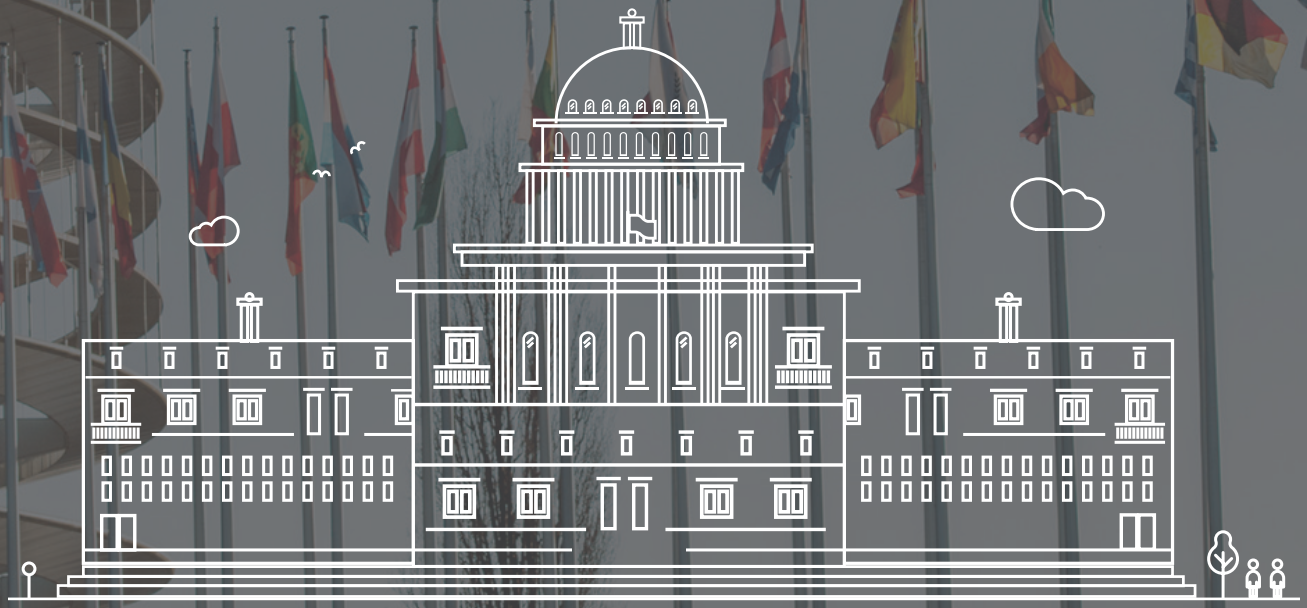
Edición México

La Privacidad de las Administraciones Públicas



pandasecurity.com

panda

Tecnocracia Tecnológica

El sector público está sufriendo una transformación sin precedentes. El uso masivo de las nuevas tecnologías es una realidad y su incorporación en todos los ámbitos es un hecho asentado.

La adopción de la tecnología constituye un factor clave en la mejora de los procesos y en el crecimiento de la economía. De hecho, la intervención de los estados en la actividad económica de sus respectivos países ha llegado, en los últimos años, a cotas nunca antes vistas. Según datos de EUROSTAT, el gasto del sector público en la Unión Europea alcanzó un 48,2% del PIB, casi igualando el aporte de la economía productiva. Un reflejo del alcance que la intervención de las Administraciones Públicas tiene en nuestras vidas.

El uso de las Tecnologías de la Información y Comunicaciones (TIC) en general y la administración online en particular son factores decisivos en esta transformación de la Administración Pública, ya que permiten a los ciudadanos y a las empresas un fácil y más rápido acceso a servicios públicos online.

A medida que las Administraciones han ido adoptando las nuevas tecnologías, se han visto expuestas a nuevos tipos de ataques.

