BOLETÍN DE VIGILANCIA TECNOLÓGICA

DPI Nº4 T1 2023

DIGITALIZACIÓN DE LA PRODUCCIÓN INDUSTRIAL

El Boletín de Vigilancia Tecnológica sobre Digitalización de la Producción Industrial es una publicación trimestral de la Escuela de Organización Industrial desarrollada en colaboración con CTIC Centro Tecnológico. Este Boletín pretende ofrecer una visión general de las tecnologías emergentes y los avances más relevantes en materia de digitalización de la producción industrial.

Esta publicación forma parte de una colección de Boletines temáticos de Vigilancia Tecnológica, a través de los cuales se busca acercar a la pyme información especializada y actualizada sobre sectores industriales estratégicos. Los Boletines seleccionan, analizan y difunden información obtenida de fuentes nacionales e internacionales, con objeto de dar a conocer los principales aspectos del estado del arte de la materia en cuestión, así como otras informaciones relevantes de la actualidad en cada uno de los campos objeto de Vigilancia Tecnológica.

Índice

— 01

Estado del Arte

Estado del arte acerca de las tendencias y novedades en el campo de la digitalización de la producción industrial.

Ciberseguridad en la Industria 4.0: Retos y recomendaciones

La Industria 4.0 trae aparejada la creación de fábricas inteligentes que ayudarán considerablemente a la industria manufacturera, ya que la tecnología digital puede ofrecer una mayor eficiencia en la fase de producción, productos de mejor calidad con menos errores y más flexibilidad para los procesos de trabajo. Pero el uso de tecnologías conectadas, inteligentes y autónomas trae consigo nuevos riesgos cibernéticos para los que la industria no está preparada. De hecho, la industria manufacturera fue en 2022 la más atacada por los ciberataques de ransomware y la industria más extorsionada, según el último informe anual de riesgos de ciberseguridad de IBM. Esto es debido al papel fundamental que desempeña la industria manufacturera en las cadenas de suministro mundiales. Las empresas del sector son objetivos populares porque son vulnerables al fallo de los sistemas, lo que crea inmediatamente problemas en la cadena de producción y suministro, ya que no se pueden permitir parar la producción durante mucho tiempo, todo ello incrementado con su dependencia de la conectividad.

En este sentido, según el último informe de Capgemini específico sobre la ciberseguridad en las fábricas inteligentes, el 80% de las organizaciones está de acuerdo en que la ciberseguridad es un componente crítico de las operaciones de una fábrica inteligente y el 79% de las organizaciones considera que el nivel de ciberamenazas es mayor en una fábrica inteligente que en una fábrica tradicional no conectada. No obstante, aunque el 51% de las organizaciones reconoce que es probable que el número de ciberataques aumente en los próximos 12 meses, los niveles actuales de preparación son bajos.

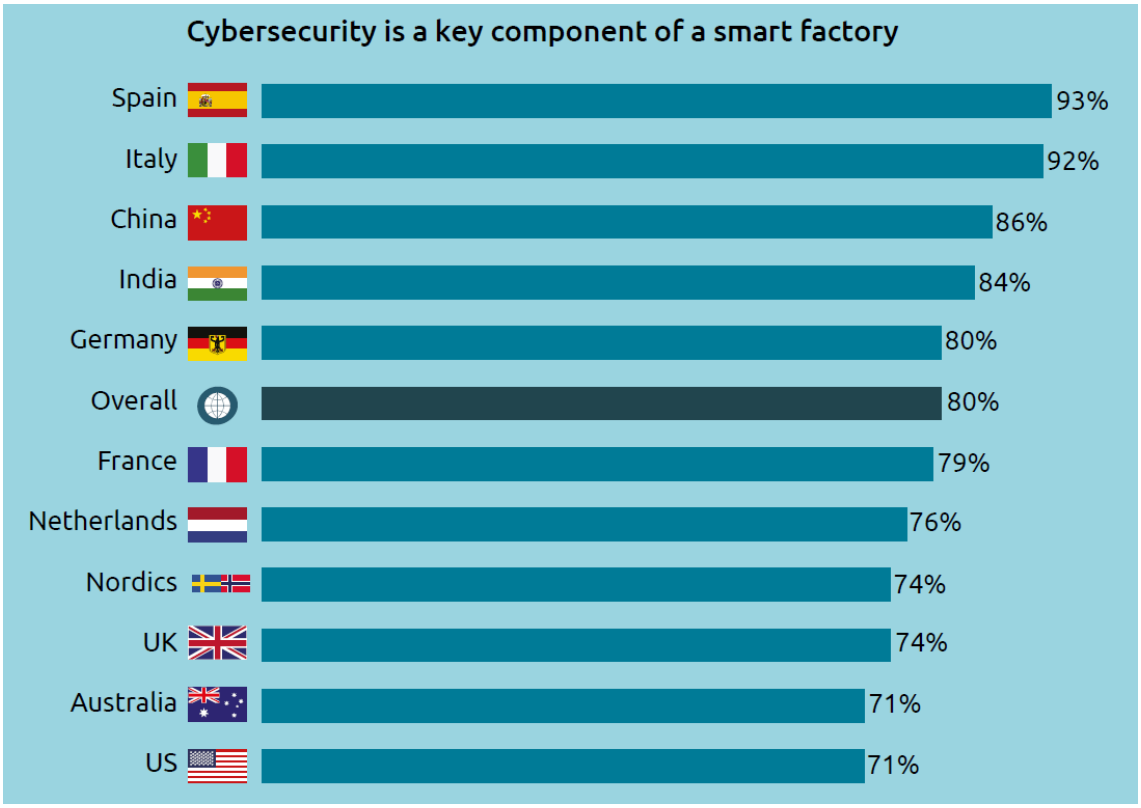

Figura 1: La ciberseguridad es un factor clave para las fábricas inteligentes. Fuente: Built to defend. Smart & secure: why smart factories need to prioritize cybersecurity, Capgemini Research Institute, 2022.

Principales retos de la ciberseguridad en entornos industriales

Dada la especial relevancia de la seguridad en la Industria 4.0, ENISA (Agencia de la Unión Europea para la Ciberseguridad) ha publicado una guía donde detalla los principales retos y recomendaciones (Informe Industry 4.0 Cybersecurity: Challenges & Recommendations).

En dicha guía ENISA define 3 grandes bloques en los que se deben enmarcar las acciones: Personas, Procesos y Tecnologías, los cuales se detallan a continuación.

1. Retos y recomendaciones desde el punto de vista de las PERSONAS

RETO: Necesidad de fomentar y armonizar los conocimientos y la concienciación en materia de seguridad de las IT / OT

En la Industria 4.0 la convergencia entre IT (Information Technology, tecnologías de la información) y OT (Operational Technology, tecnología operacional) es fundamental para su buen funcionamiento. Sin embargo, tradicionalmente las personas que participan en la implantación de nuevas soluciones suelen tener sólo conocimientos de seguridad informática u operativa, mientras que la Industria 4.0 y la fabricación inteligente requieren conocimientos en varios ámbitos. Las personas necesitan adquirir nuevas competencias para supervisar, prevenir y detectar anomalías debidas a violaciones de la seguridad, así como formarse en aspectos de seguridad de los nuevos protocolos utilizados por las soluciones de la Industria 4.0.

RECOMENDACIÓN: Fomentar el conocimiento interfuncional en la seguridad IT / OT

Es de vital importancia concienciar sobre la seguridad básica del control industrial, así como sobre la forma segura de pasar a la Industria 4.0 y la fabricación inteligente. Para hacer frente a la falta de talento en seguridad de la IoT y la Industria 4.0, es esencial cultivar estos conocimientos tanto dentro como fuera de los límites de la organización. Las personas encargadas de la seguridad dentro de las organizaciones de la Industria 4.0 deberían invertir en formaciones de ciberseguridad de vanguardia que cubran todos los aspectos necesarios específicos de la convergencia de IT/OT y la fabricación inteligente.

