it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Noviembre 2022 - nº 57

Directorio Activo, se enciende el botón de alerta

‘A la hora de escoger una herramienta es muy importante conocer tu realidad’ Cristiano Dias, H10 Hotels

‘Nadie sabe cómo contratar a un profesional de ciberseguridad’ Ottavio Camponeschi, Cyberbit

16ENISE. Afrontando el futuro juntos

Revista Secure&IT Estado de ciberseguridad en España

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

it Digital Security

Directora Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Contracorriente

Producción audiovisual Miss Wallace, Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es

Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

Directorio Activo, ¿tienes en cuenta su protección?

El Directorio Activo, o Active Directory, es el corazón de la infraestructura de TI de más del 90% de las organizaciones. Es el responsable de proporcionar la autenticación y autorización para cada recurso crítico en todo el entorno corporativo, lo que le convierte en un objetivo principal para los atacantes que buscan acceder a los datos sensibles de la empresa. Hablamos con diferentes expertos que nos cuentan qué tipo de ataques son los más frecuentes contra el AD o cuáles son las medidas básicas que deben tenerse en cuenta para protegerlo.

Además, en #ITDSOctubre, hablamos con Cristiano Dias, CISO de H10 Hotels, para quien conocer tu empresa es clave a la hora de escoger la herramienta que debe protegerla. Aprovechando un reciente viaja a Madrid hemos hablado con Ottavio Camponeschi, Senior Director EMEA de Cyberbit, una empresa que busca llevar al mundo digital el concepto de las maniobras militares para saber a ciencia cierta que los equipos están listos para hacer frente a los ciberataques.

Pedro David Marco Llorente, Main Account Manager y Fundador de Iberlayer, y Javier Cazaña, responsable de Cynet en España, son otros protagonistas de este número de IT Digital Security en el que también os resumimos el evento 16ENISE. El evento, que se celebró en León a finales de octubre, reúne cada año a más asistentes; allí tuvimos la oportunidad de tomar le pulso al sector preguntando a algunos directivos por el lema de este año, 'Facing the future together', así como de alguna que otra tendencia.

Cierra este número una revista especial con los resultados de una encuesta realizada por IT Research y patrocinada por Secure&IT que busca conocer el Estados de la Ciberseguridad en España.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

itds

Sumario

Entrevistas

Actualidad

No solo IT

Índice de anunciantes

Revista Secure&IT

Revista Anadat-Semperis

El 55% de las organizaciones de servicios financieros fueron afectadas por el ransomware en 2021

Tome medidas contra las amenazas con un equipo de expertos en respuesta

Con Sophos MDR, su empresa cuenta con el respaldo de un equipo de expertos que ofrece un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

www.sophos.com/es-es

SOPHOS
Cybersecurity delivered.

16ENISE. Afrontando el futuro juntos

Un año más León se ha convertido en el punto de encuentro del sector de ciberseguridad. Con más de 2.400 asistentes presenciales y más de 1.600 personas conectadas online, el congreso es el primero organizado bajo el mandado de Félix Barrio, director de INCIBE desde el pasado mes de junio. Encargado de clausurar el evento, el directivo destacó que "la ciberseguridad es ya una palanca de competitividad, de continuidad y de resiliencia para nuestra sociedad y nuestra economía, que son más digitales que nunca".

El evento fue inaugurado por Carmen Artigas, secretaria de Estado de Digitalización e Inteligencia Artificial, quien aseguró que “la ciberseguridad es un elemento crítico y el pilar fundamental para el éxito del plan digital de cualquier país, y que sirve como palanca clave para salvaguardar el crecimiento que impulsa la transformación digital”. Artiagas resaltó el potencial de la industria de ciberseguridad, formada en España por “más de 1.600 empresas que facturan casi 2.000 millones de euros anuales, y con unas expectativas de crecimiento que rozan el 15%”.

Bajo el lema ‘Facing the future together’, #16ENISE acogió durante dos jornadas las últimas innovaciones y tendencias del sector de la ciberseguridad, y contó con 75 ponentes nacionales e internacionales y la presencia de

"La ciberseguridad es ya una palanca de competitividad, de continuidad y de resiliencia para nuestra sociedad"

Félix Barrio,
director de INCIBE

RESUMEN JORNADA

CLICAR PARA VER EL VÍDEO

"La ciberseguridad es un elemento crítico y el pilar fundamental para el éxito del plan digital de cualquier país"

Carmen Artigas, secretaria de Estado de Digitalización e Inteligencia Artificial

82 stands comerciales e institucionales. El International Business Forum reunió, por su parte, a más de 95 participantes de 15 países, que celebraron un total de 150 reuniones con 30 compradores internacionales, según datos ofrecidos por INCIBE. En paralelo, más de 300 personas participaron en los talleres de ciberseguridad.

Durante el evento IT Digital Security quiso tomarle el pulso al sector planteando una serie de preguntas a varias empresas participantes. ¿Qué opina del lema de 16Enise? ¿es suficiente el impulso que, desde las Administraciones Públicas, se está haciendo por la ciberseguridad? ¿Vamos hacia la adopción de plataformas/arquitecturas de ciberseguridad? Llevamos años hablando de consolidación en el mercado de ciberseguridad, ¿por dónde crees que vendrá?

AuthUSB

‘Por desgracia, el de la seguridad será un mundo de grandes players’

María Cobas, Global BDM, AuthUSB

“Ojalá pudiésemos enfrentar el futuro juntos de verdad”, comenta María Cobas, BDM y co-fundadora de AuthUSB. Reconoce que “juntos podemos más”, pero que el mundo cíber está muy segmentado y “no nos ayudamos lo suficiente y no se colabora lo suficiente”, no ya en lo público/privado, sino en los privado/privado y lo público/público, aclara.

Sobre el impulso que las administraciones públicas hacen por la ciberseguridad, comenta María Cobas que no se le da la importancia que merece al producto español; “tener que salir fuera para luego poder crecer en España es muy triste. Y la Administración no ayuda”, asegura la directiva.

¿Vamos hacia el mundo de las plataformas/arquitecturas en el mercado de ciberseguridad? “Nosotros nos dedicamos al mundo OT y yo creo que sí”, asegura, añadiendo que la ciberseguridad no puede estar compartimentada, sino que “hay que verla desde el punto de vista transversal” y debe existir una arquitectura que te permita implementar diferentes tecnologías.

Respecto a la consolidación del mercado de ciberseguridad… “sinceramente veo que los grandes se van a comer a los pequeños. Por desgracia, éste será un mundo de grandes players”. ¿Por desgracia? “Sí, porque la competitividad no es la misma. Y la innovación, tampoco”, explica María Cobas, añadiendo que “cuando innovas, luchas por algo que es tuyo, y lo defiendes. El incentivo no es el mismo cuando eres un empleado de una gran multinacional”.

"El mundo cíber está muy segmentado y no nos ayudamos lo suficiente"

María Cobas, Global BDM, AuthUSB

Check Point

‘La consolidación del mercado de seguridad se tiene que producir’

David Galdrán, SE Team Leader Enterprise, Check Point

Respecto al lema de 16ENISE, ‘Facing the future together’, comenta David Galdrán, SE Team Leader Enterprise de Check Point, que refleja “la unidad que se está estableciendo por parte de los distintos fabricantes de seguridad y organismos públicos de cara a crear plataformas únicas donde se comparta la inteligencia de las distintas herramientas que disponemos de cara a minimizar los tiempos de respuesta”.

¿Cómo están impulsando las Administraciones Públicas la ciberseguridad? Para David Galdrán la nueva Ley de Contratación busca agilizar los procesos de compra; la ciberseguridad evoluciona de un mes para otro y los mecanismos de contratación llevaba a que se adquiriera tecnología obsoleta, e incluso desaparecida, “y lo que estamos viendo es que se están estableciendo mecanismos para poder agilizar estos trámites, lo que les permite tener acceso a tecnologías más modernas, más novedosas”.

"Se están estableciendo mecanismos para poder agilizar los trámites de contratación con AAPP"

David Galdrán, SE Team Leader Enterprise, Check Point

Sobre si se va hacia la adopción de plataformas/arquitecturas de ciberseguridad, comenta el directivo de Check Point, que depende del estado de la digitalización en el sector hacia el que se mire, "que es lo que está mandando a la hora de plantear distintas arquitecturas".

La consolidación del mercado de seguridad "se tiene que producir porque los vectores de ataque crecen y lo que no tiene sentido tener miles de herramientas distintas para proteger cada uno porque al final lo que consigues es que el eslabón débil de la cadena sea el propio departamento de seguridad".

