ESPECIAL

"Futuro y seguridad"

DE Tecnología & Sentido Común

ESPECIAL
AGOSTO
2024

ESPECIAL

"Futuro y seguridad"

DE Tecnología & Sentido Común

EQUIPO TYSC
Javier Peris - El Gobernauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Miguel Angel Arroyo - Hack & News
Juan Carlos Muria - Diario de una Tortuga Ninja
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Marcos Navarro - Ai Robot
Víctor Almonacid - La Nueva Administracion
Jesús López Peláz - Consejo de Amigo
Renato Aquilino - Marcos y Normas
Alex Aliaga - Radio Security
Marta Martín - Mentes Divergentes

PUBLICIDAD Y CONTRATACIÓN
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
soluciones@businessandcompany.com

EDITA
Business, Technology & Best Practices, S.L.
Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://tecnologiaysentidocomun.com
soluciones@businessandcompany.com

Manuel Serrat

Doctor en Informática por la Universitat Politècnica de València y Master en Dirección TIC de la UPM-INAP, dispone de varias certificaciones internacionales en Operación, Gestión y Gobierno de TI, tales como ITIL, FITSM, PRINCE2 y COBIT. Escritor técnico, ha sido profesor asociado en varias universidades y actualmente coordina el servicio de TI de una organización pública.

LinkedIn: https://www.linkedin.com/in/manuel-david-serrat-olmos/
Twitter: https://twitter.com/mdserrat

ISSN 2951-8180

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Sesión de Formación y Certificación en:

Sistema de Gestión de la Inteligencia Artificial

Director Académico:

Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 42001:2023
- Examen de Certificación Incluido
- Certificación ISO 42001 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 10 de Abril

+ 34 96 109 44 44
campus@escueladegobierno.es

ESPECIAL AGOSTO 2024

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

índice

#TYSC

Premios recibidos

Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

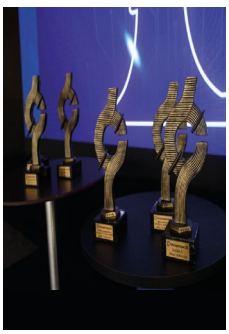
itSMF ESPAÑA

Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad

La Junta Directiva de la Asociación Profesional Española de Privacidad durante su VI Congreso Nacional de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC

apep

Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comuni- dad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.

COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.
Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.
Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.

eset

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA

La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.

AVIS@ ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021
ISO 30401:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 30300 Leader
- Certificación ISO 30401 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

Perspectivas del mercado de la ciberseguridad

En el sector de las TIC estamos ya muy acostumbrados a los diferentes hypes o palabras de moda que, periódicamente, atraen la atención de los profesionales y, sobre todo, de los inversores y responsables públicos. Blockchain, metaverso, inteligencia artificial,… son algunos de los más recientes. También la ciberseguridad ha sido uno de estos términos de moda, pero con una gran diferencia: es una necesidad transversal e imprescindible para el desarrollo de los mercados digitales y su estabilidad.

Comenzamos esta novena temporada de Tecnología y Sentido Común hablando de Futuro y Seguridad, conceptos que dan título a nuestra sección en la revista. En esta ocasión, y comenzando una nueva temporada, ¿qué mejor que plantear las perspectivas que presenta el mercado de la ciberseguridad en la situación actual?

El mercado de la ciberseguridad se puede analizar desde diferentes ópticas: la de las empresas del sector, la de los profesionales de la ciberseguridad, la de los clientes de estas empresas y profesionales, y la de los ciberdelincuentes.

Comencemos por éstos últimos. No hay duda de que los actores maliciosos tienen excelentes perspectivas de mercado. No en vano se calcula que el cibercrimen mueve un volumen de negocio mundial superior al narcotráfico, el tráfico de armas y el tráfico de pesonas. Como ya hemos escrito en varias ocasiones, incluso en algunos paises las empresas de ciberdelincuentes se comportan como cualquier otra empresa, con sus empleados, sus horarios, sus impuestos, etc. También hemos escrito en alguna ocasión sobre el floreciente mercado que representa el Ransomware-as-a-Service, la especialización de las organizaciones de ciberdelincuentes, y la enorme dificultad que tienen las fuerzas de seguridad para atribuir los delitos y perseguirlos de forma eficaz.

Ante esta situación, es de esperar que los principales perjudicados, o aquellos que tienen unas peores perspectivas en este 'mercado' son los clientes. Primero, porque son el objetivo de los ciberdelincuentes, y segundo, porque para evitarlo han de realizar gastos e inversiones. En este aspecto, y aunque la ciberseguridad no es en absoluto un producto o servicio barato, es idiscutible que sea mejor invertir X€ en protegerse que tener que gastar N veces esa cantidad si se es víctima de un ciberataque exitoso. Como dice un amigo mio, "susto o muerte". Coincidirá conmigo el lector o la lectora en que también es mejor pagar por los servicios de seguridad de una empresa legítima y del país, que pagar un rescate a una de las mafias que operan en el mercado del ransomware, por ejemplo.

CONTINÚA EN PRÓXIMA PÁGINA

Y esto nos lleva a hablar de las perspectivas de las empresas del sector de la ciberseguridad. En este caso, podemos pensar que cuanto mayor es la percepción de la amenaza, mayor es el nivel de contratación a las empresas del sector. O mejor dicho, cuanto mayor es el entendimiento de a qué se enfrentan las organizaciones públicas y privadas, más propensas serán éstas a invertir en los servicios de seguridad que aquellas proporcionan. Sobre todo, si de esas inversiones se desprende un nivel de satisfacción adecuado. Por tanto, las empresas de ciberseguridad que puedan ofrecer demostrables servicios de alto valor añadido forzosamente han de ver como su volumen de negocio tiene un alto potencial de crecimiento. Porque además, también estas empresas se están diversificando por nichos de especialización, formando un ecosistema alrededor de la ciberseguridad, que incluye servicios tales como la auditoría, el pentesting, la formación, la forénsica digital, la inteligencia de amenazas, o los productos y servicios de protección de sistemas y servicios digitales.

Sin embargo, existe un claro factor limitativo a este potencial incremento de facturación y beneficios. Son muchas las empresas del sector que llevan ya un tiempo repitiendo el mantra de que falta talento en el sector de la ciberseguridad, que les cuesta mucho contratar personal y que el personal verdaderamente profesional les sale muy caro de contratar. Por tanto, parece que las perspectivas, desde el punto de vista de estos profesionales de la ciberseguridad, podrían calificarse también como muy buenas. Y por ello, se fomenta la incorporación de jóvenes profesionales al sector, mediante formación específica a diferentes niveles o múltiples congresos de ciberseguridad, como la RootedCon Valencia que se celebra este mes de septiembre. Esas expectativas positivas, sin embargo, no se están viendo reflejadas en los salarios del sector, como denuncian repetidamente los profesionales experimentados, que si bien perciben salarios por enciam de la media del sector TIC, al menos en España no se están valorando adecuadamente, lo que lleva a muchos de ellos a trabajar para multinacionales ubicadas en otros países, en formato teletrabajo, con sueldos de esos otros países, más competitivos que los españoles.

En conclusión, para reducir las expectativas de los ciberdelincuentes, se han de potenciar las empresas españolas del sector, para lo cual se ha de disponer de suficiente talento especializado con salarios competitivos a nivel europeo, y que los clientes de esas empresas entiendan el valor añadido que los servicios que les proporcionan suponen para su actividad.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 56002 Leader
- Certificación ISO 56006 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre

Solicita tu admisión en:

+ 34 96 109 44 44
campus@escueladegobierno.es

Mensajería, privacidad, cifrado y delincuencia, todo en la batidora

En los últimos meses se ha venido hablando en Europa sobre la posibilidad de prohibir el cifrado en las aplicaciones que la mayoría de nosotros usamos, con el pretexto de que dificultan la lucha contra la delincuencia, en general. De nuevo, nos encontramos con viejos discursos en los que se pretende poner un determinado derecho o bien común por encima de otros, menos importantes desde la óptica de quien lo propone. ¿Y no me dirán el lector que ésta cuestión no merece la pena para ser analizada con cierto rigor?

Una de las medidas de seguridad que, en el caso de la administración pública española, se plantea como obligatoria en determinados sistemas de información es el cifrado de ésta, tanto en tránsito como en su almacenamiento definitivo. También se establece la necesidad de cifrado en los dispositivos móviles que almacenen determinados tipos de datos. Son medidas incluidas en el Anexo II del Esquema Nacional de Seguridad, pensadas para proteger la confidencialidad e integridad de la información que trata la Administración.

Las aplicaciones de mensajería que todos tenemos en nuestros dispositivos móviles, las aplicaciones de videoconferencia de las que venimos haciendo un unos masivo desde la pandemia, o las conexiones de red privada virtual con las que trabajamos desde cualquier lugar del mundo con acceso a Internet como si estuviésemos en la oficina, son algunos ejemplos de productos que incluyen mecanismos de cifrado para proteger al usuario de diferentes tipos de amenazas a la confidencialidad, componente fundamental de la privacidad.

Pero, ¿qué ocurre cuando el usuario de estas herramientas es un delincuente internacional, al cual las agencias policiales están investigando? Le incautan el terminal móvil o su ordenador y no pueden obtener la información almacenada porque está cifrada. O no pueden 'pinchar' sus comunicaciones porque éstas también lo están. En esta situación, los agentes policiales ven muy dificultada su tarea de proteger a la sociedad de estas personas indeseables, en casos, por ejemplo, de terrorismo o delincuencia organizada de cualquier tipo.

El debate de prohibir el cifrado en determinado tipo de aplicaciones, como las de mensajería, está servido en el seno de la Unión Europea, con España como el socio más radical en apoyo a esa propuesta. Es decir, España mantiene una postura beligerante a favor de que se prohíba en la UE el cifrado en las aplicaciones de mensajería de los ciudadanos, lo que para muchos puede representar un claro ataque a la privacidad, y cuyos beneficios son más que dudosos.

CONTINÚA EN PRÓXIMA PÁGINA

¿Por qué digo que retirar el cifrado extremo a extremo en este tipo de aplicaciones no serviría de nada? Pues porque afectaría gravemente a la seguridad y la privacidad de los ciudadanos normales, y los delincuentes, simplemente, usarían otro tipo de herramientas, si hace falta, desarrollándolas ellos mismos, dada la capacidad económica de determinadas organizaciones criminales. Es decir, estaríamos ante una medida que, de materializarse, desprotegería a la inmensa mayoría de los usuarios de las aplicaciones de mensajería, y haría que esas redes de delincuentes salieran de la masa de usuarios de las mismas para utilizar otros sistemas de mensajería que sí tuvieran cifrado. Sería el equivalente a hacernos ir a todos desnudos por la calle para evitar que nadie esconda un arma bajo la ropa.

Además, el paso de obligar a no cifrar las aplicaciones de mensajería podría ser sólo el primero, porque una vez logrado, ¿qué impediría impulsar las medidas legales orientadas a obligar también a que los soportes de información (discos, pendrives, etc.) no se pudieran cifrar? Con el mantra de la seguridad de toda la sociedad históricamente se han producido todo tipo de abusos, y no cabe duda que si esta cuestión se materializase, se producirían igualmente.