RETO: Políticas organizativas incompletas y reticencia a financiar la seguridad

Hasta hace muy pocos años, la ciberseguridad no se solía percibir como un tema a tener en cuenta a nivel de dirección en una empresa, ya que su impacto en el aumento de los ingresos o la optimización de los costes aparentemente no es directo. De este modo, la capa directiva de las empresas se ha centrado en las transformaciones tecnológicas que permiten un aumento de la funcionalidad y el valor empresarial. Esto implica las empresas no suelen disponer de estructuras de gobernanza adecuadas para la implantación segura de nuevas tecnologías y el mantenimiento seguro de las existentes.

Rara vez existen programas de seguridad definidos y, en general, se carece de programas integrales que consideren la seguridad y la protección de forma conjunta. Debe empezar a tenerse en cuenta que la seguridad de un sistema, tanto en el contexto de los proveedores como de los operadores de la Industria 4.0, requiere financiación y compromiso por parte de la alta dirección.

RECOMENDACIÓN: Fomentar los incentivos económicos y administrativos para la seguridad de la Industria 4.0

Está claro que la falta de seguridad tiene el potencial de afectar significativamente a las organizaciones. De hecho, según el último informe de Deloitte ("Estado de la ciberseguridad en España"), en el último año se ha experimentado un más que notable aumento del número de ciberataques y sofisticación de las amenazas conocidas. En este sentido, casi el 69% de las empresas afirma que ha sufrido entre 1 y 2 ciberincidentes de gravedad durante este último año, e incluso el 25% afirma haber sufrido más de 2 ciberataques.

Como consecuencia, el coste de los ciberataques e a infraestructuras críticas puede llegar a tener un impacto en paradas no programadas de entre una y dos semanas, lo que puede suponer unas pérdidas entre los 200.000$ USD y los 800.000.000$ USD, según el whitepaper "El estado de la ciberseguridad industrial".

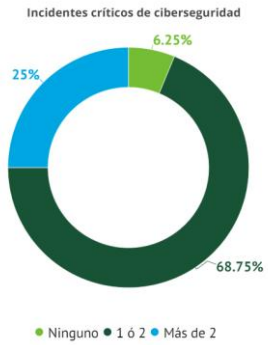

Figura 2: Incidentes críticos de ciberseguridad. Fuente: Estado de la ciberseguridad en España, Deloitte, 2022.

Por otro lado, debe empezar a considerarse la ciberseguridad no sólo como un coste, sino como una importante oportunidad de negocio: puede ser una importante ventaja competitiva para las empresas, ya que permite disponer de productos y servicios seguros, fiables y dignos de confianza. En consecuencia, la ciberseguridad es un factor que facilita las oportunidades de negocio, no un factor que las obstaculiza. Para llevarlo a cabo, son necesarios estímulos económicos y administrativos para incentivar las inversiones en seguridad de la Industria 4.0, dado que la madurez y mentalidad de las organizaciones y empresas debe crecer aún más a la hora de identificar el papel y la importancia de la seguridad.

2. Retos y recomendaciones desde el punto de vista de los PROCESOS

RETO: La responsabilidad sobre el ciclo de vida de los productos de la industria 4.0 está mal definida

La mayoría de los dispositivos del IIoT suelen construirse a partir de un gran número de componentes fabricados por múltiples proveedores, en ubicaciones dispersas administrativas y legales), a los que hay que añadir los vendedores del software integrado en los dispositivos. Esto genera una complejidad enorme en la cadena de suministro y en el ciclo de vida de los productos. Ante un problema de ciberseguridad, el reparto de responsabilidades en esta cadena tan compleja es, generalmente, una tarea pendiente.

RECOMENDACIÓN: Aclarar la responsabilidad entre los agentes de la Industria 4.0

Debe clarificarse la responsabilidad entre los actores de la Industria 4.0, abordando las cuestiones de responsabilidad en el contexto de la legislación y la jurisprudencia europeas y nacionales. Además, al realizar una contratación de un producto o suministro, debe prestarse atención a la definición de las cláusulas necesarias en el contrato para aclarar la responsabilidad entre las partes interesadas en las cadenas de suministro.

RETO: Fragmentación de las normas técnicas de seguridad de la Industria 4.0

La fragmentación de las normas e iniciativas de seguridad de la Industria 4.0 reviste especial importancia para el sector manufacturero. Las grandes empresas manufactureras suelen tener sedes repartidas por todo el mundo. En consecuencia, la falta de esfuerzos uniformes de normalización a nivel mundial da lugar a una situación en la que las sedes que pertenecen a una organización no pueden colaborar y compartir conocimientos y soluciones de seguridad entre sí, ya que están sujetas a esquemas diferentes.

RECOMENDACIÓN: Armonizar los esfuerzos sobre las normas de seguridad de la Industria 4.0

Para conseguirlo, se deberían lanzar actividades de normalización que aborden todo el espectro de la seguridad de la Industria 4.0, así como realizar análisis de las normas actuales de seguridad de la Industria 4.0 para examinar posibles lagunas, es decir, si las normas existentes abordan adecuadamente los requisitos de seguridad de la Industria 4.0.

3. Retos y recomendaciones desde el punto de vista de la TECNOLOGÍA

RETO: Interoperabilidad de los dispositivos, plataformas y frameworks de la Industria 4.0

Garantizar la interoperabilidad entre dispositivos o plataformas involucrados en la Industria 4.0 es fundamental para la seguridad ya que, en las complejas cadenas de suministro, el eslabón más débil de dicha cadena puede tener efectos perjudiciales en todo el sistema. Por lo tanto, es esencial abordar el problema de los protocolos propietarios que no siempre son seguros y adoptar marcos comunes para mejorar la funcionalidad y la seguridad de las soluciones de la Industria 4.0.

RECOMENDACIÓN: Establecer líneas de base de la Industria 4.0 para la interoperabilidad de la seguridad

Se debería fomentar el uso de *frameworks* de interoperabilidad que promuevan un lenguaje de seguridad común y el uso de protocolos para los componentes de la Industria 4.0. así como determinar niveles de seguridad específicos a lo largo de la cadena de suministro para cubrir las tres facetas de la ciberseguridad, es decir, las personas, los procesos y las tecnologías.

RETO: Limitaciones técnicas que obstaculizan la seguridad en la Industria 4.0 y la fabricación inteligente

Las dificultades para garantizar la seguridad en la Industria 4.0 se derivan también de la falta de capacidades técnicas de los dispositivos y sistemas industriales conectados, especialmente si se trata de dispositivos de gama baja. Dichos dispositivos suelen tener limitadas capacidades de procesamiento, que se dedican a realizar su funcionalidad, dejando fuera la implementación de aspectos de seguridad integrales en la fase de diseño.

Los dispositivos son, a su vez, vulnerables si sólo se implementan funcionalidades de seguridad a nivel de red ya que si un atacante irrumpe en la red, los dispositivos quedan desprotegidos frente a los ataques.

RECOMENDACIÓN: Aplicar medidas técnicas para garantizar la seguridad de la Industria 4.0

Es fundamental aplicar los principios de seguridad por diseño y privacidad por diseño para todos los dispositivos, servicios, protocolos, comunicaciones y procesos. Además, es necesario evaluar periódicamente la madurez de las soluciones de ciberseguridad implantadas, teniendo también en cuenta la información sobre ciberamenazas para supervisar el panorama de amenazas actuales y emergentes, así como estar informado del marco normativo en ciberseguridad.

Novedades en la legislación vigente

La importancia que la ciberseguridad ha ido adquiriendo en los últimos años se plasma en la aprobación en marzo de 2022 del Plan Nacional de Ciberseguridad, dotado con un presupuesto de más de 1.000 millones de euros.

Dentro de las medidas definidas en dicho Plan, destaca la creación de la plataforma nacional de notificación y seguimiento de ciberincidentes y de amenazas que permita intercambiar información, en tiempo real, entre organismos públicos y privados, así como la puesta en marcha del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos.

Por otra parte, como se indicaba previamente, es fundamental que todas las organizaciones cumplan la normativa en relación con la ciberseguridad. Cabe resaltar que durante el año 2022 ha habido importantes avances en la normativa nacional y europea, fundamentales para la ciberseguridad industrial:

- El 28 de abril de 2022 el pleno del Congreso de los Diputados convalidó la Ley de Ciberseguridad 5G que establece los requisitos de ciberseguridad específicos para el despliegue y la explotación de redes 5G.
- En diciembre de 2022, la Unión Europea aprobó la Directiva NIS 2 para sustituir a la directiva existente sobre la seguridad de las redes y sistemas de información. La directiva NIS 2 establece obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación, obligaciones relativas al intercambio de información sobre ciberseguridad, así como obligaciones de supervisión y ejecución para los Estados miembros.