Ya no sólo hay que prestar atención a los fallos comunes de la explosión tecnológica, como prevenir incidencias, disponer de sistemas de denuncia o de comunicación de incidentes. Ahora, la amenaza de los ciberataques es real y cotidiana.

Cada segundo México sufre 12 ataques cibernéticos, de los que el 60 por ciento son contra el gobierno para tratar de extraer información y provienen principalmente de complejas redes de piratas de Rusia y USA.

Actualmente los ciberataques van más dirigidos específicamente a nivel gobierno; estos son los que sufren más, al tratar de extraerles información.

La revolución tecnológica sobrevenida en la Administración Pública, la digitalización y almacenamiento de toda la información, y el auge de la oferta de servicios online para agilizar los trámites de la ciudadanía han contribuido al crecimiento exponencial de la generación, almacenamiento y gestión de cantidades ingentes de datos confidenciales. Datos que no se pueden permitir ni un solo descuido. De ahí que las Administraciones deban ir de la mano de nuevas exigencias en materia de prevención, seguridad y legislación.

Muchas de estas instituciones han relegado estas exigencias en ciberseguridad a la implantación tecnológica, con el riesgo que ello conlleva, encontrándose ahora con una importante tarea por hacer ante el nuevo panorama legislativo.

El Papel de la Ciberseguridad

Las ciberamenazas constituyen un riesgo constante que afecta de manera significativa a las Administraciones Públicas. Tanto es así que se han convertido en un potente instrumento de agresión contra las entidades públicas y los ciudadanos. De tal forma que pueden llegar provocar un serio deterioro en la calidad del servicio y sobre todo fuga de información, desde datos de los ciudadanos hasta secretos de estado.

La sociedad digitalizada es la gran beneficiaria de los avances tecnológicos, pero es también responsable de hacer un uso prudente y efectivo de estos recursos. En ese sentido, la ciberseguridad es uno de los factores clave para mejorar la experiencia del usuario, cumplir con la regulación establecida y cubrir las necesidades de protección de las Administraciones en este escenario.

En este contexto, el papel de la ciberseguridad ha cambiado drásticamente. Inicialmente, la misión principal de la seguridad informática era la de proteger la información de una manera reactiva, pero posteriormente ha evolucionado hacia una posición proactiva que identifica y resuelve los riesgos que amenazan el ciberespacio, dando paso a un Modelo de Seguridad Integral.

La seguridad, en cualquiera de sus dimensiones o ámbitos, es la primera responsabilidad de cualquier Gobierno. Históricamente, la seguridad ha sido principalmente gestionada desde el sector de la defensa, ya que los principales riesgos para las naciones tenían naturaleza militar. Sin embargo, en esta era de la hiperconexión e interoperabilidad han surgido nuevos actores y riesgos que han obligado a los Gobiernos a llevar a cabo profundas revisiones y transformaciones en sus políticas de seguridad y defensa.

Así lo reflejan leyes adoptadas en los últimos años como ocurrió en México con Nueva **Ley General de Transparencia y Acceso a la Información Pública** publicada en el Diario Oficial de la Federación el 4 de mayo de 2015.

Esta ley marcó un antes y un después en la utilización y gestión de las TIC en el Sector Público, y en su relación no presencial con ciudadanos y empresas, y entre los diferentes organismos que componen las Administraciones Públicas (Administración General del Estado, Comunidades Autónomas y Entidades Locales). Implicó una verdadera transformación normativa, organizativa, funcional y tecnológica del Sector Público, con especial atención al impacto del uso del canal internet como medio de relación entre ciudadanos y Sector Público, la verdadera apertura de las Administraciones Públicas con el mundo online.

La nueva legislación establece principios, bases y procedimientos para garantizar el derecho de acceso a la información de cualquier autoridad, entidad de los Poderes de la Unión, los órganos autónomos, partidos políticos, sindicatos, fideicomisos y fondos públicos.

