ciberseguridadTIC
seguridad en informática y comunicaciones
Tai editorial
Año I Nº 3
Abril 2023

SCA, o cómo mantener la higiene de tu código

Joanna Burkey, CISO de HP:
"Uno de los mayores desafíos del CISO es tratar de averiguar lo que no sabemos"

EcoVadis:
"La seguridad de la cadena de suministro se debe abordar con un modelo basado en Zero Trust"

IBM Cibersecurity Services:
"Ni la inteligencia artificial ni la automatización son magia"

BeDisruptive:
"Ser disruptivos no es hacer las cosas totalmente opuestas, es hacerlas un poco diferentes"

'The Security Poverty Line'

Está claro que cada vez hay más ciberdelincuentes, más amenazas y más ciberataques. No solo hay más, sino que son más sofisticados. Es lo que tiene el uso de la automatización, o de la inteligencia artificial, o de la infinidad de tecnologías disponibles también en el lado del mal.

Este mes he tenido la oportunidad de viajar a Chicago, a la HP Amplify Partner Conference, donde he podido entrevistar a Joanna Burkey, CISO de la compañía. Algunas de las preguntas eran la de siempre, como los retos o cualidades de un buen CISO. Pero también le preguntamos cómo es posible que, habiéndose incrementado la inversión en ciberseguridad, la industria esté siendo incapaz de poner freno a tanto ciberataque, cómo es posible que el ransomware esté absolutamente descontrolado. La respuesta, decía Burkey, es The Security Poverty Line, o lo que es lo mismo, la línea que divide a las organizaciones que tienen los medios y los recursos para lograr y mantener posturas de seguridad maduras para proteger los datos, y aquellas que no los tienen.

El concepto fue acuñado por Wendy Nather, Head of Advisory CISOs en Cisco en 2011. Desde entonces, la teoría de Nather ha sido ampliamente adoptada como punto de referencia para una postura de ciberseguridad aceptable. Estar por debajo de la línea de pobreza de seguridad no es envidiable para ninguna organización, porque no solo significa que es probable que carezcan de los activos para mantener los datos efectivamente seguros, o que no tengan la capacidad o la inclinación para hacerlo, sino que también pueden ser objetivos principales para atacantes y ciberdelincuentes.

Lo que ocurre es que la seguridad es cosa de todos. Ocurre que un empleado poco precavido, o una cadena de suministro poco controlada puede tener un impacto directo en esa línea. Ocurre que a veces menos es más si está bien implementado. Y ocurre que la tecnología está al alcance de todos; de los buenos, y de los malos.

SUMARIO

Directora:
Rosalía Arroyo
rosalia@taieditorial.es

Publicidad:
David Rico
david@taieditorial.es

Producción:
Marta Arias
marta@taieditorial.es

Edita:
T.A.I. Editorial, S.A.
(Técnicos y Asesores Informáticos Editorial, S.A.)
www.taieditorial.es
Avda. Fuencarral, 68
28108 Alcobendas (Madrid)
Tel. 91 661 61 02
e-mail: correo@taieditorial.es

SCA, o cómo mantener la higiene de tu código

La mayoría de las aplicaciones modernas dependen de componentes y dependencias de terceros para funcionar. Si bien el uso de código 'open source' tiene sus beneficios, también puede introducir vulnerabilidades, código malicioso y otros riesgos de seguridad en una aplicación. El análisis de composición de software, o Software Composition Analysis – SCA, es una herramienta que permite identificar estas piezas de código externo.

EN PORTADA

El SCA proporciona visibilidad de los componentes y bibliotecas de código abierto que se incorporan al software que crean los equipos de desarrollo. El análisis de la composición del software permite a los desarrolladores aprovechar de manera segura los paquetes de código abierto sin exponer a las organizaciones a vulnerabilidades innecesarias o problemas legales y de cumplimiento.

Se calcula que el mercado de Análisis de Composición de Software alcanzó un valor de 161,03 millones de dólares en 2022, y se espera que crezca una media del 22 % anual los próximos años.

El uso de componentes de código abierto se ha generalizado en el desarrollo de software moderno, y la mayoría de las bases de código de las aplicaciones modernas están compuestas por dichos paquetes. Este método permite que los desarrolladores se muevan más rápido, ya que no necesitan volver a crear código que está disponible gratuitamente y examinado por la comunidad. Sin embargo, este proceso también

Casi el 80 % del código de las aplicaciones modernas se basa en paquetes de código abierto

conlleva su propio conjunto de riesgos. SCA no solo puede ayudar a gestionar la seguridad y los riesgos relacionados con las licencias, sino que puede ayudar a garantizar que cualquier componente de código abierto integrado en las aplicaciones cumpla con ciertos estándares. De

Beneficios del uso de un SCA

Seguridad mejorada: **SCA ayuda a las organizaciones a identificar y corregir vulnerabilidades en el software que utilizan, lo que puede reducir el riesgo de infracciones de seguridad y fugas de datos.**

Cumplimiento: **SCA ayuda a las organizaciones a garantizar que cumplen con los requisitos legales y de licencia para el software que utilizan, lo que puede reducir el riesgo de problemas legales y multas.**

Mejor toma de decisiones: **SCA puede ayudar a las organizaciones a tomar decisiones informadas sobre qué componentes de software usar en sus aplicaciones, en función de factores como la seguridad, la confiabilidad y la compatibilidad del componente con otros componentes.**

Mayor eficiencia: **al identificar y administrar los componentes de software que se utilizan, las organizaciones pueden mantener y actualizar sus aplicaciones más fácilmente, lo que puede mejorar la eficiencia y reducir los costos.**

Calidad mejorada: **SCA puede ayudar a las organizaciones a identificar y solucionar problemas con los componentes de software, lo que puede mejorar la calidad y confiabilidad general de sus aplicaciones.**

esta forma, se evitan riesgos que podrían llevar a una brecha de seguridad o disputas legales en torno a una propiedad intelectual.

Para lograr esto, las herramientas SCA pueden identificar versiones específicas de código abierto y correlacionar cualquier vulnerabilidad de seguridad asociada e información de licencia. Las herramientas SCA avanzadas pueden automatizar todo el proceso, desde la detección e identificación de componentes hasta la

> Un buen proceso SCA está integrado en todo el proceso de desarrollo

asociación de vulnerabilidades o licencias y la corrección de riesgos potenciales.

El análisis de composición de software también puede generar una lista de materiales de software (software bill of materials - SBOM) de todos los recursos para compartir con partes interesadas internas y clientes externos, es decir, una lista que incluye todos los componentes de código abierto utilizados por una aplicación. El SBOM enumera los detalles sobre la versión del paquete, así como las vulnerabilidades conocidas y las licencias para cada componente en uso.

Riesgos de usar componentes de código abierto

Casi el 80 % del código de las aplicaciones modernas se basa en paquetes de código abierto.

EN PORTADA

Si bien este software es la base del desarrollo de software moderno, también es el eslabón más débil en la cadena de suministro de software, dijo Endor Labs en un informe en el que asegura que "dado que el software de código abierto viene tal cual, sin garantías de ningún tipo, cualquier riesgo de usarlo recae únicamente en los usuarios. Esto hace que la selección, la seguridad y el mantenimiento de estas dependencias de código abierto sean pasos cruciales hacia la seguridad de la cadena de suministro de software".

> En un entorno moderno DevOps o DevSecOps, SCA ha impulsado el paradigma de "shift left"

El informe de Endor Labs, que recoge los principales riesgos a la hora de utilizar código de fuente abierta, identifica las vulnerabilidades conocidas como el principal riesgo asociado con el software de código abierto. Este riesgo ocurre cuando la versión de un componente contiene código vulnerable, es introducido accidentalmente por sus desarrolladores. Si un actor de amenazas explota una vulnerabilidad conocida, podría comprometer la confidencialidad, integridad o disponibilidad del sistema respectivo o sus datos.

Apache Log4j, o Log4Shell, es un ejemplo de vulnerabilidades conocidas. Dice Endor Labs que, para evitarlas, las empresas deberían realizar escáneres regulares de software.

El segundo gran riesgo que genera el uso de software de código abierto es que se comprometa un paquete del software legítimo. Los atacantes pueden comprometer los recursos que forman parte de un proyecto legítimo existente o de la infraestructura de distribución para inyectar código malicioso en un componente. El

EN PORTADA

Las vulnerabilidades conocidas son el principal riesgo asociado con el software de código abierto

ciberataque de SolarWinds fue el resultado del compromiso de un paquete legítimo.

Según Endor Labs, el tercer mayor riesgo del software de código abierto son los ataques de confusión de nombres, en los que un atacante crea componentes cuyos nombres se asemejan a nombres de componentes de sistema o de código abierto legítimos (typosquatting), sugiere autores confiables (brandjacking) o juega con patrones de nombres comunes en diferentes idiomas o ecosistemas.