El sector industrial debe, por tanto, adaptarse para cumplir esta normativa, sobre la que se debe plantear cómo enfrentarse a los retos en el ámbito de las personas, procesos y tecnología para poder garantizar un entorno industrial seguro.

— 02

Actualidad

Recopilación de las noticias más relevantes de la actualidad nacional e internacional en materia de digitalización de la producción industrial.

09/02//2023

Las compañías avanzan hacia el nuevo paradigma de ciberseguridad

El malware sigue siendo la principal amenaza tanto para las empresas como para particulares, según el último informe de Zscaler. En particular, los ataques de ransomware aumentaron un 80% el año pasado, y resultan especialmente preocupantes para las compañías por su capacidad de cifrar información y paralizar procesos. Ante este escenario, las organizaciones se esfuerzan para adaptarse y hacer frente a estos retos, como se puso de relieve en el encuentro Ciberseguridad: cambio de paradigma, organizado por EXPANSIÓN con el patrocinio de Zscaler.
Precisamente Zscaler es la creadora de la plataforma nativa de la nube Zero Trust Exchange, que aplica el principio de que no se debe confiar de forma inherente en ningún usuario o aplicación. Este concepto parte de la suposición de que todo puede ser hostil, de modo que sólo establece confianza y permite comunicarse con una aplicación una vez que ha verificado la identidad del usuario.

“El modelo plataforma va a ser muy importante en clave de presente y futuro porque permite simplificar la operación y reducir los costes" Raquel Hernández, directora regional de Zscaler en España y Portugal.

"Durante muchos años nos habíamos centrado en las medidas preventivas, pero esa mentalidad ha cambiado: ahora buscamos predecir y estar preparados ante lo que vaya a ocurrir", puntualizó Juan Cobo, director global de seguridad de la información (CISO) de Ferrovial.

Fuente: Expansión

11/01//2023

Schneider Electric y BitSight se alían para mejorar la ciberseguridad de la tecnología operativa

Schneider Electric, líder mundial en la transformación digital de la gestión de la energía y la automatización, y BitSight, líder en la detección y gestión de riesgos cibernéticos, han anunciado una asociación estratégica para desarrollar una capacidad global de identificación de riesgos e inteligencia de amenazas de tecnología operativa (OT) pionera en su clase.

En los últimos años, tanto los actores de ciberamenazas oportunistas como los de ciberamenazas más avanzadas se han mostrado cada vez más dispuestos a atacar instalaciones industriales y operativas. Schneider Electric y BitSight consideran que su asociación es un paso importante en su compromiso de mejorar la seguridad y la resistencia de sus comunidades, mediante la detección de protocolos OT expuestos a través de Internet y su contextualización con una mejor atribución.

El objetivo de esta colaboración es reforzar la seguridad industrial y proporcionar una mayor visibilidad de la infraestructura industrial y de los dispositivos del sistema de control industrial (ICS) que pueden estar en riesgo de una violación cibernética.

La participación está abierta a todos los proveedores de OT dispuestos a compartir información sobre sus productos para mejorar las capacidades de detección y atribución de riesgos.

Fuente: Factoría del Futuro

08/02/2023

Las empresas invertirán en ciberseguridad, cloud y desarrollo de aplicaciones

Según el "Informe de presupuestos IT 2022 y estimación 2023" llevado a cabo por LiceoTIC Training, las empresas españolas aumentarán la inversión en IT este año en más de un 7%.

Del mismo modo, se prevé que el gasto en este ámbito aumente un 15%, y que el número de empleados del sector IT aumentará en más de un 6%. Ciberseguridad, cloud y desarrollo de aplicaciones serán las principales áreas de inversión TIC en 2023.

Las compañías españolas aumentarán en más de un 25% la inversión en ciberseguridad este año. Dos puntos más que el año pasado. Por otro lado, el desarrollo de aplicaciones orientadas a reducir el gasto o aumentar el crecimiento de la compañía (BI, RPA y CRM), será el ámbito en el que más se invertirá (más del 47%). Del mismo modo, se denota una evolución hacia infraestructuras cloud (más del 18%).

El sector que espera aumentar más su inversión en ciberseguridad es el de farma-salud, con un aumento de más de 36%. Le seguiría industria, con más del 34%, y logística y transporte, con más del 32%. Asimismo, el sector que menos espera invertir en ciberseguridad este año es el de servicios con un 8%. Por otro lado, el sector finanzas es el que más invertirá en el desarrollo de aplicaciones (más del 60%), seguido de finanzas (más del 50%) y servicios (más del 46%). Distribución es el sector que menos invertirá en desarrollo, con un 30%.

Fuente: itReseller

Apunte de interés

El 30 de abril finaliza el plazo de presentación de candidaturas a la 16 edición de los Trofeos de Seguridad TIC .

Organizados por la Red de Seguridad premiarán a los profesionales, proyectos, programas, operaciones y soluciones más destacados de del año pasado. Este comité, compuesto por representantes de asociaciones, organismos públicos y profesionales de la ciberseguridad, es el encargado de deliberar acerca de las candidaturas recibidas y de formular su veredicto.

Organizaciones y profesionales pueden optar a las siguientes candidaturas:

- Trofeo al Producto/Servicio o Sistema de Seguridad más innovador.
- Trofeo a la Empresa de Seguridad TIC.
- Trofeo a la Mejor Institución u Organismo Público en materia de Seguridad TIC.
- Trofeo a la Trayectoria Profesional Pública o Privada en Seguridad TIC.
- Trofeo a la Capacitación, Divulgación, Concienciación o Formación en Seguridad TIC.
- Trofeo al Centro Educativo SegurTIC.

Acceso a las bases

14/02/2023

El teléfono de ayuda 017 de INCIBE atendió más de 67.000 consultas sobre ciberseguridad en 2022

El Instituto Nacional de Ciberseguridad (INCIBE), entidad dependiente del Ministerio de Asuntos Económicos y Transformación Digital, ha atendido más de 67.000 consultas durante 2022 en su teléfono de ayuda 017 y sus diferentes canales de contacto de WhatsApp, Telegram y formulario web.

En concreto, 44.331 se gestionaron por vía telefónica, 17.014 a través de los canales de chat y 5.977 mediante correo electrónico.

El 017 es un servicio, gratuito y confidencial, financiado con fondos europeos del Plan de Recuperación, que está disponible en horario de 8 de la mañana a 11 de la noche, los 365 días del año. Está gestionado por profesionales que ofrecen asesoramiento técnico, psicosocial y legal, dependiendo de la temática de cada consulta y dirigido a las empresas y a la ciudadanía haciendo especial hincapié en los menores. En 2023 este servicio seguirá incrementando sus capacidades para aumentar el número de beneficiarios a los que puede diariamente. Consultas de empresas

Consultas de empresas

Las empresas recurrieron a este servicio para preguntar dudas sobre *phishing*, *smishing* o extorsión (20,8%), el Business Email Compromise, BEC, o del fraude del CEO (15,3%) y la concienciación de los empleados y las buenas prácticas en ciberseguridad (12,5%). Completan la lista de los temas más recurrentes: las llamadas fraudulentas, tanto de extorsión, como de estafas; el ciberataque tipo ransomware; la suplantación en redes sociales y los asuntos legales, entre otras.

Finalmente, el 33% de las consultas se centraron en los servicios profesionales, seguido en menor medida por el comercio minorista (11%), la industria (3%) y la educación (3%). Otros sectores con preocupaciones sobre ciberseguridad fueron la Administración, el ocio, las asociaciones, la salud, el comercio mayorista, las empresas de ciberseguridad, la logística y la construcción.

Desde que se puso en marcha este número corto de ayuda en ciberseguridad, en febrero de 2020, el servicio ha atendido más de 184.000 consultas, de las cuales más de 113.000 son de usuarios preocupados por su ciberseguridad. Así, se ha alcanzado un promedio de más de 1.295 consultas semanales a lo largo de 2022. La mitad recibieron ayuda preventiva (resolviendo dudas) y la otra mitad asesoramiento reactivo (ya habían sido víctimas de un incidente), con una pequeña proporción que contactó para recibir información en ciberseguridad.