Esta nueva normativa dio lugar a la necesidad de establecer los principios y requisitos de una política de seguridad en la utilización de los medios electrónicos que permita una adecuada protección de la información. Define la integración y funcionamiento del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, cuyo propósito será fortalecer la rendición de cuentas del Estado mexicano.

El Sistema Nacional de Transparencia estará integrado por el Instituto Nacional de Transparencia y Acceso a la Información; los organismos garantes de las entidades federativas; la Auditoría Superior de la Federación; el Archivo General de la Nación; y el Instituto Nacional de Estadística y Geografía.

Ciberataques:

Robo de Información

Israel's Ministry of Social Security and Welfare

En los últimos diez años se han sucedido ataques de diversa índole contra la administración pública. Uno de los casos es el protagonizado por Shalom Bilik, sucedido entre 2005 y 2006, subcontratado para el mantenimiento de los sistemas informáticos del Ministerio de la Seguridad Social y Bienestar del gobierno de Israel. Bilik accedió a una base de datos y robó información de 9 millones de ciudadanos israelís. Posteriormente esa información fue vendida. El robo no se descubrió hasta 2012, cuando él y 5 personas más, que participaron en el tratamiento y venta de los datos, fueron oficialmente acusados.

Se robaron datos de 9 millones de ciudadanos israelís.

United States Department of Veterans Affairs

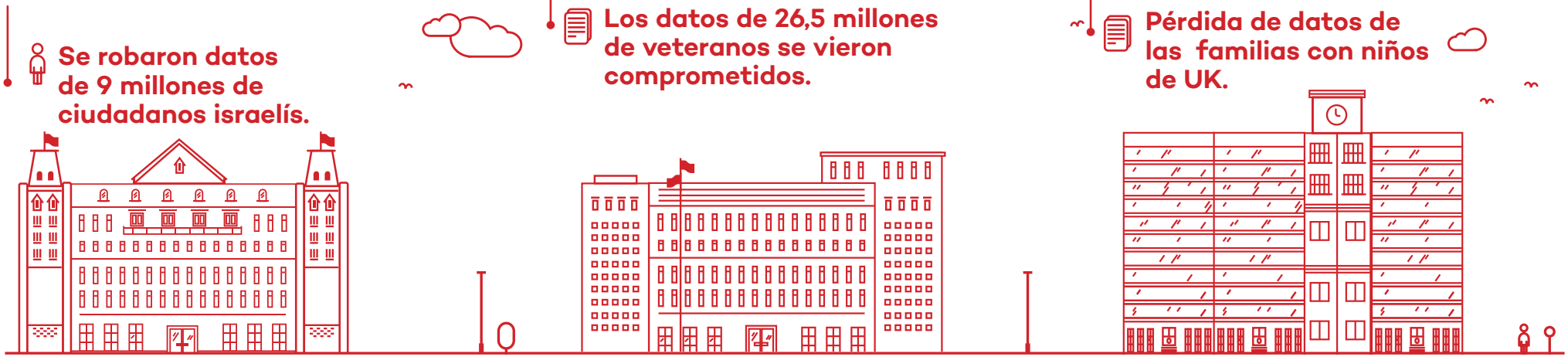
Ni siquiera nuestro hogar se puede considerar un lugar seguro y mucho menos cuando se trata del manejo de documentos de estado. Buena cuenta puede dar el empleado del United States Department of Veterans Affairs que en mayo de 2006 sufrió un robo en su casa, en el que comprometieron los datos de 26,5 millones de veteranos, incluyendo el número de seguridad social, su nombre y la fecha de nacimiento. Este empleado estaba participando en la elaboración de un estudio estadístico y se había llevado la información a casa sin permiso.

Los datos de 26,5 millones de veteranos se vieron comprometidos.

UK HM Revenue and Customs

Otro uso inadecuado de información sucedió en 2007, cuando 2 discos duros con datos personales de familias con hijos menores de 16 años del Reino Unido se perdieron. Al parecer, utilizaron una empresa de mensajería para enviar los discos, que nunca llegaron a su destino. Entre los datos robados estaban los nombres, direcciones, fechas de nacimiento y datos bancarios.