Evitar estos riesgos, dicen desde Endor Labs, pasa porque las organizaciones verifiquen las características del código antes y después de los enlaces de instalación, verifiquen las carac-

Casos de uso de análisis de composición de software (SCA)

SCA proporciona visibilidad de las dependencias de código abierto que utilizan las aplicaciones de una organización. Esta visibilidad es esencial para la gestión de vulnerabilidades y licencias, que son los dos principales casos de uso de estas soluciones.

Gestión de vulnerabilidades. Las bibliotecas de código abierto pueden contener vulnerabilidades explotables o código malicioso. Si una aplicación importa estas bibliotecas, puede ser vulnerable a la explotación o ejecutar el código malicioso. Las soluciones de SCA pueden ayudar a las empresas a obtener la visibilidad que necesitan y determinar rápidamente si existen CVE para las versiones de las bibliotecas utilizadas por la aplicación.

Gestión de licencias. El uso de código de terceros puede crear problemas de licencia para una organización, especialmente con la amplia gama de posibles requisitos de licencia. En un extremo, los derechos de autor pueden imposibilitar que una empresa use un componente o pueden requerir el pago de regalías. Por otro lado, las licencias copyleft pueden exigir que cualquier código que use un componente en particular también debe estar disponible gratuitamente y ser de código abierto. Sin visibilidad de los componentes de código abierto utilizados por sus aplicaciones, una organización no conoce las reglas de licencia y puede estar en peligro legal. Al recopilar información de licencias sobre todos los componentes de código abierto utilizados dentro de una base de código, una empresa puede obtener visibilidad de posibles problemas legales y de licencias.

EN PORTADA

> El SCA proporciona visibilidad de los componentes y bibliotecas de código abierto que se incorporan al software que crean los equipos de desarrollo

terísticas del proyecto, como el repositorio del código fuente, las cuentas del mantenedor, la frecuencia de publicación, la cantidad de usuarios intermedios, etc.

Cómo funciona una solución SCA

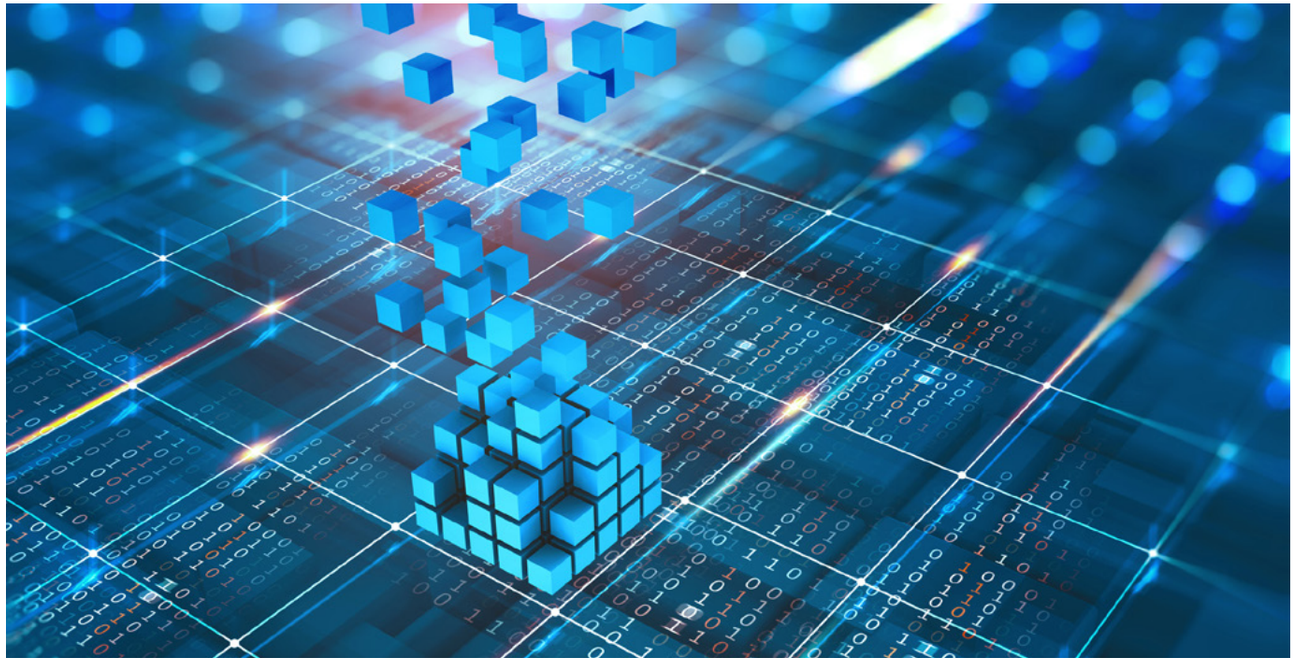
Un buen proceso SCA está integrado en todo el proceso de desarrollo. Comenzando en entornos locales, los desarrolladores deben poder verificar su código en busca de vulnerabilidades y el cumplimiento de la licencia a medida que lo escriben. Esto se puede lograr a través de los siguientes pasos identificados por Check Point:

Escaneo: una herramienta SCA comenzará con el escaneo de un código base para identificar las bibliotecas y las dependencias utilizadas por el código. En función de este escaneo, la herramienta puede generar una lista de materiales de software (SBOM) que enumera todo el código fuente abierto utilizado por la aplicación.

Documentación: la versión del software, la información de licencia y el uso por parte de una aplicación son información valiosa. Después de identificar el código fuente abierto en una base de código, un escáner SCA registrará estos datos.

Detección de vulnerabilidades: las vulnerabilidades conocidas se registran como vulnerabilidades y exposiciones comunes (CVE) junto

EN PORTADA



con el software y las versiones afectadas. Con el conocimiento de las bibliotecas de código abierto utilizadas y sus números de versión, las herramientas SCA pueden identificar vulnerabilidades conocidas dentro de la aplicación.

Al final de este proceso, la herramienta SCA ha generado un informe que contiene información sobre todas las dependencias de código abierto utilizadas por una aplicación. Esta información puede llegar al personal de seguridad o, según los hallazgos y el nivel de integración dentro de las canalizaciones de CI/CD, incluso puede bloquear la adición de nuevas confirmaciones al código base si utilizan componentes obsoletos o inseguros.

En un entorno moderno DevOps o DevSecOps, SCA ha impulsado el paradigma de “shift left” de comprobación del ciclo de vida de software. Las pruebas SCA anteriores y continuas han permitido a los desarrolladores y equipos de seguridad impulsar la productividad sin comprometer la seguridad y la calidad.

ENLACES DESTACADOS

Y el 95% de las vulnerabilidades de código abierto están en...

Google lanza un escáner de vulnerabilidades para proyectos de código abierto

Tenemos **toda la información** que necesitas

“Uno de los mayores desafíos del CISO es tratar de averiguar lo que no sabemos”

Dice Joanna Burkey, CISO de HP, que es necesario saber mucho y tener visibilidad; que la ciberseguridad no es solo tarea del CISO; que se debe tener cooperación y colaboración con personas de toda la empresa; que no estar abierto a que el mundo cambie es lo que puede hacer fracasar a un CISO y que en ciberseguridad no todo es tecnología.

Joanna Burkey, CISO de **HP**

Joanna Burkey es la CISO de HP desde abril de 2020. Antes trabajó durante varios años en Siemens AG, donde fue directora global de ciberdefensa asociada a infraestructura de IT/OT, así como productos, soluciones y servicios. Hablamos con ella durante la Amplify Partner Conference que se ha celebrado en Chicago la última semana de marzo, donde la directiva salió al escenario para decirle a los más de dos mil partners congregados y el medio centenar de medios y analistas acreditados al evento que “la seguridad no es negociable”; que una estrategia de seguridad “no significa nada si no se tienen las herramientas y los servicios adecuados que la respaldan”; y que la seguridad es compleja y cambiante, antes de hablar de HP Wolf Security, la propuesta de seguridad integrada de la compañía para los puntos finales. Un día después de la ponencia, Ciberseguridad TIC tuvo la oportunidad de mantener una entrevista con Joanna Burkey para hacerle algunas de las preguntas de siempre, como cuáles son los grandes retos de un CISO. La respuesta no se hizo esperar: “Uno de los mayores desafíos es tratar de averiguar lo que no sabemos”, dijo, añadiendo que es necesario “saber mucho y tener visibilidad”. Un segundo reto, decía Burkey,

ciberseguridadTIC

Tai editorial

ENTREVISTAS

es que la ciberseguridad no es sólo tarea del CISO, o de la organización del CISO, sino que está en manos de todo el equipo de TI; "cualquier cosa que yo, como CISO, pueda hacer para trabajar y habilitar a mis contrapartes de TI ayuda, porque mi organización establecerá una estrategia y estableceremos metas", aclaraba.

Le preguntamos por la ventaja que supone trabajar en una empresa que fabrica los dispositivos con los que trabajan sus empleados y, por tanto, solo tiene que administrar endpoints de la casa. ¿Es una CISO con suerte? "Tengo mucha suerte porque puedo usar las herramientas de HP para agregar más capas de seguridad a lo que hacemos. Pero también soy realista y sé que en el mundo híbrido la gente trabaja desde todo tipo de dispositivos, y lo sabemos. Así que incorporo a mi estrategia la máxima visibilidad para que pueda funcionar incluso cuando las personas no están en su sistema HP".

