlos I Barcelona:

- ***Cena Anual de Socios y Amigos de ADSI***
  - ***20:00 horas***

Fecha límite de inscripción 18.11.2018

Ransomware es la principal ciberamenaza, dice Europol ¿Cómo prevenirlo?

Fuente: muySEGURIDAD

El Ransomware mantiene la supremacía como la principal ciberamenaza de malware en la mayoría de los estados miembros de la Unión Europea, según el informe de Europol, Internet Organised Crime Threat Assessment(IOCTA) correspondiente a 2018.

El informe, "tiene como objetivo informar a los responsables de la toma de decisiones a nivel estratégico, político y táctico en la lucha contra la ciberdelincuencia, con el objetivo de dirigir el enfoque operativo para la aplicación de la ley en la UE", dice el informe de Europol, el órgano encargado de coordinar, apoyar y facilitar las operaciones de los cuerpos policiales europeos a nivel de la Unión.

Al igual que con otros tipos de malware, los ciberataques por Ransomware son cada vez más numerosos, sofisticados, peligrosos y masivos, como mostró WanaCryptor, un ataque bien planificado y estructurado cuyo objetivo fue lograr una infección masiva a nivel mundial, poniendo contra las cuerdas a un buen número de grandes empresas de decenas de países.

Si hasta ahora el Ransomware solía tener motivaciones exclusivamente económicas produciendo altos beneficios para los atacantes, últimamente está ampliando objetivos como método preferente de introducción de malware tal y como vimos con el ransomware NotPetya.

Cómo prevenir el Ransomware

Un Ransomware típico infecta un ordenador personal o dispositivo móvil, bloquea el funcionamiento y/o acceso a una parte o a todo el equipo apoderándose de los archivos con un cifrado fuerte y exige al usuario una cantidad de dinero como "rescate" para liberarlos.

Por ello, si el mejor de los consejos en ciberseguridad es la prevención, en el caso del Ransomware es imprescindible para frenarlo. Te recordamos algunos consejos imprescindibles para frenarlo:

1. Actualización del sistema y aplicaciones. Mantener el sistema operativo actualizado con los últimos parches de seguridad y todas las aplicaciones que tengamos instaladas es el mejor punto de partida. El mencionado WanaCryptor aprovechó una vulnerabilidad en sistemas Windows.

2. Línea de defensa. Conviene instalar y mantener una solución antimalware, incluyendo un cortafuegos correctamente configurado para permitir el acceso exclusivo de las aplicaciones y servicios necesarios

3. Herramienta Anti Ransom. Es una herramienta específica contra este tipo de ataques, que tratará de bloquear el proceso de cifrado de un ransomware (monitorizando "honey files"). Realizará un dump de la memoria del código dañino en el momento de su ejecución, en el que con suerte hallaremos la clave de cifrado simétrico que estuviera empleándose.

4. Filtro antispam. Muchos de los ataques por Ransomware se distribuyen a través de campañas masivas de correo electrónico. Además de estos filtros, debes seguir los consejos generales como no pinchar en enlaces o abrir archivos adjuntos de remitentes desconocidos.

5. Bloqueadores de JavaScript. Aplicaciones como Privacy Manager bloquean la ejecución de todo código JavaScript sospechoso de poder dañar el equipo del usuario. Esto ayuda a minimizar las posibilidades de quedar infectado a través de la navegación web.

6. Políticas de seguridad. Herramientas como AppLocker, Cryptoprevent, o CryptoLocker Prevention Kit facilitan el establecimiento de políticas que impiden la ejecución de directorios comúnmente utilizados por el ransomware, como App Data, Local App Data, etc.

7. Cuentas con privilegios. No utilizar cuentas con privilegios de administrador. El 86% de las amenazas contra Windows se pueden esquivar en caso de utilizar un usuario común en lugar de un administrador. Por eso es importante utilizar para tareas comunes un usuario común y solo dejar el administrador para cuando se vaya a hacer una serie de tareas relacionadas con la manipulación del sistema.