Pérdida de datos de las familias con niños de UK.



The White House

En 2015, Ben Rhodes, el viceconsejero de Seguridad Nacional de Estados Unidos, comunicó que la Casa Blanca había sido víctima de un ataque informático. En una entrevista con CNN, Rhodes afirmó que los atacantes obtuvieron acceso no autorizado al sistema no clasificado de los ordenadores y robaron información de gran importancia. El sistema clasificado no fue hackeado.

Acceso no autorizado al sistema no clasificado de los ordenadores.

The Office of Personnel Management

En junio de ese mismo año, supimos que el Office of Personnel Management, la agencia del gobierno federal estadounidense de recursos humanos, fue comprometida y robaron información personal de al menos 4 millones de trabajadores públicos. El ataque tuvo lugar dos meses antes, aproximadamente al mismo tiempo que la Casa Blanca fue comprometida. Sin embargo parece que ambos ataques no están conectados.

Acceso a datos personales de 4 millones de trabajadores públicos.

Insiders

Al igual que en muchos otros sectores, la mayoría de los casos de robo de información hasta el 2011 eran protagonizados por atacantes internos, empleados que tenían acceso a la información.

Los ataques de personal con accesos privilegiados suponen una de las mayores amenazas para la seguridad del ciberespacio de las naciones y empresas.

Desde un espía infiltrado por un Estado, a un empleado captado por bandas de terroristas o simplemente empleados descontentos que sustraen información por despecho, todos ellos pueden ser considerados como insiders.

Bradley Manning

En 2010 se produjo uno de los robos de información más famosos de la historia moderna, cuando Bradley Manning, soldado del ejército estadounidense, copió 700.000 documentos confidenciales y los filtró a WikiLeaks para publicarlos.

En total casi **medio millón de registros de las guerras de Irak y Afganistán, y más de 250.000 cables diplomáticos secretos de los Estados Unidos.** Mala conducta por haber infringido las leyes federales sobre divulgación de material clasificado, ayudar al enemigo entregando información de inteligencia, violación de la seguridad de la información y violación de los programas de seguridad así como espionaje son algunos de los cargos que se le han imputado a Manning.

Copió 700,000 documentos confidenciales.

Edward Snowden

Otro de los casos más sonados en los últimos años y que puso en jaque a una de las instituciones estatales con más renombre a nivel mundial como es la CIA (Agencia Central de Inteligencia) y la NSA (Agencia de Seguridad Nacional) fue el protagonizado por Edward Snowden, un exempleado que en 2013 hizo públicos, a través de los periódicos The Guardian y The Washington Post, documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore.

El Departamento de Justicia de Estados Unidos ha clasificado la participación de Snowden en el programa de vigilancia PRISM como un «asunto criminal», por lo que se desconoce la suerte que correrá.

Snowden publicó documentos secretos de varios programas de la NSA.

Ataques Contra Redes y Sistemas

A medida que avanza la tecnología y los sistemas están más conectados, los ciberdelincuentes disponen de más medios y herramientas para realizar ataques, como se demuestra en gran parte de los casos sucedidos en los últimos años.

En 2012, un simple mensaje de correo electrónico enviado a empleados del Department of Revenue de Carolina del Sur, en Estados Unidos, permitió a un atacante acceder a la red interna y hacerse con los datos de 3,8 millones de contribuyentes. Entre la información robada se encontraban números de la seguridad social y datos de cuentas bancarias.

Un ataque similar se produjo en el condado de Monterey, cuando la información personal de 145.000 residentes fue robada por atacantes externos que comprometieron un ordenador del departamento de servicios sociales. Entre la información sustraída había nombres, números de la seguridad social y direcciones.

Un email dió a un atacante acceso a la red interna y a los datos de 3,8 millones de contribuyentes.