Sobre las cualidades que cree que debe tener un buen CISO, identifica Joanna Burkey "la capacidad de crear y mantener relaciones en la

> "No estar abierto a que el mundo cambie es lo que puede hacer fracasar a un CISO"

empresa". Explicó que los días en los que un CISO podía decir simplemente, 'haz esto', se han acabado. "Hemos de tener cooperación y colaboración con personas de toda la empresa", por lo que una de las habilidades que debe tener un buen CISO es "la capacidad de construir relaciones. Trabajamos con la gente para llegar a decir sí en lugar de simplemente decir no".

¿Qué puede hacer que un CISO fracase? "No estar abierto a que el mundo cambie, como cualquier profesión. Si comienzas a pensar que solo lo que sabes es la única forma en que es, y no estás mirando a tu alrededor para ver qué está cambiando, qué es diferente, qué nueva tecnología está llegando, definitivamente te dolerá", respondió la directiva.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

> "La capacidad de crear y mantener relaciones en la empresa" es una de las cualidades que debe tener un CISO

Sobre los desafíos del trabajo híbrido, que es una de las principales propuestas de negocio de HP, menciona Joanna Burkey la visibilidad, porque hay muchas cosas de las que debes estar al tanto, así como "procesos realistas que las personas puedan seguir", porque la gente trabaja ahora de una manera diferente.

"La concienciación es sumamente importante", asegura al CISO de HP, y no solo para proteger a una empresa y a un empleador, "sino también para que las personas sepan cómo estar seguras en casa y puedan transmitir buenas prácticas a sus hijos y a su familia. Quiero que la gente viva su vida con seguridad. Y ahora que las personas están trabajando en tecnología todo el tiempo, las cosas que les enseñamos en el trabajo harán que sus vidas y sus familias sean más seguras. Es mi esperanza".

Planteadas las tecnologías de seguridad que considera indispensables en cualquier empresa mencionaba la CISO de HP que, con el trabajo híbrido, "un requisito es que los terminales deben tener seguridad. Y los terminales no son solo portátiles, son cualquier cosa". El hecho de que no podamos confiar solo en una red centralizada o servidores centralizados, hace que "tengamos que dispersar nuestra seguridad".

En seguridad, ¿todo es tecnología? "No", respondió Joanna Burkey. Aseguró que la tecnología es importante, pero también la capacidad de comunicarse, y también los procesos y la gobernanza. "Tener la mejor tecnología del mundo no significa nada si no está activada o si las personas no siguen las políticas adecuadas.

Ente las tecnologías que cobrarán cada vez más importancia menciona el *browser isolation*, o aislamiento de la navegación, así como la seguridad del firmware y de la BIOS apuntando que, aunque las estrategias de seguridad aún no se han centrado realmente en ello, "no es porque no sea importante, sino porque hay mu-

ciberseguridadTIC

Tai editorial

> "Tengo mucha suerte porque puedo usar las herramientas de HP para agregar más capas de seguridad a lo que hacemos"

cho más que hacer". Aseguraba también que se están viendo ataques exitosos creados por personas que pueden comprometer y reescribir la BIOS de una máquina, lo que significa que es "es una amenaza emergente que tenemos que planificar por ahora".

Los últimos años han demostrado que, en general, las empresas invierten cada vez más en seguridad, y sin embargo cada vez más ataques con éxito, incluido el rey de las amenazas, en *ransomware*. ¿Qué es lo que está pasando? Habla la CISO de HP de 'The Security Poverty Line', que divide a las empresas en dos categorías: aquellas que pueden implementar bien las medidas esenciales de seguridad y aquellas que no pueden. Esta línea es "una de las razones por las que HP innova en el área en la que innovamos. Queremos brindar seguridad accesible en los sistemas que estas empresas ya tienen porque puede ser muy difícil para ellas comprar productos totalmente nuevos", decía Burkey, añadiendo que hay una brecha entre las empresas que pueden mantenerse al día con lo que necesitan. Por otra parte, no hay que olvidarse del problema de recursos humanos en ciberseguridad; "no hay suficiente gente, y eso es parte del problema", aseguraba.

ENLACES DESTACADOS

"Elastic se ha introducido en el mundo de la seguridad con una aproximación XDR"

Virtual Cable: "La virtualización es un mecanismo para subsanar la falta de concienciación del usuario"

ciberseguridadTIC

Tai editorial

“La seguridad de la cadena de suministro se debe abordar con un modelo basado en Zero Trust”

Dice Francisco Sánchez Nauffal, director de seguridad IT de EcoVadis, que lo que puede hacer fracasar al CISO es que no tenga el apoyo del negocio; que lo que más le preocupa es el Shadow IT, que la tecnología de *deception* está ganando mucho peso; que es fundamental poder rodearte del talento adecuado, no solo internamente, sino también a nivel de proveedores; y que la centralización de procesos de seguridad será tendencia.

Francisco Sánchez Nauffal, director de seguridad IT de **EcoVadis**

Francisco Sánchez Nauffal es el director de Seguridad de EcoVadis, una compañía que tiene como propósito guiar a las empresas hacia un mundo sostenible proporcionando calificaciones reconocidas en todo el mundo. La pasión por el mundo cíber le llegó desde bien joven, cuando reconoce haberse acercado al lado del mal, aunque nunca fue “nada serio”.

Dice Francisco Sánchez Nauffal que, con la industrialización del cibercrimen, el gran reto del CISO no solo es saber detectar, sino también responder a tiempo y tener un mecanismo que no dependa de personas para tener cierto nivel de seguridad, “y eso cada vez es más complicado”. De forma que, en la parte más técnica, el reto está en “poder transformar lo que es la pura detección, que es donde los CISOs nos solíamos focalizar, en la detección y la respues-

ciberseguridadTIC

ta. Que sea la propia automatización la que, con ciertos parámetros, te mantenga a un nivel aceptable de seguridad, hasta que una persona pueda entrar a ver lo que ha ocurrido".

En la parte menos técnica, menciona Sánchez Nauffal que, aunque el puesto de CISO puede ser diferente de empresa a empresa, "lo que no cambia son los niveles de ansiedad, la necesidad de estar siempre disponible y alerta, nunca bajar la guardia, y mantener todo seguro al mismo tiempo, siempre en preparación por el día que esperamos que nunca llegue pero que sabemos que inevitablemente llega a todas las empresas. Y creo que eso no es sano".

Si hablamos de las cualidades que debe tener un buen CISO, menciona Francisco Sánchez Nauffal que un aspecto que se está observando cada vez más es que "el CISO no tiene necesariamente que ser una persona técnica" y que "tenemos que hablar el lenguaje del negocio". Comenta también que es curioso que "el negocio empiece a hablar también el lenguaje de seguridad. Es decir, me parece que a poca gente se le escapará lo que es un *ransomware*, o lo que es un *phishing*, porque al final son cosas del día a día. Y eso facilita esa comunicación bidireccional".

> "Lo que más me preocupa, en general, es lo que se conoce como el Shadow IT"

Relacionado con la ansiedad, o cómo reducirla, también considera importante el directivo la capacidad que debe tener un CISO de gestión de terceros; "es fundamental el poder rodearte del talento adecuado, no solo internamente, sino también a nivel de proveedores que ayuden a colaborar en mantener un entorno lo más seguro posible".

Resalta Sánchez Nauffal que un CISO que no tenga capacidad de gestión, "es bastante improbable que tenga un futuro muy largo. Lo que esperan de ti como CISO no es que seas una figura de autoridad, sino un habilitador de negocio".

Amenazas

En un mercado tan saturado de fabricantes, soluciones y propuestas, ¿cómo se escoge la solu-

ciberseguridadTIC

Tai editorial

ENTREVISTAS

> "Lo que puede hacer fracasar a un CISO es que no tenga el apoyo del negocio"

ción de seguridad adecuada? "Que haya tanta oferta facilita que las empresas podamos ser un poquito más exigentes con lo que buscamos", asegura el directivo, añadiendo que "raro sería que no hubiera nadie en el mercado que pudiera darme lo que yo necesito". Comenta también Francisco Sánchez Nauffal que, a la hora de buscar proveedores, "somos especialmente exigentes con aquello que verdaderamente es importante para nosotros", al tiempo que considera que, en general, debería evitarse el "intentar adaptar lo que hacemos, nuestros procesos, solamente porque queremos una solución o una plataforma concreta. Lo que tiene que hacer la plataforma es adaptarse a la manera de actuar de la empresa".

¿Qué amenaza le quita el sueño a Francisco Sánchez? "Lo que más me preocupa en general, es lo que se conoce como el Shadow IT", asegura el directivo; "que yo despliegue una serie de mecanismos de accesos, un entorno seguro para que mis empleados puedan trabajar y que, por conveniencia o porque prefieren hacerlo de otra forma, se busquen otras maneras y no sepamos detectarlo. Al final eso se suele traducir en situaciones de *data leak*, en aceptar condiciones de herramientas gratuitas en las que estás cediendo los derechos de información y cosas de este estilo. Esto es lo que más me preocupa, pese a que es algo que entiendo y es inherente

ciberseguridadTIC

Tai editorial

al comportamiento involuntario humano, aunque intentamos establecer mecanismos de concienciación para reducir este riesgo".