Afortunadamente, la opinión oficial española no está ampliamente respaldada dentro de la UE, con la mayoría de países optando por otro tipo de medidas, pero en estas cuestiones hay que estar siempre alerta, como ciudadanos. Todos estamos a favor de que, en el marco de una investigación policial, y con el aval de un juez, se intervengan las comunicaciones y los equipos de proceso de información de los investigados. Incluso, podríamos estar de todos de acuerdo en que las plataformas dispongan de las herramientas oportunas para, ante una orden judicial internacional, entregar la información solicitada.

Naturalmente, no se me escapa la necesidad de equilibrar los derechos a la seguridad individual y colectiva con la privacidad, pero también habría que esperar cierta proporcionalidad en las medidas de seguridad propuestas frente a las amenazas existentes. Y, por qué no, explorar otras opciones, como ya se ha hecho en el pasado reciente, donde una agencia gubernamental proporcionaba en la Deep Web una aplicación de mensajería segura, específicamente orientada a la delincuencia. Por supuesto, la aplicación era operada por los agentes y obtuvo resultados con la detención de multitud de facinerosos en varios países.

Seguridad, sí. Privacidad, también. Estado Policial, por supuesto que no.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación TSG4® Yellow Belt
- Certificación UNE 71404 Executive
- Módulo 1: MasterGEIT®
- Módulo 1: MasterPPM®

MPPM® MGEIT® eGob®

Del 15 al 23 de marzo

+ 34 96 109 44 44
campus@escueladegobierno.es

De barcos, capitanes y un mar embravecido

No se preocupe el lector, que no se ha equivocado de revista ni de sección. Está leyendo la sección Futuro y Seguridad de Tecnología y Sentido Común. Sin embargo, la analogía de los barcos, los capitanes y el mar embravecido es perfectamente válida para explicar la situación en la que se encuentran muchas de las Administraciones Locales en España en lo referente a la Ciberseguridad. La analizamos en este artículo.

En mí es habitual mantener cierto contacto con profesionales TIC de las Administraciones Locales, pero recientemente he podido compartir más tiempo con un grupo de estos profesionales gracias a una formación en la que he participado. Y pese a que no me han sorprendido en absoluto los comentarios que estas personas han realizado sobre la situación de la Ciberseguridad en sus entidades, sí que he podido constatar que, pese a que su nivel de concienciación al respecto es muy alto, no consiguen que esta cuestión 'cale' en las capas directivas de las mismas, esto es, el personal electo y los funcionarios habilitados de carácter nacional, más concretamente, los que ejercen las funciones de secretaría general.

Con un Esquema Nacional de Seguridad (ENS), de obligatoria aplicación desde 2010 para todas las Administraciones Públicas, muchas de éstas aún están pendientes de realizar las más básicas adaptaciones que el ENS exige: Y no me refiero a las adaptaciones tecnológicas, ya que el personal al cargo se esfuerza diariamente en ello, sino sobre todo, a aquellas cuestiones que tienen que ver con las cuestiones organizativas. Sin ir más lejos, es patente la falta de una Política de Seguridad de la Información, exigida por el artículo 12, y que ha de definir aspectos tales como los objetivos o misión de la organización, el marco regulatorio en el que se desarrollará sus actividades, los roles o funciones de seguridad, con sus deberes y responsabilidades, la estructura y composición del comité para la gestión y coordinación de la seguridad, las directrices para la estructuración de la documentación de seguridad del sistema, o los riesgos que se derivan del tratamiento de los datos personales.

Este documento parece relativamente sencillo de elaborar, pero los comentarios que recibí de los profesionales TIC eran, mayoritariamente, de que la dificultad para aprobar y publicar una Política de Seguridad radicaba, en su caso, en la negativa de las capas directivas de la entidad local a asumir las responsabilidades que los roles definidos en el artículo 13 del ENS, que son los roles de responsable de la información, responsable del servicio, responsable de sistemas y responsable de seguridad. Éste último rol, por la experiencia vivida, suele ser el más complicado de asignar a alguno de los puestos de la entidad local, ya que parece que tiene una elevada componente tecnológica.

Esta dificultad no es más que la postrera demostración de la desidia o dejadez de la mayoría de directivos de la Administración Local, sean funcionarios o políticos, en cuestiones relacionadas con la ciberseguridad. Y ello, pese a que ya hace un tiempo la Federación Española de Municipios y Provincias, junto al Centro Criptológico Nacional, elaboró un estupendo documento, el "Prontuario de Ciberseguridad para Entidades Locales", actualizado en diciembre de 2022 con los cambios de la nueva versión del ENS, y en el cual, en resumen, se indica que la máxima responsabilidad de la ciberseguridad de la entidad local es de la persona que ostenta la Alcaldía (o Presidencia de Diputación o Mancomunidad). Sin embargo, el prontuario también asigna responsabilidades a otros órganos o personas del municipio, especialmente, a los funcionarios habilitados de carácter nacional.
En un estupendo resumen que se incluye como anexo al Prontuario, se detallan con claridad estas responsabilidades.

CONTINÚA EN PRÓXIMA PÁGINA

Pese a la existencia de este documento, y contra toda lógica, ni las personas electas ni los funcionarios de alto rango aceptan de buen grado estas responsabilidades, por lo general. De ahí la queja del personal TIC de las entidades locales a la que me he referido al inicio del artículo.

Estamos pues, en plena aplicación de la analogía del barco (la entidad local), el capitán (alcalde/sa, secretario/a general,….) y el mar embravecido (la amenaza de los ciberdelincuentes), pero en una situación en la que el capitán, aunque no abandona el barco, deja en manos de los marineros rasos el gobierno de la nave en plena tormenta, eludiendo asumir sus responsabilidades, e incluso, en los casos más extremos, ignorando la tormenta porque eso son 'líos de los informáticos'. Y si esto ocurre con algo que es la aplicación de un Real Decreto obligatorio, es fácil imaginar qué ocurre con las buenas prácticas en cuestiones como la gestión de cibercrisis, donde el Centro Criptológico Nacional también tiene un estupendo documento, llamado 'BP29 – Gestión de cibercrisis para entidades locales', y en el que también se asignan responsabilidades a estos 'capitanes', expertos en la elusión de las mismas, por lo visto hasta el momento.

La sugerencia general de los asistentes a la formación a la que me he referido con anterioridad fue que es urgente que en los planes de formación para personal electo se incluyan as cuestiones que tienen que ver con la ciberseguridad, el ENS y las funciones y responsabilidades en la materia que asumen los electos municipales. Igualmente, se planteó que esa formación se realizara a través de los colegios de secretarios e interventores al mayor número posible de ellos, para que asuman también sus responsabilidades y dediquen el tiempo y los recursos oportunos. Es curioso ver cómo este personal TIC se preocupa de la formación de sus superiores, en lugar de lo que sería lógico. Y esto es así porque las carencias formativas en este tema y la falta de interés en asumir nuevas responsabilidades generan un coctel muy perjudicial para el avance de la ciberseguridad en las administraciones locales.

Es lamentable constatar que, trece años después de la aprobación del ENS, aún haya tantísimas entidades locales, algunas de un tamaño respetable, que se encuentren en esta pelea interna, cuando lo que deberían estar haciendo es implementando los planes de adecuación necesarios para obtener la certificación de cumplimiento del ENS, lo que generaría confianza en los ciudadanos de su municipio o provincia, confianza que se ve muy dañada al ver casos de grandes ayuntamientos, como Sevilla, Castellón u Oviedo, paralizados por la acción de los ciberdelincuentes.

Si el personal TIC de las entidades locales está comprometido, existen leyes, normas y guías que deben o pueden utilizarse, y hay apoyo de otras entidades públicas y empresas, sólo hacen falta 'capitanes' que quieran llevar el 'barco' a puerto seguro, porque entiendan que muchos de los servicios que su entidad local proporciona a la ciudadanía están prestándose con el apoyo directo o indirecto de la tecnología, por lo que una paralización de ésta por un ciberincidente puede paralizar la actividad de su municipio.

Como siempre decimos en esta sección, 'sólo no puedo, pero con amigos, sí'.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Análisis de Negocio y Gestión por Procesos

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BPA Leader
- Certificación BPM Executive
- Módulo 2: MasterGEIT®
- Módulo 2 MasterPPM®

MPPM® MGEIT® eGob®

Del 5 al 13 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

A Dios rogando, y con el mazo dando: el negocio del filtrado

Todos estamos implicados en la lucha contra el cibercrimen. Todos queremos una Internet más segura para la infancia. Todos queremos una digitalización de las economías donde la confianza sea posible para el adecuado desarrollo de un mercado global de bienes y servicios. Mentiras que estamos habituados a escuchar o leer, y sobre las que reflexiono en mi artículo de este mes.

Uno de los lemas de esta sección de Tecnología y Sentido Común es 'sólo no puedo, pero con amigos, sí'. Con este lema, escuchado en convenciones de ciberseguridad, trato de reforzar el concepto de que en este barco debemos estar todos, colaborando y compartiendo información para acotar cada vez más el campo en el que la ciberdelincuencia pueda actuar, pero siempre manteniendo un adecuado equilibrio con los derechos fundamentales de las personas. Usuarios de Internet, operadoras de telecomunicaciones, expertos en ciberseguridad y Fuerzas y Cuerpos de Seguridad del Estado debemos estar alerta y participar de un bien común como es nuestra seguridad en las redes.

Pero recientemente, a raíz de un post en LinkedIn de un reputado experto en ciberseguridad, se suscitó un interesante intercambio de opiniones que me han llevado a escribir este artículo. Pongo al lector en antecedentes. Este reputado experto expresaba en su post una cuestión que, en esencia se resumía en lo siguiente: ¿por qué ciertos proveedores de acceso a Internet/ operadoras de comunicaciones, de carácter transnacional filtran o impiden el tráfico hacia una lista de webs o dominios utilizado para "infringir las leyes de propiedad intelectual" (traducción: webs de intercambio de enlaces o donde se tiene acceso a televisión por IP de forma gratuita, y en las que se puede ver desde retransmisiones deportivas hasta películas o series), simplemente porque ciertas organizaciones privadas alimentan esas lista, sin control judicial de ningún tipo, y sin embargo, no se hace lo mismo hacia dominios o webs que se están usando para actividades de ciberdelincuencia de otro tipo?.

Lo que este experto planteaba, sin entrar en la validez legal o no del filtrado del tráfico de sus clientes, equivalente a la censura, es que igual que se llevaba a cabo esa actividad de filtrado ante cierto tipo de destinos, podría hacerse hacia destinos bien conocidos por ser utilizados para actividades de ciberdelincuencia, como estafas on line, ransomware, etc.

A partir de este planteamiento, con el que podemos estar bastante de acuerdo desde un punto de vista teórico, los comentarios al post fueron muy variados, y algunos de los mismos se centraron en un aspecto poco claro, y que, de ser así, demostraría la hipocresía de los proveedores de servicio de acceso a Internet. Ese aspecto es EL NEGOCIO.

