ciberseguridadTIC

Tai editorial

Cuadernos

ciberseguridadTIC
seguridad en informática y comunicaciones
Tai editorial

Año I Nº 1 • Bimensual

Enero - Febrero 2024

Entrevistas:

Ángel Gálvez, CISO de Avolta:
"A un servicio gestionado le pido proactividad"

Amador Aparicio de la Fuente, CISO de Zunder:
"Lo que marca la diferencia de una organización a otra es el tiempo de respuesta"

IR A PÁGINA ANTERIOR

IR A PÁGINA SIGUIENTE

EDITORIAL

Primer Cuaderno CST

Rosalía Arroyo
rosalia@taieditorial.es

Inmersos en el día a día, noticia a noticia, y evento tras evento, vamos recogiendo el pulso a un sector, el de la ciberseguridad, extremadamente dinámico y más amplio de lo que a simple vista pudiera parecer. Porque, siendo ciberseguridad, no es lo mismo proteger una red que un dispositivo, controlar los datos o las identidades, hablar de herramientas o de arquitecturas. Y así, semana tras semana nos atragantamos de información de todo lo que llega al mercado, de todo lo que ocurre, de todo lo que se reinventa sigla a sigla.

Realizar entrevistas a actores claves dentro de un mercado específico ofrece un valor incalculable para comprenderlo en profundidad y obtener una visión más completa del mismo. Si se trata de los responsables de ciberseguridad o TI de las empresas, llegamos a entender sus verdaderas necesidades, preocupaciones y retos, que difieren no solo dependiendo del tamaño de la empresa, sino del sector en el que se mueven, del lastre de una tecnología adoptada años atrás o incluso de un futuro que promete mucho más de lo que puede ofrecer.

Las entrevistas permiten obtener información que no siempre se encuentra disponible en fuentes de datos tradicionales como estudios de mercado o informes. Al interactuar directamente con los participantes del mercado, se puede obtener información extra sobre sus opiniones, comportamientos y motivaciones.

A través de las entrevistas se puede contextualizar la información recopilada y comprender mejor las dinámicas del mercado. Esto permite identificar factores relevantes que pueden influir en las decisiones de las empresas.

Las entrevistas pueden ayudar a identificar nuevas oportunidades de mercado o a comprender mejor las necesidades insatisfechas de los consumidores. Pueden ser una herramienta útil para construir relaciones con actores claves del mercado. Esto puede ser beneficioso para obtener información en el futuro, realizar colaboraciones o acceder a nuevos recursos. Y eso es lo que nos ha llevado a agrupar las entrevistas que vamos publicando en la web de Ciberseguridad TIC en estos Cuadernos CST que llegarán al mercado cada dos meses. Nos estrenamos con el que estás viendo en un formato digital con una cuidada maquetación. Esperemos que te guste.

Rosalía Arroyo

“Veracode: Si yo tengo una aplicación que lleva años funcionando, voy a encontrar miles de vulnerabilidades”

Para Eduardo García Sancho, responsable de Veracode para la región de Iberia, cómo generar código de forma segura sin que sea una interrupción en el ciclo de trabajo de los desarrolladores es la principal solicitud de los clientes de la compañía, que en sus 17 años de vida ha analizado varios trillones de líneas de código de miles de aplicaciones.

Eduardo García Sancho, responsable Veracode Iberia

Veracode es una empresa fundada en 2006 que ofrece múltiples tecnologías de análisis de seguridad en una única plataforma, incluido el análisis estático (o pruebas de caja blanca), el análisis dinámico (o pruebas de caja negra) y el análisis de composición de software. La compañía presta servicios a más de 2.500 clientes en todo el mundo y lleva evaluadas varias decenas de miles de millones de líneas de código. Desde hace más de un año y medio Eduardo García Sancho es quien dirige la compañía en la región de Iberia tras haber ocupado otros puestos de responsabilidad en Syneto, KEMP Technologies o SMC. Hablamos con él la evolución de la compañía en un mercado, el de Application Security Testing (AST), en el que Veracode ha sido considerada líder durante más de ocho años.

Como plataforma de análisis de seguridad de aplicaciones, Veracode proporciona una serie de herramientas para detectar y analizar vulne-

ENTREVISTAS

rabilidades en el código fuente de las aplicaciones. En los últimos años la compañía ha realizado mejoras en la plataforma "para ofrecer un sistema de seguridad más intuitivo y mucho más integrable en los ciclos de desarrollo", nos cuenta Eduardo García Sancho, añadiendo que se ofrece información sobre las vulnerabilidades detectadas en las aplicaciones, incluidas el saber de dónde provienen o qué tipo de vulnerabilidades son; "el último paso es la remediación de las mismas. Es fundamental, y es donde más hemos evolucionado".

Clientes

Preguntado por el perfil de cliente de Veracode, responde el directivo que, en general, "cualquiera que tenga una aplicación desarrollada por ellos mismos, o por un tercero para ellos mismos". Identifica dos grandes grupos de clientes. Los primeros son entidades grandes que por su tamaño tienen una serie de aplicaciones y portales, bien sea para uso interno o externo, que son altamente explotables.

> "El segundo gran diferencial de Veracode es que somos la oferta más completa del mercado"

Además, hay un segundo grupo de clientes que tienen equipos de desarrollo de aplicaciones para terceros y, por tanto "están especializadas en el desarrollo de software". Con este tipo de clientes se hace hincapié no sólo en que entreguen a los clientes una buena aplicación en el tiempo correcto, "sino que también sea segura". En opinión de Eduardo García la disputa entre estos fabricantes de software y sus clientes es "entender que la seguridad no es opcional, que debe ser obligatoria".

Aunque quizá deberían ir de la mano, menciona

ENTREVISTAS

> "Asimilar que la seguridad es mejor integrarla antes que no después es un aspecto fundamental"

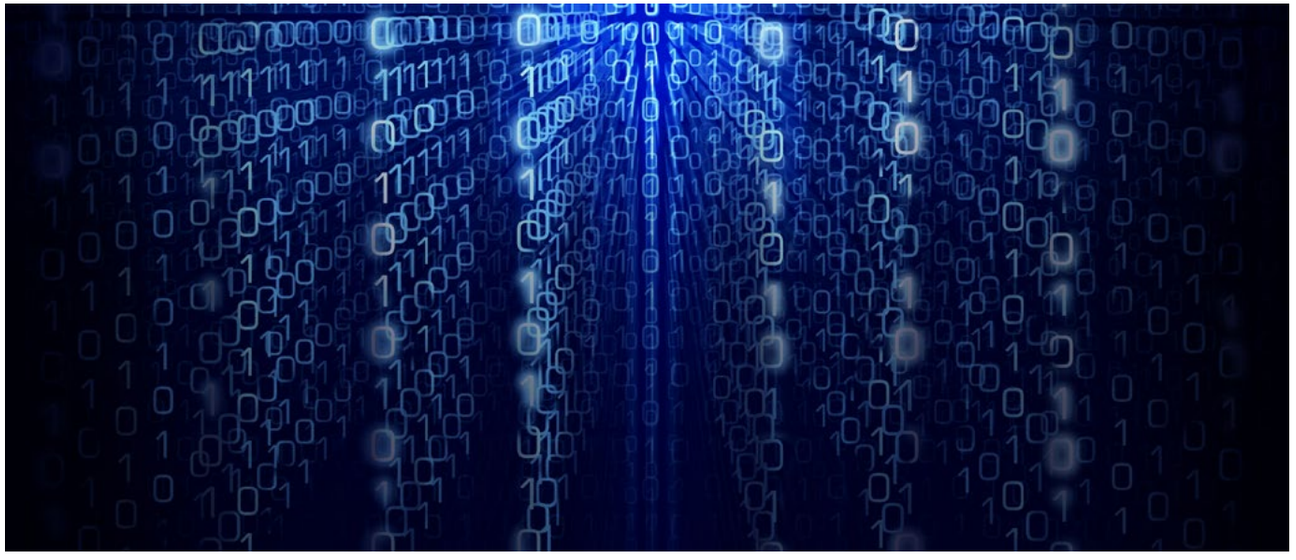
el directivo de Veracode que cuando se habla de desarrollo de software el mercado diferencia entre calidad y seguridad; "el hecho de que una aplicación sea funcional, fluida y utilizable hace referencia a la calidad, mientras que el concepto de seguridad es que no sea vulnerable". Añade que el concepto de la calidad del software se ha asumido enseguida, mientras que la seguridad "en la mayoría de los casos no está asimilada todavía y se está empezando a integrar", impulsadas por directivas como el ENS o Dora.