La seguridad de la cadena de suministro está recibiendo cada vez más atención y se están haciendo aproximaciones muy interesantes para, de alguna manera, exigir o garantizar que la cadena de suministro trabaje con una cierta seguridad. Cuando preguntamos a Francisco Sánchez Nauffal cómo se está abordando desde EcoVadis la seguridad de la cadena de suministro, responde que se piden ciertos niveles de garantía dependiendo del tipo de información que se trabaje con terceros. En todo caso, se apuesta por el modelo Zero Trust, "no porque no haya una confianza con el tercero, sino precisamente porque uno no sabe qué le puede haber pasado al tercero y cómo, a través de un tercero, te puede pasar algo a ti".

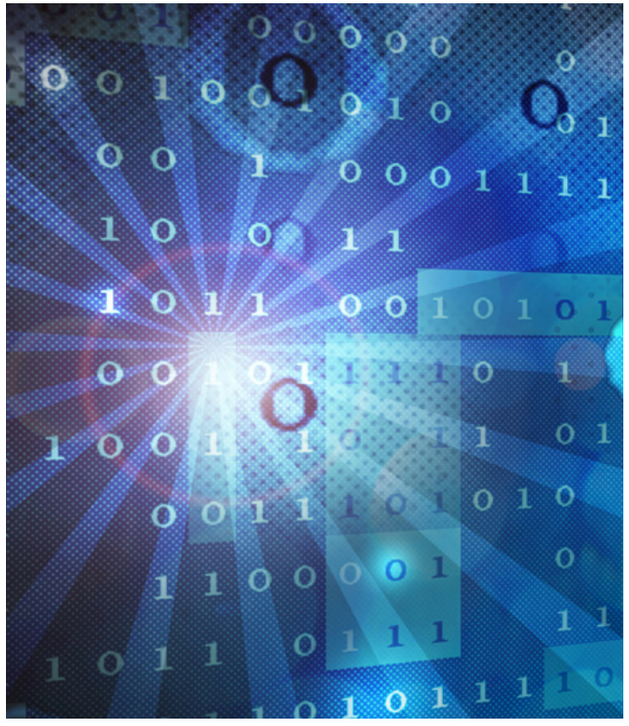
Tecnologías

Planteado qué tecnologías de seguridad considera imprescindibles en cualquier empresa,

"La centralización de procesos de seguridad será tendencia"

identifica Sánchez Nauffal la capacidad de detección y respuesta automática, "que para mí es fundamental. Es más, sin esa capa se me hace muy difícil justificar por qué se necesitan el resto de capas de seguridad, porque tú implementas medidas de seguridad en base a las cosas que ves o que anticipas con idea de protegerte ante esas posibles amenazas". Por lo tanto, "lo importante es tener la capacidad de detección".

Mirando hacia el futuro, tiene claro el director de seguridad de EcoVadis que la tecnología de *Deception* "va a ganar mucho peso". La tecnología de *Deception*, o de engaño, es una categoría de soluciones de ciberseguridad que detectan amenazas en una fase temprana con bajos índices de falsos positivos. La tecnología despliega señuelos realistas (por ejemplo, dominios, bases de datos, directorios, servidores, aplicaciones, archivos, credenciales, migas de pan) en una red junto a activos reales para que actúen como señuelos. En el momento en que un atacante interactúa con un señuelo, la tecnología empieza



a recopilar información que utiliza para generar alertas de alta fidelidad que reducen el tiempo de espera y aceleran la respuesta a incidentes. En opinión de Sánchez Nauffal "esta tecnología ganará mucho peso y nosotros la estamos analizando para para ver cómo podemos beneficiamos al máximo de ella".

> "Que haya tanta oferta facilita que las empresas podamos ser un poquito más exigentes con lo que buscamos"

También será tendencia, en opinión del CISO de EcoVadis, "la centralización de procesos de seguridad", que implica el no trabajar con tantas tecnologías diferentes, con tantos proveedores distintos, "sino buscar a alguien que sea mi especialista en todas esas tecnologías que estoy utilizando. Y esto me parece que aporta más valor que una tecnología concreta porque haya cierto gap".

"Lo que puede hacer fracasar a un CISO es que no tenga el apoyo del negocio", responde el responsable de ciberseguridad de EcoVadis. Explica que, ante una situación de crisis, "es fundamental que se tenga ese apoyo y esa complicidad entre el CISO y el resto del Comité Ejecutivo. Si no tienes ese apoyo, si el comité directivo no confía en ti como experto de ciberseguridad, tienes todas las de perder, independientemente de lo que hagas".

ENLACES DESTACADOS

Iberdrola: "De cara a futuro va a ser muy importante la convergencia de tecnologías"

Armis: "Hoy es más necesario que nunca que los equipos de IT, OT y ciberseguridad trabajen en la misma dirección"

“Ni la inteligencia artificial ni la automatización son magia”

Dice Daniel Zapico, Associate Partner de IBM Cybersecurity Services, que la compañía siempre ha sabido adaptarse al mercado y tener una cierta visión de futuro; que, junto con la seguridad de las identidades y los datos, los servicios de Zero Trust, son los más demandados; que detrás de la inteligencia artificial y la automatización hay mucha investigación y mucho profesional, y que la amenaza estrella sigue siendo el *ransomware*.

Daniel Zapico,
Associate Partner de **IBM Cybersecurity Services**

En los consejos de dirección de las empresas existe una preocupación mucho mayor en materia de ciberseguridad. Lo dice Daniel Zapico, ahora Associate Partner de IIBM Cybersecurity Services, y quien durante los últimos años ejerció como CISO en diferentes empresas, la última, Air Europa. En opinión del directivo, el aumento de los ciberataques y el contexto geopolítico parece estar removiendo conciencias en sectores como el industrial, telecomunicaciones o sanidad, menos maduros en ciberseguridad que otros como el bancario y asegurador, obligados por la regulación.

Preguntado por la demanda del mercado y la evolución de la oferta de la compañía, que tiene propuestas en tornos a la seguridad del cloud del dato, amenazas internas, *ransomware*, XDR, Zero Trust... responde Zapico que una de las cualidades de IBM es que siempre “ha sabido adaptarse al mercado y tener una cierta visión de futuro”, además de saber “centrarse en los servicios de valor”.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

La compañía se fundó en 1911 como Computing-Tabulating-Recording Company, o CTR, para renombrarse como International Business Machine, o IBM, en 1924 después de la fusión de cuatro empresas; es la empresas tecnológica con más patentes, ha realizado decenas de adquisiciones y entre sus invenciones pueden mencionarse el cajero automático, el disquete, el disco duro o la memoria RAM. Recuerda Daniel Zapico que la compañía reorganizó su estructura en dos unidades de negocio: IBM Technology, más centrada en producto (hardware y software), e IBM Consulting, que es donde está la parte de Cybersecurity Services, además de otros servicios de valor en torno a la transformación digital o entornos cloud.

En opinión del Daniel Zapico, "el valor que tiene IBM es no conformarse con la presencia que ya tiene en el mercado, sino querer aportar soluciones de valor". Añade que lo que más se está demandando es "la seguridad en cloud, seguridad de las identidades y seguridad de los datos", algo que, asegura, tiene todo el sentido porque "sabemos que el punto de entrada del ataque son las identidades y el objetivo final los datos, lo que les convierte en dos elementos importantísimos para las compañías". Junto con las seguridad de las identidades y los datos, los servicios de Zero Trust, o Confianza Cero, es el tercero que más demanda tiene (junto con Seguridad en Cloud), muy en la línea de la transformación de las compañías.

> "Entre los servicios que la compañía presta a sus clientes está el ayudarles a adoptar modelos llamados de cripto agilidad, o Crypto Agility"

ciberseguridadTIC

Tai editorial

ENTREVISTAS

Al mercado le gusta cada vez más hablar de inteligencia artificial y de automatización, pero hay que plantearse cómo puede garantizarse esa inteligencia y cómo puedes garantizar esa automatización. Preguntado por cómo lo están abordando las empresas según la experiencia de IBM, asegura Daniel Zapico que "ni la inteligencia artificial ni la automatización son magia. Detrás de estos dos elementos hay mucha investigación, mucho profesional y muchos años de desarrollo".

Sin identificarse como un experto, habla el directivo de IBM Cybersecurity Services de una inteligencia artificial basada en algoritmos, en identificación de patrones y de anomalías, todo lo cual es muy tangible. Lo mismo ocurre con la automatización, asegura, añadiendo que "desde el punto de vista de IBM lo importante no es la

> "La seguridad en cloud, seguridad de las identidades y seguridad de los datos es lo que más se está demandando"

inteligencia artificial per sé, o la automatización per sé, sino qué se consigue con ello. Lo que buscamos es la eficiencia". Y en esa búsqueda de la eficiencia habla Zapico de cualquier actividad que no aporte valor, como son las actividades repetitivas, detección de patrones... cosas que requieren mucho trabajo manual o muchísimo esfuerzo.