Analicemos sucintamente en qué afecta al negocio de los operadores de comunicaciones el hecho de que existan servicios ilegales de, por ejemplo, televisión por IP que sirvan contenidos protegidos por la normativa de propiedad intelectual o industrial, o sobre los que se generan derechos de imagen. En la actualidad, casi todos los grandes operadores de comunicaciones o proveedores de acceso a Internet, al menos en España, incluyen en su oferta paquetes de televisión, o incluyen servicios de streamming como Netflix, HBO o Amazon Prime Video. Por tanto, los servicios de televisión por IP ilegales les provocan un perjuicio claro en sus cuentas de resultados,

ya que el tráfico que les obliga a cursar el video bajo demanda no se corresponde con servicios que ellos estén comercializando de ese tipo. Por tanto, hay una COLISIÓN entre el interés del usuario de las redes de comunicaciones y el de las grandes operadoras, y dado que ellas tienen la sartén por el mango, eliminan esa competencia desleal que reduce sus cuentas de resultados. Resumen: el filtrado de contenidos ilegales beneficia a la operadora dos veces, ya que se reduce el tráfico que han de cursar y el usuario ha de gastar un dinero adicional en disponer de ciertos servicios de video bajo demanda. Como dicen en los casinos, "gana la Banca", a costa del cliente.

Analicemos ahora sucintamente en qué afecta a esos mismos operadores de comunicaciones el hecho de no filtrar webs maliciosas. Como en el caso anterior, las grandes operadoras tienen divisiones que ofrecen productos y servicios de ciberseguridad para empresas y particulares. Por tanto, y aunque parezca extraño, da la impresión de que hay una COLUSIÓN entre los intereses de esas operadoras y las de los ciberdelincuentes, en el sentido de que a mayor ciberdelincuencia, mayores son las

CONTINÚA EN PRÓXIMA PÁGINA

probabilidades de que las empresas y particulares contraten los servicios de ciberseguridad que sus operadores de comunicaciones les ofrezcan. Es algo parecido a lo que se decía en los años 90 del pasado siglo al respecto de los virus y las empresas que desarrollaban antivirus, ya que éstas eran las más interesadas en que ese tipo de malware proliferar, ya que ello les garantizaba el negocio. No estoy acusando a nadie de complicidad con el cibercrimen, Dios me libre. Me estoy refiriendo, en este caso, a que filtrar, de forma predeterminada y sin cargo para el cliente, el tráfico de o hacia webs maliciosas bien conocidas repercutiría negativamente en las cuentas de resultados de las grandes operadoras de comunicaciones, aunque redundase en un beneficio para sus clientes. Resumen: el filtrado de webs maliciosas de forma predeterminada perjudica a esos operadores, que ofrecen esos servicios por un precio, y por eso no se hace. De nuevo "gana la Banca", a costa del cliente.

De ahí que en la entradilla de este artículo se diga que frases como "Todos estamos implicados en la lucha contra el cibercrimen" o "Todos queremos una Internet más segura para la infancia" o "Todos queremos una digitalización de las economías donde la confianza sea posible para el adecuado desarrollo de un mercado global de bienes y servicios" son expresiones que quedan muy bien en las conferencias o en los folletos publicitarios, pero que no dejan de ser mentira en boca de ciertas compañías.

¿Es legítimo que las empresas a las que me he referido oferten determinados servicios bajo suscripción por un precio? Lo es. Pero ¿es legítimo que aprovechen su posición para acabar con la neutralidad de la red y conseguir que sus clientes paguen más para estar (sobre el papel) más seguros? En mi opinión, no lo es. Y me hago otras preguntas:

•¿Por qué todos los operadores europeos no usan para la resolución DNS el servicio dns0.eu? Este servicio, cumpliendo el RGPD y administrado por una ONG francesa, indica en su web que "aumenta enormemente la tasa de detección de dominios maliciosos, especialmente en sus primeras horas críticas, combinando inteligencia de amenazas examinada por humanos con heurística avanzada que identifica automáticamente patrones de alto riesgo".

•¿Hay suficiente normativa europea, y con un nivel de cumplimiento adecuado, que ayude a los ciudadanos a tener un nivel base de seguridad en el uso de Internet sin tener que contratar paquetes de servicios adicionales a los operadores de comunicaciones?

•¿Somos los ciudadanos lo suficientemente conscientes de cómo se mercadea con nuestros datos y con nuestra ciberseguridad? (Creo que hay pruebas suficientes de que no).

Ante esta situación, los clientes sólo podemos hacer una cosa: poner nuestras propias medidas de seguridad, quizá gastando un dinero importante, y tratar de mantener a nuestros operadores lo más neutros posible, cambiando de operador las veces que haga falta, si es necesario. Quizá nos cuentes más esfuerzo, pero al menos mantendremos un cierto grado de libertad que, en los tiempos que corren, nos sabrá al gloria.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Proyectos

OpenPM² (PjM) + ISO 21502

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PjM) Executive
- Certificación ISO 21502 Leader
- Módulo 3: MasterGEIT®
- Módulo 3 MasterPPM®

MPPM® MGEIT® eGob®

Del 19 al 27 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Inteligencia Artificial en actividades maliciosas (I)

A estas alturas, la Inteligencia Artificial parece que es onmipresente, y no cabe duda que sus avances en los últimos años han sido espectaculares. Y como ocurre con cualquier nueva tecnología o avance, sus luces y sus sombras se hacen patentes en cuanto comienza a ser utilizada, provocando debates y críticas en la sociedad. Sin embargo, en este caso, la ciberdelincuencia ha encontrado un nuevo filón en los diferentes sistemas de inteligencia artificial para llevar a cabo sus siniestras actividades.

En esta sección de Tecnología y Sentido Común nos hemos cuidado mucho, hasta ahora, de comentar, analizar, o incluso mencionar, a los sistemas de inteligencia artificial (IA), cuya irrupción en el gran público ha sido tan comentada en el último año y medio. La presentación mundial y popularización de sistemas de inteligencia artificial generativa, como ChatGPT o Dall-e, que rápidamente han sido integrados por organizaciones como Microsoft en sus productos de consumo, ha resultado sorprendente, cuanto menos.

Sin embargo, rápidamente estos sistemas han provocado la alerta a diferentes estamentos sobre aspectos como la ética de su uso, su impacto en el empleo, o los problemas de orden social y de seguridad que pueden suponer. Alumnos que piden a una IA que les elabore los trabajos para clase, evitándose el esfuerzo de tener que realizarlos por sí mismos, pero privándose con esta acción del objetivo primario del encargo de esas tareas, que no es otro que el aprendizaje. Abogados que preparan escritos ante los tribunales apoyándose tanto en la IA, que acaban usando referencias legales inexistentes, provocando daños a sus clientes y a ellos mismos, y no sólo en su reputación profesional. Mujeres que son víctimas de un nuevo tipo de acoso y violencia al ver sus caras integradas perfectamente en videos de contenido sexual, generados por una IA y publicados por descerebrados o personas vengativas. Basten estos tres ejemplos, de los que todos estamos al corriente, para hacer notar que esta tecnología requiere de un armazón legal nuevo, y de nuevas herramientas para la detección de este tipo de documentos, fotografías, audios o videos generados por la IA, que impidan que cualquiera de nosotros podamos vernos involucrados en una situación problemática por la acción combinada de una mala persona y una herramienta de IA mal utilizada.

CONTINÚA EN PRÓXIMA PÁGINA

Por supuesto, la razón de hablar de esta cuestión en esta sección de la revista no es hacer un comentario sobre la ética de sus diferentes usos, o sobre las diferentes herramientas que cualquiera tiene a su alcance. En este artículo nos vamos a centrar en tratar de analizar y sacar conclusiones sobre los diferentes métodos en los que los ciberdelincuentes están utilizando para sacar provecho de los sistemas de IA, sean públicos o sean construidos ad hoc por estas redes de delincuencia organizada, que recordemos que, si algo tienen, es potencial económico para ello.

Partiendo de la base de que el eslabón más débil de la cadena de la ciberseguridad es el usuario de los sistemas de información, podemos llegar a la conclusión rápida de que el principal uso de los sistemas de IA será la generación de elementos para facilitar los ataques de ingeniería social, bien sea para facilitar la instalación de ransomware, bien para la realización de algún tipo de estafa de carácter económico, por ejemplo. Sin embargo, hay otros elementos frente a los que un sistema de IA utilizado para el mal puede resultar útil. Por ejemplo, se podría entrenar a un sistema de IA para tratar de buscar y explotar vulnerabilidades en sistemas perimetrales, o para localizar información de interés sobre la organización a atacar y sus empleados, buscando el punto débil de alguno de ellos para que sea un blanco adecuado para extorsiones o sobornos que lleven al atacante a obtener un acceso legítimo a los sistemas de la organización objetivo.

Un sistema de IA generativa construye elementos de información a partir de sus modelos de aprendizaje, habiendo sido entrenado con volúmenes inmensos de información procedentes de múltiples fuentes. Cuando el usuario realiza una petición (o prompt) en lenguaje natural, estos sistemas la analizan y comienzan su tarea. Cuánto más concreta sea la petición, mejores resultados se obtendrán. Por tanto, son sistemas que, a un coste muy reducido, permitirán a los ciberdelincuentes generar los elementos necesarios para apoyar su actividad. Y un ejemplo claro de ello es su uso en los ataques de vishing, o phishing por voz. Con sólo unos segundos de grabación de la voz original de una persona, hay sistemas de IA capaces de generar todo un discurso con dicha voz, acercándose ya incluso a poder hacerlo en tiempo real.

En esta situación, imagine que una persona del departamento financiero de una organización recibe una llamada falsa de quien ella cree que es el director financiero, la gerencia o el CEO de la misma, indicándole que ha de hacer una determinada operación de transferencia de fondos. Esa persona, que conoce a voz de su superior, y aunque extrañada, ante una orden directa se ve obligada a realizar dicha operación. Cuando se descubre que falta dinero, todos los ojos de la sospecha se dirigirán a esa persona, quien alegará que recibió la orden telefónicamente de su superior, quien evidentemente lo negará, ya que no hizo dicha llamada. Y los problemas legales para esa persona del departamento financiero no habrán sino comenzado, ya que probablemente se le considere, de entrada, cómplice de la desaparición de esos fondos, cuando lo que ha sido es víctima de un engaño creado mediante un sistema de IA generativa en apoyo de la actividad de los ciberdelincuentes.

¿Y cómo se protege uno de esa amenaza? “Zero trust”, o confianza cero. En las organizaciones de cierto tamaño, se suele conseguir con procedimientos, dobles validaciones y comprobaciones previas, como hacen muchas administraciones públicas españolas antes de pagar un solo euro. Pero para tratar de torcer los procedimientos los ciberdelincuentes también son capaces de crear documentos falsos, correos electrónicos fraudulentos, perfiles de personas en todo tipo de servicios on line, webs falsas, etc. Por tanto, suele ser una buena práctica tratar de comprobar la información a través de medios totalmente diferentes a los que el propio potencial ciberdelincuente nos ofrezca.