Retos

"El principal hándicap que hay en seguridad hoy en día es el equipo", asegura Eduardo García Sancho cuando le preguntamos por los retos que llevan a sus clientes a buscar una empresa como Veracode. Comenta que los equipos de desarrollo no quieren verse molestados por temas de seguridad, y mucho menos que se paralice su trabajo, mientras que el equipo de seguridad quiere influir en el equipo de desarrollo para que desarrolle con seguridad. "Cómo generar código de forma segura sin que sea una interrupción en el ciclo de trabajo de los desarrolladores es la principal solicitud de los clientes", asegura el directivo, añadiendo que lo que buscan son herramientas integrables y automatizadas que no interrumpan el trabajo del equipo de desarrollo, y ofrezcan la información necesaria al equipo de seguridad para que pueda tomar las decisiones correctas y hacer las modificaciones de código correctos "ralentizando el desarrollo lo menos posible".

El segundo reto es "el conocimiento". Porque una vez que se incorpora la herramienta de Veracode, ¿cómo se gestionan las vulnerabilidades detectadas y como se aprende a desarro-

ENTREVISTAS



llar sin generar tantos fallos? Para dar respuesta a este reto, la compañía no solo ofrece formación dentro de la plataforma, sino, y algo que se valora muchísimo, "conceptos como inteligencia artificial que me ayuda a auto remediar ese código que se detecta vulnerable y cambiarlo a código no vulnerable. Y es donde estamos avanzando muchísimo".

Aunque lo ideal es empezar de cero, lo más frecuente es que el cliente con el que se empieza a trabajar ya tenga varias aplicaciones con varios años o meses de antigüedad, y que la aplicación esté en el ciclo de entrega o de producción. Explica el directivo de Veracode que, dependiendo del tipo, los análisis pueden ser inmediatos, de pocos minutos, horas o un día, y añade que "el principal problema no es cuánto tiempo tardo en analizar la aplicación o en qué parte del ciclo de desarrollo está la aplicación, sino en los resultados. Si yo tengo una aplicación que lleva años funcionando voy a encontrar miles de vulnerabilidades".

El siguiente paso, dice Eduardo García, es cómo gestiono la resolución de esa cantidad

> "El principal hándicap que hay en seguridad hoy en día es el equipo"

de vulnerabilidades. El primer paso, explica el directivo es poder categorizar esos fallos "para empezar a solucionar lo más severo, lo más explotable", al tiempo que se ayuda al cliente a entender su postura de seguridad.

Respecto a los lenguajes de programación con el que esté escrito el código, Veracode soporta más de cien lenguajes de programación y frameworks diferentes.

Diferencial

Llevar 17 años siendo una plataforma en la nube, una plataforma SaaS es, según nos cuenta Eduardo García, el principal diferencial de Veracode respecto a su competencia. Son 17 años "analizando varios trillones de líneas de código, miles y miles de aplicaciones, y miles y miles

ENTREVISTAS

de clientes. Y todos esos datos anonimizados forman parte de nuestra capacidad de aprendizaje", dice el responsable de Veracode en España, añadiendo que, una vez que se detecta una vulnerabilidad, se identifica y se comparte con toda la base de clientes de la compañía.

Frente a la nube, las plataformas on-premise requieren una serie de infraestructuras. Y lo más destacado es que la información del análisis del sofware que realizaba cada compañía se quedaba en su poder, no se compartía el conocimiento, "con lo cual el resto de los clientes no se han aprovechado nunca de la inteligencia de las detecciones, del conocimiento, que individualmente cada uno podía aportar. Y esto redunda en que nosotros estamos ahora en un porcentaje inferior al uno por ciento de falsos positivos".

El segundo gran diferencial de Veracode "es que somos la oferta más completa del mercado". La compañía ofrece una amplia variedad de opciones, desde el análisis estático al dinámico, pasado por el análisis de librerías de terceros, análisis de infraestructura y de contenedores, pentesting-as-a-service, formación, sistemas de remediación, servicios específicos para ayudar a gestionar las vulnerabilidades encontradas e inteligencia artificial aplicada a la remediación. "Ahora mismo no hay ningún competidor en el mercado que dé una oferta tan completa", asegura Eduardo García, quien añade que es muy fácil empezar a trabajar con Veracode y obtener resultados fiables.

La oferta de la compañía se ofrece a través de una plataforma a la que también pueden integrarse sistemas de reporting o de información de terceros. "Nuestra plataforma ofrece capacidades de gobernanza y de analítica muy potentes que son integrables con distintos sistemas", asegura Eduardo García.

> "Nuestra plataforma ofrece capacidades de gobernanza y de analítica muy potentes que son integrables con distintos sistemas"

ENTREVISTAS

Veracode Fix

La Inteligencia Artificial es, en opinión del directivo, el elemento que ha marcado un hito dentro de la compañía. Explica que todos los clientes tienen el mismo problema: no poder abordar la resolución de vulnerabilidades. Saber que se tienen 7.523 vulnerabilidades de las que 150 son altamente explotables genera una situación insostenible en un mercado que, además, adolece de personal. La propuesta de la compañía para este problema es Veracode Fix. Los datos de 17 años y miles de clientes "me han proporcionado la capacidad de entrenar una inteligencia artificial solamente con datos comprobados por nuestros consultores", dice Eduardo García, incidiendo en que no se utiliza open source ni datos de codificación externos a la plataforma de la compañía. Ese conocimiento permite a los clientes aceptar una propuesta de corrección y cambio de código en el momento en que se detecta una vulnerabilidad; "eso es un avance inmenso", asegura, "porque no solo tengo una capa de control, que es el análisis que hacemos del código, sino de corrección que hace la inteligencia artificial".

Añade Eduardo García sobre Veracode Fix que es un hito enorme "porque en esas conversaciones con los clientes les quitas un problema que ya no es relativo a cómo me enfrento a la seguridad, sino cómo me enfrento a falta de personal, a presupuesto que no tengo y a tiempo que me falta. Solucionar de un plumazo estos tres aspectos es un antes y un después".

Lanzado el pasado verano y disponible para los lenguajes de programación principales (Java, JavaScript, PHP y Python), Veracode Fix está siendo adoptado por el 90 % de los nuevos clientes de la compañía. Además, es habitual que los clientes lo adquieran en los procesos de renovación de contratos.

Adquisiciones

Fundada en 2006, Veracode caminó en solitario durante casi diez años. En 2014 tres de los cuatro grandes bancos de la lista Fortune 100 eran clientes de la compañía. En marzo de 2017, dos años después de intentar una salida a bolsa que no se cumplió después de haber recaudado 40 millones en una ronda de inversión liderada por Wellington Management Company, la compañía fue comprada por CA Technologies por 614 millones de dólares en efectivo.

Poco duró el idilio, porque en julio de 2018 Broadcom anunció la compra de CA Techno-

ENTREVISTAS

logies por 18.900 millones. Una vez cerrado el acuerdo, Broadcom vendió Veracode a Thoma Bravo por 950 millones de dólares. Cuatro años después, en marzo de 2022, Veracode fue vendida a otra gran firma de inversión, TA Associates, por 2.500 millones de dólares.

Bajo el paraguas de TA Associates, Veracode ha realizado dos adquisiciones: Jarooma en abril de 2022 y Crashtest en diciembre del mismo año. Preguntado por el impacto que estas adquisiciones han tenido en la compañía, resalta la de Jarooma, que es la base de Veracode Fix. Explica el directivo que Jarooma se compró por su tecnología de auto remediación a la que "le faltaba el ser alimentada con conocimiento para poder hacer todo el trabajo que hace". Jarooma, asegura, "nos dio esa capacidad de inteligencia artificial que, con los datos que nosotros teníamos, ha evolucionado".

En cuanto a Crashtest Security, "viene a complementar nuestro análisis dinámico". Explica que Veracode cuenta con una tecnología de análisis dinámico "extremadamente potente, muy profundo. Pero muchos clientes nos pedían algo más sencillo". Con Crashtest la compañía ofrece una doble capa de análisis dinámico en función de los intereses del cliente: si es un análisis profundo se utiliza el análisis dinámico estándar de Veracode, y si se quiere un análisis superficial, muchísimo más rápido e integrado en el ciclo de desarrollo de las principales vulnerabilidades que voy a ver en la superficie, se utiliza Crashtest, que hoy ha evolucionado y se llama Veracode DAST (Dynamic Application Security Testing) Essentials.

> "Bajo el paraguas de TA Associates, Veracode ha realizado dos adquisiciones: Jarooma en abril de 2022 y Crashtest en diciembre del mismo año."

Crecimiento

El crecimiento de la compañía va de la mano de la integración de la seguridad dentro del ciclo de desarrollo. Para Eduardo García, "asimilar que la seguridad es mejor integrarla antes que no después es un aspecto fundamental".

Un segundo impulsor del crecimiento es la normativa. Al respecto menciona el responsable de Veracode para la región de Iberia el Esque-

ENTREVISTAS

ma Nacional de Seguridad, Dora o NIS2 comentando que resulta sorprendente que haya muchas empresas que no todavía no han dado pasos para cumplir con esta última.