Se robaron números de la Seguridad Social y direcciones.

Ataques con Fines Políticos

El pasado 2015 fue un año en el que las instituciones públicas sufrieron numerosos ataques con motivaciones políticas (a través de hackeos de cuentas de redes sociales para lanzar propaganda) o de espionaje (políticos, altos mandatarios).

Ciberterrorismo y Ciberespionaje

Las bandas del crimen organizado (ciber-gangs) han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece con el objetivo de obtener información sensible para su posterior uso fraudulento y el lucro económico.

En enero de 2015, al mismo tiempo que Obama daba a conocer una serie de iniciativas legislativas para ayudar en la lucha contra la ciberdelincuencia, un grupo de atacantes relacionados con ISIS se hicieron con el control de las principales cuentas de redes sociales del pentágono. Para ello, irremediablemente tuvieron que hacerse con información de cuentas de correo, contraseñas, usuarios... Unos datos y credenciales que no contaban con el grado de seguridad necesario para evitar la intromisión y mal uso.

Ahora los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas. Esta táctica fue la utilizada por el conocido grupo Syrian Electronic Army que consiguió comprometer la página web de la armada de Estados Unidos, publicando contenido propagandístico a favor del régimen sirio de Assad.

De nuevo la Administración Estadounidense se convirtió en el blando de cibercriminales cuando James Comey, director del FBI, dijo en un foro de seguridad que habían detectado un creciente interés por parte de terroristas sobre estrategias para lanzar ataques ciberterroristas contra Estados Unidos. No especificó el tipo de ataques y dijo que parecía que estaban todavía en los inicios de planificación, tratando de ver cómo de efectivos podrían llegar a ser, pero que potencialmente se trata de un problema que puede ir a más.

Con sabotaje de centros industriales, asesinatos de científicos y **el uso del virus informático Stuxnet, la fase secreta de la guerra contra Irán comenzó la pasada década** con el caso de espionaje llevado a cabo por los servicios de inteligencia de Estados Unidos e Israel, llegando a la conclusión de que Irán contaba con una planta de enriquecimiento de uranio en su territorio. Mantenida durante un tiempo en secreto, esta instalación salió a la luz pública en septiembre del 2009 tras la denuncia que hizo Barack Obama.

Hacktivismo

El auge de este movimiento se produjo principalmente durante 2011 cuando el hacktivismo se convirtió en una de las mayores amenazas para los gobiernos y organismos. El anonimato y la libre distribución de información a través del ciberespacio, esencialmente a través de Internet, son sus principios. Los hacktivistas se agrupan de manera descentralizada utilizando el under-ground de Internet para comunicarse y planificar sus acciones.

El parlamento alemán fue víctima de un ataque donde consiguieron comprometer diferentes ordenadores y llegaron a robar información de los mismos. Se cree que el ataque vino de Rusia, aunque es difícil que se pueda llegar a demostrar quién estuvo detrás realmente.

El 25 de julio de 2015, unos hackers rusos consiguieron comprometer el sistema de correo electrónico no clasificado del Pentágono, del que robaron información. Según fuentes oficiales se trató de un ataque muy sofisticado y que claramente había algún gobierno detrás del mismo.

De la misma manera, este año tres grupos de atacantes latinoamericanos consiguieron comprometer los servidores de correo del ejército boliviano, descargándose los correos electrónicos que posteriormente publicaron en parte. Consiguieron acceder a la información fácilmente a través de un antiguo agujero de seguridad en el servicio Zimbra de VMWare, que los responsables de seguridad del ejército no habían parcheado.

Las Administraciones públicas, en concreto toda la rama de defensa y seguridad nacional de cada país, son muy conscientes de los riesgos a los que se enfrentan. **En 2016 el Departamento de Defensa estadounidense ha presentado un programa piloto de recompensas llamado "Hack the Pentagon", donde se ofrecerán recompensas a los hackers que logren encontrar fallos de seguridad en las páginas web, aplicaciones y redes pertenecientes al Pentágono.**

Hackers rusos comprometieron el sistema de correo electrónico del Pentágono.