Fuente: INCIBE

— 03

Tendencias tecnológicas

Nuevas patentes, prototipos y resultados de investigación.

Nº de Publicación: EP4143712A1
Fecha: 08/03/2023

Método y sistema para evaluar la eficacia de los controles de ciberseguridad en un entorno OT

La tecnología operativa (OT) es una parte integral de las infraestructuras críticas, ayudando a facilitar las operaciones en industrias vitales como la electricidad, el petróleo y el gas, el agua, el tratamiento de aguas residuales, el transporte y la fabricación. El creciente problema de la ciberseguridad y su impacto en los entornos OT presenta riesgos fundamentales para las empresas y sus operaciones. Existe una necesidad urgente e insatisfecha de una solución de ciberseguridad que pueda evaluar la postura de seguridad de un entorno OT en tiempo real o casi real e identificar problemas de ciberseguridad en el entorno OT.

La presente patente describe un sistema, un método y un programa informático para medir, supervisar, evaluar y valorar una postura general de ciberseguridad para un entorno OT, identificando problemas o vulnerabilidades que pueden exponer potencialmente el entorno OT a ciberamenazas o ciberataques. Además, la solución permite guiar al usuario o efectuar acciones efectivas inmediatas de resolución o remediación de manera oportuna ante la sospecha de un posible ataque.

Nº de Publicación: EP4152692A1
Fecha: 22/03/2023

Aceleración del flujo de trabajo de ciberanálisis

Las amenazas a las redes de comunicación pueden adoptar diversas formas, por lo que existen servicios de suscripción para conocer las amenazas de red mediante información periódica. La información proporcionada por dichos servicios puede ser utilizada por las organizaciones para identificar amenazas contra sus redes y activos asociados, pero se trata de gran cantidad de información que debe analizarse en el menor tiempo posible.
La presente patente define un dispositivo de pasarela de inteligencia de ciberamenazas en el que se definen reglas para filtrar eventos de comunicaciones de paquetes TCP/IP con el objetivo de identificar comunicaciones correspondientes a indicadores, firmas y patrones de comportamiento de amenazas de red.
La pasarela crea un registro del evento de amenaza y lo envía a una cola de tareas gestionada por una aplicación de flujo de trabajo de ciberanálisis, mediante un cálculo de la probabilidad de que dicho evento sea una amenaza real, basándose en algoritmos de aprendizaje automático. Su principal ventaja es acelerar el flujo de trabajo al reducir la tasa media de servicio por parte de los ciberanalistas, pudiendo detectar las amenazas más rápidamente.

Nº de Publicación: EP4127935A1
Fecha: 08/02/2023

Gemelo Digital de una infraestructura IT

El software moderno cambia constantemente mediante diferentes actualizaciones, pero estos cambios deben probarse antes de migrar completamente a los servidores de IT corporativos para garantizar que no causarán consecuencias no deseadas. Hoy en día, las pruebas de software corporativo requieren que los técnicos de IT internos tengan acceso a sofisticados entornos de pruebas de preproducción que puedan imitar el comportamiento de las principales aplicaciones que dirigen el negocio de una empresa.

Con la presente patente se crea un gemelo digital de una infraestructura informática para identificar un grupo de servidores críticos (llamados "servidores base") necesarios para replicar la infraestructura informática en un entorno de computación en nube. Para ello se rastrea dicha infraestructura informática y se analizan diversos datos de telemetría, conexión y red comparándolos con conjuntos de datos de otros servidores conocidos. A continuación, el gemelo digital puede desplegarse bajo demanda en el entorno de computación en nube utilizando scripts ejecutables que imitan a los servidores base y sus configuraciones particulares, creando una réplica de la infraestructura de IT para diversos fines.

Nº de Publicación: EP4111373A1
Fecha: 04/01/2023

Inferencia robusta de inteligencia artificial en dispositivos de computación en el borde

Los recientes avances en la tecnología de procesadores y la IA han permitido que los sistemas operativos en tiempo real que se ejecutan en dispositivos informáticos periféricos ejecuten de forma eficiente la predicción (también denominada "inferencia") a partir de modelos de redes neuronales, que residen en el núcleo de la IA. El entrenamiento de los modelos de redes neuronales se realiza sobre datos de muestra de la población objeto de estudio. Por ello, es difícil garantizar la precisión y el rendimiento de los modelos de redes neuronales una vez implantados. Por ejemplo, en un entorno de producción que cambia dinámicamente, los modelos de redes neuronales pueden enfrentarse a entradas para las que no han sido ampliamente entrenados y generar predicciones inexactas.

De este modo, la presente patente presenta un sistema para apoyar la inferencia de inteligencia artificial en un dispositivo de computación en el borde asociado con un proceso físico o planta, que incluye un módulo de entrenamiento de red neuronal, un módulo de prueba de red neuronal y un gemelo digital del proceso físico o planta.

Tecnologías de inteligencia artificial, privacidad y seguridad

Elliott D y Soifer E (2022) Tecnologías de inteligencia artificial, privacidad y seguridad. Frente. Artefacto Intel. 5:826737. doi: 10.3389/frai.2022.826737

En general, hemos visto que los sistemas de IA tienen un impacto en la privacidad de varias maneras, pero no siempre de la forma en que la gente podría pensar que lo hacen. Los sistemas de IA desafían varias características comúnmente asociadas con la privacidad, como el privilegio epistémico que las personas generalmente disfrutan con respecto a la información sobre sí mismos y el tipo de control sobre la información sobre uno mismo con el que cuentan las personas en las interacciones interpersonales ordinarias. Sin embargo, no está claro que esto, por sí solo, tenga mucho impacto en la privacidad. Esto es cierto, hemos argumentado, en gran medida porque la privacidad per se preocupa fundamentalmente por un interés en cómo nos perciben otras personas, y los sistemas de IA no forman el tipo de percepciones que pueden interferir con este interés. Sin embargo, debemos ser conscientes de que la presencia de grandes cantidades de información sobre personas dentro de los sistemas de IA crea un mayor riesgo de que se viole la privacidad, si esa información es accedida por un ser capaz de formar percepciones sobre la base de esos datos.

Creemos que mejorar la claridad de estos conceptos y las relaciones entre ellos es muy importante para poder explicar a las personas lo que hacen y no tienen motivos para preocuparse con respecto a las tecnologías de IA y la privacidad.

Sobre la gestión de la confianza en redes vehiculares *ad hoc*: una revisión exhaustiva

Che H, Duan Y, Li C y Yu L (2022) Sobre la gestión de confianza en redes ad hoc vehiculares: una revisión exhaustiva. Frente. Internet. Cosas 1:995233. doi: 10.3389/friot.2022.995233

Los problemas de seguridad siempre han representado una gran amenaza y desafío para Internet de las cosas (IoT), especialmente las redes vehiculares ad-hoc (VANET), una subcategoría de IoT en el campo automotriz. Los métodos tradicionales para resolver estos problemas de seguridad cada vez mayores en las VANET se basan principalmente en la criptografía. Como un complemento eficaz y eficiente de esas soluciones, las soluciones de gestión de confianza y los modelos de reputación se han explorado ampliamente para hacer frente a la intrusión de vehículos maliciosos o egoístas y la suplantación de datos falsificados, con el objetivo de mejorar la seguridad, la fiabilidad, la honradez y la imparcialidad generales de las VANET.

Para mantener la integridad del artículo, esta encuesta comienza brindando información básica sobre las VANET, incluidos los componentes básicos y la arquitectura general. Luego, muchos ataques en VANETs son investigados, analizados, y comparado para comprender la relevancia funcional de los siguientes métodos de confianza y reputación. Varios enfoques ofrecen varias contramedidas contra este tipo de ataques. Al mismo tiempo, el último desarrollo de tecnologías emergentes como blockchain, redes definidas por software y computación en la nube abre nuevas posibilidades para modelos y sistemas de gestión de confianza y reputación cada vez más prometedores en VANET. Posteriormente, la encuesta revisa los modelos y esquemas de confianza y reputación más importantes que se mencionan ampliamente en la literatura con base en nuestra taxonomía basada en técnicas desarrollada, en contraste con la taxonomía popular "centrada en la entidad, centrada en los datos, híbrida" en el campo, para adaptarse al reciente desarrollo tecnológico de estos esquemas de gestión en VANETs.