Enthec

'Una nación que no da importancia a la seguridad, es una nación perdida'

María Isabel Rojo, CEO, Enthec

¿El lema de 16ENISE, 'Facing the future together', "me parece maravilloso porque, ahora más que nunca, hay que unificar energías", asegura María Isabel Rojo, CEO de Enthec. Añade que tenemos un ecosistema de ciberseguridad muy floreciente, que en España y Europa hemos dependido muchísimo de tecnología extranjera y que "es el momento de que podamos impulsar esta tecnología propia para encontrar esa independencia, esa evolución y esa innovación. Juntos es como realmente lo vamos a conseguir".

Respecto al impulso de la Administración Pública por la ciberseguridad, dice María Isabel Roja que, "llegue al puerto que llegue, el impulso, el esfuerzo y la sensibilidad de la administración pública nos aporta muchísimo". Añade que la aportación no sólo hay que verla desde el punto de vista de las empresas, sino como nación, "porque una nación que no da importancia a la seguridad, es una nación perdida. Si tienes una nación segura con un tejido industrial seguro vas a tener una economía extraordinariamente floreciente".

"Llegue al puerto que llegue, el impulso, el esfuerzo y la sensibilidad de la administración pública nos aporta muchísimo"

María Isabel Rojo, CEO, Enthec

¿Crees que el futuro de la seguridad pasa por la adopción de plataformas/arquitecturas? “El futuro de la seguridad lo dictan los malos. Nosotros vamos adoptándonos a ellos”, asegura, añadiendo que para empresas con cierto pasado adoptar una plataforma de seguridad “va a costar muchísimo dinero y esfuerzo”.

En relación a la consolidación del mercado de seguridad, tiene claro la CEO de Enthec que “llega no tanto en el mercado, sino en que haya dinero para que las empresas puedan consolidar muy bien sus tecnologías, ser fuertes y poder afrontar los riesgos. Ahí es donde llega la consolidación”.

ESET

‘La consolidación tiene que venir por parte del servicio’

Calos Tortosa, Responsable de grandes cuentas, ESET España

Destaca Carlos Tortosa, responsable de grandes cuentas de ESET, que el lema de 16ENISE tiene relación con el cambio de eslogan de la compañía ‘Progress. Protective’; en ambos casos se busca “conjugar a nivel de protección, hacerlo juntos. A mí me da la sensación de que el sector es lo suficientemente corporativo, independientemente de la competencia. No intercambiamos tecnología, pero sí información y la visión de la tecnología. El slogan invita a buscar esa protección de manera conjunta para lo que puede venir”.

Respecto al impulso de las administraciones públicas por la ciberseguridad, destaca el directivo de ESET dos vertientes. Por un lado, todo lo que se ha puesto en marcha con el kit digital, y por otro “estamos detectando en la gran administración pública una gran necesidad de mejora y estamos consiguiendo que una cantidad importante de administración pública, partiendo de una concienciación, sí que mejore y al final esté mejor protegida”.

Preguntado sobre si se tiende a la adopción de plataformas/arquitecturas de ciberseguridad, responde Carlos Tortosa que el cliente sí que monta su propia estructura, pero que se sigue padeciendo la falta de talento “porque tú puedes tener una gran estructura/arquitectura con un alto nivel de protección, pero siguen faltando especialistas que la controlen”.

¿Por dónde crees que vendrá la consolidación del mercado de ciberseguridad de la que tanto tiempo se lleva hablando? “La consolidación tiene que venir por parte del servicio, y siempre tiene que ir a parar a que el servicio me lo de alguien que sepa de qué está hablando. Por detrás podrán ir soluciones arquitecturas… pero al final, y también enlazándolo con el tema del talento, si yo dentro de mi compañía no puedo permitirme captar ese talento

"A mí me da la sensación de que el sector es lo suficientemente corporativo, independientemente de la competencia"

Calos Tortosa, Responsable de grandes cuentas, ESET España

que necesito para mi protección, lo busco fuera y lo subcontrato con empresas que son especialistas”. Añade que esos servicios asociados a herramientas de seguridad pueden ser ofrecidos por empresas pequeñas “pero muy especializadas” y que, por tanto, no serán los grandes integradores los que se vayan a llevar todo el mercado.

Forensic & Security

‘La apuesta por ciberseguridad no sigue el mismo criterio en todas las administraciones públicas’

Pilar Vila, CEO, Forensic & Security

"Debe haber colaboración en seguridad, así como de compartición de información”, dice Pilar Vila en referencia al slogan de 16ENISE, ‘Facing the future together’. Añade que quizá no sea fácil articular esa capacidad, pero sí muy adecuada el “llegar a un entendimiento y trabajar en colaboración”.

Sobre el impulso que la Administración Pública hace por la ciberseguridad, opina la CEO de Forensic & Security que se necesita una mejora. Comenta que en ocasiones “la apuesta por ciberseguridad no sigue el mismo criterio en todas las administraciones públicas (diputaciones, ayuntamientos, etc.). Aunque el CCN intenta marcar unas pautas, no todos las siguen”; añade que hay mucho desconocimiento porque no todo lo que intenta trasladar el CNN llega a toda la Administración Pública

¿Nos encaminamos hacia el mundo de las plataformas/arquitecturas? Yo creo que no porque los grandes players van a favorecerse a sí mismos. Sí que saldrán plataformas nuevas como empresas independientes que agreguen o favorezcan el entendimiento entre diferentes players grandes”, comenta en esta ocasión Ignacio Díaz, CTO de la compañía.

Finalmente preguntamos por la consolidación del mercado de seguridad. Opinan en Forensic & Security que en realidad no habrá consolidación porque cada vez se pierde más canal y cada vez hay más fabricantes. A pesar de que las grandes empresas, con mayor músculo financiero, hacen grandes comparas, también se generan entre ellas escisiones; “yo creo que esto seguirá aumentando y no habrá consolidación”.

"Habría que llegar a un entendimiento y trabajar en colaboración"

Pilar Vila, CEO, Forensic & Security

Redtrust

‘En ciberseguridad tiene que haber una estrategia’

Daniel Rodríguez,
Director General, Redtrust

"Creo que es un lema muy acertado”, asegura Daniel Rodríguez, director general de Redtrust, cuando le preguntamos por el lema de 16ENISE. ‘Facing the future together’, asegura, hace referencia a la esencial colaboración que, en materia de ciberseguridad, debe haber entre las instituciones públicas y las privadas; “en ciberseguridad tiene que haber una estrategia conjunta”.

El impulso que la administración pública hace en ciberseguridad es, en opinión de Daniel Rodríguez, “de una manera bastante adecuada desde hace bastantes años”. Recuerda el directivo lo avanzada que está España en ciberseguridad respecto a otros países europeos y comenta que las sanciones que pueden llegar a tener las empresas privadas en cuanto seguridad no se corresponden con las que luego, por el mismo caso o por el mismo problema, se establecen en el ámbito público”.

"El final del camino no existe, es todo una evolución constante y poco a poco veremos por dónde se consolida el mercado"

Daniel Rodríguez, Director General, Redtrust

creo que eso nos ayuda a las empresas para poder brindar más servicios".

"No hay un solo punto de consolidación", dice el director general de Redtrust cuando le preguntamos por dónde cree que se producirá la consolidación del mercado de ciberseguridad de la que tanto tiempo se lleva hablando. "El final del camino no existe, es todo una evolución constante y poco a poco veremos por dónde se consolida el mercado", concluye.

Secure&IT

'INCIBE tiene la obligación de obligarnos a colaborar entre nosotros'

Francisco Valencia, CEO, Secure&IT

"El mercado de ciberseguridad se consolidará y se comoditizará, y esto creo que es bueno para el mercado, pero también es un riesgo para el sector"

Francisco Valencia, CEO, Secure&IT

¿Nos encaminamos hacia el mundo de las plataformas/arquitecturas de ciberseguridad en la empresa? "Sí, totalmente. Creo que hay un mix de arquitecturas y de posibles soluciones para cada uno de los problemas y tienen que trabajar todas en el mismo entorno. Las arquitecturas van evolucionando, se van externalizando muchos puntos y

"El lema está relacionado con que la unión hace la fuerza. Yo creo que el que estemos aquí todos juntos trabajando por mejorar la seguridad de las empresas y administraciones es bueno, e INCIBE tiene la obligación de obligarnos a colaborar entre nosotros", responde Francisco Valencia cuando le pedimos una opinión sobre el lema de 16ENISE, 'Facing the future together'.

Sobre el impulso que la administración pública hace respecto a la ciberseguridad, dice el directivo de Secure&IT que, aunque queda muchísimo por hacer, "también creo que está avanzando bastante". Destaca que se han creado organismos tanto policiales como dentro de la Administración y también en el seno de la Unión Europea, que están ayudando a definir estrategias, "y aunque de momento están haciendo aún cada uno la guerra por su lado,

como hay tanto por hacer en el caso que vayan haciendo cosas".