Atacantes latinoamericanos comprometeieron los servidores de correo del ejército boliviano.

A pesar de los esfuerzos invertidos por la Administración Pública en ciberseguridad, uno de los ataques más recientes que se ha conocido es el que ha tenido como víctima al Comité Nacional del Partido Demócrata en EEUU, que ha reconocido que al menos desde hace un año sus sistemas estaban comprometidos. Se han encontrado evidencias que apuntan a que los atacantes pertenecen a la inteligencia rusa, y han tenido acceso a correos electrónicos, chats y documentos de investigación de todo tipo. Todos los ordenadores del departamento de investigación habían sido accedidos y algunos archivos habían sido robados.Sin ir más lejos, este pasado mes de julio con la difusión pública de correos internos del Partido Demócrata en Wikileaks. Un total de 19.252 correos electrónicos con 8.034 archivos adjuntos procedentes de servidores del Comité Nacional Demócrata estadounidense que abarcan de enero de 2015 a mayo de 2016.

Según la versión de la empresa de seguridad informática contratada por el Comité Nacional Demócrata, **la infiltración sería obra de al menos dos grupos diferentes de hackers vinculados con alguna agencia gubernamental rusa en una maniobra para favorecer a Donald Trump.**

Ahora, a tres meses de las elecciones de Estados Unidos, el FBI confirma el hackeo de por lo menos dos bases de datos electorales llevado a cabo por hackers extranjeros que habrían extraído información de los votantes de al menos de una de ellas. La investigación está en curso y se rastrean las IPs que han aparecido, de nuevo, previamente en foros rusos de hackeo. ¿Casualidad?

Para evitar que se produzcan nuevos casos de ataques a instituciones de la administración pública se hace necesario la existencia de un marco regulatorio y legislativo común, con una responsabilidad compartida entre los Estados, bilateralmente o a través de organismos supranacionales.

Un año sin protección

El sistema del Partido Demócrata de EEUU se vio comprometido durante un año.

19,252 emails con 8,034 archivos adjuntos

del US Democratic National Committee fueron difundidos.

Dos bases de datos electorales fueron atacadas

por hackers extranjeros.

Cambio Legislativo

El cambio del marco regulatorio llevado a cabo este 2016 en la Unión Europea ha venido propiciado por la disposición por parte de la administración de recursos eficaces ni una capacidad de respuesta suficiente ante los continuos (y en constante incremento) incidentes debidos a ciberataques. A esto hay que sumarle la necesidad de expertos en ciberseguridad, no satisfecha ni por la formación pública ni por la privada.

Otros factores que han propiciado este cambio en el marco rector de la seguridad es el hecho de que, como hemos visto en los ejemplos anteriores, la seguridad de los Estados ya no está restringida a la defensa de sus fronteras y su soberanía, sino que también debe garantizar el bienestar de sus sociedades frente a los nuevos riesgos.

Una de las principales motivaciones de las leyes referidas a la protección de datos de carácter personal es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas, y especialmente de su honor, intimidad y privacidad personal y familiar:

Estas normativas hacen referencia a un componente esencial para incrementar las capacidades de la tecnología móvil, analítica y proceso de datos usado por la Administraciones Públicas y la mayoría de empresas: el cloud computing. El cliente que contrata servicios de cloud computing sigue siendo responsable del tratamiento de los datos personales.

De esta manera, quien ofrece la contratación es un prestador de servicios que tiene la calificación de “encargado del mantenimiento”.