Proyecto X 2.0

Programa de crecimiento de tecnología profunda, financiado por la UE, que busca garantizar la ampliación de las nuevas empresas de tecnología profunda de la UE al proporcionar un programa de crecimiento personalizado y centrado en la industria que actuará como un catalizador en la entrega de aplicaciones y soluciones tecnológicas listas para el mercado en 5 áreas de impacto clave: Fabricación y Economía Circular, AgriTech, HealthTech y BioTech, Ciudades Inteligentes y Sostenibilidad, y Datos e IA).

Distribuirá 1,5 millones de euros en servicios de innovación y ampliación a 50 empresas emergentes de tecnología profunda y contribuirá a la oferta del programa EIC. De noviembre de 2022 a noviembre de 2024 X2.0 lanzará cinco convocatorias abiertas.

Fuente: X2.0

Proyecto Enjambre

El objetivo del proyecto Enjambre es obtener un pre-prototipo de un sistema autónomo de captura, monitorización y evaluación del comportamiento y seguridad de infraestructuras IT/OT y su tráfico de datos.

Pretende validar, a través de pruebas de concepto y pre-prototipos, una solución modular que incorpore herramientas, tecnologías y conocimientos fuera del habitual alcance de las pymes como la Inteligencia Artificial, la ciberseguridad, la Industria 4.0 y la ciber-inteligencia.

Financiado por el Ministerio de Industria, Comercio y Turismo dentro del programa de apoyo a las AEI para contribuir a la mejora de la competitividad de la industria española, y con el apoyo de la Unión Europea a través del Plan de Recuperación, Transformación y Resiliencia con la referencia AEI-010500-2022b-187.

Fuente: Cloud Center Andalucía

EMAPA 4.0

El proyecto de investigación Industrial Emapa 4.0 tiene por objetivo desarrollar una plataforma avanzada de automatización de Pentesting orientada a empresas manufactureras en el ámbito de la Industria 4.0.

Se trata de la construcción de un prototipo a nivel de laboratorio de una plataforma de Pentesting adaptada a las características IT-OT de la industria 4.0 que permita el tratamiento masivo de datos procedentes de diversas fuentes.

Fuente: Mnemo

CyberKit4SME

El proyecto CyberKit4SME, financiado con fondos europeos, desarrollará herramientas que permitan a las pequeñas empresas ser más conscientes de los riesgos para poder controlarlos, preverlos y gestionarlos. En concreto, diseñará herramientas de aislamiento y cifrado asequibles y fáciles de usar para proteger los datos. Las herramientas de cadena de bloques también se desarrollarán para permitir que las pymes compartan inteligencia e informes de incidentes con los equipos de respuesta a emergencias informáticas.

Tiene como objetivo democratizar un conjunto de herramientas y métodos de seguridad cibernética que permitan a las PYME/ME: Aumentar la conciencia sobre los riesgos, vulnerabilidades y ataques de seguridad cibernética; Monitorear y pronosticar riesgos; Gestionar los riesgos utilizando medidas de seguridad organizativas, humanas y técnicas con mayor confianza; y Colaborar y compartir información en un esfuerzo colectivo de seguridad y protección de datos.

Fuente: Cyberkit4sme

04
Agenda

Congresos, ayudas, modificaciones normativas y otros hitos relevantes del calendario del sector industrial en materia de digitalización.

¿Qué ha ocurrido?

Informática forense y Ciberinteligencia

Madrid, 22/02/2023

Congreso organizado por Red de Seguridad y Ondata Internacional, dirigido a los profesionales de la investigación digital y la ciberseguridad, tanto de las fuerzas de seguridad, cómo de organismos gubernamentales y del ámbito corporativo.

Su objeto ha sido acercar las últimas tecnologías y tendencias para la investigación de delitos, procesos de eDiscovery, cumplimiento de normativas, gestión de riesgos y respuesta a incidentes.

El Congreso ha servido para obtener información práctica y conocimientos exclusivos sobre estas materias conectando con desarrolladores, especialistas, ingenieros de hardware… además de servir para contactar con los principales fabricantes internacionales.

Conferencia Internacional sobre la Ley de Ciberseguridad de la Unión Europea

Bruselas, 29-30/03/2023

La Conferencia Internacional sobre la Ley de Ciberseguridad de la Unión Europea trata sobre esta normativa que formalizará un marco europeo de certificación de ciberseguridad para productos, servicios y procesos TIC.

Se ha desarrollado para ayudar a la comunidad de estándares a prepararse para la evolución de los marcos basados en el riesgo destinados a abordar la fragmentación del mercado en la UE. La Ley de Ciberseguridad de la UE, ahora en las primeras etapas de desarrollo, eventualmente creará un organismo europeo independiente de amplio alcance para la regulación de la ciberseguridad como parte del objetivo del "mercado digital único".

¿Qué ha ocurrido?

Connections on the Road Madrid 2023

Madrid, 23/02/2023

Los líderes de la Industria, clientes, socios y expertos comparten los conocimientos, mejores prácticas y los consejos técnicos necesarios para innovar con confianza.

En el evento se tratan las últimas tecnologías de mitigación de ransomware, incluidas las brechas de aire, la inmutabilidad y el engaño cibernético integrado.

THE INDUSTRY'S PREMIER DATA SERVICES EVENTS

CONNECTIONS

II Congreso de Ciberseguridad de Andalucía

Málaga, 22-23/03/2023

El II Congreso de Ciberseguridad de Andalucía está organizado por el gobierno autonómico a través de la Agencia Digital de Andalucía (ADA).

Administración Pública, instituciones, empresas y ciudadanía se informan de las últimas tendencias y necesidades en materia de seguridad digital.

El evento dispone de 1.200 m^2 de zona expositiva de las principales empresas del sector y tres escenarios diferenciados para charlas, mesas de debate, demostraciones y talleres.

Próximamente

III Congreso de Seguridad Digital y Ciberinteligencia (C1b3rWall)

Ávila, 20-22/06/2023

El C1b3rWall2023 es un Congreso de Seguridad Digital y Ciberinteligencia. Profesionales del sector TIC privado, profesionales del sector TIC público, Fuerzas y Cuerpos de Seguridad y Fuerzas Armadas nacionales e internacionales, así como universidades y Formación Profesional se darán cita en este Congreso.

15 Encuentro de la Seguridad Integral (Seg2)

Madrid, 22-23/04/2023

La revista Red Seguridad y Seguritecnia organizan el 15 Encuentro de la Seguridad Integral (Seg2) el 22 de junio, tras el éxito de la anterior edición con más de 30 ponentes de organizaciones públicas, privadas y asociaciones, y más de 2.000 conectados,

Próximamente

III RSA Conference 2023

San Francisco, 24-27/04/2023

El Foro más importante para la industria de la ciberseguridad, III RSA Conference tendrá lugar el próximo mes de abril en San Francisco, este año Bajo el lema '*Stronger together*',El Instituto Nacional de Ciberseguridad de España (INCIBE) e ICEX España Exportación e Inversiones, con la colaboración de la Oficina Económica y Comercial de España en Los Ángeles (EE.UU.), organizan la participación española en esta nueva edición Con el objetivo de seguir potenciando las internacionalización de las empresas de nuestro sector

RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

TECNOSEC

Madrid, 26-27/04/2023

La II Feria Congreso de Alta Tecnología de Seguridad e Inteligencia, se realizará desde el 26 al 27 de abril en el Pabellón de Cristal de Madrid. Este evento de ciberseguridad también contará con la participación de la feria DRONExpo. Se trata de un evento de Altas Tecnologías de Seguridad e Inteligencia. Enclave ideal para propiciar encuentros nacionales e internacionales y cultivar contactos valiosos para la industria de la seguridad.

TECNOSEC

26-27 ABRIL 2023 MADRID

Publicada la Directiva NIS 2

La Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión, conocida como Directiva NIS 2 deroga su anterior versión y modifica el Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Establece obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación, obligaciones relativas al intercambio de información sobre ciberseguridad, así como obligaciones de supervisión y ejecución para los Estados miembros.