Añade que una de las cosas que se ha percibido en los últimos años es que los atacantes son cada vez más eficientes, que los defensores tienen que ser iguales y que "la inteligencia artificial y la automatización ayudan en la reducción de costes y a poner foco en lo que aporta valor".

ciberseguridadTIC
Tai editorial

ENTREVISTAS

Clientes

IBM es una empresas con muchos años de vida, que a lo largo de su historia se ha ido transformando y cuyos servicios y propuestas solo estaban al alcance de unos pocos con billetera abultada. ¿Ha cambiado la visión que se tiene de IBM? Responde Zapico que, efectivamente, la empresa lleva muchos años en el mercado, que tradicionalmente se ha trabajado con clientes muy grandes que siguen siendo importantes para la compañía, "pero eso no quita que tenga sentido, y de hecho lo hacemos, colaborar con compañías pequeñas, incluso startups". Añade que no hay que perder de vista que el foco es la transformación, tanto tecnológica como de procesos o de negocio, y "las startups son precisamente compañías que están muy dispuestas a ello. Son compañías que adoptan tecnología, y sobre todo tecnología moderna porque está en su propia naturaleza. Están dispuestas a transformar en modelos más ágiles, y eso es una de las cosas que hacemos en IBM Consulting".

Computación Cuántica

La computación cuántica es un tema relevante para IBM, que lleva muchos años muy comprometida con el desarrollo de sistemas avanzados. Fue en 2019 cuando la compañía presentó el IBM Q System One, el primer ordenador cuántico para uso comercial. La computación cuántica tiene un impacto directo en la seguridad porque su capacidad de cómputo puede adivinar las claves de cifrado tradicionales. Para

ciberseguridadTIC
Tai editorial

ENTREVISTAS

> "El valor que tiene IBM es no conformarse con la presencia que ya tiene en el mercado, sino querer aportar soluciones de valor"

hacer frente a la situación, IBM ha participado en la co-creación de tres de los cuatro algoritmos seleccionados por el NIST en Estados Unidos, algoritmos que ya están incluidos en productos de la compañía y que se postulan como garantes de la seguridad.

Además, entre los servicios que la compañía presta a sus clientes está el ayudarles a adoptar modelos llamados de cripto agilidad, o Crypto Agility, que no es otra cosas que "tener la capacidad de reemplazar algoritmos que en un momento dado pueden considerarse débiles por otros más robustos, o Quantum Safe de una manera ágil".

Índice anual de inteligencia de amenazas

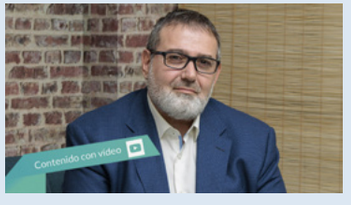
Lanzado recientemente el IBM Security X-Force Threat Intelligence Index 2023, pedimos a Daniel Zapico una valoración del mismo. Le llama la atención que el sector más atacado haya sido el de manufactura o industria, por encima del sector financiero. La reflexión lleva a Daniel Zapico a comentar que la lectura que se puede obtener de lo que está pasando es que los ciberdelincuentes "son cada vez más eficientes y más eficaces y además van variando las técnicas y los mecanismos de ataque".

También resalta el directivo que "los principales mecanismos de ataque y objetivos que se están persiguiendo son, sobre todo, la extorsión", que pone de manifiesto que lo que buscan los ciberdelincuentes es la monetización de los ataques.

No se olvida de destacar que, desgraciadamente, la estrella de los informes, año tras año, es el *ransomware*, que llega a producir una triple extorsión, "algo que vamos viendo desde hace muchísimos años y no parece que cambie".

ENLACES DESTACADOS

"Elastic se ha introducido en el mundo de la seguridad con una aproximación XDR"



Vectra AI:
"La visibilidad de la red es crítica"

“Nuestro presupuesto de I+D es de un millón de euros. Creemos que, si no hay innovación, no hay capacidad de aportar valor añadido”

BeDisruptive es una empresa joven que, en muy poco tiempo, ha dado mucho que hablar. Para unos, se está posicionando como el principal competidor de Telefónica en el mercado de SOCs, para otros, es un gran misterio que mirar de reojo y, los menos, no saben de dónde ha salido.

Alejandro Aliaga, General Co-Director de **BeDisruptive**

Para desvelar incógnitas y conocer a BeDisruptive, Ciberseguridad TIC habla con Alejandro Aliaga, General Co-Director de la compañía, quien empieza a contarnos que la aventura comienza en el país vecino, en Italia, un mercado bien conocido por uno de los tres socios de la compañía, que también ejerce como CEO, José Ángel Delgado. Sobre Italia, dice Alejandro Aliaga que tiene un nivel de madurez diferente al español y que es donde “vimos una oportunidad de negocio muy grande” porque, entre otras cosas, hay menos MSSP, o proveedores de servicios de seguridad gestionada, que es a lo que se dedica la compañía.

BeDisruptive aterriza en 2016 en Roma, desde donde se presta servicio a toda Italia. Asegura Alejandro Aliaga que el talento español está muy valorado en Italia, que España está muy bien posicionada en ciberseguridad y que “todo el conocimiento de los expertos que tenemos en España nos ha permitido trabajar mucho, y muy bien, en Italia”.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

> "Escuchar a los clientes, entender dónde están y acompañarlos, es una de las cosas que queremos hacer. Y eso es un punto diferenciador"

BeDisruptive inicia su actividad en Roma, cuando lo habitual es que las empresas tecnológicas se establezcan en Milán... "Sí, pero no hemos descartado Milán", donde la compañía tendrá presencia a finales de año. Se opta por Roma porque es donde está la Administración pública, que es cliente objetivo de la compañía, junto con otros sectores, como Industria y Banca. En todo caso, haciendo honor al nombre, la compañía establece el SOC en la capilla de un antiguo convento de techo abovedado.

El objetivo de la compañía es apoyar la transición tecnológica y proteger la información y los activos de sus clientes. Asegura Aliaga que BeDisruptive busca a sus clientes en la mediana y gran cuenta y que al cliente no solo hay que darle confianza, sino que hay que acercarse a él y escucharle.

Se ofrecen servicios de SOC, que van desde la monitorización de la seguridad, toda la parte de detección y respuesta, inteligencia de amenazas o seguridad ofensiva, que se apoya en consultoría para "tener una oferta que ayude al cliente a entender dónde está y dónde quiere llegar en esa transformación digital" de una forma diferente porque "es importante no llegar vendiendo una caja. Escuchar a los clientes, entender dónde están y acompañarlos es una de las cosas que ya estamos haciendo mejor que nadie. Y eso es un punto diferenciador". Por cierto, que si el SOC de Roma es disruptivo por estar en un antiguo convento, el

ciberseguridadTIC

Tai editorial

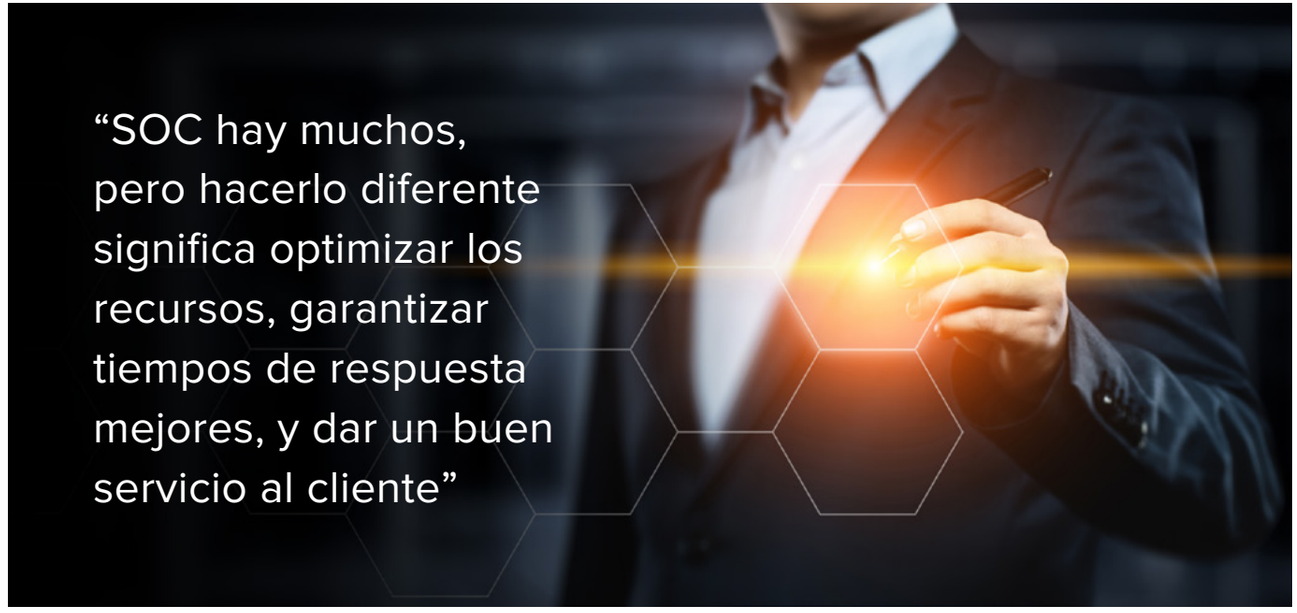
de Madrid podría ser el más alto de España al estar en una planta 33. Parece que la cuestión es diferenciarse.