Planteamos también a Francisco Valencia si finalmente se tiende hacia el mundo de las plataformas/arquitecturas de ciberseguridad. Asegura que sí, y además como servicio comoditizado, "es decir, empiezan a haber estructuras de ciberseguridad que se venden as-a-service y que las empresas están empezando adoptar de una forma más cómoda y más asequible".

Si es que viene, ¿por dónde crees que vendrá la consolidación del mercado de ciberseguridad?

"Yo creo que se consolidará, y se comoditizará, y esto creo que es bueno para el mercado, pero también es un riesgo para el sector, porque cuando aparezca alguien diciendo que te da toda la seguridad por 20€ al mes, posiblemente no se de pie a los buenos y grandes proyectos de seguridad".

SonicWall

'No creo en las plataformas, y sí en las capas de seguridad'

Sergio Martínez, Iberia Regional Manager, SonicWall

"En este mundo tan complejo en el que todo va a peor es bueno que todos unamos fuerzas para intentar incrementar la ciberseguridad en todas las organizaciones", comenta Sergio Martínez en referencia al lema de 16ENISE, sobre el que asegura que "es muy acertado".

Sobre si la Administración Pública está impulsando adecuadamente la ciberseguridad, asegura el directivo de SonicWall que "está empezando". Añade que está empezando a hacer caso al Esquema Nacional de seguridad (ENS), a valorar discursos que se mantienen desde hace tiempo", pero "en la administración hay mucho por hacer".

Preguntado sobre si vamos hacia el mundo de las plataformas/arquitecturas de ciberseguridad, comenta Sergio Martínez que "esto de la informática se hace a capas. Nunca se hace todo de golpe, y lo que sí es cada vez más importante es la interoperabilidad entre las capas; que haya APIs que se puedan hablar entre ellas, que hay un elemento de visibilidad y control, que puedes hacer en recogida de datos y telemetría de los diferentes puntos que conforman tu infraestructura…". Dicho esto, asegura no creer en las plataformas "y sí en las capas, que pueden ser de diferentes fabricantes si pueden trabajar de forma coordinada entre ellos, siempre con la visibilidad y el control central para poder darle inteligencia a todo".

¿Por dónde crees que vendrá la consolidación del mercado de ciberseguridad? Duda Sergio Martínez que alguna vez se produzca la tan comentada consolidación porque el mercado "está cada vez más atomizado, cada vez hay más actores, cada vez hay problemas nuevos, cada vez más dispositivos", comenta, añadiendo que de lo que era el mercado de ciberseguridad hace diez años a lo que es ahora "fíjate lo que ha cambiado y lo que cambiará dentro de diez años". Negando la consolidación comenta

"En este mundo tan complejo en el que todo va a peor es bueno que todos unamos fuerzas para intentar incrementar la ciberseguridad en todas las organizaciones"

Sergio Martínez, Iberia Regional Manager, SonicWall

también el directivo de SonicWall que habrá "una mayor introducción de la inteligencia artificial que haga que sea cada vez más importante el punto central que coordine todos los esfuerzos para poder dar respuesta a todos los incidentes que se van produciendo. Si tuviera que apostar por algo, sería por ese punto central de visibilidad, control y respuesta automática".

Sophos

'La consolidación del mercado se realizará a nivel de servicios'

Javier Huito, Senior Enterprise Account Executive, Sophos

Para Javier Huito, Senior Enterprise Account Executive de Sophos, el eslogan de 16ENISE, 'Facing the future together', "cubre completamente los objetivos de Sophos, que tienen que ver con consolidar telemetría e información de múltiples fabricantes para poder cubrir realmente los ataques actuales. Creemos que es la única vía para poder estar en línea con la sofisticación de los ataques".

Respecto al impulso de la administración pública por la ciberseguridad, comenta Javier Huito que se ha visto cómo la Administración pública ha invertido muchísimo dinero "en crear aproximaciones que no cubren realmente las necesidades reales de protección, teniendo en cuenta la sofisticación y el grado

"Afrontar el futuro juntos es la única vía para poder estar en línea con la sofisticación de los ataques"

Javier Huito, Senior Enterprise Account Executive, Sophos

de profesionalización del cibercrimen", y añade que la inversión tiene que mantenerse "pero hacer que todas las piezas trabajen de forma coordinada y que se adapten a controlar y a detectar las amenazas reales que se están produciendo en este momento".

Hace referencia el directivo de Sophos a la red nacional de SOC que se quiere poner en marcha desde de las Administraciones Públicas para comentar que, aunque se busca consolidar telemetría

WatchGuard

‘La ciberseguridad es muy importante, pero sigue sin ser la principal preocupación de los CEO’

Carlos Vieira, Country Manager WatchGuard Spain

"No puedo estar más de acuerdo con el lema de este año", dice Carlos Vieira cuando le pedimos que valore el de 16ENISE, ‘Facing the future together’. “Por los desafíos que el futuro nos plantea tenemos que afrontar el futuro de una forma conjunta”, asegura el directivo.

Sobre el impulso que las administraciones públicas están haciendo respecto a la ciberseguridad comenta el directivo que, aunque hay mucho por hacer, o que las subvenciones de los programas Next Gen “están llegando más lentamente de lo que nos gustaría”, “estamos en el camino correcto”

¿Crees que vamos hacia la adopción de plataformas/arquitecturas de ciberseguridad? “Desde el punto de vista del fabricante no tengo ninguna duda”, dice Carlos Vieira comentando además que todos los productos de la compañía ya se ofrecen de manera gestionada desde una única consola

proveniente de múltiples vectores, “los tiempos de respuesta, que realmente es lo importante, están completamente fuera de tiempo teniendo en cuenta que una arquitectura actual de seguridad es vulnerada en menos de dos minutos. Tenemos que mejorar esos tiempos y que las herramientas que se pongan en marcha tengan esa capacidad de detección y añadir una capa de respuesta ante estos incidentes”.

Respecto a la consolidación del mercado de ciberseguridad, comenta Javier Huito que se producirá a nivel de servicios; “los servicios cada día van a ser más importantes”. Asegura Javier Huito asegurando además que “el futuro pasa por crear un modelo de servicio en que directamente lo que ofrezco sea una capa por encima de la tecnología, que sea capaz de trabajar abiertamente con todos los fabricantes que existen en los clientes finales”.

"El mundo de las plataformas es la única forma de tener una detección, la respuesta más rápida, más efectiva para Facing the future together"

Carlos Vieira,
Country Manager WatchGuard Spain

"dando respuesta a la simplicidad que se requiere por parte de los clientes".

El mundo de las plataformas, concluye, "es la única forma de tener una detección, la respuesta más rápida, más efectiva para Facing the future together".

El de la ciberseguridad es un sector muy dinámico en el que constantemente aparecen nuevas empresas que cubren diferentes nichos dentro de las arquitecturas de ciberseguridad. Opina Carlos Vieira que la consolidación del mercado se producirá, y que se hará en tres entornos diferentes, del lado de los mayoristas, en el mercado de integradores/partners/MSSPs, y fabricantes. Respecto al primero, "hemos asistido a esta consolidación desde unos años atrás, y todavía hay espacio para hacer un fine tunning". Del lado de los partners "nos falta hacer ese proceso de consolidación, que creo que se va a haber en los próximos dos o tres años".

Finalmente, desde el punto de vista de los fabricantes, comenta el director general de WatchGuard que es donde queda mucho más por hacer y donde una posible crisis que muchos avecinan tendría un fuerte impacto. Por una parte, "la ciberseguridad es muy importante, pero sigue sin ser la principal preocupación de los CEO", por lo que hay límites en los presupuestos a los que se pueden acceder. Menciona también la "burbuja bursátil" que rodea a muchos fabricantes de nicho, y que una crisis económica podría pinchar.

Enlaces de interés...