A estas normativas públicas, se le une una exigencia privada que también impulsa el negocio de Veracode y que viene de la mano de los ciberseguros, "que cada vez están piden unos requerimientos más altos. De forma que, si quiero conseguir una cobertura relativamente amplia a un precio relativamente razonable, tengo que mostrar que mi postura de seguridad es amplia. Y en la parte de aplicaciones es fundamental poder decir que se ha codificado de forma segura. Ahí es donde también estamos tratando con muchísimos clientes".

Respecto al interlocutor de Veracode, se habla con el CISO, "que tiene un interés especial por su responsabilidad es la seguridad de la empresa", y con el responsable de desarrollo. "El caso ideal es que haya un especialista en seguridad de las aplicaciones, que suele ser el interlocutor que más nos interesa", explica Eduardo García.

El peligro de la IA

Entre las muchas cosas que se les atribuyen a las diferentes herramientas de IA Generativa, como Chat GPT, es su capacidad de generar código. Lo que en principio puede parecer una ventaja, o un peligro si quien lo utiliza es el ciberdelincuente, puede crear un verdadero problema si no sabemos de dónde coge el código esa IA generativa, porque lo que puede generar es un código inseguro que además pueda tener incluso problemas de derechos de autor.

En opinión de Eduardo García, "son herramientas interesantes y de futuro para ayudar en ciertas parcelas, pero es importante que tengamos la comprobación de seguridad de lo que estoy codificando. Si yo sé que todas las herramientas, y es el 100% de ellas, que hacen generación de código se han alimentado de fuentes open source, sé que la propia generación de código es inseguro, lo cual hace más importante la utilización de herramientas de comprobación de ese código".

ENLACES DESTACADOS

El 32% de las aplicaciones tienen fallos de seguridad en su primer escaneo

Veracode: "A pesar de la velocidad y eficiencia que la IA aporta al desarrollo de software, no necesariamente produce código seguro"

Ángel Gálvez: "A un servicio gestionado le pido proactividad"

Tiene claro Ángel Gálvez, CISO de Avolta, que tener una actitud positiva es una de las principales cualidades de un CISO, así como capacidad de formación; que ahora mismo, tener un buen backup es tener un backup libre de ransomware; que los datos son la joya de la corona en cualquier empresa; que se apuesta por el servicio gestionado, pero que "el conocimiento se tiene que quedar en la casa"; que la ciberinteligencia será una tecnología imprescindible y que a veces no es necesario tener la mega plataforma con la última tecnología, "sino algo más sencillo que explotes al 100 %".

Ángel Gálvez, CISO de **Avolta**

Ángel Gálvez es el CISO de Avolta, la compañía resultante de la combinación de los negocios de Dufry y Autogrill. Se estrenó en el mundo de la ciberseguridad a través de un proyecto de continuidad de negocio, "de los primeros que se hacían en España", en los tiempos en los que, en lo que a ciberseguridad se refiere, lo habitual era la autoformación.

Tras más de doce años en AXA, donde ocupó diferentes puestos relacionados con la ciberseguridad, Ángel Gálvez se convirtió en Global CISO de Dufry en julio de 2019. Habla de esta última etapa como una de las más retadoras; una etapa que le ha permitido desarrollar la ciberseguridad de Dufry prácticamente desde cero. El siguiente paso en su carrera es la integración de cuatro compañías totalmente diferentes, tanto desde el punto de vista tecnológico como de madurez o cultura que no solo afectan a la parte cíber, sino a todos los niveles de negocio de IT; "que todas estas empresas sigan con la misma actividad desde el punto de vista de negocio con impacto cero y que todo sea mejorando la seguridad es un reto", asegura el CISO Global de Avolta.

ENTREVISTAS

> "Tener una actitud positiva es una de las principales cualidades que debería tener un buen CISO"

Preguntado por las principales cualidades que debería tener un CISO, tiene claro Ángel Gálvez que la primera es "tener una actitud positiva". Añade la capacidad de formación, tener la mente abierta a todo lo que pueda ocurrir, estar alineado con la parte de negocio, tener flexibilidad, así como tener una "buena comunicación y relación con todos los elementos de la empresa, porque al final somos una unidad transversal que damos servicio a toda la organización".

Respecto a las prioridades que establece en materia de ciberseguridad, tiene claro Ángel Gálvez que lo principal "es hacer las cosas básicas" para mantener el negocio operativo. ¿Cuáles? "Corrige las vulnerabilidades, controla a tus usuarios privilegiados, controla el perímetro y que los usuarios de tu empresa tengan buena concienciación y hagan su día a día de forma segura y de forma lógica", dice el directivo, explicando que la mayoría de los incidentes se generan por fallos en los procesos de seguridad y control básicos (vulnerabilidades, protección del perímetro, gestión de usuarios, etc,).

Menciona también el backup como un elemento básico de la ciberseguridad y aclara que, ahora mismo, "tener un buen backup es tener un backup libre de ransomware y con fácil recuperación para que el tiempo de indisponibilidad sea el menor posible".

Asegurando que la protección del dato a nivel global es clave, identifica la fuga de información como el tipo de amenaza que más le preocupa; "además, con todos los sistemas abiertos, y la flexibilidad que hay en trabajos y dispositivos,

ENTREVISTAS

cada vez es más complicado proteger el dato", comenta. Otro elemento en el que se pone foco en Avolta es la disponibilidad de los servicios y aplicaciones de negocio.

En un mercado saturado de fabricantes y propuestas, ¿cómo escoger? Hay varios criterios, dice Ángel Gálvez. Uno de ellos es "la experiencia que puede haber de esa herramienta en otras compañías", además del "soporte y evolución de la misma", así como la capacidad de integración que tenga con otras soluciones tecnológicas, "y las funcionalidades que te va a aportar, cómo se adapta lo que tú necesitas".

Hace tiempo que se habla de la pérdida del perímetro de seguridad tradicional que algunos colocan en los datos, y otros en la identidad. En opinión de Ángel Gálvez eso depende de cada empresa, aunque "los datos son la joya de la corona de cualquier empresa". En el caso de Avolta, que el dato es estratégico para el negocio está claro a nivel de comité ejecutivo, y sobre el dato se va construyendo el resto de protección de la información. No significa que la identidad no sea también muy importante para la compañía, sobre todo relacionada con el dato: quién accede a que dato, cuándo, cómo... "pero las

> "Tener un buen backup es tener un backup libre de ransomware y con fácil recuperación"

identidades las puedes reconstruir, y si pierdes los datos tu negocio deja de funcionar".

El mercado de servicios gestionados no deja de crecer. Según datos de Allied Market Research, se llegarán a los 77.010 millones de dólares en 2023, con un crecimiento medio anual del 12,8 % hasta entonces. Avolta no es ajena a esta tendencia y en la compañía existen diferentes servicios gestionados. Lo que tiene claro Ángel Gálvez es que "el conocimiento se tiene que quedar en la casa". Explica que a veces se externaliza tanto que el conocimiento se va fuera "y luego puede haber problemas en la continuidad de las operaciones".

¿Qué le pides a un servicio gestionado? "Proactividad y experiencia", asegura Ángel Gálvez.

ENTREVISTAS

Comenta que muchos servicios gestionados son pasivos y que hay poca proactividad en el sentido de: voy a entender tu negocio y te voy a proponer mejoras con respecto a tu negocio. Es decir, a los servicios gestionados les falta personalizar, saber adaptarse al negocio o necesidades del cliente.

"La pérdida de confianza" es lo que haría fracasar como CISO a Ángel Gálvez. Explica que incluso cuando ocurre un incidente, y a quien no le ha ocurrido le va a ocurrir, "si hay confianza en que las cosas se están haciendo bien no pasa nada, se corrige, se aprende, se mejora y se continúa trabajando más fuerte".

> "Las identidades las puedes reconstruir, pero si pierdes los datos tu negocio deja de funcionar"

Preguntado por qué tecnología cree que será imprescindible en un futuro no muy lejano, a un medio plazo, tiene claro Ángel Gálvez que se irá a tener la máxima proactividad posible en seguridad, y no reactividad. Explica que siempre quedará una base de reactividad, pero que "hay que moverse lo máximo posible a ser más proactivos, el adelantarse a todo lo que te pueda ocurrir". ¿Ciberinteligencia? "Exactamente", responde el directivo añadiendo el uso de tecnologías que añadan inteligencia al comportamiento humano, así como la gestión del riesgo en tiempo real y poder establecer servicios adaptativos a ese nivel de riesgo, "de forma que, sin preocuparte, automáticamente se vaya cambiando la capacidad de protección y de seguridad en aquellos servicios más críticos". Tiene también claro Gálvez que la tecnología que lo hace posible está disponible para la venta, "pero todavía no hay suficiente madurez para implementarla".