En referencia a la ubicación datos, los países del Espacio Económico Europeo ofrecen garantías suficientes y no se considera legalmente que exista una transferencia internacional de datos. El Espacio Económico Europeo está constituido por los países de la Unión Europea e Islandia, Liechtenstein y Noruega

Tecnología y Legislación

La aparición de actores de orígenes y motivaciones heterogéneas con capacidad de actuar en cualquiera de las dimensiones de la seguridad, dificulta la atribución de las agresiones y disminuye la capacidad de respuesta de los Estados. La legislación actual no está adaptada a los nuevos ciberdelitos ni a las nuevas necesidades tanto tecnológicas como de gestión de la información.

En el año 2015, se establecieron nuevas reglas para hacer a Latinoamérica más sólida ante las amenazas cibernéticas. La Directiva sobre Seguridad en las Redes y sistemas de Información, tiene por objeto aumentar los estándares en ciberseguridad y reforzar la cooperación entre los Estados miembros en estas materias, al tiempo que establece nuevas obligaciones para los operadores de servicios esenciales e infraestructuras críticas (energía, el transporte, la salud y las finanzas), así como para los proveedores de servicios digitales (mercados en línea, motores de búsqueda y servicios en nube).

Además, la Directiva exigirá a cada Estado de la UE que designe a una o más autoridades nacionales y que elabore una estrategia para afrontar las ciberamenazas que deberá responder al contenido de dicha Directiva que, sin lugar a dudas, obligará a una actualización de la Estrategia Nacional de Ciberseguridad.

Igualmente, plantea crear una red de equipos de respuesta a incidentes de seguridad informática (red de CSIRT o “Computer Security Incident Response Teams”) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros, y promover una cooperación operativa rápida y eficaz.

En tal sentido, los operadores de servicios esenciales deberán notificar sin dilación indebida a la autoridad competente o al CSIRT los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan. Del mismo modo deberán operar los proveedores de servicios digitales cuando el incidente tenga un impacto significativo en la prestación de los servicios a los que alude la Directiva (mercado en línea, motores de búsqueda en línea y servicios de computación en la nube). En otras palabras, no todos los prestadores de servicios digitales estarán obligados a practicar esta notificación.

Por lo tanto, habrá que estar muy atento a esta nueva normativa europea de ciberseguridad y que, a buen seguro, implicará la promulgación de nuevas normas nacionales y la modificación o modulación de otras que están en vigor.

Los expertos en ciberseguridad alertan a Gobiernos y a ciudadanos de la importancia de defender los sistemas de internet con más fuerza y seguridad que nunca, ya que si no se toman medidas al respecto, en un futuro podríamos sufrir consecuencias nefastas.

Solución para Adaptarse al Cambio

Las Administraciones están propiciando el cambio desde un modelo de ciberseguridad enfocado en la protección de la información (Information Security), a un modelo de Seguridad Integral basado en la gestión de los riesgos del ciberespacio (Information Assurance).

Para las instituciones, el éxito en materia de ciberseguridad recae en unos requisitos que permitan cumplir las siguientes exigencias:

Información en tiempo real

Estar informadas en tiempo real de las infracciones y agujeros de seguridad relativos a datos, como la destrucción accidental o ilícita, pérdida, alteración, divulgación no autorizada o la transmisión remota.

Data Protection Regulation

El cumplimiento del artículo 35 de la "General Data Protection Regulation" relativa a la protección de datos, con un seguimiento regular y sistemático de datos sujetos a gran escala.

Informes de países extranjeros

Informar de todas las posibles transferencias de archivos de datos a países extranjeros.

Privacidad

Mejorar los actuales derechos individuales y apoyar nuevos derechos a ser olvidado y la portabilidad de los datos en todos los archivos de datos distribuidos.

Protección

Asegurar la delegación a otros procesadores de: borrado, presentación de informes y los requisitos de aviso, y el mantenimiento de las actividades de transformación.

Adaptive Defense 360

El aumento de la cobertura y uso de internet requieren que México tenga una estrategia Nacional e integral de ciberseguridad, señaló la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la información (Canieti).