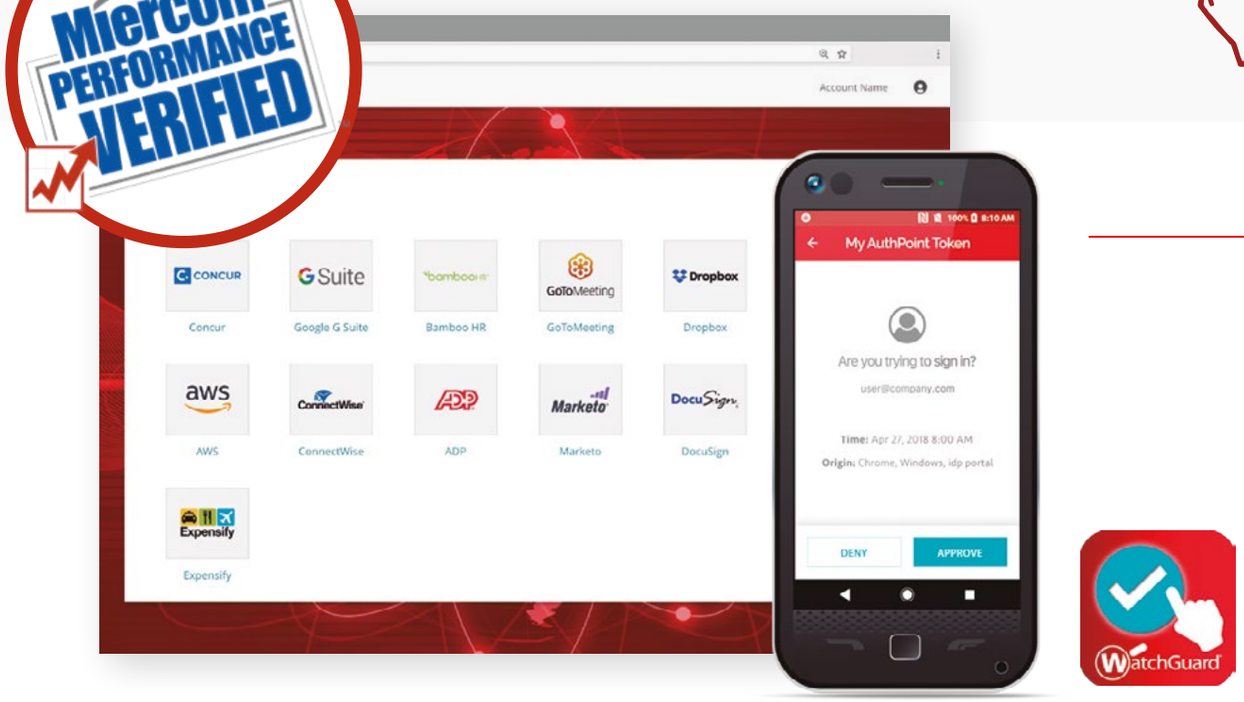
- INCIBE
- 16ENISE

Compartir en RRSS

WatchGuard AuthPoint

1 de cada 5 personas utiliza sistemáticamente contraseñas poco seguras o compartidas

¿Cuántas de estas personas trabajan en su organización?



AuthPoint proporciona autenticación multifactor (MFA) en una plataforma de nube fácil de usar.

La aplicación móvil AuthPoint hace que cada intento de inicio de sesión sea visible y, como es un servicio en la nube, no es necesario implementar hardware. Puede administrarse desde cualquier lugar y ofrece integraciones con aplicaciones de terceros, incluidas populares aplicaciones de la nube, servicios web, VPN y redes.

Ventas España: +34.917.932.531 Email: spain@watchguard.com WEB: www.watchguard.com/es

Estado de CIBERSEGURIDAD en España

Elaborado por:

itRESEARCH

Para:

Secure&IT by LKS

www.secureit.es

Estado de ciberseguridad en España

Este documento busca conocer la situación de las empresas a la hora de hacer frente a los ciberataques y ciberamenazas, cada vez más numerosas y más sofisticados, así como la importancia de las labores de formación y concienciación, o qué tipo de amenazas preocupan más.

Ahora más que nunca, la ciberseguridad es esencial para nuestro futuro; después de todo, es vital para proteger todo aquello en lo que confiamos hoy. Sin embargo, a raíz de las migraciones masivas a la nube y la transformación digital, muchas organizaciones aún no han alcanzado la cima de sus operaciones de seguridad debido a algunos desafíos clave, como un panorama de amenazas en constante evolución y una creciente complejidad de los entornos híbridos y de múltiples nubes.

IT Digital Security, en colaboración con Secure&IT, ha realizado una encuesta entre profesionales españoles durante los meses de junio a septiembre de 2022 para conocer qué tipo de amenaza preocupa más a las empresas, qué aspecto se valora más a la hora de trabajar en una empresa, qué tecnologías se tienen implementadas o cuáles son las tendencias de inversión en ciberseguridad.

Por otra parte, existe una preocupación generalizada de que la fuerza laboral aún no está preparada para hacer frente a las ciberamenazas con éxito debido a la falta de experiencia en ciberseguridad y TI a nivel local. Los planes de formación y conciención, ¿interesan a las empresas? ¿tienen planes de inversión?

El objetivo de este estudio es conocer la situación de las empresas a la hora de hacer frente a los ciberataques y ciberamenazas, cada vez más numerosas y más sofisticados, así como la importancia de las labores de formación y concienciación, o qué tipo de amenazas preocupan más.

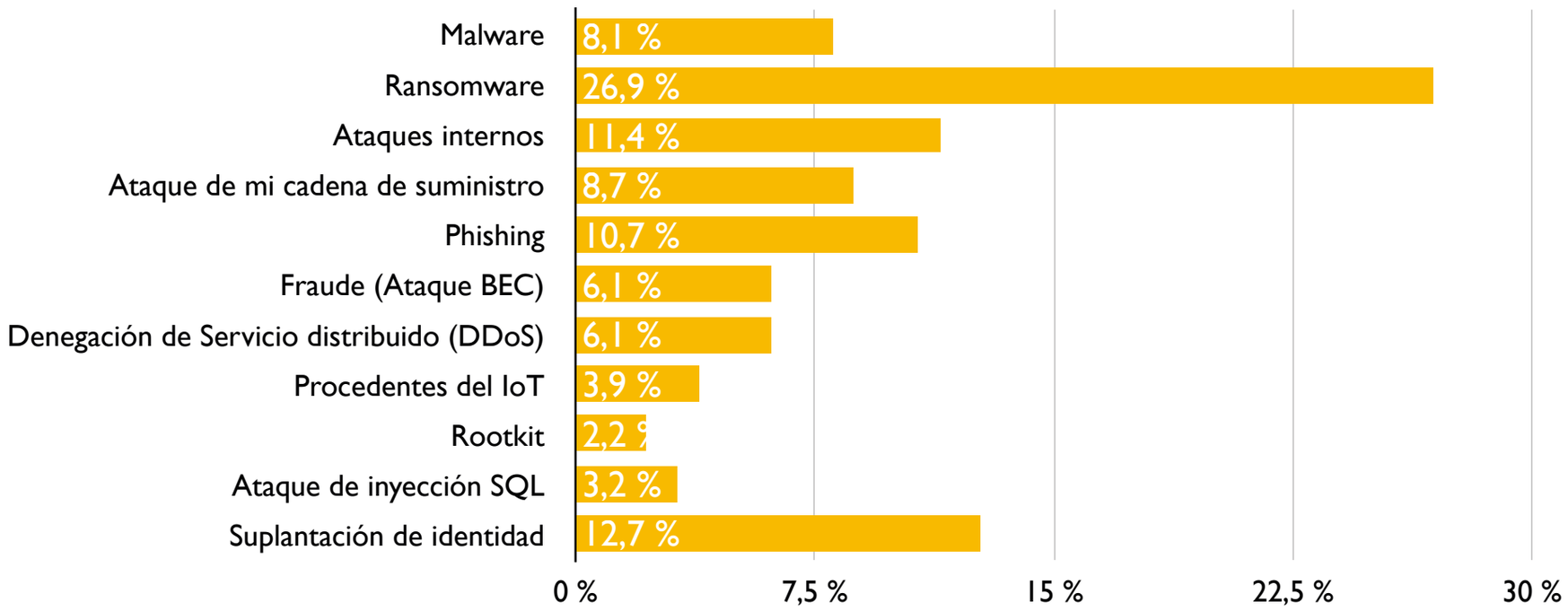
"Hay que considerar al empleado como un aliado. Y para que alguien sea un aliado en tu empresa y en cuestiones de seguridad de la información y de protección de datos, que para mí van totalmente de la mano, es fundamental enseñar"