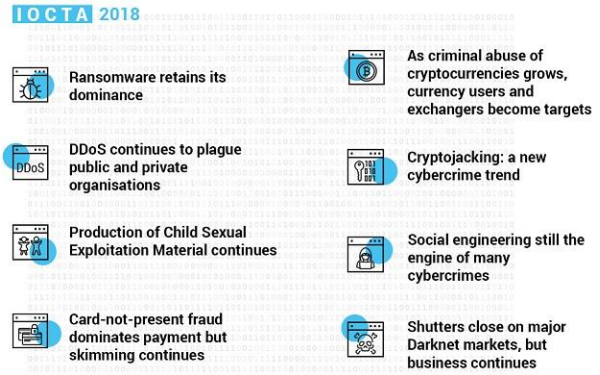
8. Extensiones de archivos. Mostrar las extensiones para tipos de ficheros conocidos es una buena práctica para identificar los posibles ficheros ejecutables que quieran hacerse pasar por otro tipo de fichero. No es raro ver a un fichero .exe con el icono de un documento de Word. Si no se ve la extensión, el usuario posiblemente no pueda distinguir si es un documento de Word o un ejecutable malicioso, aunque también es bueno recordar que un documento de Microsoft Office también puede contener malware.

9. Máquinas virtuales. Emplear máquinas virtuales para aislar el sistema principal es otra técnica efectiva. En un entorno virtualizado la acción de los ransomware no suele materializarse.

10. Backup. Realizar copias de seguridad de los datos importantes como tarea de mantenimiento regular es la medida más efectiva para minimizar los daños en caso de ser infectado. La copia de seguridad debe alojarse en un medio externo distinto al del equipo para poder recuperar los archivos desde un sitio "limpio" y no tener que pagar el "rescate" exigido por estos ciberdelincuentes.

Otro tipo de malware en crecimiento

Europol señala en su informe otro tipo de malware en tendencia al alza. Uno de ellos es el cryptojacking, un ataque que requiere muchos menos recursos y gran rendimiento y es utilizado aprovechando las máquinas de las víctimas para explotar las criptomonedas.



Europol también espera que los kits de explotación como el principal vector de ataque de infecciones sigan disminuyendo, siendo reemplazados lentamente por otras técnicas y métodos más modernos, como el Protocolo de escritorio remoto (RDP), la ingeniería social y el correo no deseado o spam, con el Phishing como protagonista de las técnicas de ataque.

Las violaciones de datos también han aumentado después de la entrada en vigor del GDPR de la UE en mayo de 2018, el mayor cambio normativo de privacidad de las últimas dos décadas y un cambio de rumbo en la manera de recopilar y manejar los preciados datos personales.

Noticias

La Secretaría de Estado de Seguridad evalúa los procedimientos antiterroristas con Policía Nacional, Guardia Civil, Mossos y Ertzaintza

La Secretaría de Estado de Seguridad celebró el pasado 14 de noviembre una reunión de la Mesa de Coordinación del Plan de Protección y Prevención Antiterrorista, un encuentro que ha servido para evaluar los procedimientos y actuaciones en la lucha contra el terrorismo con los máximos responsables de Policía Nacional, Guardia Civil, Mossos d'Esquadra y Ertzaintza.

La reunión estuvo presidida por la secretaría de Estado de Seguridad, Ana Botella, y han participado en ella el director del Gabinete de Coordinación y Estudios del Ministerio del Interior, José Antonio Rodríguez, altos mandos de la Guardia Civil y de la Policía Nacional, el jefe de los Mossos d'Esquadra, Miquel Esquius, y el jefe de la Ertzaintza, Jorge Aldekoa.

La mesa realizó la evaluación de las actuaciones y medidas adoptadas en el marco del nivel 4 de alerta antiterrorista; ha valorado los procedimientos de comunicación y colaboración ante incidentes de potencial carácter terrorista; y analizó la coordinación con policías locales y empresas de seguridad privada.

Formación

Curso DSICE - XIII Edición

Especialización en Dirección de Seguridad en Infraestructuras Críticas y Estratégicas

20% de descuento para asociados a entidades colaboradoras

Posibilidad de bonificación a través de FUNDAE

El Primer Curso específicamente dirigido a la Protección de Infraestructuras Críticas.

- **Programa orientado al Plan Nacional de Infraestructuras Críticas.** Profundice en todas las medidas a considerar en los **Planes de Seguridad del Operador** o en sus **Planes de Protección Específicos**, así como en los **Planes de Apoyo Operativo**.

- **Curso online compatible con la actividad laboral** 300h totalmente online, más visitas y jornadas presenciales opcionales.
- **Más de 30 Profesores,** expertos internacionales en cada materia del curso.
- **Certificado Universitario**. Diploma emitido por el Instituto Universitario General Gutiérrez Mellado (UNED).
- **Habilitación de Director de Seguridad**. Con opción para acceder a la habilitación de Director de Seguridad (Ministerio del Interior).