Preguntamos también al Global CISO de Avolta por la tendencia de las plataformas. Y es que en el mercado de ciberseguridad se ha pasado de un 'best of breed' que, entre otras cosas, ha

ENTREVISTAS

> "A veces no es necesario tener la mega plataforma con la última tecnología, sino algo más sencillo que explotes al 100 %"

añadido mucha complejidad, a una apuesta por plataformas en las que integrar la máxima cantidad de herramientas de seguridad, propias y de terceros, que simplifique la operación y mejore la visibilidad.

Comenta Ángel Gálvez que es cierto que "cada vez hay más integración entre los fabricantes, cosa que es muy útil. Pero estas plataformas globales que integran diferentes servicios, sistemas, automatizaciones, etcétera, hay que saber muy bien cómo se configuran y como se implementan, porque luego hay que introducir la lógica de negocio y las necesidades específicas de cada uno. La misma configuración no vale para todos y esto enlaza con la proactividad que deberían tener los servicios gestionados" comentada anteriormente.

Dice también el Global CISO de Avolta que a veces no es necesario tener la mega plataforma con la última tecnología, "sino algo más sencillo que explotes al 100 %. En mejor tener las mínimas soluciones estrictamente necesarias, pero bien configuras, al máximo rendimiento, y que cubran los procesos básicos. Y con eso tienes el 80% de tu seguridad está garantizadas.

No podemos despedirnos de Ángel Gálvez sin hablar del uso de que se está haciendo en Avolta de la Inteligencia Artificial. Nos cuenta que ya hay algunos servicios basados en IA para la parte de negocio, relacionado sobre todo en cómo usar el dato en marketing, promociones, ventas, etcétera, además de un servicio externo más consultivo. "Aquí el principal problema, como siempre, es cómo proteger el dato y qué información alimenta a estas fuentes de inteligencia artificial. Porque hay que tener mucho cuidado con la información interna que es compartida hacia fuentes externas", dice el directivo.

ENLACES DESTACADOS

Debate. Unificar para identificar

Según Palo Alto el rol del CISO evolucionará hacia un Chief AI Security Officer (CAISO)

Rockwell Automation: “Zero Trust permite seguir avanzando en la digitalización de los entornos industriales”

La ciberseguridad en el mundo industrial centra la conversación mantenida con Andreu Cuartiella y César Delgado Villalba, de Rockwell Automation, desde donde aseguran que la seguridad tal cual se aplica en el mundo IT no es compatible con cómo se debe hacer en el mundo OT.

Andreu Cuartiella, director comercial para la región de EMEA de Lifecycle Services

Con más de 120 años de historia, Rockwell Automation es un proveedor de equipos, software y servicios de automatización industrial con sede en Milwaukee, Wisconsin. La compañía divide su oferta en tres pilares. El negocio de Intelligence Devices, el que más ingresos genera con un 45 % del total, incluye toda una gama de componentes industriales como variadores, motores, sensores y más. El negocio de Software & Control (30 %) es el responsable de proporcionar soluciones tanto de hardware como de software para el control y la gestión de la información. Por último, Lifecycle Services, que representa el 25% del total, se centra en consultoría, mantenimiento y servicios gestionados, asegurando un soporte sostenido para sus productos y sistemas a lo largo de sus ciclos de vida. En esta área de negocio donde se recoge la propuesta de ciberseguridad de la compañía. Comentar también que Rockwell Automation divide sus mercados objetivo en manufactura discreta, que incluye la industria automotriz y

ENTREVISTAS

> "La seguridad tal cual se aplica en el mundo IT no es compatible con cómo se debe hacer en el mundo OT"

de semiconductores; industrias híbridas, como alimentos y bebidas; e industrias de procesos como petróleo y gas.

En una conversación mantenida con Andreu Cuartiella, director comercial para la región de EMEA de Lifecycle Services, y César Delgado Villalba, director de desarrollo de negocio de ciberseguridad, nos contaba el primero que la ciberseguridad en el mundo industrial "va de la mano de la evolución de las redes de comunicación industriales". Hasta no hace tanto cada fabricante de equipos de control industrial diseñaba su propia red, con su protocolo y sus conectores específicos, y fue "el despliegue de ethernet en los años 2000 lo que supuso

César Delgado Villalba, director de desarrollo de negocio de ciberseguridad de Rockwell Automation

un cambio importante porque generó la necesidad de servicios de infraestructura de red", y llevó a pensar en la ciberseguridad en el mundo OT, algo que hasta entonces no era foco de atención porque, entre otras cosas, y como nos cuenta Andreu Cuartiella, muchas veces "las redes OT estaban totalmente desconectadas de las redes IT".

El interés por llevar la ciberseguridad al mundo OT, ¿fue impulsado por los clientes o por los fabricantes? Dice Andreu Cuartiella que desde Rockwell se hizo mucha pedagogía. Recuerda que el mundo IT siempre ha estado muy al tanto de la problemática de la ciberseguridad, "pero no así el mundo OT".

Quizá la primera gran diferencia eran los propios roles en el sector; "había una línea muy difuminada de hasta dónde llegaba el responsable de IT y dónde el responsable de ingeniería". En todo caso, en Rockwell Automation entienden que la ciberseguridad es un elemento relevante y se empiezan a establecer alianzas con terceros, como Cisco, Claroty, Fortinet, Crowdstrike... que permiten a la compañía contar con un ecosistema de fabricantes de seguridad "que complementan nuestras soluciones para tener una red de control industrial segura".

Además, conscientes de la de la importancia de la ciberseguridad en el mundo, se realizan

ENTREVISTAS

una serie de adquisiciones “muy focalizadas y muy especializadas en el campo de la ciberseguridad”, continúa diciendo Andreu Cuartiella. La última de estas adquisiciones ha sido, el pasado mes de noviembre, la de Verve Industrial Protection, un sistema de inventario de activos y de gestión de vulnerabilidades, que reporta al segmento operativo Lifecycle Services de la compañía.

Por el punto de inflexión que supuso, destaca Andreu Cuartiella las compras de Avnet Data Security, un proveedor de ciberseguridad con sede en Israel con más de 20 años de experiencia en la prestación de servicios de ciberseguridad, en enero de 2020; y la de Oylo, una empresa española focalizada en proporcionar una amplia gama de servicios y soluciones de ciberseguridad de sistemas de control industrial (ICS), a finales del mismo año.

Muchos son los retos a los que se tiene que hacer frente en la seguridad del mundo industrial. El mayor de ellos es que “la seguridad tal cual se aplica en el mundo IT no es compatible con cómo se debe hacer en el mundo OT”, dice

> “La ciberseguridad para OT tiene que ser llevada a la práctica por profesionales de OT”

César Delgado Villalba. Explica el director de desarrollo del negocio de ciberseguridad de Rockwell Automation que, en IT, las compañías están acostumbradas a desplegar controles basados en determinados frameworks de referencia, pero en el mundo OT, además, hay un proceso detrás, y es necesario que “las personas que hacen una implantación de medidas de ciberseguridad en OT conozcan este proceso”. Es en el conocimiento de ese proceso donde radica el valor de Rockwell; “somos capaces de ir al cliente y decirle: además de este firewall, de la seguridad endpoint, o del control de servidores, debes poner un elemento que te haga análisis del agua en la red de distribución para ver, por ejemplo, si la composición de los ele-

ENTREVISTAS

mentos químicos que se han utilizado durante la fase de potabilización del agua son los que deben de ser, porque detrás hay personas".

Queda claro que uno de los retos que hay en el mundo OT es que "no hay profesionales que vengan del mundo OT y que tengan conocimientos a su vez de ciberseguridad. La ciberseguridad para OT tiene que ser llevada a la práctica por profesionales de OT", dice César Delgado.

En opinión de Andreu Cuartiella no se puede hablar de retos sin obviar "la consecuencia". Explica que la cuando en el mundo IT no se aplica bien un parche y se para el servidor de correo, o se cae el ERP... dos horas después se puede recuperar el tiempo perdido. En el mundo OT "lo menos malo que puede pasar es que se pare la producción, que la planta deje de fabricar", lo cual tiene una consecuencia económica importante, pero ni se están poniendo en riesgo la maquinaria, ni las personas.

Antes de entrar en el detalle de la propuesta de valor de Rockwell en cuanto a la seguridad del mundo industrial aclara César Delgado Villalba que Rockwell no solo presta servicios de soluciones de ciberseguridad para productos de Rockwell; "nosotros fabricamos PLCs y hardware que instalamos en las fábricas. Pero no hacemos seguridad solamente para nuestro propio producto. Nosotros somos un prestatario de servicios, un integrador de soluciones que presta servicios de ciberseguridad a industrias que utilizan cualquier fabricante de automatización". Clasifica el directivo los servicios de ciberseguridad de Rockwell Automation, enmarcados todos ellos bajo la normativa NIS, en tres grandes áreas. Un primer Servicio de Consultoría y Asesoramiento "con el que se ayuda a los clientes a entender qué es lo que tienen que hacer y cómo lo tienen que hacer" y donde la compañía se encuentra con diferentes perfiles y niveles

> "En el mundo OT lo menos malo que puede pasar es que se pare la producción"

ENTREVISTAS

> "El IoT está rompiendo el paradigma de la ciberseguridad en el entorno industrial"

de madurez; "algunos no saben ni por dónde empezar y otros sí, pero no saben cómo".