Por ejemplo, si se recibe por email una comunicación de que se desea cambiar la cuenta en la que se cobran las facturas, ese cambio debe confirmarse llamando por teléfono a la empresa que emite esas facturas usando los medios de contacto que se tuvieran previamente registrados. Si recibimos una llamada de alguien desconocido que dice que es del soporte técnico informático de la organización, antes de darle acceso se debería confirmar lo que esa persona está diciendo, a ser posible, contactando directamente con quienes hayan podido hacer la petición de que se preste ese servicio, o incluso, tratando de retrasar esa intervención a otro momento para dar tiempo a hacer las comprobaciones oportunas.

Par resumir, cualquier precaución previa es poca cuando se trata de evitar caer en la trampa de los ciberdelicuentes, y actualmente ya no podemos creernos ni siquiera lo que ven nuestros ojos u oyen nuestros oídos a través de medios electrónicos.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Programas

OpenPM² (PgM) + ISO 21503

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PgM) Executive
- Certificación ISO 21503 Leader
- Módulo 4: MasterGEIT®
- Módulo 4 MasterPPM®

MPPM® MGEIT® eGob®

Del 3 al 11 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Evento de Cierre de Temporada 2024 de las Revistas Tecnología y Sentido Común y Stakeholders.news

El 19 de julio de 2024, las revistas Tecnología y Sentido Común y Stakeholders.News celebraron el Cierre de su novena y tercera temporada respectivamente con un interesante evento en la sede de UNE Asociación Española de Normalización, en Madrid.

En una tradición que se inició el pasado año 2023, las revistas Tecnología y Sentido Común y Stakeholders.News prepararon un cierre de temporada a la altura tanto de la calidad de sus contenidos como del nivel de sus colaboradores. Con la inestimable colaboración de UNE Asociación Española de Normalización, el día 19 de julio de 2024 se reunió en Madrid un granado grupo de profesionales, entre los que estaban algunos de los colaboradores de nuestras revistas.

El evento comenzó con una bienvenida a cargo de Paloma García, Directora de Programas de Normalización y Grupos de Interés de UNE, y de Javier Peris, Director de las revistas Tecnología y Sentido Común y Stakeholders.News, en el que agradecieron a los presentes su asistencia, sobre todo a aquellos afectados por el incidente global en sistemas de información de grandes compañías de todo tipo que se dio en esa fecha.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Tras la bienvenida, se dio paso al ponente principal del evento, Ramsés Gallego, primer español (y tercer europeo) en ser nombrado para el "Hall of Fame" de ISACA internacional, evento que tuvo lugar en este 2024. Renombrado conferenciante, deleitó al público asistente con su charla "De Gestionar a Gobernar …. con 'G' de Ganar", en la que glosó las bondades de dar ese salto hacia el gobierno de las Tecnologías de la Información, sobre todo en los aspectos relacionados con la ciberseguridad. Ciertamente, un lujo contar con él para el evento.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

El siguiente acto fue la mesa redonda con cinco de los autores que colaboran con la revista Tecnología y Sentido Común en el que participaron: Alejandro Aliaga líder de la seccion “Radio Security”, Renato Aquilino líder de la sección “Marcos y Normas”, Marlon Molina líder de la seccion “Es Tendencia”, Marcos Navarro líder de la seccion Ai Robot” que a partir de la proxima temporada pasará a llamarse “Ai Futuro” y Manuel Serrat líder de la seccion “Futuro y Seguridad”.

Durante la mesa redonda de Tecnologia y Sentido Común, estos cinco representantes respondieron a las preguntas del presentador y director de la revista, Javier Peris, acerca de los contenidos de la temporada que terminaba, y de qué se podía esperar de sus secciones en cuanto a contenidos y novedades en la décima temporada de la revista.

Alejandro Aliaga centró su intervención en recordad que el objetivo de su sección “Radio Security” es concienciar a los lectores de que existen vectores de ataque no convencionales asociados con las comunicaciones inalámbricas, y que, por la evolución tecnológica, es difícil que éstos se reduzcan.

Por su parte, Renato Aquilino, en su sección “Marcos y Normas” ha centrado sus contenidos en poner de manifiesto el gap existente entre las normas y quienes las escriben, frente a quienes las han de convertir en realidad en las organizaciones, algo que resulta extremadamente complejo en algunos casos.

Por lo que respecta a Marlon Molina, con su sección “Es Tendencia”, ha tratado de contar a los lectores en esta temporada que termina los temas que, mes a mes, han atraído la atención del sector por diferentes motivos.

Marcos Navarro anunció que su sección, a partir de la décima temporada, cambiaba de enfoque y de nombre, para explicar cómo es la vida en 2024, sólo dentro de diez años, gracias a tecnologías como la Inteligencia Artificial y la Robótica.

En cuanto a Manuel Serrat, explicó que con su sección “Futuro y Seguridad” ha tratado de poner el foco en aquellos aspectos de la evolución tecnológica que pueden suponer algún tipo de riesgo, y concienciar a los lectores para evitarlos.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Finalizada esta mesa redonda, se llevó a cabo la segunda Mesa Redonda, que contó con cuatro de los colaboradores de la revista Stakeholders.News: Juan Manuel Domínguez líder de la Seccion "Organizaciones Resilientes", Luis Morán líder de la sección "Personas y Procesos", José Antonio Puentes líder de la seccion "Tendiendo Puentes" y Juan Jesús Urbizu líder de la seccion "Tecno-transformación".

Dada la temática de la revista, fundamentalmente dirigida a aquellos profesionales de la gestión de proyectos, programas y portfolios y áreas conexas, las preguntas para los participantes en la mesa redonda se centraron en poner de relieve la necesaria aplicación de estándares y buenas prácticas en cada uno de los ámbitos que tratan las diferentes secciones de la revista.

Juan Manuel Domínguez, a través de su sección "Organizaciones Resilientes", expuso aspectos tales como que, en Japón, con aproximadamente 120 millones de habitantes, hay 45.000 empresas centenarias, frente a las poco más de 5.000 que existen en España con 48 millones de habitantes.

Luis Moran comentó algunos de los temas que había tratado durante esta tercera temporada en su sección "Personas y Procesos", y avanzó alguna de las cuestiones que va a tratar en la cuarta temporada de la revista.

José Antonio Puentes (sección "Tendiendo Puentes") compartió con los presentes algunas vivencias personales, relacionadas con las dificultades que la gestión de proyectos enfrenta en determinadas organizaciones.

Por último, Juan Jesús Urbizu, que estas temporadas ha escrito en su sección "Tecno Transformación", apuntó algunas de las cuestiones más relevantes a las que se enfrenta el gestor de proyectos, programas y portfolios en relación con la digitalización de las organizaciones, y más desde la irrupción para el gran público de los sistemas de inteligencia artificial.

CONTINÚA EN PRÓXIMA PÁGINA

Tras las dos mesas redondas, Javier Peris anunció el nombramiento de los tres embajadores de la revista Stakeholders.News en Hispanoamérica más concretamente en Puerto Rico, Uruguay y El Salvador.
En Puerto Rico contaremos cada mes con la participacion de Nesty Delgado en Uruguay contaremos con Daniel Sorokins y en el pais de la eterna sonrisa "El Salvador contaremos con Luis Guardado quienes fueron nombrados y serán a partir de ahora Embajadores de Stakeholders.news.

Los actos de cierre de temporada terminaron con la entrega de los premios Tecnología y Sentido Común y Stakeholders. News, en esta ocasión en su edición de 2024.

El "Premio Tecnología y Sentido Común 2024" recayó en el Consejo General de Colegios Profesionales de Ingeniería Informática (CCII), por su aportación al progreso de la sociedad de la información, el impulso al desarrollo ético de los avances tecnológicos y la defensa y promoción de la ingeniería en informática. El premio fue recogido por José García Fanjul, secretario del CCII y vicedecano del Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Por otro lado, el "Premio Stakeholders.News 2024" fue otorgado a la Agencia para la Administración Digital de la Comunidad de Madrid, por haberse convertido en referente en la innovación y digitalización de la administración pública y por su compromiso con el cumplimiento y la excelencia del servicio al ciudadano. Este premio fue recogido por Zaida Sampedro Préstamo, subdirectora general de Transformación y Gestión del Cambio de la Agencia para la Administración Digital de la Comunidad de Madrid.

Al terminar el acto, todos los presentes pudieron disfrutar de un magnífico networking alrededor de un espectacular catering que se sirvió en las mismas instalaciones de UNE, con lo que se dio por cerrada la temporada de ambas revistas. ¡Nos vemos en septiembre!

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

UNE Normalización Española

Progreso compartido

une.org

Inteligencia Artificial en actividades maliciosas (II)

En el artículo del número del mes pasado de Tecnología y Sentido Común se introdujo una visión general de las amenazas que el uso de la inteligencia artificial para actividades maliciosas plantea. Este mes, vamos a fijar nuestra atención en cómo se están utilizando diferentes herramientas de inteligencia artificial para llevar a cabo uno de los ataques más 'interesantes' desde el punto de vista delictivo, el fraude al CEO, en sus diferentes variantes, y sobre todo, cómo tratar de prevenir caer en él.

Como casi cualquier tecnología de la Historia, estaremos todos de acuerdo que la Inteligencia Artificial (IA) puede ser utilizada para fines beneficiosos o para lo contrario. Ya vimos en el artículo de enero de 2024 de Tecnología y Sentido Común que, precisamente, el uso malicioso de esta potente tecnología suponía nuevos retos para las organizaciones, tanto a nivel técnico como a nivel organizativo. En dichas organizaciones, fundamentalmente aquellas en las que los procesos de gestión no tienen el nivel de madurez adecuado, la generación de un 'desvío' en alguno de los procesos que incluyen aspectos monetarios puede ser un atractivo aliciente para que se sufra un intento de ataque conocido como 'fraude al CEO', del que ya hemos escrito en alguna ocasión. Y lamentablemente, los sistemas de inteligencia artificial generativa suponen una herramienta especialmente útil para este tipo de ataques.

En cualquier ataque, hay una fase de reconocimiento de los objetivos. Ningún mando militar en su sano juicio plantea una operación bélica en terreno desconocido, para lo cual siempre hay misiones de reconocimiento y de recopilación de información de inteligencia, previas a la operación principal. El primer uso de sistemas de IA será, por tanto, aprovechar la información existente, tanto en la web 'superficial' como en la Deep Web para recopilar dicha información y **generar conocimiento útil** para el atacante sobre el objetivo a atacar. ¿Y de qué tipo de conocimiento estamos hablando? Pues, por ejemplo: 1. Nombres, cargos, teléfonos y direcciones de correo de personal de la organización, con especial interés en quienes tienen acceso a fondos; 2. Organigrama directivo; 3. Actividades, volumen de negocios, sedes, filiales, proveedores, socios, etc.; 4. Infraestructura informática y de comunicaciones, incluyendo dominios registrados.... Todo este conocimiento, recopilado y destilado por una IA, queda a disposición del atacante para las siguientes fases del ataque, ya que es importante una rápida reacción de éste ante cualquier imprevisto o duda.