Establece para los Estados miembros obligaciones en relación con las siguientes cuestiones, de forma resumida: elaborar, mantener y comunicar a la Comisión un listado de entidades esenciales e importantes; adoptar, notificar a la Comisión y evaluar periódicamente una estrategia nacional de ciberseguridad; designar autoridades competentes de ciberseguridad, supervisión y punto de contacto único, así como notificar a la Comisión y garantizar recursos para que puedan realizar su función; articular una plan nacional para gestión de crisis de ciberseguridad, así como designar autoridades competentes y determinar capacidades; designar equipos de respuesta a incidentes de seguridad informática (CSIRT), así como garantizar recursos, capacidades técnicas y cooperación efectiva; designar CSIRT para la divulgación coordinada de vulnerabilidades; garantizar la cooperación a escala nacional (junto con disposiciones relativas a la cooperación en el ámbito europeo); y, en relación con la supervisión y ejecución, garantizar que las autoridades competentes supervisen efectivamente y adopten las medidas necesarias incluyendo régimen sancionatorio.

Establece para las entidades en su alcance, indicadas en sus anexos I y II, obligaciones tales como las siguientes, de forma resumida: adoptar medidas de gobernanza, gestión de riesgos de ciberseguridad e información (*reporting*); adoptar medidas técnicas y organizativas proporcionadas para gestionar los riesgos de ciberseguridad; así como para prevenir y minimizar el impacto de posibles ciberincidentes; notificar los incidentes de ciberseguridad al CSIRT o autoridad competente correspondiente; que los gestores reciban formación sobre los riesgos de ciberseguridad, siendo responsables en cuanto a la adopción de las medidas adecuadas; utilizar esquemas europeos de certificación; remitir a las autoridades competentes la información requerida y notificar cualquier cambio en la misma.

Publicada la Directiva NIS 2

Adicionalmente se contemplan el intercambio voluntario de información de ciberseguridad entre entidades esenciales e importantes y la notificación, de forma voluntaria, a las autoridades competentes o a los CSIRT cualquier incidente, amenaza cibernética o cuasi incidente relevante.

Amplía su ámbito de aplicación para abarcar a entidades medianas y grandes de más sectores críticos para la economía y la sociedad, incluyendo proveedores de servicios públicos de comunicaciones electrónicas, servicios digitales, gestión de aguas residuales y residuos, fabricación de productos críticos, servicios postales y de mensajería, así como a las Administraciones Públicas (en el caso de España Entidades de la Administración General del Estado; Entidades de administraciones públicas de Comunidades Autónomas; y se podrá determinar su aplicación a entidades de la Administración Pública a nivel local).

Otras novedades reseñables de la Directiva NIS 2, son, por ejemplo, que contempla la seguridad de la cadena de suministro y las relaciones con los proveedores; y que introduce la responsabilidad de la alta dirección por el incumplimiento de las obligaciones de ciberseguridad.

Acceso a la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Activado el proceso de adhesión de proveedores para ayudar a modernizar pymes y autónomos del sector del transporte por carretera

El Ministerio de Transportes, Movilidad y Agenda Urbana (Mitma) ha publicado el Anuncio de Adhesión para que empresas del ámbito tecnológico y digital soliciten su adhesión como al programa de ayudas para modernizar pymes y autónomos del sector del transporte por carretera.

El programa, dotado con 110 millones de euros, forma parte den la inversión 4 del componente 6 del Plan de Recuperación, Transformación y Resiliencia (PRTR) y persigue incrementar la eficiencia de las empresas de transporte por carretera mediante la digitalización y la introducción de nuevas tecnologías.

Las ayudas se otorgan en concurrencia simple a través de las comunidades y ciudades autónomas, a las que se han transferido los fondos europeos NextGenerationEU, conforme a lo estipulado en el Real Decreto 902/2022, de 25 de octubre. Este Real Decreto contiene también las bases reguladoras de las convocatorias a las que deberán sujetarse las comunidades y ciudades autónomas para conceder las subvenciones.

Proveedor de servicios

Con el fin de facilitar la gestión de las ayudas, la búsqueda de los servicios acordes a las necesidades de las empresas beneficiarias y la implantación de las soluciones de modernización subvencionadas se ha creado la figura de los Proveedores de Soluciones de Modernización.

Así, las empresas del ámbito tecnológico y digital que sean proveedoras de alguna de las soluciones de modernización incluidas en el Real Decreto, y que cumplan las condiciones fijadas en el Anuncio para ser Proveedor de Soluciones de Modernización, podrán solicitar a Mitma su adhesión al programa de ayudas, mediante el procedimiento publicado en la sede electrónica del Ministerio.

Las empresas que quieran adherirse al programa pueden hacerlo en cualquier momento hasta el a través de sede electrónica de Mitma. No obstante, las CCAA que lo deseen podrán publicar anuncios de adhesión complementarios al del Ministerio.

Para poder adherirse al programa, entre otros requisitos, las empresas tecnológicas deberán tener el domicilio fiscal y el centro de prestación de las soluciones en la Unión Europea y una facturación acumulada de, al menos, 100.000 euros en los dos años anteriores o 50.000 en el año anterior en proyectos similares (70.000 o 35.000 euros de facturación, respectivamente, para autónomos sin trabajadores a su cargo).

Las empresas adheridas al programa serán las únicas que podrán prestar las soluciones de modernización subvencionadas a las pymes y autónomos beneficiarios de las ayudas. Mitma habilitará en su web un registro de Proveedores de Soluciones de Modernización, que recogerá todas las empresas que se han sumado al programa. Para hacer la búsqueda más rápida y cómoda, se podrá filtrar por categoría, por tipo de servicios de transporte que presta (mercancías, colectivo de viajeros, cargadores…, por comunidades autónomas donde prestan servicio y por la región donde tenga la sede fiscal el proveedor.

Soluciones de modernización subvencionables

Las empresas tecnológicas podrán solicitar su adhesión al programa para una o varias de las nueve categorías de soluciones de modernización subvencionables:

- Categoría 1: Gestión de documentos de control electrónicos.
- Categoría 2: Sistema de tacógrafo inteligente de segunda generación.
- Categoría 3: Integración de documentos de control electrónicos en los sistemas de gestión.
- Categoría 4: Implantación de sistemas de planificación de recursos empresariales (TMS/ERP).
- Categoría 5: Implantación de sistemas de ayuda a la explotación (SAE).
- Categoría 6: Actualización de sistemas de ayuda a la explotación (SAE).
- Categoría 7: Ayudas a los servicios de transporte de viajeros.
- Categoría 8: Implantación de aplicaciones para reclamaciones por medios electrónicos.
- Categoría 9: Mejora de sistemas de ticketing.

El Real Decreto establece los contenidos mínimos de las actuaciones subvencionables de cada una de estas categorías, así como las cuantías de estas en función del tamaño del destinatario último que las solicite.

Los destinatarios últimos podrán elegir hasta un máximo de dos soluciones de modernización de entre las establecidas como elegibles para su tamaño y tipo de actividad. En el caso de que elijan dos categorías, podrán firmar Acuerdos de Prestación de Soluciones de Modernización con dos Proveedores adheridos distintos, si así lo desean.

Cheque moderniza

Una vez publicadas las convocatorias por parte de cada Comunidad y Ciudad Autónoma, los destinatarios últimos (autónomos y pymes) tendrán hasta el 30 de junio de 2024 para solicitar las ayudas en la comunidad autónoma donde tengan su residencia fiscal. Las solicitudes serán atendidas por orden de presentación hasta el agotamiento de los fondos.

Los destinatarios últimos adjudicatarios recibirán un "cheque moderniza", que deberán emplear en la contratación de las Soluciones de Modernización para las cuales se le ha concedido la subvención, formalizando para ello Acuerdos de Prestación de Soluciones de Modernización con los Proveedores de Soluciones de Modernización de su elección.

Con el Acuerdo formalizado, se procederá a la prestación de la solución de modernización por parte del Proveedor. El pago de la prestación se realizará por el destinatario último, mediante la cesión al Proveedor de la parte del "cheque moderniza" asociado al Acuerdo suscrito y el abono de la parte correspondiente de los costes no subvencionables.