Una segunda área son los Servicios de Integración, que es el despliegue de soluciones, porque "hay clientes que no tienen las cualificaciones o conocimientos necesarios para desplegar estas soluciones en su propio entorno".

Habla César Delgado Villalba de despliegue de soluciones tecnológicas, pero también administrativas que ayudan a las organizaciones a organizarse para que haya responsables de la ciberseguridad dentro de la propia empresa.

El tercer pilar de la oferta de la compañía son los Servicios Gestionados, porque "una vez que sabemos lo que tenemos que hacer, y una vez que lo hemos implantado, hay que operarlo. De nada te sirve implantar una solución de detección de incidentes si no hay nadie que va a estar dando respuesta a las alertas".

A la hora de ofrecer estos servicios de ciberseguridad en el mundo OT, ¿quién es vuestro interlocutor? "Empieza a ser habitual que el CISO tome la responsabilidad", responde Andreu Cuartiella. Recuerda que hace unos años se presentaba una disyuntiva entre la gente de IT y la de ingeniería, pero que ahora es frecuente que el CISO sea el responsable de la ciberseguridad de toda la compañía, incluida la parte de OT.

Comenta Cuartiella que se llega a dar el caso de que muchas veces hay más endpoints que proteger en la red de OT que en la de IT. Y es que en una fábrica donde hay mucha automatización "podemos estar hablando de miles de dispositivos en la planta de producción".

Comenta César Delgado que, aunque es cierto que se tiende a que el CISO tenga una visión global de cuál es el riesgo de la organización, tanto en el lado IT como en el lado OT, "la existencia de un rol específico para la cibersegu-

ENTREVISTAS

ridad OT depende del nivel de madurez de la propia organización". Añade que, "en estos procesos de madurez de las empresas, según IT va cogiendo responsabilidad sobre el ámbito OT, va queriendo llevar a la práctica los mismos procedimientos que ellos llevan haciendo en el lado IT al mundo OT. Pero el mundo OT no está preparado para llevar a cabo estos procedimientos de esta manera". Un ejemplo de ellos es todo lo que tiene que ver con las actualizaciones e implantación de parches, que en el mundo industrial es tremendamente complicado, y a veces imposible.

Planteado el impacto que pueda tener 5G, u otras tecnologías que puedan estar por llegar, en el mundo OT, tienen claro Andreu Cuartiella que "el mundo industrial es conservador por defecto" y que "todas las tecnologías que van al mundo industrial tienen que ser cosas muy probadas, muy aceptadas". Se suma que los ciclos de vida en los entorno de IT y OT son radicalmente diferentes.

> "El mundo industrial es conservador por defecto"

"El IoT está rompiendo el paradigma de la ciberseguridad en el entorno industrial", asegura César Delgado Villalba, añadiendo que se ha pasado de tener entornos aislados sin conectividad hacia el exterior, o una conectividad limitada a través de una DMZ, "a un entorno en el cual tienes cientos o miles de dispositivos que están comunicando directamente a través de Internet con una plataforma de analítica que está en la nube, por ejemplo. Vamos a un escenario totalmente diferente, a una arquitectura que va contra todas las reglas tradicionales del mundo OT, una arquitectura totalmente abierta de comunicación masiva hacia el exterior".

En este nuevo escenario se apuesta por el modelo Zero Trust "como el mecanismo que nos va a posibilitar que estos entornos operen de manera segura", dice César Delgado, añadiendo que es lo que permite que las políticas de

ENTREVISTAS

privilegio mínimo "sean llevadas a cabo a lo largo y ancho de todos los activos de la planta" y "seguir avanzando en la digitalización de los entornos industriales". Habla también el directivo de la relevancia de Zero Trust al dar protagonismo a la identidad, no solo de las personas, sino de los propios activos.

Planteado si el IoT está teniendo, en los entornos industriales, el mismo impacto que tuvo la movilidad y el cloud en los entornos IT: difuminar ese perímetro que tan cuidadosamente crearon los firewalls, IPS y demás herramientas, dice César Delgado que "el IoT está rompiendo este perímetro de seguridad que se estaba ejerciendo dentro de la propia planta y nos estamos yendo hacia un modelo extendido en el cual el firewall, el proxy o la DMZ ya no son suficientes para proteger la planta". En un entorno IoT en el que quienes se comunican con el exterior no son usuarios "se tienen que utilizar mecanismos de autenticación diferentes basados en certificados digitales".

> "Llevamos sufriendo ataques enfocados específicamente al Industrial Control System desde los últimos 14 años"

Con más o menos repercusión e impacto, lo cierto es que "llevamos sufriendo campañas, ataques enfocados específicamente al Industrial Control System desde los últimos 14 años", dice Andreu Cuartiella. En ese, "goteo continuo de campañas de ciberataques" se ha visto que hay una serie de vulnerabilidades debido a la existencia de equipos antiguos, o equipos que no están parcheados. Una situación que ya no solo contempla que haya una cultura de ciberseguridad o no, sino una cuestión práctica: tengo que aplicar un parche, pero no puedo hacerlo hasta dentro de tres meses, que es cuando tengo la siguiente parada de producción.

Al final, cada incidente es un incentivo, un detonante, para que se invierta en programas de ciberseguridad e incluso se actualicen normativas y regulaciones, comenta Cuartiella.

ENLACES DESTACADOS

Crecen las amenazas contra la infraestructura crítica debido a anomalías en las redes OT e IoT

El sistema sanitario, en el punto de mira de los ataques OT

Infoblox: “Las empresas se plantean la inversión en la seguridad del DNS muy tarde”

Infoblox anuncia SOC Insights, una nueva funcionalidad de su BloxOne Threat Defense que apuesta por un futuro en el que el análisis de incidencias y riesgos de seguridad estarán basado en IA y en inteligencia de seguridad DNS.

Joaquín Gómez, CyberSecurity Lead Southern Europe de **Infoblox**

2023 fue un año intenso para Infoblox. En enero se nombraba un nuevo CEO, Scott Harrel, un ex Cisco, y en mayo se producía un cambio de imagen de marca que reflejara que, además de empresa de redes de misión crítica, tiene mucho que decir en el mercado de ciberseguridad. Hace más de cuatro años que la compañía lanzaba al mercado BloxOne Threat Defense, considerada como la primera solución de seguridad híbrida que aprovecha los servidores DNS para establecer una primera línea de defensa y optimizar la orquestación global de la seguridad corporativa. A finales del año pasado Infoblox anuncia la disponibilidad, como parte de su plataforma BloxOne Threat Defense, de DNS De-

ENTREVISTAS

infoblox ciberseguridadTIC

> "Somos capaces de proporcionar toda la información de todos los dispositivos cualquiera que tenga una IP, de forma que las empresas sean capaces de discernir todo lo que tienen"

Juan de la Vara, Senior Manager Solution Architects para el Sur de Europa de **Infoblox**

tection and Response, una solución que permite visualizar la infraestructura de potenciales atacantes a medida que se crean para detener de forma temprana amenazas conocidas y probables sin comprometer el rendimiento de la red, bloquear los ataques que otras herramientas de seguridad pasan por alto y reducir drásticamente los tiempos de respuesta (Mean Time To Respond, MTTR) ante incidencias de seguridad.

Ahora la compañía anuncia SOC Insights, una nueva funcionalidad basada en IA que reduce drásticamente el número de alertas que llegan al SOC. De este lanzamiento y otras cosas hemos hablado con Joaquín Gómez, CyberSecurity Lead Southern Europe de Infoblox, y Juan de la Vara, Senior Manager Solution Architects para el Sur de Europa de la compañía. Empezamos por el principio, por entender la empresa. Infoblox es una compañía que sigue creciendo centrada en tres grandes áreas. La primera tiene el objetivo de ayudar a los clientes en su transición hacia la nube, lo que implica que las soluciones de la compañía ya pueden

ENTREVISTAS

> "Nuestro mensaje de seguridad es sencillo de explicar, de entender y de replicar"

desplegarse tanto on-premise como en cloud. Explica Juan de la Vara que la adopción de entornos multinube genera retos importantes en las empresas y que "la visión de Infoblox es que podemos simplificar todo el crecimiento de las empresas hacia el cloud o multicloud gracias a nuestra tecnología, de forma que la gente puede tener un punto de control único, un punto de visión único para cualquier tipo de soluciones de DNS principalmente".