CONTINÚA EN PRÓXIMA PÁGINA

Una vez recopilada la información necesaria, comencemos por lo más simple y clásico: el correo electrónico. Cualquiera, prácticamente sin coste, puede obtener la ayuda de una IA para: a) generar nombres de dominio muy parecidos a los de la organización que se pretende atacar, y registrarlos; b) generar direcciones de correo muy similares a las de los miembros relevantes de la Dirección de la organización, y alojarlas en el lugar oportuno de Internet para no ser localizado; y c) generar mensajes de correo convincentes, en el idioma adecuado a la organización atacada o a las personas a las que se pretende engañar, con lenguaje formal o informal dependiendo de la información recopilada en la fase de reconocimiento. En los **casos más conocidos de fraudes al CEO por correo electrónico** se suele aludir a una necesidad de hacer algún tipo de pago confidencial urgente, sin pasar por los procedimientos habituales, y posiblemente saltándose la cadena de mando organizativa. Son mensajes que suelen recibir las personas al cargo de las cuentas corrientes, desde, supuestamente, la dirección de la persona que ostente la dirección general, indicándole que se va a recibir un correo de una determinada persona externa, y que en dicho correo se le van a dar instrucciones precisas para realizar un pago por determinados servicios, de los que debe mantener una total confidencialidad, al tratarse de una operación estratégica para la organización.

Una variante de este tipo de fraude por email es mucho menos elaborado y se basa fundamentalmente en hacer creer a la organización cliente que la empresa proveedora ha cambiado de cuenta corriente de cobro, de manera que las siguientes facturas deberán abonarse en dicha nueva cuenta. Obviamente, dicha cuenta es de los delincuentes.

¿Cómo podemos protegernos de este tipo de fraudes? Resulta obvio que en ambos ejemplos el problema es de procedimientos, ya que éstos deberían ser respetados por todos, especialmente por la alta dirección. Los procedimientos operativos deben tener el grado de madurez suficiente para que no se pueda realizar pago alguno sin la correspondiente validación interna, a ser posible, doble. En el primer caso, y manteniendo la confidencialidad, la persona que recibe el correo del CEO debería recurrir a su superior directo de forma física, no por ningún método electrónico, para que valide esa operación documentalmente. En el segundo caso, y siempre por métodos de contactos registrados con anterioridad al correo sospechoso recibido (teléfono, email, correo electrónico, etc.), confirmar que la organización proveedora ha solicitado realmente ese cambio de dirección de correo.

La mecánica de los ataques más novedosos de fraude al CEO va a provenir de los métodos utilizados para generar los elementos de comunicación con la persona atacada. Los ciberdelincuentes pueden llamar al CEO con cualquier excusa, obtener una grabación de su voz, y utilizando una IA especializada, a partir del texto adecuado que otra IA les pueda generar, generar un audio con la voz de esa persona diciendo lo que el texto generado refleje. Es decir, estarían falsificando la voz del CEO con el texto que les convenga. Dicho audio puede enviarse por mensajería instantánea, algo muy habitual en la actualidad, para convencer a la persona a quien se pretende engañar para la transferencia de fondos. Más aún, se están experimentando avances en las tecnologías IA de generación de voz y video de manera que ya se podría estar en condiciones de mantener una videoconferencia con un ciberdelincuente, y que la voz y la imagen que oyésemos o viésemos fuesen las de la persona a quien se suplanta. Es decir, estaríamos ante una falsificación de la identidad a través del video, en tiempo real.

En los casos en los que nos encontremos ante intentos de fraude usando voz (vishing) o video falsificados, las posibilidades de protección se reducen mucho en las organizaciones. Quizá, considerando la voz o el video como un primer factor de autenticación, sería conveniente que, en determinadas relaciones interpersonales por medios electrónicos, **se establecieran como segundo factor de autenticación palabras clave**, para validar que, efectivamente, se está hablando con la persona real y no con una IA operada por ciberdelincuentes. Esto requiere, obviamente, de un nivel de concienciación sobre los peligros de estos sistemas de inteligencia artificial y de su posible uso malicioso que están muy por encima de los habituales en la inmensísima mayoría de las organizaciones, pero que van a acabar siendo necesarias.

En todos los casos comentados en este artículo, si el resultado de la pesquisa de comprobación demuestra que se trata de algún tipo de intento de fraude, lo recomendable es recopilar toda la información posible y denunciar ante las autoridades el suceso, manteniendo un silencio en las comunicaciones con los ciberdelincuentes hasta que la Policía nos indique qué hacer.

Seguiremos sobre este tema en el número de marzo de TYSC.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Service Management FitSM + ISO 20000

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación FitSM Executive
- Certificación ISO 20000 Leader
- Módulo 5 MasterGEIT®
- Módulo 5 MasterPPM®

Del 17 al 25 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Inteligencia Artificial en actividades maliciosas (y III)

En los dos números anteriores de Tecnología y Sentido Común se introdujo una visión general de las amenazas que plantea el uso de la inteligencia artificial para actividades maliciosas, y su aplicación a un tipo concreto de actividad: el fraude al CEO. Este mes, vamos centraremos la atención en cómo diferente sistemas de inteligencia artificial pueden ayudar a que un atacante logre comprometer sistemas de forma más o menos automatizada, para cerrar esta serie de artículos.

Desde hace tiempo se ha dicho que la informática era 'para vagos', y aunque se puede estar en desacuerdo con según qué interpretaciones de esa expresión, no deja de tener cierta razón. Relacionamos con frecuencia ciertos avances tecnológicos con realizar 'menos esfuerzo' o en hacer tareas 'más rápidamente'. Desde la época de la Revolución Industrial, la puesta en funcionamiento de máquinas se ha asociado a que ciertos trabajos se realizaban con menor esfuerzo o con menos personal, lo que ha derivado frecuentemente en una fuerte oposición a casi todos estos avances tecnológicos, cuyo primera manifestación fue el ludismo a principios del siglo XIX.

Sin embargo, en pocos de los avances tecnológicos que la Humanidad ha venido logrando se ha hablado tanto sobre la capacidad de dichos avances de poder acabar incluso con esa Humanidad que los ha creado como con la Inteligencia Artificial, Tal vez a la altura de la bomba atómica, el cambio climático o la microbiología. ¿Y a qué se debe el revuelo, posiblemente justificado? Pues a que en la actualidad la IA ha conseguido alcanzar unos niveles de rendimiento y utilidad inesperados para algunos, gracias a la enorme cantidad de información disponible en Internet, y por supuesto, a los esfuerzos investigadores en la materia que se vienen realizando desde hace bastantes años.

Pero me van a permitir una licencia argumental sobre la IA para continuar con el fondo de este artículo: desde algunos puntos de vista, la IA no es más que un nivel superior de automatización, aunque es obvio que con un nivel de calidad en sus resultados que se parece mucho a la creatividad humana. Y como tal automatización, lo que permite es que sus usuarios puedan, de forma simple y cómoda, obtener ciertos resultados que les son muy útiles y que les habrían costado cierto esfuerzo obtener. Por ejemplo, redactar un resumen de una novela de 300 páginas en minutos, crear una imagen realista sin necesidad de modelos, decorados o fotógrafos, o encontrar y explotar las vulnerabilidades de un sistema de información, que es el asunto que nos ocupa este mes.

Imagine el lector que una organización de ciberdelicuentes disponga de un sistema de Inteligencia Artificial capaz de sondear un sistema de información de cualquier organización, identificar sus componentes tecnológicos, localizar las posibles vulnerabilidades de dichos

CONTINÚA EN PRÓXIMA PÁGINA

componentes, tratar de explotarlas, e introducir un malware en el sistema si los pasos anteriores tienen éxito.
Súmele a estas funcionalidades la capacidad de deducir quienes son los empleados de la organización y sus perfiles en redes sociales, la capacidad de chatear de forma realista con ellos y de crear cebos de ingeniería social, como los que comentamos en el artículo del mes pasado. Y todo ello, mientras los ciberdelincuentes estás descansando o haciendo actividades de ocio, todo de forma desatendida.

La situación descrita requiere de un elevadísimo nivel de automatización de procesos, pero también de la capacidad de aprendizaje del sistema, de ahí la conveniencia de usar sistemas ad hoc de IA para estos fines. Y lamentablemente, la situación descrita, hoy por hoy, ya no es ciencia ficción, de acuerdo a algunas fuentes expertas en el mercado de la ciberseguridad. En convenciones de hacking se muestran ejemplos de expertos de sombrero blanco (los 'buenos') que se ganan la vida descubriendo vulnerabilidades y notificándolas a la empresa fabricante o usuaria.

Los más avezados ya han podido automatizar estos procesos, y simplemente los lanzan antes de irse a la cama, y si hay suerte, cuando se levantan por la mañana tienen alguna 'presa' en su morral virtual. Pero esas mismas técnicas las pueden utilizar los ciberdelincuentes, y ciertamente con muchos más recursos para implementar su propio sistema de IA y hacer las inversiones en equipos y comunicaciones necesarias. Porque no sólo de sistemas de IA comerciales vive el ciberdelincuente.

Un sistema de IA creado ad hoc por estos grupos de ciberdelicuentes puede ser entrenado para ir adaptando sus vectores de ataque a las respuestas que un humano pueda dar a sus interacciones por cualquier medio (email, mesajería instantánea, etc.), e incluso, a las que sistemas como cortafuegos o sistemas de detección y prevención de intrusiones pueda ir estableciendo en respuesta a la identificación de determinados ataques. Por esa razón los fabricantes de sistemas de seguridad también están incorporando mecanismos de IA para articular la defensa, en lo que bien podríamos llamar 'combate de las', en el que, mientras unas tratan de encontrar por donde comprometer el sistema, otras tratan de protegerlo sin la intervención de ningún operador humano. Cualquiera que haya visto el clásico film 'Juegos de Guerra' de 1983 puede imaginarse este enfrentamiento entre Inteligencias Artificiales como una especie de juego de ajedrez en el que quien puede perder es la organización cuya defensa se enfrenta a la IA de los ciberdelincuentes, por mucho que éstos puedan despilfarrar recursos en caso de fracaso.

Por otro lado, hay un problema adicional al hecho de que sea una IA quien intente violentar un sistema. Su capacidad de aprendizaje despedaza los sistemas actuales de atribución (casi siempre presunta) de la acción maliciosa, basados en táticas, técnicas y procedimientos (TTPs, o sea, los tipos preferidos de ataque) que determinados grupos de ciberdelincuentes llevan a cabo. Por tanto, puede decaer la utilidad (y el interés) de herramientas como la matriz de MITRE ATT&CK para los expertos en ciberseguridad, al menos, por lo que respecta a la posible atribución del ataque, lo que podría redundar en una mayor dificultad para ejercer su trabajo para los investigadores de este tipo de delitos.