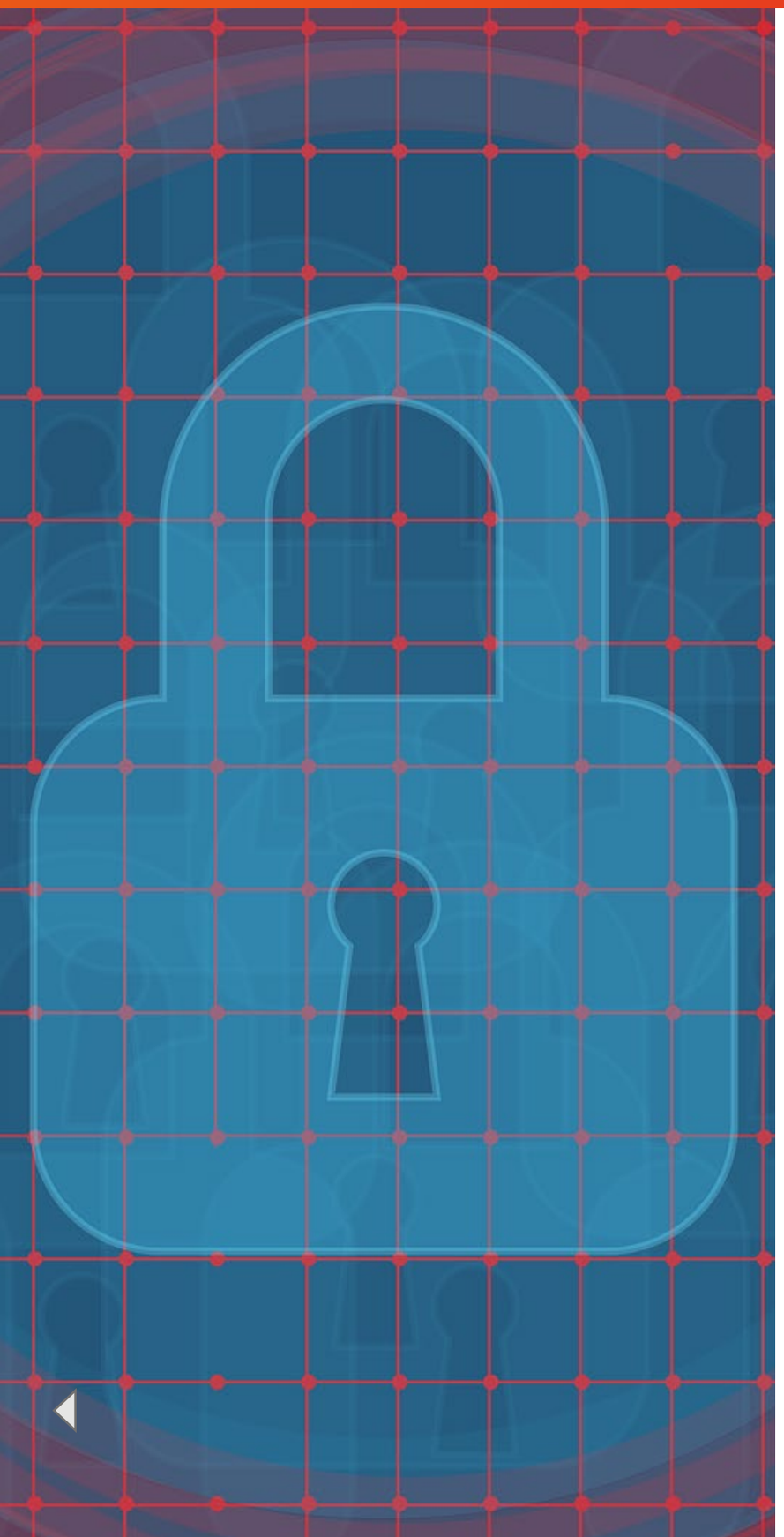
Gustavo Lozano García, CISO, ING

¿Qué tipo de ataque le preocupa más?

Los ciberataques se han multiplicado en los últimos años, pero hay amenazas que preocupan más que otras. El ransomware es, desde hace unos años, una de las que más preocupa. Indican los expertos que el ransomware ha descendido, pero a cambio de ser más dirigido y más peligroso. De once amenazas propuestas, un 26,9% de las respuestas han seleccionado el ransomware como el tipo de ataque que les preocupa más, seguido de la suplantación de identidad (12,7%), los ataques internos (11,4%) o el phishing (10,7%).

Los rootkits, o paquetes de software malicioso diseñados para permitir el acceso no autorizado a un equipo o a otro software, que fueron muy populares hace una década, parecen estar pasando a mejor vida. Además de utilizados por los ciberdelincuentes para acceder a los equipos, fueron utilizados por avezados usuarios para hacer lo que se denominaba un "jailbreak" en iOS o "rooting" en Android con el fin de obtener permisos de superusuario, algo que el fabricante bloquea principalmente por razones comerciales, pero también para proteger la seguridad del dispositivo. La utilización de este tipo de equipos modificados en entornos empresariales fue un dolor de cabeza para los responsables de seguridad. Hoy, sólo preocupa al 2,2%.



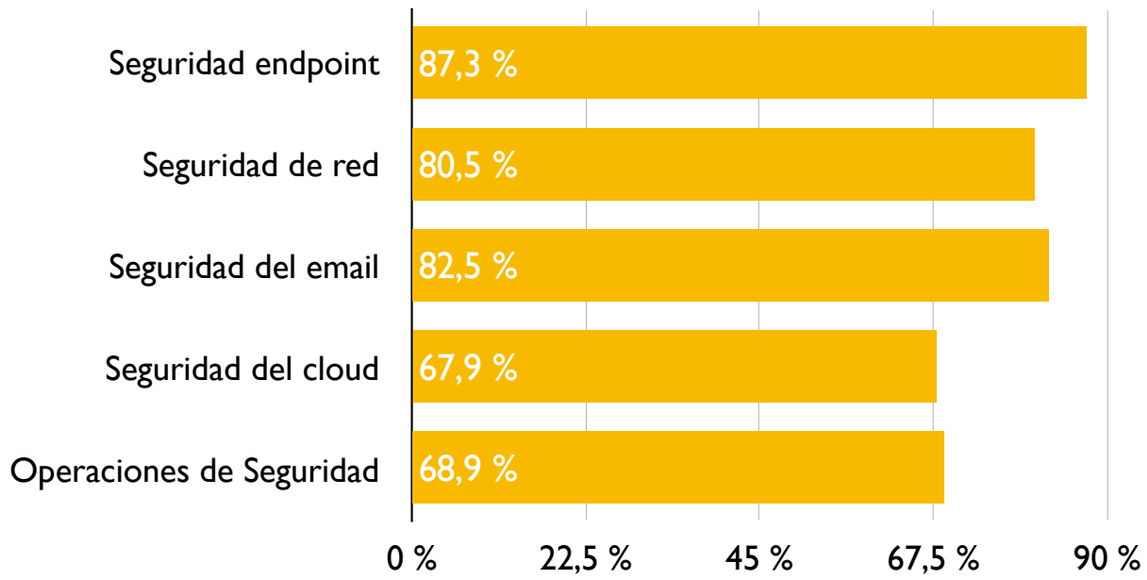


¿Qué tipo de tecnologías tiene implantadas?

En este estudio se plantearon una serie de tecnologías de seguridad básicas que toda empresa debería, en mayor o menor medida, tener implementadas. Los datos recogidos no sorprenden.

Un 87,3% de los encuestados tienen implementaciones de seguridad endpoint en sus empresas. También es amplia la adopción de seguridad de red, existente en el 80,5% de los negocios, pero preocupa más la seguridad del email, que está disponible en el 82,5% de las empresas españolas. No es mala opción teniendo en cuenta que el correo electrónico es uno de los principales vectores de ataque utilizados por los ciberdelincuentes.

La seguridad del cloud (67,9%) y las Operaciones de Seguridad (68,9%) (SecOps), que mantienen y restauran las garantías de seguridad del sistema a medida que los adversarios directos lo atacan, también son tecnologías utilizadas, aunque en menor medida.



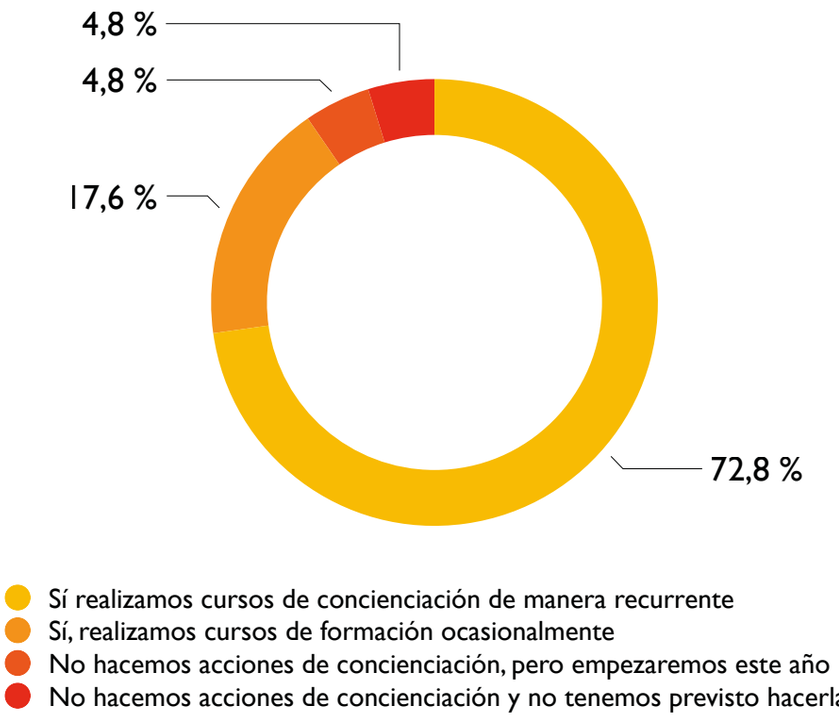
Formación y concienciación del usuario

Por muy buenas tecnologías que una empresa tenga implementadas, el error humano puede ser fatal. Hace años que los planes de formación y concienciación de los empleados forman parte de los planes de seguridad de muchas empresas.