El segundo foco de crecimiento de la empresa tiene que ver con la visibilidad, "ser capaces de proporcionar toda la información de todos los dispositivos – cualquiera que tenga una IP, de forma que las empresas sean capaces de discernir todo lo que tienen". Es algo que la compañía ha realizado en entornos on-premise y que ahora se mueve a la nube, "de forma que seamos capaces de proporcionar toda esa visibilidad de cualquier tipo de dispositivo que esté en la red", incluido el IoT, lo que lleva a Infoblox a "poner más foco en el mundo IoT".

En esta parte de la visibilidad, la propia raíz de Infoblox es un valor diferencial. Como nos cuenta Juan de la Vara, las capacidades de la compañía en gestión DDI (DNS, DHCP e IPAM) "nos coloca en una posición ideal para ser capaces de proporcionar esta visibilidad en cualquier tipo de entorno, incluidos aquellos en los que no se pueden desplegar agentes".

La tercera área de foco es aumentar las capacidades de seguridad de la compañía. Se apuesta por aumentar las capacidades de defensa de BloxOne Threat Defense añadiendo una capa de inteligencia artificial "para eliminar ruido a los equipos de SOC (Security Operation Center) y enviar menos eventos, pero más relevantes". La última novedad en este apartado es SOC Insights, una solución de gestión y orquestación de operaciones de seguridad (Security Opera-

ENTREVISTAS

tions Center, SOC) basada en Inteligencia Artificial que optimiza las operaciones SOC y reduce drásticamente los tiempos de detección y respuesta ante amenazas de DNS.

En los orígenes

Desde sus inicios, el foco de la compañía ha sido gestionar e identificar dispositivos conectados a redes. Es decir, el foco de Infoblox ha sido ofrecer productos que pueden ayudar a los ingenieros de redes a ver la red completa y automatizar las tareas más básicas. Las tres funciones básicas que Infoblox ayuda a administrar se denominan DDI (DNS, DHCP e IPAM). Para aquellos que no estén familiarizados con la terminología de redes, DNS es el sistema que convierte una dirección web en su dirección IP subyacente. DNS es un aspecto fundamental de Internet que debe configurarse y funcionar correctamente, y es un posible punto débil de seguridad. DHCP significa Protocolo de configuración dinámica de host y es el sistema responsable de asignar direcciones IP automáticamente. La última parte del acrónimo significa protocolo de Internet y engloba otros aspectos básicos de la red. Infoblox puede ayudar a reducir el personal de TI simplificando la configuración y el mantenimiento de las redes.

> "En las empresas menos maduras funciona el 'good enough' y que no llegan a entender que el DDI es la base de todo. Si no funciona el DNS, tu empresa no funciona"

El foco hacia el mercado DDI ha hecho que los clientes tipo de Infoblox hayan sido siempre empresas grandes, de miles de empleados. Pero la madurez y evolución del mercado, además de una ampliación de la oferta de la compañía, donde los servicios de ciberseguridad son cada vez más importantes, están ampliando las oportunidades en empresas más pequeñas, incluso de 500 empleados. En opinión de Juan de la Vara,

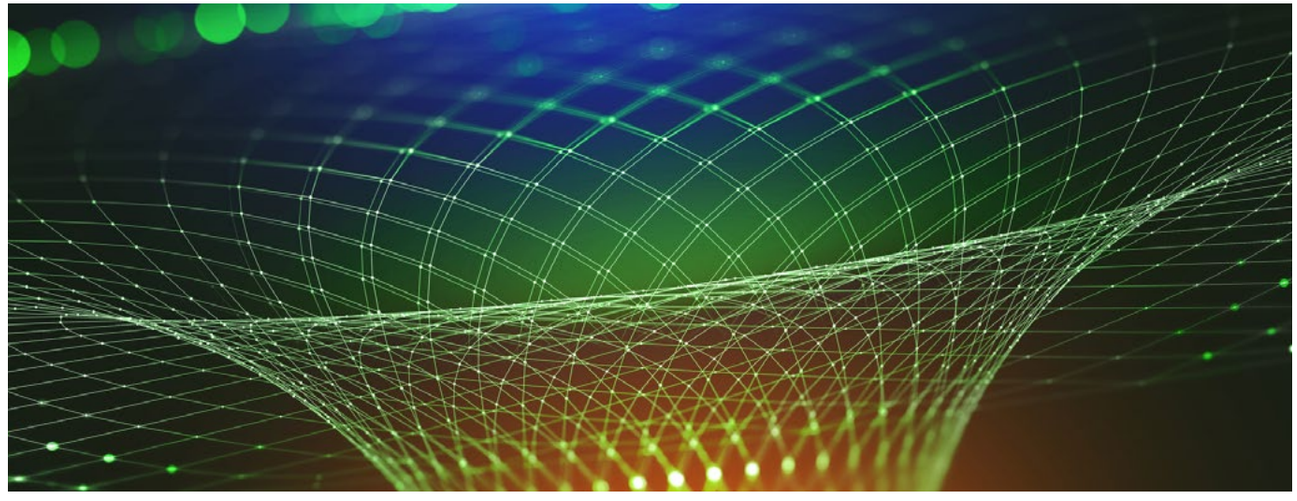
ENTREVISTAS

el mensaje de seguridad funciona bien "porque es un producto diferencial en el mercado".

Dice también el directivo que en las empresas menos maduras funciona el 'good enough' y que "no llegan a entender que el DDI es la base de todo. Si no funciona el DNS, tu empresa no funciona". Este es el mensaje que se está llevando con equipos dedicados a ese segmento de mediana empresa, "un mercado nuevo para nosotros, pero donde la empresa está creciendo". En todo caso, en opinión de Joaquín Gómez, director de Ciberseguridad de Infoblox para Sur de Europa, "las empresas se plantean la inversión en la seguridad del DNS muy tarde".

Proteger desde el DNS es adelantarse. Frente a una amenaza lo habitual es que las empresas de seguridad endpoint se centren en analizar la propia amenaza, el malware: analizan qué hace, cómo se comporta. La pregunta que nosotros nos hacemos es preguntarnos ¿por qué te ha llegado? ¿quién te lo ha enviado?, explica Joaquín Gómez, añadiendo que los criminales suelen contratar infraestructuras de distribución de contenido y que "si conseguimos parar esas redes especiales de distribución de contenido, el malware ya no te llega. Eso es lo que nosotros hacemos".

El mensaje que lanza el CyberSecurity Lead Southern Europe de Infoblox es que los ciberdelincuentes pueden utilizar el sistema de dominios en diferentes ámbitos. Uno es utilizando de forma maliciosa para engañar, instalar un malware o comunicarse con el malware, "pero también para suplantar un dominio". Lo que necesita un cliente es que el sistema de dominios proporcione información de una amenaza o de una IP... "Lo que estamos haciendo es consolidar en un único fabricante todas y cada una de las acciones que yo le puedo pedir al sistema de dominios para ayudar a la seguridad en tres diferentes ámbitos: en la detección de amenazas; en la parte de inteligencia, investigación de amenazas y respuesta; y en la parte de reputación de marca para que nadie me suplante". Normalmente las empresas tienen hasta tres productos para hacerlo todo, "y normalmente no llegan a nuestro nivel de profundidad. El mensaje es: consolida todo el sistema de seguridad que use el sistema de DNS en un único fabricante".



ENTREVISTAS

Infoblox SOC Insights

Decíamos al comienzo que el último anuncio de Infoblox es SOC Insights, una nueva capacidad para su plataforma BloxOne Threat Defense lanzada en 2019. Esta nueva funcionalidad representa un salto adelante en la detección y prevención de amenazas aprovechando el poder del DNS como una primera línea de defensa proactiva.

Explica Joaquín Gómez que hace un año la compañía añadió Inteligencia Artificial para detectar de una forma anticipada si un domino es malicioso nada más nacer. Lo que ahora se ha hecho, explica Joaquín Gómez, es aplicar la inteligencia artificial a la parte de SOC, a la parte de detección y respuesta. “El problema de los responsables de operación es que reciben millones de alertas”, dice Joaquín Gómez, señalando que la cantidad de logs que genera el DNS puede ser inmanejable. Lo que propone la compañía con SOC Insights es: en lugar de enviar los logs al SIEM/SOAR, “aplicamos inteligencia artificial a la información que tenemos, y agrupamos en todo un incidente completo con toda la información desde nuestro sistema”.

Es decir, SOC Insights permite reducir el tiempo de respuesta ante incidencias al eliminar el tiempo empleado en consolidar alertas individuales en un repositorio de información utilizable. El informe generado por esta herramienta proporciona, de forma rápida y fácil, todos los detalles sobre la infraestructura del atacante, eventos relacionados y dispositivos comprometidos, así como datos de inteligencia de DNS exclusivos, proporcionados por Infoblox. Esto elimina la necesidad de rastrear cada alerta individual o de esperar a que los administradores de red proporcionen la información sobre usuarios y dispositivos para conocer el contexto en el que se está produciendo la amenaza.