Lamentablemente, estamos ante una carrera armamentística de IAs de la que sólo estamos viendo las primeras etapas, y en la que se van a invertir ingentes cantidades de dinero y energía, lo cual puede agravar, como ya advierten algunas voces, los problemas de sequía derivadas de la mala gestión del agua y del cambio climático. **Porque en este entorno VUCA, ni ningún problema viene solo, ni ninguna solución es simple**.

Postdata: este mes ha salido a la luz pública un caso de fraude al CEO en Hong Kong con el uso de deepfakes generados con inteligencia artificial, tema de mi artículo del mes de febrero, y que alcanza los 24 millones de euros.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Seguridad de la Información

CSX + ISO 27001

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación CSX Executive
- Certificación ISO 27001 Leader
- Módulo 6: MasterGEIT®

MGEIT® eGob®

Del 7 al 15 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

La resiliencia personal, y la dicotomía entre el hoy y el mañana

Ante un evento potencialmente grave o catastrófico, se pone de manifiesto cuándo una organización, una sociedad, una familia o un individuo es capaz de responder adecuadamente y de sobrevivir a dicho evento, un concepto que podemos definir como "resiliencia". Sin ser una definición extraída del diccionario, todos comprendemos el concepto. En este artículo analizamos algunos aspectos que pueden ayudar en tener una mejor resiliencia personal, a la luz de recientes acontecimientos luctuosos que han sucedido en los últimos tiempos.

El pasado mes de febrero, un pavoroso incendio devoró en poco tiempo un edificio de más de 120 viviendas en la ciudad de Valencia (España), causando diez víctimas mortales y cuantiosísimos daños materiales. Una ola de solidaridad vecinal y de apoyo institucional se volcó en los afectados, en un ejemplo magnífico de lo que es una sociedad comprometida y empática con el sufrimiento ajeno. Pero este suceso, a quienes nos preocupa la seguridad (lo cual no sé si calificar de bendición o maldición) nos dio qué pensar.

Sin ánimo más que de ejemplificar, podemos pensar que en este tipo de edificios su diseñador o arquitecto pudo tener más en mente su aspecto que un muy improbable riesgo de incendio en fachada y su resistencia al fuego, algo entendible en un bien que se va a comercializar como de 'alto standing', y que ha de aparecer ante el posible cliente como atractivo y de calidad. Seguro que el edificio cumplía con la normativa vigente en el momento de su diseño, licencia y construcción. Sin embargo, se ha podido observar en este caso que, ante este tipo de eventos muy poco probables y con potenciales consecuencias catastróficas, conocidos en ciertos ámbitos como 'cisnes negros', se pone de manifiesto la necesidad de que cada uno de nosotros evaluemos nuestra resiliencia personal o familiar en caso de que un suceso así se nos presente en la vida.

Sin embargo, el ser humano, o la mayoría de los seres humanos actuales, estamos tan enfocados en el día a día que no nos da tiempo a pensar en nuestra resiliencia, que no es más que tener planificado qué hacer si suceden ciertos eventos. Y no me refiero solamente a cuestiones catastróficas, sino también otras de carácter financiero, profesional o personal, que con un poco de previsión puedan afectarnos menos o nos permitan adaptarnos mejor a dichos eventos. Pero esta sociedad actual se comporta así, y hay muchos ejemplos de ellos que deberían hacernos reflexionar.

Sin ir más lejos, en varios países una compañía ha estado los últimos meses escaneando el iris de personas que, voluntariamente, se han prestado a ello a cambio de un pago en criptomonedas. Lo han hecho pensando en el hoy, no en el mañana y en las consecuencias que ceder esa información personal pueda tener en su futuro.

CONTINÚA EN PRÓXIMA PÁGINA

Han optado por mercantilizar parte de su resiliencia, ajenos a las consecuencias futuras, y desconocedores de que lo que están prácticamente regalando puede ser muy valioso.

Afortunadamente, los organismos de protección de datos de varios lugares han tomado cartas en ele asunto y están investigando el tratamiento de datos de dicha compañía.

En el otro extremo se encuentran aquellas personas que planifican las actividades, evalúan riesgos, preparan su futuro y evitan en lo posible tomar decisiones poco meditadas o impulsivas. Recientemente, a raíz del luctuoso incendio de Valencia, pude participar en una conversación a través de redes sociales sobre algunas de las medidas de protección de la resiliencia personal y familiar que las personas que participábamos en la conversación teníamos. Y no me estoy refiriendo a los clásicos seguros de hogar, salud, decesos, etc. que puede suscribir si lo considera oportuno, sino a acciones o actitudes que demuestran un deseo de reducir el impacto de ciertos eventos en nuestra vida diaria, cada vez más digital, pero en la que hay activos del mundo físico que merece la pena valorar su protección.

Por ejemplo, documentos como escrituras, títulos universitarios, certificaciones, álbumes de fotografías en papel, etc. Algunos de ellos, en caso de destrucción serían irreemplazables, y por ello merecen ser tenidos en cuenta, por ejemplo, en caso de evacuación urgente de nuestra vivienda. Este tipo de situaciones de previsión tuvieron un momento álgido entre las empresas tras el incendio de la Windsor en Madrid, donde se perdió documentación y otro tipo de activos de multitud de organizaciones. Sin embargo, a nivel personal estas eventualidades es raro que conciencien sobre las posibilidades de reducir el impacto de los desastres en nuestras vidas o en las de nuestros seres queridos.
En una circunstancia como un incendio en un edificio de viviendas sería muy complicado pararse a recoger todos esos elementos antes de evacuar ordenadamente, salvo que se tuvieran ya agrupados y todos los miembros del domicilio tuviesen claro qué tenían que coger. Pero hay otras situaciones, sobre todo en áreas cercanas a bosques, urbanizaciones, etc., en la que puede ocurrir que se ordene evacuar de forma preventiva si, por ejemplo, se está en zona de peligro de un incendio forestal, en la que hay algo más de tiempo para realizar una evacuación ordenada. Y es en esa circunstancia cuando haber pensado un poco y haber actuado en consecuencia puede mejorar mucho nuestra resiliencia.
Trabajar hoy para el mañana, dirían nuestros abuelos.

Pongamos algunos ejemplos:

•Las fotos en formato papel se pueden escanear en buena calidad y subirse a la nube, o en su defecto, almacenarlas en un sistema de copia de seguridad. No hace falta tirarlas una vez escaneadas, pero si se pierden en algún desastre no se perderá el recuerdo que nos evocan al mirarlas (cada vez menos, todo sea dicho).

•Los documentos irreemplazables se pueden colocar en una caja, idealmente ignífuga, aunque si lo que se rata es de poder moverla lo suyo es usar una caja grande de plástico o cartón, donde se puedan guardar esos documentos y se pueda coger rápidamente y cargar en el vehículo de evacuación. Tener en su interior un inventario de los documentos que almacena tampoco estaría de más. Y si, además, por si acaso, hemos podido escanear los documentos, si finalmente se destruyeran podríamos imprimir copias de validez limitada o nula, pero que podrían facilitar el proceso de solicitar a las entidades emisoras copias totalmente válidas.

•Las joyas, recuerdos familiares o el dinero en efectivo es más fácil que ya se encuentren a buen recaudo, pero hay que pensar también en lo que se tardaría en sacarlos de una caja fuerte, en caso de que allí estuviesen, y cómo transportarlos, si son elementos frágiles u obras de arte.

•Los equipos informáticos y de copias de seguridad deberán estar entre los elementos a salvar en primer lugar, junto a los documentos, ya que en ellos solemos tener información irreemplazable, de la que en muchas ocasiones no hay copia de seguridad ni en local ni en la nube. Raros somos quienes lo hacemos, pese a las recomendaciones y advertencias….

En fin, en este artículo he tratado de despertar en el lector la idea de que es necesario pensar en qué elementos de los que nos rodean nos son imprescindibles, si son o no reemplazables, y en caso de que no lo sean, cómo podemos mejorar nuestra resiliencia protegiéndolos mejor, o al menos, siendo más conscientes de nuestra dependencia de ellos.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Continuidad de Negocio

BCI + ISO 22301

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BCI Executive
- Certificación ISO 22301 Leader
- Módulo 7: MasterGEIT®

MGEIT® eGob®

Del 5 al 13 de julio

+ 34 96 109 44 44
campus@escueladegobierno.es

¿Vulnerabilidad o funcionalidad? Los fallos en el hardware

Estamos acostumbrados, en el ámbito de la ciberseguridad, a hablar de vulnerabilidades, centrándonos sobre todo en las que proceden del software que nuestros dispositivos electrónicos ejecutan. Sin embargo, existen vulnerabilidades en los sistemas que proceden de otras fuentes, entre otras, el propio hardware del equipo. Y el mayor riesgo se produce cuando esa vulnerabilidad ha sido implementada de forma consciente, como puerta trasera al sistema. ¿Vulnerabilidad o funcionalidad? Depende de quien la mire.

En el ya lejano 2011 me hallaba cursando mis estudios de Master en Ingeniería de Computadores cuando, en una asignatura, el docente apuntó una línea argumental acerca de las funcionalidades no documentadas en determinados microprocesadores, que podrían constituir una forma de acceder, manipular o incluso sabotear el dispositivo. Este comentario dio pie a una interesante conversación grupal en la que pudimos exponer nuestras opiniones sobre quienes tenían capacidad de realizar esas modificaciones en los diseños de los chips, y obviamente en ese momento surgían las agencias de inteligencia de las superpotencias como las candidatas perfectas para ello. Sin embargo, estoy seguro que esa discusión hoy en día pondría sobre la mesa la posibilidad de que organizaciones de ciberdelicuentes pudiesen estar detrás de esas manipulaciones.

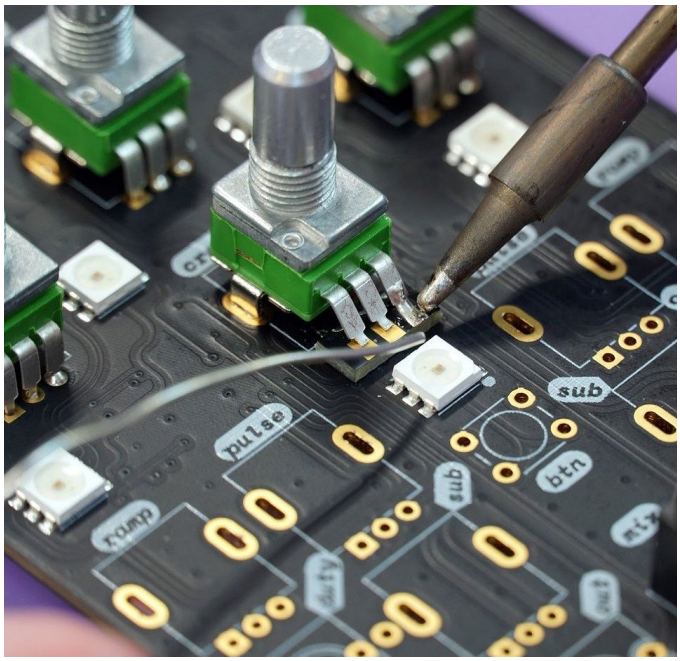
Téngase en cuenta que, tras el diseño de un microprocesador y su construcción, lo que se chequea es que las funcionalidades documentadas se realicen correctamente, pero no se comprueba que no haya otras funcionalidades no documentadas, precisamente porque se parte de la base de que el diseño sólo busca cumplir con los requisitos del cliente. Pero ¿quién nos garantiza de que el equipo de diseñadores no pertenece a alguna de esas organizaciones interesadas en disponer de esas funcionalidades ocultas? Lo que a nosotros nos parece una vulnerabilidad peligrosa, para un agente externo se considera una funcionalidad valiosa.