Más Información en el siguiente enlace

II Jornada de Seguridad e Inteligencia

Las revistas Seguritecnia y Red Seguridad, junto con la Fundación Borredá, organizan la II Jornada de Inteligencia y Seguridad el próximo 21 de noviembre en el auditorio de Naturgy en Madrid para continuar la línea de acción con la que se mejora el conocimiento que el sector privado, y muy especialmente el relacionado con la seguridad corporativa, tiene sobre el concepto y aplicaciones prácticas de la inteligencia como elemento de apoyo en el proceso de toma de decisiones.

El mundo se ve asediado por amenazas de todo tipo que afectan directamente no sólo a nuestra capacidad de desarrollo, sino incluso al simple ejercicio de las funciones sociales básicas. Frente a ellas, los Estados despliegan sus elementos de protección, Fuerzas Armadas y Fuerzas de Seguridad, convenientemente guiados por la acción de los servicios de inteligencia. Pero la responsabilidad de la seguridad es compartida y no es sólo el Estado quien tiene que hacer frente a las amenazas. Hoy, el sector privado ya asume decididamente la protección de sus activos en un proceso complejo perfectamente planificado, cuyo éxito dependerá, en gran medida de su capacidad de anticipación.

Para ello las empresas deben contar con el apoyo de la inteligencia del Estado, pero ante la diversidad de intereses y la sobreabundancia de información deben dotarse también de recursos para elaborarla y transformarla en su propia inteligencia como instrumento más eficaz de ayuda en el proceso de toma de decisiones de cualquier tipo, especialmente las relativas a su propia seguridad.

Puede consultar el programa en el siguiente enlace

Puede registrarse en la jornada en el siguiente enlace

Legislación

ORDEN INT/1149/2018, DE 29 DE OCTUBRE, POR LA QUE SE REGULA LA ORGANIZACIÓN Y EL FUNCIONAMIENTO DE LA RED NACIONAL DE RADIO DE EMERGENCIA.

PDF de la disposición en el siguiente enlace

REAL DECRETO 1340/2018, DE 29 DE OCTUBRE, POR EL QUE SE APRUEBAN LAS NORMAS ESPECIALES REGULADORAS DE LAS SUBVENCIONES QUE SE OTORGARÁN EN RÉGIMEN DE CONCESIÓN DIRECTA A LAS COMUNIDADES AUTÓNOMAS Y CIUDADES DE CEUTA Y MELILLA PARA LA ATENCIÓN A LOS MENORES EXTRANJEROS NO ACOMPAÑADOS ACOGIDOS EN EL AÑO 2018.

PDF de la disposición en el siguiente enlace

Revistas

Seguritecnia Nº 457. Octubre

Nuevo número de **SEGURITECNIA**, con reportajes, entrevistas y artículos, destacando:

- **Editorial:** La complementariedad es necesaria
- **Seguripress**
- **Especial:** Seguridad en museos
- **Entrevista:** Bob Hwang. Director General de Hanwha Techwin Europe

Enlace: ver revista digital

Cuadernos de Seguridad Nº 337. Octubre

En este número de **CUADERNOS DE SEGURIDAD**, además de las secciones habituales de «Seguridad», «Cuadernos de Seguridad estuvo allí», «Estudios y Análisis», o «Actualidad, el lector encontrará:

- **Editorial:** «Ante un nuevo entorno tecnológico».
- **En Portada:** «Ciberseguridad, ante una nueva era».
- **Entrevistas:** «Alberto Hernández, Director General de INCIBE».
- **Artículos:** «Inteligencia sobre amenazas y la importancia de los analistas de malware».

Enlace: ver revista digital

¿Quieres ser Socio de ADSI – Asociación de Directivos de Seguridad Integral?

Para iniciar el proceso de alta como Asociado, envíe un e-mail a secretario@adsi.pro , indicando nombre y apellidos, una dirección de correo y un teléfono de contacto.

En cuanto recibamos su solicitud le enviaremos el formulario de Solicitud de Admisión.

¿Quién puede ser socio de ADSI – Asociación de Directivos de Seguridad Integral?

Puede ser socio de **ADSI**:

- Quien esté en posesión de la titulación profesional de Seguridad Privada reconocida por el Ministerio del Interior (T.I.P. de Director de Seguridad, Jefe de Seguridad, Detective Privado o Acreditación de Profesor de Seguridad Privada).
- Todo Directivo de Seguridad que posea, a criterio de la Junta Directiva de la Asociación, una reconocida y meritoria trayectoria dentro del sector.