Definiendo BeDisruptive como una "boutique tecnológica", la compañía quiere estar "con aquellos clientes que de verdad quieran y aprecien esa calidad". Añade Aliaga que esto no significa "que la gente no pueda estar con nosotros. Cualquier empresa que de verdad quiera estar bien atendida, que se le cuiden todos los detalles, que se esté muy pendiente de ellos... que nos llamen. Estaremos encantados de trabajar con ellos".

SOC

Respecto a los SOC, otra cosa que se dice es que BeDisruptive está haciendo las cosas de una manera diferente. Se habla tanto del iSOC, o SOC inteligente, como de una apuesta por SOC alineados con el mundo industrial, que es donde se espera una gran oportunidad de negocio.

Menciona Alejandro Aliaga que se ha realizado una gran inversión. "El presupuesto que hemos dedicado a I+D es de un millón de euros porque creemos que, si no hay innovación, no hay capacidad de aportar un valor añadido" dice el directivo, añadiendo que se ha creado una red de SOC que están federados.



En opinión de Aliaga, SOC hay muchos, "pero hacerlo diferente significa optimizar los recursos, garantizar tiempos de respuesta mejores y dar un buen servicio al cliente, indistintamente de quién esté detrás como operador".

También destaca Alejandro Aliaga el valor humano, el contar con profesionales que vienen de haber trabajado en varios centros de operaciones de seguridad: "para hacer SOC diferentes, tienes que tener experiencia, tienes que venir de un pasado. Nos hemos sentado con ellos y les hemos pedido que intenten cambiar las cosas que saben que no funcionan, que piensen en cómo lo harían de forma diferente". En esto consiste ser disruptivo, ser BeDisruptive, asegura el directivo; "ser disruptivos no es

ciberseguridadTIC

> "Si todo sigue funcionando como hasta ahora y la aceptación que hemos tenido continúa, creemos que vamos a crecer muchísimo más"

hacer las cosas totalmente opuestas, es hacerlas un poco diferentes. Y en esa pequeña diferencia es donde está el valor que aportamos", pues la experiencia previa, el conocimiento de la plantilla y aprender de los errores es lo que aporta ese valor diferencial.

La página web de la compañía es escueta, algo que ha alimentado, nos dicen que adrede, el misterio en torno a BeDisruptive. Dice Alejandro Aliaga que siempre intentan rodearse de los mejores *players*, y deja caer algunos nombres, referentes del mercado, como Palo Alto, Tenable, o Splunk, que se suman a otros no mencionados y a "otros muchos que están por llegar. Nosotros estamos siempre muy pendientes de cuáles son esas tecnologías que nos ayuden a dar un buen servicio. Lo que queremos es rodearnos de los mejores".

Economía

Según información pública a la que ha accedido Ciberseguridad TIC, la compañía ha pasado de facturar unos 23 millones de euros en 2019 a casi 50 millones en 2021. ¿Cómo se consiguen estas cifras? Responde Alejandro Aliaga que

ENTREVISTAS

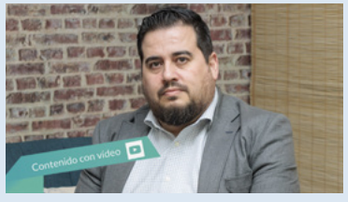
BeDisruptive lleva trabajando desde 2016 en el mercado italiano, un mercado que, recuerda, es 2,5 veces el PIB español, un territorio muy grande "que nos ha permitido hacer un volumen de negocio muy alto".

Respecto a las previsiones, "si todo sigue funcionando como hasta ahora y la aceptación que hemos tenido continúa, creemos que vamos a crecer muchísimo más. Sin poder decirte unos números exactos, se esperan cifras bastante más grandes, además de presencia en otros países".

Otros países, que incluyen la apertura de oficinas en Panamá "y, si todo va bien, porque al final es complejo abrir nuevos mercados, estaremos el año que viene en Estados Unidos", concretamente en Washington.

En el mercado también se comenta que BeDisruptive está haciendo una fuerte apuesta económica para la contratación de talento. Lo cierto es que a sus filas se suman cada vez más empleados. Reconoce el General Co-Director de la compañía que encontrar talento es muy complicado, y más en Italia que en España. "Para poder conseguir que ese talento venga a nosotros, al final tenemos que enamorar a la gente", y esa capacidad de enamorar está en las oficinas, en la inversión en tecnología, en cómo se cuida al empleado... "y poco a poco hemos tenido ese efecto llamada" que no solo ha ayudado a que parte del mercado les mire de reojo, sino a que "crezcamos tan rápido". CST

ENLACES DESTACADOS



Engie: "Los CISO somos habilitadores y estamos cada vez más cerca del negocio"

Bitdefender: "El mercado está sufriendo la irrupción de la inteligencia artificial al servicio de los hackers"

“Las compañías están mucho más abiertas de lo que ellas mismas pueden suponer”

Dice María Rojo que emprender en España en durísimo, pero que merece la pena; que los datos no están controlados, entre otras cosas porque las empresas son ecosistemas vivos y cambiantes; que Kartos es el buque insignia de la compañía, capaz de escanear las tres capas de la red: Internet, darkweb y deepweb; y pide que, por una vez, se regule a tiempo cuando le preguntamos por ChatGPT.

María Rojo, CEO de **Enthec**

María Rojo es la CEO de Enthec, una empresa de la que se dice que es el caso de éxito del mundo de la ciberseguridad. El camino no ha sido fácil, ni rápido. “Enthec nace de mi experiencia profesional. Vi que realmente había una carencia, un campo donde la ciberseguridad tenía que crecer” nos cuenta su fundadora. Explica que el mercado estaba muy acostumbrado a mirar de puertas para dentro, “y se nos olvidaba todo lo que hay de puertas para afuera, que es la mayoría”.

Mientras desarrollaba su trabajo en Airbus Militar, María Rojo empezó a realizar pruebas de concepto, “y cuando me fui a llevar mi pequeño monstruo a más de 100 empresas que visité para ver si tenía algún sentido”, empezó a ver la cara de terror de los responsables a los que enseñaba todo lo que esa empresa tenía expuesto en Internet. La pregunta ¿pero tú de dónde has sacado todo esto? fue la base del nacimiento de Enthec.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

La compañía fue creciendo poco a poco y, en opinión de María Rojo "si podemos ser un caso de éxito fue el cambio enorme que supuso Enthec antes y después de INCIBE". Fue durante la celebración de ENISE 2021 cuando Kartos, el buque insignia de Enthec, recibió el primer premio del programa de aceleración de empresas emergentes 'Cybersecurity Ventures'. María Rojo recogió un cheque por valor de 34.000 euros por su solución de monitorización. Este cambio, dice hoy la directiva, "supuso un cambio radical para la compañía".

El dato

Hace tiempo que se habla del dato como el activo más importante de la empresa. De hecho, es uno de los sitios donde se ha colocado el perímetro de seguridad perdido con la llegada de la movilidad y la nube. ¿Están controlados los datos? "Si te dijera que sí perdería mi trabajo", responde entre risas María Rojo. Asegura que no se pueden controlar los datos al cien por ciento, entre otras cosas porque las empresas son entidades vivas; "tanto la parte más virtual, como son las máquinas, como la parte de las personas, es un ecosistema vivo. La gente manda correos, comparte archivos, los sistemas se conectan... Las compañías están mucho más abiertas de lo que ellas mismas pueden suponer. Así que el dato está ahí fuera, y la pena es que hayamos tardado tanto en darnos cuenta de la grandísima importancia que tienen los datos".

> "Emprender en España es durísimo. Pero merece la pena"

Preguntada por lo que suele encontrarse cuando va a ver a los clientes, la respuesta no puede

ser más clara: “Una ignorancia total de lo que tienen ahí fuera”. Explica que cuando se ve la herramienta, Kartos, funcionando, cuando ven los documentos expuestos firmados por el director, con su rúbrica, su DNI, el correo, teléfono, código fuente de aplicaciones móviles bancarias, documentos de marketing con todos los planes estratégicos de la compañía… “se echan las manos a la cabeza y preguntan ¿cómo ha llegado todo eso ahí? Lo interesante es mirar para fuera a la vez que para dentro”, asegura María Rojo.

Explica la fundadora que Enthec tiene “cientos de robots monitorizando, ingestando la información a nuestros sistemas, donde se tiene una capa de tratamiento de datos y de inteligencia artificial muy potente, y a las empresas le damos lo que realmente les interesa, la información de valor para ellos”.