Pensemos en funcionalidades que puedan ir desde “leer toda la información que pasa por el procesador” hasta “destruir el chip”. Porque estoy seguro que el lector no creerá que entre esas funcionalidades ocultas estén el hacer cálculos más rápido o un modo para consumir menos electricidad para funcionar. Todas esas funcionalidades ocultas, a las que podemos llamar también “puertas traseras hardware”, irán siempre en detrimento de la privacidad y seguridad del usuario final del computador sobre el que se monten los chips “infectados de serie”.

Lo que les estoy contando no es ciencia ficción o una paranoia más. Hace alrededor de dos años, el fabricante de servidores Supermicro investigó una posible modificación no documentada de las placas base de sus equipos en una fábrica china. El asunto se cerró sin mucha más información al respecto, salvo un comunicado de la marca indicando que sus placas eran seguras y no contenían ningún elemento que no debiera estar ahí. Personalmente, me sonó a la famosa frase de Obi Wan Kenobi, e Star Wars Episode I, “Éstos no son los androides que estáis buscando”, acompañada de un movimiento de la mano y dirigida a los stromtroopers imperiales de Mos Eisley.

Mucho más recientemente, en este 2024, ha surgido la noticia de que el gobierno chino ha prohibido el uso de microprocesadores Intel y AMD, de diseño norteamericano, en todos los equipos gubernamentales, obligando a su sustitución por alternativas chinas. Este movimiento puede verse como una fase más de la guerra comercial existente entre ambos países en el ámbito de los semiconductores, pero encierra también dudas de ciberseguridad, fundadas o infundadas, por parte del gobierno del gigante asiático, de que esos chips pudieran usarse en contra de sus intereses, en concepto amplio. Algo, por cierto, que algunos gobiernos occidentales ya apuntaron en el caso del fabricante chino Huawei, vetado en varios ámbitos tecnológicos en dichos países por sus vínculos con el gobierno chino y las dudas sobre su comportamiento.

CONTINÚA EN PRÓXIMA PÁGINA



Ya no sólo hemos de preocuparnos por las vulnerabilidades que el software aloja, que pueden ser parcheadas cuando se identifican, mediante las correspondientes actualizaciones. Ya no podemos siquiera confiar en que fabricantes privados de semiconductores no estén incluyendo puertas traseras en los mismos siguiendo las "indicaciones" de agencias gubernamentales de inteligencia o mafias de ciberdelincuentes. Vulnerabilidades hardware que no son parcheables, por cierto, salvo sustituyendo el hardware defectuoso.

Pero ¿es factible que alguien pueda garantizar que estas puertas traseras no han existido siempre? Es fácil entender que el número de combinaciones posibles de estimulo de los pines de los chips pueden ser llegar a ser inmensa, y chequear qué hace cada una de ellas, excluyendo además las documentadas "legítimas", puede ser muy costoso. ¿Podría una entidad europea dedicarse a ello y certificar que están libres de ese tipo de puertas traseras? Es muy dudoso que eso sea factible, pero además, nos encontraríamos entonces con que esa entidad sería objetivo número uno de esos agentes maliciosos que han dedicado tanto esfuerzo a insertarlas en el dispositivo, por lo que tratarían de infiltrar personal a sus órdenes, manipular los procesadores de muestra para que no funcionen igual en según qué entorno de test, etc.

Por tanto, nos encontramos ante una situación en la que, como consumidores, estamos totalmente indefensos, ya que salvo que alguien detecte, corrobore y haga públicos los resultados de un estudio de ese tipo sobre un determinado producto, no tendremos ni conciencia del problema, ni podremos pedir las correspondientes indemnizaciones.

Como ciudadanos, además, también nos vemos perjudicados cuando, usando esas puertas traseras, se puedan dar casos de espionaje industrial a nuestras empresas nacionales, sabotajes a infraestructuras críticas, o robo de información a nuestras administraciones públicas. Imaginen las consecuencias que tendría que, en caso de guerra híbrida, un agente extranjero dispusiera de un *killswitch* que dejara inoperativos los computadores de ciertos sistemas militares.

De ahí la importancia, a mi juicio, que debe tener una cierta soberanía europea sobre el diseño y fabricación de semiconductores, aspecto que cuenta con líneas de inversión en los planes de resiliencia y recuperación posteriores a la pandemia por el COVID-19. Tampoco estaría de más que se instituyera una agencia europea que revisara cualquier hardware que quisiera venderse en Europa, y le hiciera todo tipo de tests, pero eso es ciertamente una utopía.

Quizá si el mercado europeo de fabricación de semiconductores pudiese llegar a un punto en el que los ciudadanos europeos optásemos sólo por tecnologías europeas, se podría estar más confiado.

Pero asegurar que esas medidas preventivas y de vigilancia fueran suficientes o si tendrían éxito es harina de otro costal. De alguna manera habrá que andar ese camino, y cualquier camino comienza con un primer paso. ¿Cuál será?

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Gobierno de I&T

COBIT + ISO 38500

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COBIT Executive
- Certificación ISO 38500 Leader
- Módulo 8: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Humanos biónicos. ¿Llegó la hora?

Las ciencias de la computación llevan muchos años avanzando. La robótica da pasos lentos, pero seguros. Y la inteligencia artificial ha sido el *trending topic* del último año y medio. Junto con los implantes corporales y las redes de área corporal, ¿toda esta tecnología abre la puerta a un nuevo escalón en la evolución de nuestra especie, los humanos biónicos? ¿Cuáles son los riesgos que asumiremos en esa faceta de la evolución? Hagamos suposiciones.

En los años 70 del siglo pasado, la serie de televisión "El hombre de los seis millones de dólares" presentaba a un personaje al que, tras un accidente en el que sufre varios daños importantes, se le implantan diferentes elementos biónicos, que le conferían mayor fuerza, velocidad y visión que a un ser humano completamente biológico. También la película de los años 80 "Robocop" imaginaba un futuro en el que se podía potenciar la acción policial a través del uso de agentes del orden con miembros y órganos robóticos implantados en su cuerpo, y cuyo programa piloto se llevaba a cabo en un policía moribundo. Ambos relatos se basan, por supuesto, en el concepto de cyborg, u organismo cibernético, híbrido de ser vivo y robot, del que su exponente más terrorífico fue el personaje de Arnold Schwarzenneger en la saga "Terminator", donde interpretaba a un cyborrg asesino venido del futuro.

Analizando las tecnologías necesarias para que se pueda construir un cyborg, muy resumidamente podemos decir que hacen falta los siguientes elementos:

1.Potencia computacional muy elevada, con alta miniaturización y optimización de consumos eléctrico y disipación de calor.

2.Redes de comunicaciones compatibles con la fisiología humana, para aprovechar las estructuras del propio cuerpo para la transmisión de datos.

3.Implantes biocompatibles, que no provoquen rechazo en los tejidos vivos ni se vean degradados por la acción de los fluídos y microorganismos del cuerpo.

4.Un interfaz hombre-máquina que permita al cerebro humano el acceso y control de las redes y los implantes, o que permita a un computador, a modo de cerebro, controlar los órganos y miembros del cuerpo.

5.Un sistema de inteligencia artificial que permita al cyborg interactuar con el entorno de manera similar a como lo haría un ser vivo.

6.Un sistema de alimentación que produzca el combustible necesario para proporcionar energía tanto a la parte biológica como a la parte artificial del cyborg.

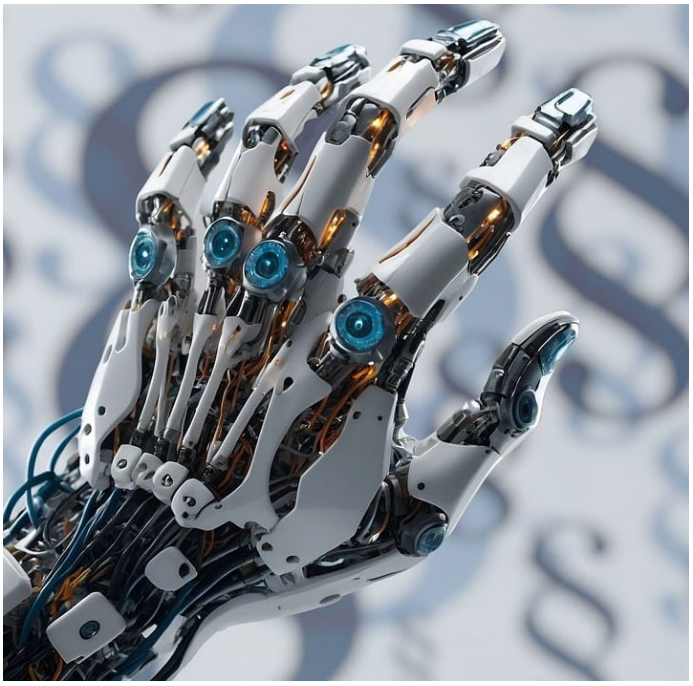
7.Sistemas robóticos de reducido tamaño, bajo consumo y alta durabilidad, que puedan formar miembros funcionales tales como brazos, piernas o exoesqueletos.

Atendiendo a cómo está el desarrollo tecnológico en la actualidad, podemos concluir que, de los seis elementos básicos indicados, en mayor o menor medida, todos ellos están en explotación o en alguna fase de investigación y desarrollo. Por tanto, ¿qué (o cuánto) falta para que podamos ver en la calle personas biónicas o cyborgs?

Es indiscutible que el punto 1 del esquema anterior está más que logrado y se dispone de tecnología más que suficiente. La tecnología de microprocesadores digitales está muy desarrollada, y aunque la computación puede seguir otros derroteros como la fotónica o la cuántica, la tecnología digital actual bastaría para equipar un cyborg.

Sobre el punto 2, los avances en redes de baja energía y protocolos de comunicaciones de largo alcance llevan unos 15 años investigándose. Yo mismo, que no sioy experto en la materia, realicé un trabajo académico de investigación sobre el panorama existente en el ámbito de las redes de área corporal (Body Area Networks) en 2.011. Por tanto, es muy probable que en la actualidad ya se cuente con tecnología apropiada, o al menos, con el germen de la misma, para que las comunicaciones entre el cerebro y los implantes biónicos de un cyborg pudieran funcionar a la velocidad y ancho de banda requeridos.