Tras la prestación de la solución de modernización, el Proveedor, en nombre del destinatario último, deberá presentar la justificación de las acciones realizadas.

Fuente: La Moncloa

España invertirá 1.000 millones en un nuevo fondo europeo para startups tecnológicas

La vicepresidenta primera y ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño, ha formalizado la puesta en marcha de la iniciativa European Tech Champions (ETCI) en una declaración conjunta con los ministros de Economía de Alemania, Francia, Italia y Bélgica en el marco del Eurogrupo.

Este nuevo fondo europeo de apoyo a startups tecnológicas punteras en crecimiento contribuirá a facilitar la financiación a empresas emergentes innovadoras más punteras de Europa con capital europeo, con el fin de crear un ecosistema emprendedor que permita el desarrollo de proyectos punteros con potencial a escala global. El nuevo fondo europeo cuenta ya con compromisos por valor de 3.750 millones de España, Alemania, Francia, Italia, Bélgica y el grupo Banco Europeo de Inversiones (BEI).

El Gobierno de España ya ha aprobado, en el Consejo de Ministros del 7 de febrero, una contribución inicial de 400 millones de euros para el nuevo fondo europeo. En una segunda fase, la aportación comprometida de España alcanzará los 1.000 millones de euros este año.

La contribución española se realizará a través del fondo Next Tech, una iniciativa del Plan de Recuperación para fomentar el desarrollo de proyectos digitales innovadores de alto impacto y la inversión en empresas en crecimiento (scale-ups) mediante el refuerzo de los instrumentos públicos de financiación, la atracción de fondos internacionales y la potenciación del sector de capital riesgo.

Fuente: Plan de Recuperación

Just in Time

El factor humano de la ciberseguridad

La Ingeniería Social trata de utilizar a los trabajadores para acceder a los recursos de la empresa

En el artículo “Ciberseguridad en la Industria 4.0: Retos y recomendaciones” del inicio de este boletín se han indicado tres grandes bloques de recomendaciones en los que ENISA definía como principales para la ciberseguridad la Industria 4.0: personas, procesos y tecnología. A continuación, nos centraremos en el primero de ellos, es decir, cómo las personas tienen gran relevancia a todos los niveles para garantizar la ciberseguridad.

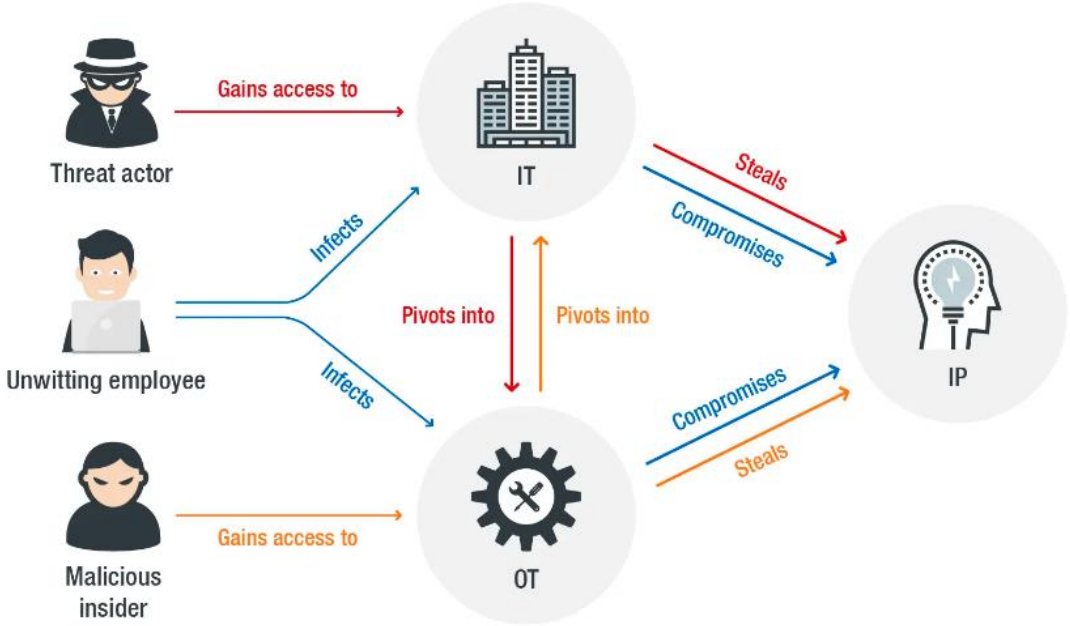

Figura 3. Efectos de las acciones involuntarias de un empleado respecto a la ciberseguridad. Fuente: Security in the Era of Industry 4.0: Dealing With Threats to Smart Manufacturing Environments, Trendmicro.

En la Figura 3 se observa cómo cualquier empleado, de manera involuntaria, puede comprometer a todo el sistema, ya que ya sea a través de su acceso a la IT (Information Technology, tecnologías de la información) o a través de la OT (Operational Technology, tecnología operacional), la amenaza se expandirá, robando o comprometiendo la Propiedad Intelectual (IP) del negocio.

Los ciberataques que tratan de explotar un error humano o un comportamiento humano con el objetivo de obtener acceso a información o servicios son conocidos como ingeniería social. Utilizan diversas formas de manipulación para engañar a las víctimas para que cometan errores o entreguen información sensible o secreta. Se trata de técnicas para engañar a los usuarios para que abran documentos, archivos o correos electrónicos, visiten sitios web o concedan a personas no autorizadas acceso a sistemas o servicios. Y aunque estos trucos pueden abusar de la tecnología siempre dependen de un elemento humano para tener éxito.

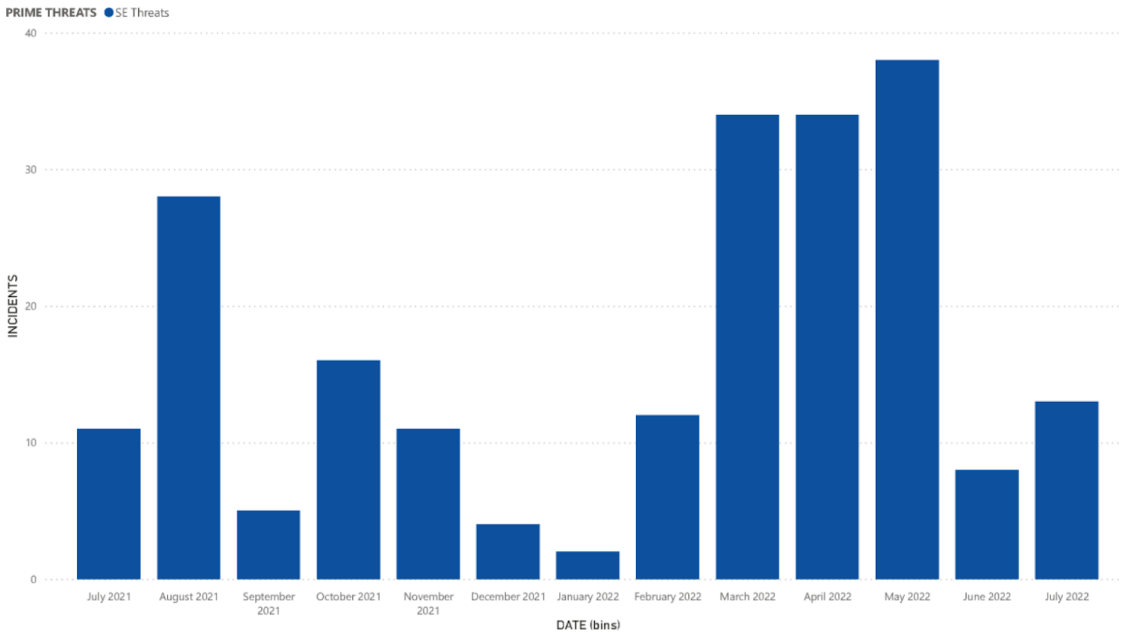

Figura 4. Series temporales de las principales amenazas en Ingeniería Social detectadas por ENISA. Fuente: ENISA Threat landscape 2022.

Dentro de la ingeniería social, la técnica más comúnmente utilizada es el *phishing*. Según INCIBE (Instituto Nacional de Ciberseguridad), el *phishing* "es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo".