Enthec escanea las tres capas de la red: Internet, darkweb y deepweb. Apunta María Rojo que se tiende a pensar que la darkweb es solo TOR, pero hay muchas más, y que Enthec está en cinco de ellas. Lo que hace Kartos es buscar información que suponga tanto un riesgo de ciberseguridad, como competitivo o reputacional de la compañía. Aclara que Kartos no es una herramienta de reputación, sino que se centra en que pueda haberse filtrado algún documentos interno de la empresa que pueda suponer un riesgo.

Cliente y cadena de suministro

Empresas grande o pequeñas, con mucha o poca presencia en Internet y pertenecientes a cualquier vertical son clientes potenciales de Enthec, porque “las empresas son todas lo mismo: sistemas y archivos”, dice María Rojo.

Añade que la herramienta ha de estar totalmente automatizada y que se ofrecen distintos tipos de licencias para distintos tamaños de compañías. “Tenemos desde pequeños bufetes de abogados, pequeñas compañías industriales

hasta aseguradoras o hidroeléctricas. Lo más interesante es que ya no solamente cubrimos a la compañía, sino que ayudamos a la compañía a cubrir todas las terceras partes de la misma a las que podemos escanear y mirar tranquilamente porque, al no ser intrusivos, podemos mirar también cómo está la seguridad de tus socios, de tus compañeros de negocio".

Canal, emprendimiento y ChatGPT

Enthec vende exclusivamente a través de canal de distribución. Es algo que, en opinión de María Rojo, "tiene todo el sentido del mundo" porque cuando un cliente ve todo lo que sale de la herramienta lo que plantea es: ¿quién me arregla esto? El apoyo del canal se vio rápidamente porque "nosotros no hacemos consultoría y buscamos el socio adecuado que ayude a nuestros clientes".

> "Al no ser intrusivos, podemos mirar también cómo está la seguridad de tus socios, de tus compañeros de negocio"

Emprender en España es... "durísimo. Todo lo que diga es poco. Pero merece la pena", asegura María Rojo, aun reconociendo que "gubernamentalmente se está haciendo un esfuerzo tremendo, que hay muchas subvenciones a empresas tecnológicas".

Comenta, desde su experiencia, que muchos proyectos fracasan porque "no saben dónde se

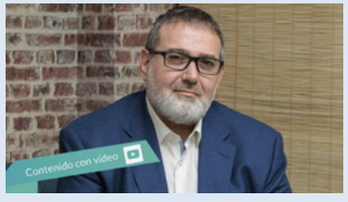
> "La pena es que hayamos tardado tanto en darnos cuenta de la grandísima importancia que tienen los datos"

están metiendo. Algunos dan un paso atrás y no aguantan lo que a veces hay aguantar. Yo siempre digo lo mismo, es durísimo, no te voy a engañar, pero de verdad merece muchísimo la pena. Conoces a gente maravillosa y haces cosas que no harías en ningún otro contexto".

Ya que vuestra herramienta integra inteligencia artificial, ¿qué opinión te merece ChatGPT?

"Más que opinión yo lo que haría aquí es un llamamiento. Pediría a políticos, juristas, abogados y toda la gente que hacen las leyes y normas que nos rigen que, por favor, por una vez no lleguen tarde a regular esto. Porque bien utilizado es potentísimo, pero puede que mal utilizado o sobre utilizado nos lleve a muchos problemas". CST

ENLACES DESTACADOS



Vectra AI:
"La visibilidad de la red es crítica"

Hillstone Networks:
"La complejidad es el activo más caro"

ciberseguridadTIC

editorial

“Hay que fortificar el acceso a la identidad digital”

Daniel Rodríguez es el director general de Redtrust, una compañía que proporciona una gestión integral del ciclo de vida de los certificados digitales en las organizaciones. A pesar de llevar muchos años en activo, ha sido a raíz de la pandemia cuando el uso del certificado digital se ha disparado. El proceso de digitalización en el que se ha visto inmerso el mundo entero, y la explosión del teletrabajo, han provocado un incremento del uso del certificado digital tanto para autenticarse como para firmar digitalmente.

Daniel Rodríguez, director general **Redtrust**

Desde 2019, Redtrust forma parte de Keyfactor, multinacional experta en soluciones de criptoagilidad y PKI en la nube. En abril de 2021 PrimeKey, creadora de EJBCA, se incorpora al grupo. Una alianza clave para la definición de estrategias IAM, tendencia que apunta a una mejora en la gestión de los accesos de usuarios al entorno corporativo y donde el certificado digital adquiere gran relevancia.

La custodia de los certificados digitales se ha vuelto crucial para la gestión de la identidad digital y las estrategias de ciberseguridad de las organizaciones. De hecho, un estudio realizado por Redtrust recoge que el 37 % de compañías españolas tiene previsto establecer mecanismos para la gestión de identidad de usuarios y dispositivos

Planteado que el futuro de la ciberseguridad gira alrededor de la gestión de la identidad, preguntamos a Daniel Rodríguez cuáles son las principales amenazas contra la identidad. Responde el directivo que no sólo hay que tener en cuenta la identidad digital de usuarios, clientes o partners, sino los controles de acceso o la seguridad del propio dato. En todo caso, asegura, la principal amenaza para la identidad digital es

ciberseguridadTIC

Tai editorial

ENTREVISTAS

la propia “suplantación de la identidad”, lo que lleva a que haya que “fortificar el acceso a la identidad digital de cada uno de los empleados y de los usuarios en general”.

Desde el punto de vista de la seguridad, el empleo del certificado digital como vector de ataque y su uso ilícito para suplantar la identidad de los usuarios, son dos aspectos que las empresas deben tener en cuenta. Resaltan desde Redtrust la importancia de la custodia de los certificados en un gestor especializado para obtener un mayor nivel de control y protección sobre ellos

Para el 78 % de empresas la gestión de la identidad de usuarios es una prioridad alta a la hora de detectar situaciones de seguridad anómalas. El certificado digital se convierte en el mecanismo de autenticación más robusto para verificar la identidad del usuario. Su inclusión en las estrategias IAM permite asegurar la gestión y control de accesos de los empleados a la red, sistemas o nube de la empresa.

Entre los retos a la hora de proteger la identidad digital no sólo menciona Daniel Rodriguez el propio acceso, sino “la verificación de que quien está detrás de esa identidad digital sea quien realmente tiene que ser”. Asegura el director general de Redtrust que en la verificación se ha avanzado muchísimo; menciona la

> “Tener los certificados digitales centralizados hace que el administrador de la propia plataforma tenga una facilidad de uso que antes no tenía”

existencia de los OTP y sistemas biométricos y dice que “debajo de todo esto tiene que haber una fortaleza en cuanto a la criptografía, en cuanto a comunicación segura, en cuanto a no repudio”. Tiene claro el directivo que la base de la identidad digital tiene que ser el certificado digital, “o al menos esa infraestructura de clave pública que puede garantizar esa comunicación segura”.

El certificado digital es el medio más utilizado por las empresas para blindar la seguridad de su identidad digital y de sus comunicaciones *online* con otras entidades u organismos públicos. Además, su uso a nivel interno ofrece numerosos beneficios a la hora de asegurar la integridad y el no repudio de la información. Por medio del certificado las empresas se autentican, realizan y agilizan trámites electrónicos: gestión de pagos e impuestos, presentación de licitaciones, contrataciones, etc., firman digitalmente documentos, cifran emails y archivos o restringen el acceso a datos confidenciales, entre otros casos de uso. “Poder centralizar esos certificados y gestionarlos de una manera mucho más amigable” es la propuesta de valor de Redtrust. Asegura su director general que el hecho de poder tener los certificados digitales centralizados “hace que el administrador de la propia plataforma tenga una facilidad de uso que antes no tenía”, una usabilidad que es muy importante a la hora de proporcionar seguridad y que lleva al directivo a decir: “No creemos que pueda ser posible incrementar la seguridad sin detrimento de la usabilidad. No funciona”.

Más que el aumento de la cantidad de identidades digitales, la normativa es lo que está impulsando más el negocio de Redtrust. Reconoce Daniel Rodríguez que en España la normativa es favorable a este tipo de productos y soluciones;

"Latinoamérica es un mercado creciente y muy interesante"

"el hecho de que la Administración Pública haya forzado a las empresas a tener el certificado digital para autenticarse frente a sus servicios favorece y genera todo este tipo de negocio".

Menciona también el directivo la concienciación como otro de los impulsores del negocio; "el que las empresas consideren la suplantación de identidad como una amenaza real hace que la mayoría de las empresas apuesten por este tipo de soluciones".

¿Qué métodos están utilizando las empresas para verificar la identidad de los usuarios? ¿se tiene en cuenta que las máquinas también son identidades? El sistema de clave pública, que es en el que se basa la tecnología de Redtrust, se basa también en una verificación presencial. Explica Daniel Rodríguez que cuando se emite un certificado "tiene que haber una presencialidad para demostrar que la persona que está emitiendo el certificado es quien dice ser", que anteriormente "había también los certificados jurídicos que solamente representaban a la empresa, pero que no tenían personalidad asociada", pero que con las nuevas normativas ya no es así y "siempre tiene que haber un representante legal asociado a ese certificado que representa a la empresa".