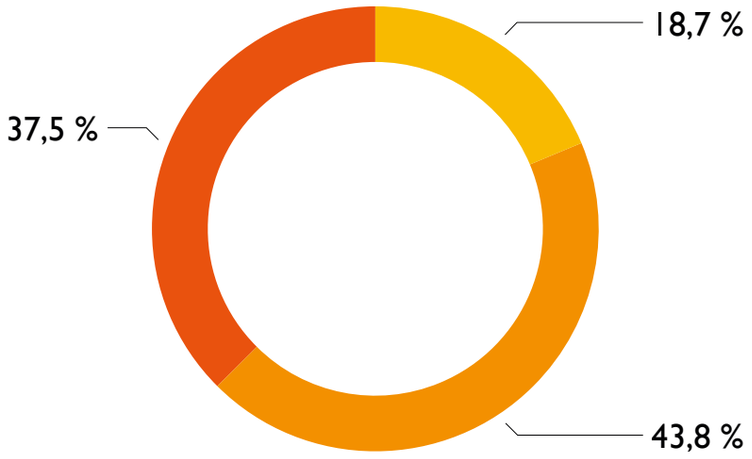
Entre otras cosas, estos planes ayudan a los usuarios a detectar un phishing que lleve a un robo de credenciales, que a su vez permita un acceso no autorizado, que termine en una brecha de seguridad, que deje escapar información sensible. Un desastre.

En el 90,4% de las empresas se realizan planes de formación y concienciación. Los más efectivos son los recurrentes, que son la opción del 72,8% de las empresas, mientras que un 17,6% opta por formación y concienciación de una manera más ocasional.

Del 9,6% de las empresas que aún no concienciación a sus empleados en ciberseguridad, la mitad planea hacerlo y la otra mitad no tiene intención de adoptarlo.



Estado de ciberseguridad en España



Asesoramiento externo

La ciberseguridad es un asunto complejo. No sólo desde el punto de vista tecnológico habida cuenta de la cantidad de herramientas que se utilizan, sino desde el punto de vista de normativas, más o menos dependiendo del sector en el que se trabaje.

Sólo el 18,7% de las empresas trabajan todo internamente, y un 81,3% buscan asesoramiento tecnológico y legal fuera de la empresa.

La mayoría, un 43,8% opta por solicitar asesoramiento en la parte legal y de cumplimiento, mientras que un 37,5% opta por solicitar asesoramiento en la parte tecnológica.

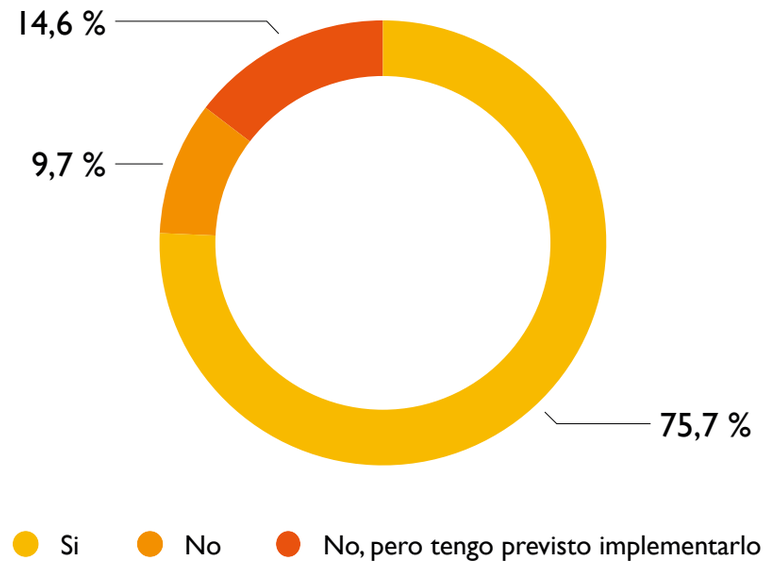
PCI DSS, HIPAA, GDPR, ISO… la lista de normativas que las empresas deben cumplir hoy en día es tan larga como tediosa. En cuanto a las tecnologías, ya sabemos lo rápido que avanzan.

¿Haces uso de servicios de monitorización de SOC?

El SOC, o centro de operaciones de seguridad, es el que ayuda a las empresas a tener el control sobre lo que está sucediendo con la seguridad de sus empresas. Está compuesto por una plataforma tecnológica y un equipo técnico y humano que está altamente cualificado y posee las herramientas necesarias para, monitorizar, analizar, prevenir y dar respuesta ante cualquier incidente de seguridad. Gracias al SOC se acelera y simplifica la detección de amenazas, la respuesta a incidentes y la gestión del cumplimiento normativo a las empresas.

Los sistemas de información generan millones de eventos y alertas desde los procedentes de sistemas de seguridad como el firewall, waf, IDS/IPS, control de accesos, etc., a los generados por otras plataformas o servicios, como ERP o el DNS. Por eso, los SOC se han convertido en parte indispensable de la operativa de seguridad. Así lo entienden, al menos el 75,7% de los profesionales encuestados, que aseguran hacer uso de servicios de monitorización de SOC.

Del 24,3% de empresas que no lo hacen, un 14,6% tiene previsto implementar este tipo de servicios.



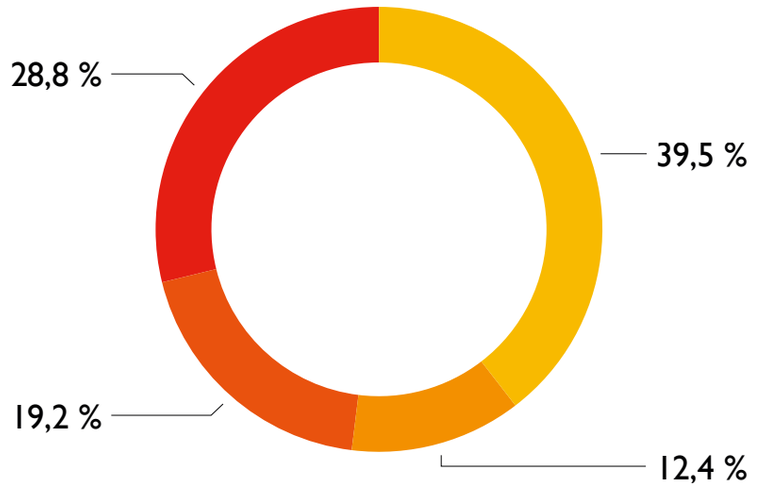
¿Qué aspectos valora más a la hora de trabajar en una empresa?

Tras el salario económico, la capacidad de teletrabajar es, para el 28,8% de los encuestados, el aspecto que más valora a la hora de trabajar en una empresa. No es tema baladí teniendo en cuenta que contratar y retener a profesionales del mundo de la ciberseguridad se está convirtiendo en un verdadero dolor de cabeza para las empresas.

La pandemia abrió las puertas al trabajo remoto, que por otra parte ya era más o menos habitual en muchas empresas. Ahora se avanza hacia lo híbrido, lo que supone un reto desde el punto de vista de la ciberseguridad.