El concepto, explica el responsable de Infoblox para la región de Iberia, es: “en vez de centralizar la inteligencia en un punto único, lo que estamos haciendo es adelantar esa inteligencia al edge del DNS, en el punto origen de DNS. Esa es la evolución que hemos hecho como expertos en saber qué hay a nivel de DNS”.

Añade también Joaquín Gómez que, para aquellos que trabajen con un MDR, la ventaja de las evoluciones que Infoblox está realizando en su plataforma BloxOne Threat Defense, es reducir el tráfico que llega a ese MDR, “un tráfico que, además, está contextualizado”.

Impacto en el SIEM

El mercado de la detección y respuesta, aplicada tanto al endpoint (EDR), como a la identidad (ITDR) o a la suma de puntos finales, redes y

ENTREVISTAS

demás (XDR), está teniendo un fuerte impacto en el SIEM. Como ya explicábamos en un reportaje publicado en Ciberseguridad TIC, a medida que los ciberdelincuentes se vuelven más sofisticados, los volúmenes de datos aumentan y los costes SIEM se disparan. Ahora gran parte del análisis de lo que ocurre en las empresas se realizan en los EDR, XDR..., reduciendo la dependencia del SIEM. A esta tendencia se suma Infoblox con SOC Insights, que se encargará de analizar toda la información que se genere a nivel de DNS, que no es poca.

La situación está llevando a muchos fabricantes a establecer alianzas porque, por más que todos aseguran poder hablarse entre ellos a través de las indispensables API, una integración cuidada siempre es mejor.

> El último anuncio de Infoblox es SOC Insights, una nueva funcionalidad basada en IA que reduce drásticamente el número de alertas que llegan al SOC

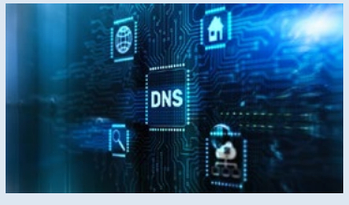
Sin poder dar demasiados detalles, Infoblox trabaja en un ecosistema de alianzas, BloxOne Threat Defense Ecosystem, que permite a sus productos integrarse con otras soluciones del mercado. Es uno de los aspectos que, nos cuenta Joaquín Gómez, viene impulsado por el nuevo CEO de la compañía, Scott Harrell. Se plantea también que el producto no solo se venda a cliente final, sino que sea operable a través de MSP, "que se pueda operar como servicio".

Canal

"Estamos intentando abrir canal", dice claramente Joaquín Gómez. Se busca un canal "que quiera diferenciarse del resto y que nos lleve a empresas más medianas y pequeñas", asegura el directivo.

En opinión de Juan de la Vara, hay oportunidades en partners especializados en seguridad porque "nuestro mensaje de seguridad es sencillo de explicar, de entender y de replicar".

ENLACES DESTACADOS

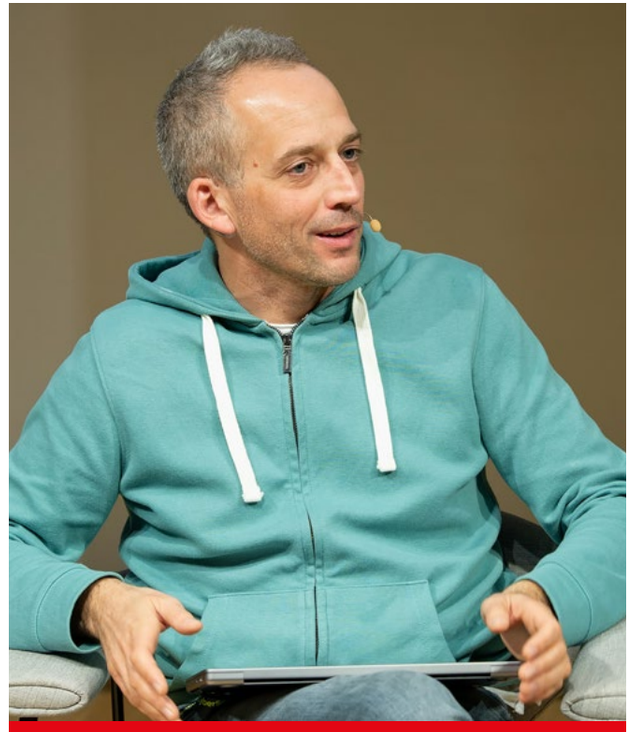


Infoblox añade detección y respuesta al DNS

Infoblox anuncia nueva estrategia de integración de networking y seguridad

“Lo que marca la diferencia de una organización a otra es el tiempo de respuesta”

Tiene claro Amador Aparicio de la Fuente, CISO en Zunder, que para ser un buen CISO tienes que ser un buen líder y crear cultura de ciberseguridad; que no se pueden asumir riesgos de los proveedores con los que trabajan las empresas; que haciendo lo básico bien, “minimizas muchísimo la superficie de exposición”, que los insiders son una de las mayores amenazas de las empresas y que le gustaría tener “una herramienta para detectar suplantaciones de identidades digitales a través de los rasgos biométricos”.



Amador Aparicio de la Fuente, CISO de Zunder

Amador Aparicio de la Fuente es CISO en Zunder, empresa palentina de referencia en España y el sur de Europa que opera puntos de recarga ultra- rápida para coches eléctricos. Lleva más de 15 años en el mundo de ciberseguridad ofensiva y desde hace un tiempo se ha convertido en responsable de ciberseguridad. “Durante los últimos 15 años de mi vida ha estado haciendo hacking ético, buscando vulnerabilidades antes de que los ciberdelincuentes las exploten”, nos cuenta Amador Aparicio, que aplica toda esta experiencia en su rol de CISO, un papel que, según el directivo tiene dos vertientes: por un lado la más normativa, que es “la gestión de la información”, y por otro, el conocimiento tecnológico. “Tanto un responsable tecnológico como un responsable de ciberseguridad “deben tener una base tecnológica para entender los productos, para entender las amenazas. Por mi experiencia, primero apostaría por la parte tecnológica, porque al final la normativa se aprende”, asegura.

Habiendo prestado servicios de hacking ético, “tengo la experiencia de haber visto empresas

ENTREVISTAS

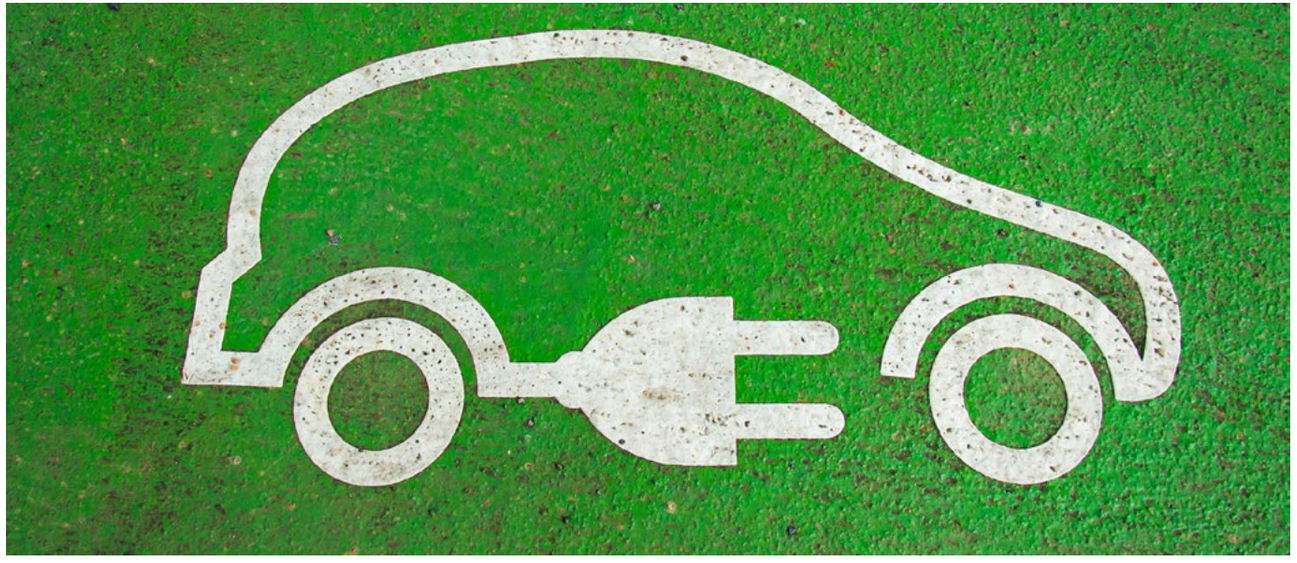
vulneradas", lo que hace que se sea "muy consciente de las consecuencias que puede tener una organización cuando sufre un ciber incidente". Y es lo que le lleva a resaltar que, entre las cualidades de un buen CISO, está el "comprender las amenazas y los desafíos del mundo digital en el que estamos". No es la única. Añade Amador Aparicio el contar con inteligencia emocional para tener habilidades de liderazgo, porque "para ser un buen CISO tienes que ser un buen líder, y para ser un buen líder pues tienes que estar codo a codo con tus compañeros"; además de tener conocimiento de las regulaciones que afectan a la empresa a la que estás sirviendo; tener la habilidad de tomar decisiones bajo presión, en situaciones de crisis; ser un buen comunicador y "tener la capacidad de explicar conceptos que son complicados de una manera sencilla para que todo el mundo los entienda"; tener la habilidad de educar y concienciar a tus compañeros y crear cultura de ciberseguridad "son cosas sencilla pero eficientes", asegura, añadiendo que un buen CISO también

"Por muy compleja que sea una contraseña, como alguien más que tú la sepa, ya no vale"

debe poder adaptase y "ajustar la estrategia de seguridad de la organización en función de cuáles sean las tendencias presentes y futuras".