En ese sentido, la implementación de tecnologías avanzadas como Adaptive Defense, como complemento al antivirus tradicional o a la seguridad perimetral, facilita el cumplimiento con el ENS y los requisitos técnicos mencionados anteriormente, puesto que **Adaptive Defense ofrece un servicio de seguridad garantizada frente a amenazas y ataques avanzados y dirigidos a las empresas a través de cuatro pilares:**

Visibilidad:

Registrando la trazabilidad de cada acción realizada por las aplicaciones en ejecución.

Detección:

Monitorizando constantemente todos los procesos en ejecución y bloqueando en tiempo real los ataques dirigidos, zero-day y otras amenazas avanzadas diseñadas para pasar desapercibidas a los antivirus tradicionales.

Respuesta:

Ofreciendo información forense para investigar en profundidad cada intento de ataque, así como herramientas de remediación.

Prevención:

Evitando futuros ataques al bloquear las aplicaciones que no se comporten como goodware y utilizando tecnologías avanzadas anti-exploit.

Adaptive Defense protege los equipos informáticos permitiendo ejecutar únicamente el software lícito, mientras supervisa y clasifica todos los procesos ejecutados en el parque informático del cliente en base a su comportamiento y naturaleza. Además completa su oferta de seguridad ofreciendo herramientas monitorización, análisis forense y resolución para poder determinar el alcance de los problemas detectados y solucionarlos.

A diferencia de los antivirus tradicionales, **Adaptive Defense utiliza un nuevo modelo de seguridad que le permite adaptarse de forma precisa al entorno particular de cada empresa,** supervisando la ejecución de todas las aplicaciones y aprendiendo constantemente de las acciones desencadenadas por cada uno de los procesos.

Tras un breve periodo de aprendizaje Adaptive Defense 360 es capaz de ofrecer un nivel de protección muy superior al de un antivirus tradicional, al tiempo que proporciona una información valiosa sobre el contexto en el que se sucedieron los problemas de seguridad a fin de poder determinar su alcance e implantar las medidas necesarias para evitar que se vuelvan a suceder.

Adaptive Defense 360 es un servicio multiplataforma compatible con Windows, Linux, Mac OS X, Android y alojado en la nube; por lo tanto no requiere de nueva infraestructura de control en la empresa, manteniendo de esta manera un TCO bajo.

Al tratarse de un servicio gestionado de seguridad desde la nube, los requerimientos exigidos por el ENS aplica de manera directa al proveedor de la misma. La solución Panda Adaptive Defense descansa en el cloud Azure de Microsoft.

Microsoft Azure ha pasado una rigurosa evaluación por parte de BDO, un auditor independiente, que emitió un comunicado oficial de su cumplimiento. BDO certifica que las medidas de seguridad en este servicio, así como sus sistemas de información e instalaciones de procesamiento de datos, cumplen con alto nivel con el RD 3/2010 sin necesidad de medidas correctivas. Microsoft es el primer proveedor de servicios cloud a hiperescala en recibir esta certificación en España.

Finalmente y en relación con la **Ley General de Transparencia y acceso a la Información Pública, el Reglamento General de Protección de Datos comenzó a aplicarse a partir del 4 de Mayo del 2015**, hay que destacar que Adaptive Defense no recoge ninguna información de tipo personal y en ningún caso se envía información personal al cloud, facilitando así el cumplimiento de la normativa de protección de datos actual y futura.

Una protección contra amenazas avanzadas y ataques dirigidos, capaz de detectar comportamientos extraños. Un sistema que asegura la confidencialidad de los datos, la privacidad de la información, el patrimonio y la reputación empresarial. Esto es Adaptive Defense, el único sistema de ciberseguridad avanzado que combina protección de próxima generación y la última tecnología de detección y remediación con la capacidad de clasificar todos los procesos en ejecución.

Más información:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Llamando al:

+52 55 8000 2381

o via email mexico@pandasecurity.com

panda

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

pandasecurity.com

panda