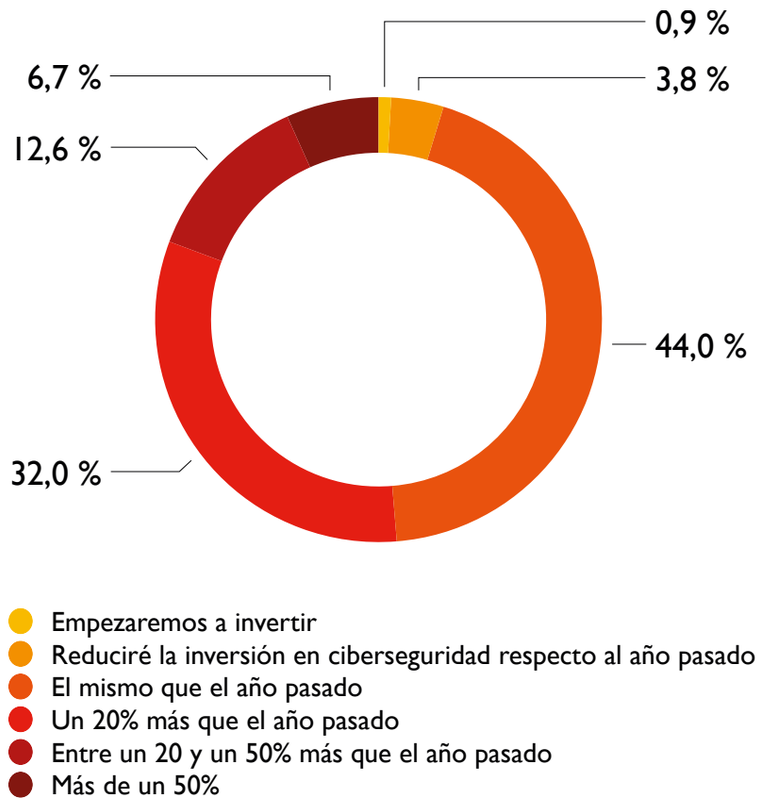
Después del salario económico y la capacidad de trabar desde casa, la flexibilidad horaria es, para el 19,2% de los encuestados el tercer elemento a tener en cuenta a la hora de trabajar en una empresa.

Para un 12,4% también cuenta lo que se conoce como salario emocional, que incide directamente en el rendimiento de los profesionales y, por tanto, en la competitividad de la compañía. Aquí entra desde ofrecer un seguro médico, formación, servicio de cafetería gratis, etc.



- Salario económico
- Salario emocional (Seguro médico, Formación, servicio de cafetería...)
- Flexibilidad horaria
- Capacidad de teletrabajo

Estado de ciberseguridad en España



Niveles de inversión

Lo último que se les ha pedido a los encuestados para este estudio es que indiquen los niveles de inversión en ciberseguridad para este año que, según datos de un informe de IDC alcanzará los 1.749 millones de euros, un 7,7% más que en 2021.

El 44% de las empresas han mantenido los mismos niveles de inversión que el año pasado, mientras que un 51,3% los han aumentado en mayor o menor medida. Sólo un 3,8% los han reducido, y un 0,9% asegura que empezará a invertir.

Respecto a las empresas que invierten más en ciberseguridad este año, un 32% aumenta sus niveles de inversión un 20% más que el años pasado; un 11,6% entre el 21% y el 50%; y un 6,7% habrá aumentado su inversión cuando acabe el año más de un 51%.

utimaco®

SOLUCIONES de CIBERSEGURIDAD

Síguenos en:

www.realsec.com

MÉXICO
Av. Jaime Balmes 8 piso M6-A,
Colonia Los Morales, Polanco, Alcaldía
Miguel Hidalgo, C.P 11510, Ciudad de México
Tfno.:+52 (55) 44 35 00 45
E-mail: infomexico@realsec.com

OFICINAS CENTRALES
ESPAÑA
C/ Infanta Mercedes 90. Planta 4.
28020 Madrid
Tfno.: +34 91 449 03 30
E-mail: info@realsec.com

realsec
by utimaco®

‘A la hora de escoger una herramienta es muy importante conocer tu realidad’

(Cristiano Dias, H10 Hotels)

Considera Cristiano Dias, CISO de H10 Hotels, que la concienciación y la formación continua son aspectos clave de la ciberseguridad empresarial; que el CISO debe tener en mente el negocio; que hay que estar considerando las ciberamenazas para ser más resiliente, o que apostar por infraestructuras tecnológicas montadas en cloud es parte de un futuro que ya está aquí.

Cristiano Dias es el CISO de H10 Hotels, una compañía de origen español que cuenta con una sede en Barcelona y más de 67 hoteles repartidos por el mundo. Antes fue CISO de Moventia, puesto que alcanzó después de ejercer como arquitecto de sistemas durante varios años. Porque para llegar a ser CISO hay que ir “aprendiendo y especializándose con el tiempo”, reconoce el directivo, añadiendo que en tecnología el aprendizaje es continuo.

Comenta que ha tenido la oportunidad de ver el nacimiento y evolución de Internet desde las primeras conexiones, y que se considera un “apasionado de la red y, sobre todo, de la ciberseguridad”. Para ser CISO no sólo te tiene que gustar la tecnología, sino su dinamismo en un mercado tan cambiante, “porque lo que hoy estás haciendo, mañana ya no te sirve”. El trabajo del CISO es “duro”, porque la seguridad 100% sabemos que no existe.

“Dentro de la ciberseguridad, la información y la formación son piezas clave. De nada te sirve

montar una estructura con las mejores soluciones de seguridad si no tienes un equipo formado y concienciado", asegura Cristiano Dias, para después añadir que se busca estar constantemente informado y compartiendo la información con todo el equipo.

Respecto a los retos a los que debe enfrentarse un CISO destaca el CISO de H10 Hotels que el principal es alinear el negocio y la infraestructura con las necesidades de seguridad de la compañía; "cómo proteger cada activo, cada servicio de la empresa, de la manera más adecuada para poder seguir creciendo".

"Hay muchos ataques que son muy dirigidos, pero sabemos que hay muchas compañías que han caído en ataques muy básicos"

En un mercado tan saturado de fabricantes, soluciones y propuestas, que además evolucionan tan rápidamente, ¿cómo escoger? "Es muy importante conocer la realidad que tú tienes", asegura Cristiano Dias. Explica que no tiene sentido que una compañía se plantee implementar un EDR, que es la solución más sofisticada para la protección del endpoint, si no tiene una infraestructura capaz de absorber toda la información, el conocimiento, que generan estas herramientas.

De forma que, antes de adoptar una herramienta, es muy importante saber si tu infraestructura está preparada. Hay que ir adquiriendo madurez con herramientas menos sofisticadas, que un

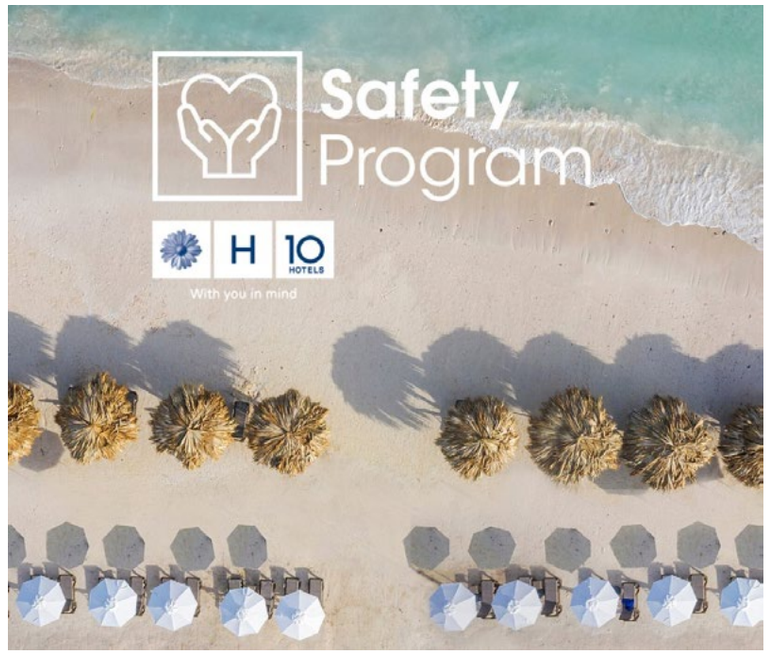
equipo sea capaz de gestionar, e ir evolucionando, “porque uno de los problemas que tenemos es la obsolescencia de los sistemas”, asegura, recordando que en ocasiones no es posible hacer actualizaciones. Esto lleva al CISO de H10 Hotels a proponer que se tiene que buscar un plan B para mitigar un riesgo sin las herramientas más modernas. “A la hora de escoger una herramienta intento buscar la mejor, pero la mejor que se adecúe al ecosistema que tengo”, concluye.

¿Qué tipo de amenaza le quita el sueño a Cristiano Dias? Como a casi todos, el ransomware, y sobre todo por la manera en que va evolucionando. “Constantemente hay ataques dirigidos y yo intento imaginarme en todo momento situaciones para ser resilientes si llega un ataque”, nos cuenta, añadiendo que es importante estar haciendo este tipo de ejercicios para tener un plan de respuesta ante incidentes lo más completo posible.