Figura 5. *Phishing*. Fuente: INCIBE

Los datos del último informe de IBM sobre ciberseguridad (IBM Security X-Force Threat Intelligence Index 2023) confirman la importancia del phishing, ya que en 2022 (por segundo año consecutivo) el phishing fue la causa principal de infección, identificado en el 41% de los incidentes. Se observó, además, un aumento del 100% en los intentos de secuestro de conversaciones por mes, en los que un atacante se hace pasar por otra persona y utiliza conversaciones de correo electrónico existentes con fines nefastos.

Diversos avances tecnológicos (Inteligencia Artificial, procesamiento del lenguaje…) han traído como consecuencia una sofisticación del *phishing*, siendo cada vez más difícil para los usuarios el detectarlo. Es por ello que las empresas deben invertir recursos en formar a sus empleados para evitar este tipo de ataques, ya que así estarán evitando posibles daños a su organización en el futuro. Como en muchos casos los ataques de phishing pueden tratar de hacerse pasar por la propia empresa, se debe proporcionar a los empleados unos consejos básicos de prevención como los siguientes:

- ❑ No deben transmitir nunca información confidencial personal o de la empresa por correo electrónico;
- ❑ No deben confiar nunca en un mensaje de correo electrónico basándose únicamente en su supuesto origen, ni en el uso de imágenes o logotipos aparentemente oficiales;
- ❑ No se debe hacer nunca clic en un enlace sin comprobar antes su destino, pasando el cursor por encima de la URL para determinar el destino del enlace.
- ❑ Deben desconfiar de los correos electrónicos con saludos genéricos y estilo gramatical inadecuado;
- ❑ Deben ser conscientes de que las líneas de asunto atractivas o agresivas suelen utilizarse para incitar a la gente a hacer clic en un enlace o a realizar otras acciones de alto riesgo;
- ❑ Deben tener especial cuidado con los correos electrónicos que amenazan o instan a la "acción inmediata" ya que se utilizan a menudo para asustar e intimidar a los destinatarios para que actúen precipitadamente, antes de que se pueda comprobar si las acciones a las que insta el mensaje son verdaderas.

Los últimos datos existentes parecen corroborar la implicación cada vez mayor de las empresas en la formación de sus empleados ya que según el último informe de Deloitte ("Estado de la ciberseguridad en España"),el número de empresas que no dedican tiempo a formar y concienciar a sus empleados se ha reducido en un 14%. Se ha puesto de manifiesto, además, la clara relación existente entre el nivel de formación y concienciación de los empleados y el número de incidentes de ciberseguridad sufridos: las empresas que imparten más de 20 horas de formación y concienciación a sus empleados han recibido únicamente el 15% de los incidentes en el último año.

De este modo, una buena estrategia de formación en concienciación en materia de ciberseguridad para los empleados aportará beneficios no sólo para los empleados sino para la propia empresa.

Por qué debes tener perfiles especializados en ciberseguridad en tu empresa

En los últimos cinco años, ha habido una demanda creciente en las empresas de todo el mundo de perfiles especializados en ciberseguridad. Con una sociedad cada vez más digital, se prevé que este índice de empleabilidad siga creciendo durante, al menos, otros tres años. En España en concreto, se estima que el valor de mercado generado por este sector alcanzará los 2.000 millones de euros en 2024, lo que supone una evolución anual que supera el 8%, según datos del estudio "Análisis y Diagnóstico del Talent de Ciberseguridad en España" realizado por ObservaCiber, entidad adscrita al Instituto Nacional de Ciberseguridad (INCIBE).

Sin embargo, el número de personas especializadas en ciberseguridad no aumenta al mismo ritmo que las necesidades de las empresas. Si se tiene en cuenta la cantidad de ofertas para puestos relacionados publicadas en nuestro país, se publican 1,6 ofertas por cada especialista y, de hecho, se considera que el año que viene, ya llegaremos al doble de ofertas de trabajo que de personas que las puedan suplir. En este sentido, la previsión es que para 2024, sean necesarios más de 83.000 profesionales para cubrir la demanda de talento en ciberseguridad en España.

Figura 6. Objetivos que persigue el informe "Análisis y Diagnóstico del Talent de Ciberseguridad en España."

Más ataques y más elaborados

Líderes en ciberseguridad a nivel internacional argumentan que las empresas necesitan no solo cubrir los puestos existentes, sino aumentar el número de funciones en su personal debido a los muchos lugares por donde las organizaciones pueden sufrir ataques. Además, éstos se dan cada vez con más frecuencia y mayor sofisticación.

Por estos motivos, según refleja el estudio de INCIBE, casi la mitad de las empresas españolas optan por formar a su personal en materia de ciberseguridad. Reciclan perfiles de las áreas de negocio o ventas formándoles para saber prevenir y resolver las amenazas que puedan llegar por vía digital. Sin embargo, dado el alto perfil de rotación, esta solución puede no ser la idónea.

Otra de las conclusiones del estudio es que deben llevarse a cabo iniciativas para incrementar la presencia de mujeres en posiciones de ciberseguridad, donde ya destacan los programas de impulso en investigación, aunque se pone de manifiesto la necesidad de implementar programas específicos que impulsen la presencia femenina. En relación, a esto, la brecha de género se refleja ya en la etapa universitaria en la que solo el 18% de las personas graduadas especializadas en esta materia son mujeres.

Este desajuste entre la oferta y la demanda es un problema que ocurre más allá de nuestras fronteras, sobre todo ahora que el teletrabajo se ha impuesto en muchas empresas y muchas firmas internacionales buscan profesionales españoles, con una amplia formación y con sueldos más bajos que perfiles similares en otros países europeos. Esto conlleva que la retención de talento por parte de las empresas nacionales sea algo más complicada.

Consejos para encontrar candidaturas

Una de las soluciones a esta situación que pueden plantear las empresas es elaborar mejores descripciones de los puestos de ciberseguridad. Casi siempre, las ofertas de trabajo incluyen un listado amplio con las características de una candidatura ideal, con un listado de tareas bastante desgranado. Personas expertas en recursos humanos aconsejan cambiar la forma en la que se redactan las ofertas. Recomiendan exponer las tareas que realmente una persona del equipo realizaría en su día a día, para ello, invitan a establecer un nivel, para lo que podemos ayudarnos de preguntas como ¿Qué necesito? ¿Qué tareas básicas necesito que se realicen?, de esta manera, evitaremos incluir tareas que podrían echar para atrás algunas candidaturas, dejando fuera del proceso de selección a personas que podrían encajar muy bien en las necesidades de la organización, pero que, simplemente, aún no haya realizado nunca alguna de las tareas que teníamos en mente.

Asimismo, teniendo en cuenta que, por el momento, en España no existe formación reglada sobre ciberseguridad, otra recomendación para las empresas que busquen perfiles de este tipo es huir de los criterios de selección basados en titulación. Desde el punto de vista organizacional, es muy interesante contar en el equipo con variedad de niveles de experiencia y una reserva de talento más diversa. Esto puede incluir personas que se han reciclado profesionalmente y por tanto tienen conocimientos de otros sectores, personas que hayan estudiado o tengan experiencia en nuevas disciplinas o personas con habilidades transferibles. De esta manera se fomenta la resiliencia y versatilidad de la empresa.

En este sentido, otra de las recomendaciones a la hora de redactar una oferta de trabajo es eliminar el requerimiento de un mínimo de experiencia. Si buscamos un perfil que se desarrolle en nuestra empresa y que pueda aportar su *background* y flexibilidad, con una experiencia mínima, le cerramos la puerta a candidaturas que pueden tener muchas posibilidades en un puesto de entrada.

La manera de aprovechar al máximo estos consejos es incluyendo en la estrategia empresarial un compromiso formativo y con el desarrollo profesional de las personas que componen la organización.

Créditos

DIRECCIÓN:

EOI Escuela de Organización Industrial
Fundación EOI F.S.P.
C/ Gregorio del Amo, 6
28040 Madrid
Tel: 91 349 56 00
www.eoi.es

ELABORADO POR:

Fundación CTIC
Centro Tecnológico para el desarrollo en Asturias de las Tecnologías de la Información y la Comunicación
www.fundacionctic.org

Boletines

DE

Vigilancia Tecnológica

CEPI Centro de Estrategia y Prospectiva Industrial