Esto implica una doble vertiente, porque el certificado es de una persona, pero representa a una empresa, "con lo cual hay intereses cruzados a la hora de verificar quién está detrás de

ENTREVISTAS

una operación, si es la persona o la empresa". Comenta Daniel Rodríguez que en estos casos la verificación, o el asegurarse de que quien está emitiendo un certificado es quien dice ser, "se tiene que seguir haciendo casi al estilo clásico", y asegura que se ha avanzado mucho en vídeo personación de los certificados, pero que al final "tiene que haber un contacto persona a persona, aunque sea por videollamada, para verificar que la persona es quien dice ser".

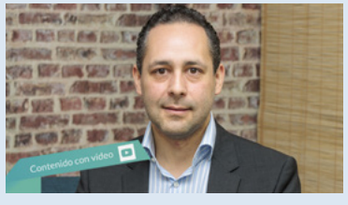
En cuanto a las máquinas, "aunque hay puntos de mejora, se ha avanzado bastante", dice el director general de Redtrust. Explica que hasta hace unos años se emitían certificados de empresa sólo con tener un correo que tuviese el dominio de esa empresa, lo que generaba puntos de fallo, y de mejora. "Ahora las empresas que emiten certificados que van a ser utilizados no por usuarios sino por máquinas, ya tienen más puntos de verificación".

> "Verificar que quien está detrás de una identidad digital sea quien realmente dice ser es un reto"

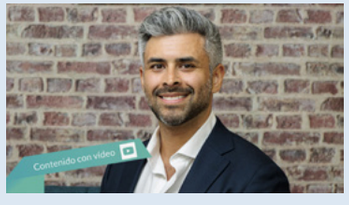
Entre los clientes tipo de Redtrust está el que, sin tener por qué tener un negocio grande, "tiene necesidad de gestionar muchos certificados digitales o tienen una interacción habitual con la administración pública, que suelen ser empresas que están fuertemente reguladas". Una segunda tipología de cliente es la gran cuenta, que normalmente hacen uso de los certificados en un ámbito mucho más extenso. Al final la compañía tiene una solución "para todo tipo de empresas", desde las que tienen muchos usuarios y pocos certificados, a las que tienen muchos certificados y pocos usuarios.

De cara a este 2023, las previsiones de la compañía son las de seguir creciendo. Además, el camino hacia la internacionalización iniciado en 2022 continuará este año; explica Daniel Rodríguez que se han empezado a hacer acciones en Latinoamérica, "donde hemos visto un mercado creciente y muy interesante".

ENLACES DESTACADOS



"El paso de la criptografía tradicional hacia la protección con algoritmos post cuánticos requiere tiempo" (Utimaco)



Semperis: "La protección y resiliencia del Directorio Activo es la protección y resiliencia de negocio"

Ransomware, ¿qué hay detrás de los titulares?

La amenaza del *ransomware* se ha instalado en el día a día de empresas, administraciones públicas y usuarios, y ya no es extraño ver sus efectos en las noticias. En medio de este panorama, es vital comprender cómo y por qué los ciberdelincuentes tienen éxito con tanta frecuencia. Esta información proporcionará la base sobre la cual las organizaciones se protegerán en el futuro.

Para hablar de tendencias, herramientas o técnicas que están permitiendo que los actores de *ransomware* prosperen, así como que medidas pueden tomar las empresas para administrar el riesgo y reforzar sus defensas, Ciberseguridad TIC ha organizado un debate en el que han participado portavoces de empresas relevantes del sector: Josep Albors, director en investigación y concienciación de ESET España; Álvaro Fernández Díez, Sales Manager Iberia de Sophos; Sergio Martínez, country manager de SonicWall Iberia; Santiago Campuzano, Country Manager Veeam Iberia y Raúl Guillén, Director de Estrategia de Ciberseguridad de Trend Micro.

Empezamos preguntando a nuestros invitados por la situación y evolución del *ransomware*,

DEBATES

una amenaza que ha pasado de ser indiscriminada a impactar contra empresas cada vez más grandes a las que se les exige rescates millonarios. Los ataques de *ransomware*, dicen los expertos, son cada vez más dirigidos y complejos, y ya no solo amenazan con cifrar la información, sino con hacerla pública.

También pedimos a nuestros invitados que identifiquen los retos a los que se enfrentan los responsables de ciberseguridad. Se menciona el reto cultural, la existencia de soluciones inconexas y mal operada y una ciberseguridad mal operada

Los EDR (Endpoint Detection and Response) han ocupado su lugar como la solución de seguridad para los puntos finales. Ya no sólo se trata de identificar y detectar un ataque, sino de responder. La llegada de los EDR, ¿ha mejorado la defensa contra el *ransomware*?

Para muchos el *ransomware* se soluciona con una buena copia de seguridad. Además, ¿habría que focalizarse en la recuperación? Dicen los expertos que el *backup* y la recuperación tienen que estar totalmente alineados y que hay que comprobar que esté bien hecho.

Por último, hablamos de la figura del negociador y preguntamos si hay que sorprenderse de la existencia de casos como el del Hospital Clínic de Barcelona.

Accede al debate completo, así como al resumen del mismo y los vídeos de los participantes descargando el documento.

Afrontando los ciberataques con una aproximación Zero Trust

Zero Trust es una evolución significativa de la seguridad de red tradicional que confiaba automáticamente en los usuarios y puntos finales dentro del perímetro de la organización. Este nuevo modelo de confianza cero requiere que las organizaciones monitoricen y validen continuamente que un usuario y su dispositivo tienen los privilegios y atributos correctos, lo que supone adoptar políticas de múltiple factor de autenticación, de gestión de identidades, control de accesos, etc.

Para hablar de qué viene a solucionar el modelo Zero Trust, por qué hay que adoptar el modelo, qué pilares aborda o cuál es el papel del endpoint, Ciberseguridad TIC ha celebrado un debate que ha contado con la presencia de Julio Valpuesta Hernández, EMEA Security Transformation Architect de Symantec Iberia; Eusebio Nieva, director técnico de Check Point Iberia; José Luis Paletti, Senior Presales Engineer de WatchGuard Iberia; Isabel López, Sales Engineer Manager de Samsung Iberia y Miguel López, Sales Ingenieer de Trend Micro Iberia.

ciberseguridadTIC

Tai editorial

DEBATES

Empezamos preguntando a nuestros invitados qué viene a solucionar el modelo Zero Trust y por qué hay que adoptarlo. La pérdida de perímetro, el aumento de la superficie de ataque y poder ofrecer una seguridad más homogénea son algunas de las razones aportadas durante el debate.

También preguntamos a los expertos cuáles son los principales pilares que aborda el modelo Zero Trust. Identifican el principio de privilegios mínimos, verificar siempre, control de accesos o controlar qué está utilizando el usuario como las bases del modelo.

A la hora de hablar de cómo debe implementarse un modelo de confianza cero se habla de planificación, de identificar la información sensible o de saber lo que se tiene antes de abordarla.

Está claro que el mayor impacto a la hora de adoptar una estrategia de Zero Trust es el empleado. ¿Cómo se logra ese equilibrio entre la adopción de este modelo y la buena experiencia de usuario? Es otra de las preguntas que planteamos para el debate.

Por último, planteamos a nuestros invitados cuál es el papel del endpoint en los modelos de confianza cero. Todos coinciden en que es "básico para la implementación de protección Zero Trust".

Accede al debate completo, así como al resumen del mismo y los vídeos de los participantes descargando el documento.

PCI DSS 4.0: Nueva etapa en la ciberseguridad bancaria

Después de leer infinidad de artículos y explicaciones sobre cómo afecta esta nueva PCI DSS 4.0 (estándar mundial que proporciona una línea base de requisitos técnicos y operativos diseñados para proteger los datos del titular de tarjetas), la conclusión de Javier Martín-Moreno, Líder Técnico Ciberseguridad Sopra Steria España, es que los cambios en la propia banca cada vez son más rápidos.

MÁS INFORMACIÓN

Los ciberataques en el sector sanitario aumentan cerca de un 50% en 2022: la ciberseguridad sigue siendo un reto

José Antonio Sánchez Ahumada, Sales Director Iberia de Claroty, asegura en esta tribuna que la escasa visibilidad, comunicación y coordinación entre las partes interesadas en seguridad, biomédicas, de ingeniería clínica y empresariales crea brechas que convierten en casi un imposible la mitigación de los riesgos.

MÁS INFORMACIÓN

Cómo abordan los desarrolladores la seguridad desde el diseño

Para Massimiliano Costa, fundador y CEO de Develhope, es clave que los desarrolladores y los programadores aprendan a comprobar si los códigos fuente adquiridos de tercero son legítimos, ya que el uso de paquetes de software y código de fuente abierto para construir y mantener los sistemas puede dar lugar a ciertas vulnerabilidades.

MÁS INFORMACIÓN