CONTINÚA EN PRÓXIMA PÁGINA



Sobre el punto 3, ya hace años que se realizan implantes biocompatibles, tales como marcapasos, implantes dentales, implantes cocleares, etc., por lo que esa tecnología ya está disponible, aunque quizá la escala de los implantes actuales no tiene nada que ver con el tamaño de un brazo o pierna biónico.

Por lo que respecta al punto 4, hay avances recientes en sistemas de conexión del cerebro humano con dispositivos externos, tales como los implantes Neuralink, que impulsa una de las empresas del hipermillonario Elon Musk. Esta tecnología esta concebida para que la persona a la que se le instala el implante pueda controlar dispositivos externos solamente con pensarlo, como si de telepatía se tratase.

Pero si este tipo de tecnología evoluciona lo suficiente, podría controlar miembros biónicos si se consigue salvar la cuestión relativa a la forma en la que el cerebro humano maneja ciertas funciones vitales de forma inconsciente, tales como respirar o hacer latir del corazón, a través del sistema nervioso autónomo. O si consigue cosas como pedirle a las piernas que corran o salten sin tener que pensar qué músculos lo permiten y pedirles que se contraigan o extiendan para lograrlo. Por tanto, en este aspecto aún hay un importante margen de mejora.

Sobre el punto 5, no hay duda de que en los últimos cinco años se han producido enormes avances en sistemas de Inteligencia Artificial, y que si el test de Turing no ha sido aún superado por una de ellas, muy pronto se logrará. Pese a ello, a la IA aún le quedan unos años para que su funcionamiento se asemeje al funcionamiento del cerebro humano y pueda controlar los sistemas de un cyborg cuando hay problemas en el cerebro biológico.

Al respecto del punto 6, hay que tener en cuenta que un cyborg tendrá que alimentar tanto a su parte biológica, mediante vasos sanguíneos que transporten nutrientes y oxígeno a las células, y a su parte robótica, alimentandola con electricidad. Por tanto, se tendrán que desarrollar métodos de producción y almacenamiento eléctrico optimizados a partir de la generación de energía biológica o a través de sistemas de carga. En este aspecto, es probablemente donde la biotecnología tenga más trecho que recorrer.

Finalmente, y aunque la robótica avanza también a una velocidad importante, con empresas como Boston Dynamics o las empresas rusas de robots-soldado, los requisitos para que sistemas robóticos puedan convivir con tejido vivo aún no son una realidad, y tampoco parece que sean una prioridad, ya que la orientación del mercado robótico actual se centra en el apoyo a tareas humanas repetitivas o pesadas, como los robots de las fábricas de automóviles, por ejemplo) o al desarrollo de androides que puedan ayudar en sus domicilios a personas con discapacidad.

Pero imaginemos un mundo en el que todo esto ya es posible y se consigue el logro de ¿fabricar? un ser humano biónico. Dejando de lado cuestiones éticas, y viendo cómo es nuestro mundo digital actual, ¿Ud. se arriesgaría a recibir órganos biónicos? ¿Se habrá tenido en cuenta la ciberseguridad en el desarrollo de todos los elementos tecnológicos a los que me he referido anteriormente? ¿Qué consecuencias tendría un ataque a todos los miembros biónicos de un determinado fabricante?

Allá donde implantemos tecnología, ésta ha de ser desarrollada con la seguridad en mente, o el desastre, más tarde o más temprano, está asegurado. ¿Es Ud. Sarah Connor?

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno Corporativo COSO + ISO 37000

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COSO Executive
- Certificación ISO 37000 Executive
- Módulo 10: MasterGEIT®
- Módulo 1:0 MasterPPM®

MPPM® MGEIT® eGob®

Del 22 al 30 de noviembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Brechas de datos: el Titanic de nuestra Seguridad y Privacidad

La segunda mitad del mes de mayo de 2024 ha sido desastrosa por lo que a las brechas de datos de personas españolas se refiere. Grandes corporaciones del IBEX 35, alguna que otra multinacional, e incluso agencias gubernamentales han reportado incidentes de este tipo, en los que datos identificativos más o menos sensibles de clientes y ciudadanos se han visto filtrados masivamente. ¿Qué hacemos ahora?

Quizá se deba a cuestiones geopolíticas, debido a la postura del Estado español frente a la invasión rusa de Ucrania, o el genocidio en Gaza. Quizá sea una simple coincidencia y varios grupos de ciberdelincuentes han materializado filtraciones casi simultáneamente, tal vez en una especie de 'pique' a ver quienes son más audaces o efectistas. Pero lo que es una realidad es que en la segunda quincena del mes de mayo diferentes organizaciones han sufrido brechas de seguridad que han supuesto la filtración de datos de, supuestamente, millones de españoles.

Empresas como Ayesa, Iberdrola, Santander o Telefónica han denunciado haber sido violentadas, o que datos de sus clientes han sido robados, generalmente, a través de otras empresas que les prestan servicios. Hablamos de filtraciones de casi un millón de personas, al parecer, la mayor de ellas, aunque el hecho de que algunas de estas empresas sean multinacionales implica que también pueden haberse filtrado datos de empresas y ciudadanos de otros países, sin estar del todo calro el alacnce de los datos sustraídos. También Ticketmaster ha denunciado el robo de datos de más de 500 millones de clientes a nivel global, y en este caso, se sabe que entre la información sustraída se encuentran datos de tarjetas de crédito. Y Decathlon también ha sufrido un ataque de este tipo en el que ya se puede considerar un mayo negro en lo que a la ciberseguridad y privacidad se refiere.

Siendo muy graves estas filtraciones, el mes terminó con la denuncia de la Dirección General de Tráfico, que investiga la Guardia Civil, de que en la Dark Web se venden los datos de 34 millones de conductores españoles y de sus vehículos, supuestamente robados a la DGT. Y no sólo se vende la base de datos completa, sino que también se venden consultas puntuales a la misma.

Como ya he explicado en artículos previos, el gran problema de estas filtraciones no es, en si mismo, el robo de los datos, sino todo lo que los delincuentes pueden hacer con ellos. Teniendo acceso a todas esas fuentes de datos, y con un trabajo de minería de datos, o alimentando una inteligencia artificial, las bandas de ciberdelincuentes pueden armar potentes campañas de suplantación de identidad o de phishing extremadamente perfeccionadas, y por tanto, con una alta probabilidad de éxito. El elevado volumen de datos sustraidos parece apuntar a que uno de los objetivos es precisamente, entrenar con ellos a inteligencias artificiales desarrolladas por esos grupo de ciberdelincuentes.

CONTINÚA EN PRÓXIMA PÁGINA

Sin ánimo de ser alarmista, con los datos filtrados en casi cualquiera de esas filtraciones de mayo, y con un poco de investigación en redes sociales, se puede fabricar un DNI español falso sin demasiados problemas. Y con ese DNI se pueden cometer muchos tipos de fraudes, sólo hace falta un poco de imaginación, sobre todo, si se combina con datos de tarjetas de crédito.

Bien es cierto que en filtraciones anteriores ya había muchos datos nuestros circulando por lugares nada recomendables, pero éstas últimas vienen a demostrar que nadie está a salvo de un ataque informático dirigido por parte de un grupo criminal adecuadamente motivado, y que el mercado de los datos robados está siempre hambriento de nuevas capturas con las que alimentar sus actividades ilegales.

Los expertos en la materia auguran una oleada de correos, SMS o llamadas fraudulentas, tratando de hacer 'picar' a las personas cuyos datos han sido recientemente filtrados, ya que la probabilidad de que esos datos sean de calidad es alta. En este asunto, los ciudadanos estamos a bordo de nuestro propio Titanic, y va a ser trabajoso esquivar al iceberg (o a legiones de icebergs) que van a ponerse en nuestro camino a partir de ahora debido a estas filtraciones.

Lo más importante es qué podemos hacer al respecto. Por supuesto, no podemos hacer desaparecer esa información del mercado negro, eso está descartado. Como ciudadanos de a pie, sólo podemos estar mucho más alerta aún, y no hacer caso a mensajes de correo electrónico que aleguen ser de compañías de las que somos clientes y en las que se alegue cualquier motivo para que rellenemos algún tipo de formulario con datos, claves, etc. Sobre todo, si se aduce algún tipo de urgencia en ello. Es decir, debemos ser mucho más vigilantes ante correos de phishing, que ahora serán mucho mejores que los que hemos venido viendo en el pasado, o mensajes en Whatsapp o Telegram o SMS con enlaces, o incluso llamadas telefónicas sospechosas.

Desde el punto de vista de los Estados democráticos, en este caso, el español, se desconoce si tienen algún tipo de plan o estrategia, no sólo para mejorar la protección de los sistemas de información, más allá del Esquema Nacional de Seguridad o la Directiva Europea NIS2. Me estoy refiriendo a que, quizá, ha llegado el momento de que no sólo nos defendamos, y que comencemos a atacar, no sólo a los grupos de ciberdelicuentes 'normales', sino también a los grupos auspiciados por gobiernos de países que están demostrando sernos hostiles. Y quizá ha llegado también el momento en que lo que ha sido una especie de ciberguerra más o menos encubierta en estos pasados años se convierta en un conjunto de acciones coordinadas con decisiones a nivel comercial y/o diplomático. Quizá ha llegado el momento de desconectar a ciertos países de Internet, y que sus empresas no puedan comerciar con las de los países que sí respetan las reglas internacionales de respeto a la legalidad y soberanía de los demás. Y por supuesto, debemos potenciar las unidades policiales que tratan con la ciberdelincuencia, de manera que, en coordinación con otros países de nuestro entorno, puedan actuar con rapidez y contundencia, incluso, a través del ataque a las infraestructuras que usen los grupos de ciberdelicuentes para sus actividades.

Por otro lado, también es urgente que nosotros, los ciudadanos, tomemos conciencia de qué es lo que está en juego cuando nuestros datos se filtran o son usados para entrenar una inteligencia artificial, y tomemos medida. Debemos responsabilizarnos más de lo que publicamos en redes sociales, publicando sólo lo imprescindible, o incluso, no publicando nada. Debemos responsabilizarnos de saber manejar enlaces recibidos por cualquier medio, y verificarlos antes de clicar en ellos. Debemos tomar conciencia como empleados de que manejamos datos de otras personas, y que de nuestra falta de profesionalidad o precauciones pueden verse negativamente afectados.

Debemos, en resumen, tomar el timón de nuestro Titanic personal y poner atención en la singladura del mundo digital. Y quien no quiera hacerlo, se hundirá en cuanto colisione con los icebergs.

Para terminar este último artículo de la temporada, me permito desearle al lector unas felices y merecidas vacaciones, y esperando que continúen siguiéndonos en la 10ª temporada de Tecnología y Sentido Común.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión de Beneficios y Gestión de Portafolios

P4MGO!® BfM Leader
P4MGO!® PfM Leader

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Metodología P4MGO!®
- Exámenes de Certificación Incluidos
- Certificación P4MGO!® BfM Leader
- Certificación P4MGO!® PfM Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Octubre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

P4MGO!

NUEVOS MASTERS

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es