Preguntado por las prioridades que se marca en materia de ciberseguridad en Zunder, tiene claro Amador Aparicio que una de ellas es la "protección de datos sensibles. Eso es fundamental y debe incluir el cifrado de los datos en reposo, de los datos en tránsito o la implementación de controles de acceso adecuados". Otro punto importante a tener en cuenta es "el tener la capacidad de identificar amenazas, evaluarlas y mitigarlas" y, sobre todo, "cómo respondes a los incidentes que te van a pasar. Porque lo que marca la diferencia de una organización a otra es el tiempo de respuesta. En función de cómo respondas a la amenaza, puede que tu empresa continúe o no".

ENTREVISTAS



> "Educar y concienciar en seguridad, es fundamental y algo crítico"

Explica también el CISO de Zunder que, dado las características del negocio, que ofrece la venta de energía a través de los cargadores ultra rápidos para coches eléctricos, "la cadena de suministro es una cosa fundamental". Tiene claro Amador Aparicio que "nosotros no podemos, o no deberíamos, asumir riesgos de los proveedores de servicios con los que con los que trabajamos", lo que supone "conocer muy bien los productos que tú contratas o que te ofrecen esos proveedores, y tener la capacidad de poder identificar cuáles son los riesgos que esos productos pueden presentar". En ese poder identificar los riesgos, el directivo ha llegado a analizar el material industrial que tienen los cargadores de la compañía porque "considero que debo tener la capacidad de ver cuáles son los riesgos básicos. Y cuando digo lo básico es que muchas veces en ciberseguridad, haciendo lo básico bien, minimizas muchísimo la superficie de exposición de los sistemas".

¿Qué tipo de amenaza te quita el sueño? "A mí lo que me quita el sueño es que mi organización no continuara por un ciberataque. Eso es lo que me quita el sueño de verdad", responde Amador Aparicio. Menciona de manera más específica la fuga de datos; "no me puedo permitir que los datos sensibles de nuestros clientes acaben en internet" por dos cosas: por el prestigio reputacional "y porque la gente perdería la confianza de los servicios que nosotros prestamos", asegura el directivo; y una denegación de servicio que impida que el cliente pueda acceder a un servicio por el que está pagando.

Asegurando que un CISO debe tener muy claro cuál es el core de su organización y cuáles son los riesgos que impactarían sobre ese core, asegura el directivo d Zunder que otra de las cosas que le quita el sueño es "una amenaza que yo no controlase y que pudiera impactar de una manera directa en el core de mi organización".

ENTREVISTAS

zunder ciberseguridadTIC

> "Para ser un buen CISO tienes que ser un buen líder, y para ser un buen líder tienes que estar codo a codo con tus compañeros"

Planteado qué tecnología de seguridad considera imprescindible, comenta Amador Aparicio que la tecnología avanza, pero la base de esa tecnología es prácticamente la misma, "lo que pasa es que cada vez hay más capacidad de cómputo y más nube". Con esta premisa, considera imprescindible en cualquier organización "un firewall para filtrar todo el tráfico". También considera fundamental contar con un antivirus y antimalware, e inaceptable que sea gratuito; "cuando escuchéis a alguien que diga que el mejor antivirus es no tener un antivirus, o que no hace falta tener un antivirus, huye de esa persona porque no tiene ni idea de seguridad". Entiende como imprescindible tener un sistema capaz de detectar y prevenir intrusiones, además de otro que detecte las fugas de información porque, "aunque no lo parezca, una de las mayores amenazas que sufren las organizaciones es precisamente la exfiltración de información de carácter sensible por parte de los insiders, de la gente que trabaja para para la propia organización".

Continúa con su lista de imprescindibles añadiendo el doble factor de autenticación porque, "por muy compleja que sea una contraseña, como alguien más que tú la sepas, ya no vale"; un buen control de accesos "para restringir el acceso a sistemas, aplicaciones o datos críticos de una organización"; protección del correo electrónico, "porque es el principal vector de entrada de todo lo que tiene que ver con el phishing y el ransomware". Asegura también que "si quieres ser un buen CISO, más vale que estés atento a las actualizaciones y los parches";

ENTREVISTAS

que la seguridad en la nube "es una cosa muy importante"; y que educar y concienciar en seguridad, "es fundamental y algo crítico". No se olvida de un sistema de backup, recuperación y continuidad de negocio "si no quieres morir después de ser víctima de un incidente".

¿Qué te haría fracasar como CISO? "Lo que no cuesta es llegar, lo que cuesta es mantenerse", responde Amador Aparicio. Añade que nunca le han hecho una entrevista para ser CISO, sino que "han confiado en mí, y doy las gracias por ello. Pero claro, tú tienes que demostrar que eres merecedor de esa confianza y de ese respeto".

Mirando hacia delante, hacia algunas tecnologías o amenazas que puedan ser perturbadoras, se menciona la computación cuántica asociada, de manera concreta, al cifrado. Asegura el CISO de Zunder que no es algo que le preocupe porque "esas máquinas que puedan poner en peligro la criptografía que tenemos actualmente es algo que va a tardar muchos años en venir. Además, se está investigando mucho sobre criptografía cuántica, protocolos criptográficos, etc.".

"No me puedo permitir que los datos sensibles de nuestros clientes acaben en internet"

Considera importante el auge de la inteligencia de amenazas. Recordando que el cibercrimen genera más ingresos que la venta de armas o el tráfico de drogas, dice Amador Aparicio que los cibercriminales están invirtiendo y que las ciber amenazas son cada vez más complicada de detectar.

Sobre la Inteligencia Artificial relacionada con la ciberseguridad, tiene claro el CISO de Zunder que hay que realizar un control de una posible fuga de información que se puede producir por subir datos a una máquina que no sabemos dónde está ni lo que hace, entre otras cosas porque "de la misma manera que existen

ENTREVISTAS

vulnerabilidades para las máquinas que están conectadas a Internet, también se puede hacer hacking a los sistemas de inteligencia artificial generativos". Menciona de manera específica el prompt injection, una técnica que tiene como objetivo manipular la entrada o instrucciones que se le proporcionan a un sistema de Inteligencia Artificial.

En todo caso, "más que la inteligencia artificial, me preocupan de verdad los ataques clásicos" como los de phishing o ransomware, por "la capacidad y facilidad que hay hoy en día para clonar en tiempo real la voz y video para hacer una suplantación de una persona".

En una situación idílica, sin complicaciones de tiempos o presupuestos, "se me ocurre una tecnología futura, pero que a mí me gustaría tener: un sistema para garantizar que cuando yo tengo una videollamada, las personas que aparecen son las que tienen que estar y no son una suplantación", asegura Amador Aparicio. Concreta el directivo: "me gustaría tener una herramienta para detectar suplantaciones de identidades digitales a través de los rasgos biométricos".

¿De qué proyecto se siente más orgulloso Amador Aparicio? "De haber detectado cosas antes de que los cibercriminales lo hubieran hecho. Y, sobre todo, orgulloso del equipo de sistemas y del equipo de desarrollo que tenemos, que lo han resuelto todo. Me siento orgulloso de trabajar con gente que tiene actitud", responde Zunder.

Por último, ¿qué haces cuando no eres CISO? "Me gusta mucho estar con mis hijas, de once y siete años, y salir a correr", responde, añadiendo que está al final de su tesis y forma parte del grupo de investigación de la Universidad de Valladolid, donde es profesor asociado. También disfruta "tomando una cerveza con mis amigos".

ENLACES DESTACADOS

Lena Smart: "Si mis políticas y procedimientos no ayudan a que nuestro negocio crezca, he fracasado como CISO»

Debate. Transformando el comportamiento de los usuarios