El IoT es una realidad en los hoteles, donde ya empiezan a verse recepciones totalmente digitalizadas, sin intervención humana. Además, empresas como la de Cristiano Dias deben enfrentarse a clientes accediendo a sistemas de reserva, a redes wifi… ¿Cómo se afrontan todo este tipo de situaciones específicas del sector hospitality? “En cuanto a las redes corporativas trabajamos con segmentación y aplicando controles de acceso estrictos”, dice el directivo, añadiendo que se tienen herramientas capaces de monitorizar la red 24/7 y un SOC propio gracias a que se cuenta con una oficina en el Caribe para cubrir la diferencia horaria.

Sobre la importancia, o no, de la inteligencia artificial en la seguridad empresarial, dice Cristiano Dias que se trabaja con machine learning en la herramienta de detección de anomalías. También le preguntamos por la concienciación, que para el directivo tiene una gran importancia porque “como te había dicho al comienzo de la entrevista, la concienciación es la parte más vital dentro de tu entorno, porque hay muchos ataques que son muy

"Trabajamos con segmentación y aplicando controles de acceso estrictos"



"De nada te sirve montar una estructura con las mejores soluciones de seguridad si no tienes un equipo formado"

dirigidos, pero sabemos que hay muchas compañías que han caído en ataques muy básicos".

Preguntamos a Cristiano Dias por las tecnologías de seguridad básicas que toda empresa debería tener. Propone el CISO de H10 Hotels un firewall, un antivirus con funcionalidades avanzadas, o EDR, que esté bien configurado, y un IDS que ayude en la detección de alertas básicas. Estas son las tres piezas con las que debería iniciarse un programa de ciberseguridad. Añade como otros aspectos básicos el mantener los equipos actualizados y dar acceso sólo a lo que se necesite.

Mirando hacia adelante, apuesta Cristiano Dias por tener "las infraestructuras tecnológicas montadas en cloud, donde tengo los datos distribuidos", además de contar con un SOAR (Security Orchestration, Automation and Response).

Enlaces de interés...

- 'La inspección de tráfico de red en tiempo real es fundamental' (Jesús M. Doña, EMASA)
- 'En general, no se aprovecha todo el potencial que ofrece la tecnología que has implantado' (Gustavo Lozano, ING)
- 'La IA nos ayuda muchísimo, pero hay que acompañarla con inteligencia humana' (José Israel Nadal, Age2)
- 'La seguridad se convertirá en una ventaja competitiva de las empresas' (Pablo Masaguer, CISO, Sociedad Textil Lonia)
- 'Lo importante, y más en el ámbito de la seguridad, no es tanto la solución o producto que vayas a seleccionar, sino el proveedor' (Roberto González, Grupo Primavera)

Compartir en RRSS

Controla los certificados digitales para una identidad digital segura en entidades **bancarias y financieras**

Controla y gestiona permisos de uso

Firma digitalmente documentos

Usa los certificados en cualquier lugar

Cumple con la normativa del sector

Descubre más sobre nuestra solución en
redtrust.com/sectores/banca-fintech

redtrust
a **KEYFACTOR** company

‘Nadie sabe cómo contratar a un profesional de ciberseguridad’

(Ottavio Camponeschi, Cyberbit)

Llevamos décadas hablando de tecnologías, pero es el factor humano el que marca la diferencia. Así lo asegura Ottavio Camponeschi, Senior Director EMEA de Cyberbit, una compañía que abre oficina en España de la mano de Blas Simarro para promover un cambio: “No vendemos firewalls, ni IPS, ni EDR. Vendemos algo que es mucho menos tangible y más valioso. Estamos promoviendo un cambio cultural en el mundo: que la tecnología por sí misma no vale. Necesitas gente preparada”.

Rosalía Arroyo

Cyberbit es una empresa israelí, fundada en 2015 con el objetivo de trasladar las maniobras militares tradicionales al mundo virtual, a la ciberseguridad. Nos lo cuenta Ottavio Camponeschi, Senior Director EMEA de la compañía, durante un breve encuentro mantenido en un reciente viaje del directivo a Madrid. Igual que las maniobras militares sirven de preparación para una guerra, Cyberbit permite hacer prácticas de ciberataque y ciberdefensa a los responsables de ciberseguridad de las empresas, y hacer frente a situaciones de crisis a los altos ejecutivos. La propuesta se creó en el seno del Mossad y las IDF (Fuerzas de Defensa de Israel), dentro de las cuales se ha utilizado antes de expandirse al mundo.

Con la tecnología de Cyberbit, que este año abre oficinas en España de la mano de Blas Simarro,

"Ya es hora en que las empresas miren hacia las personas y se aseguren de convertirlas en el elemento central de lucha contra los ciberdelincuentes"

se puede practicar y ejercitar la manera de reaccionar ante los ciberataques, explica Ottavio Camponeschi, quien añade que actualmente "esta es una práctica muy común en toda la industria de defensa, pero también en los grandes bancos, las grandes empresas de telecomunicaciones. Todos nuestros clientes utilizan la plataforma para ejercitarse".

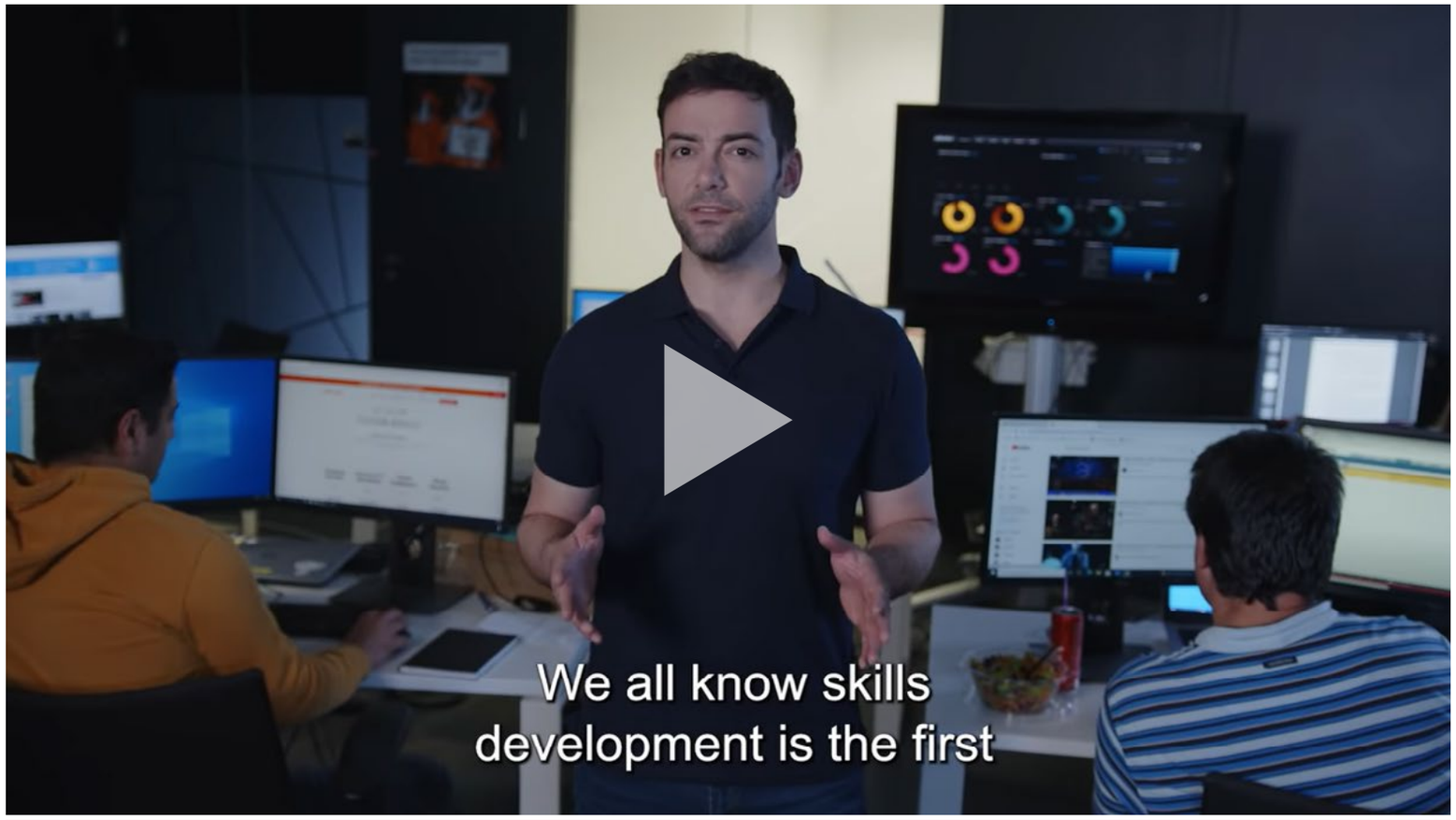
Planteado si la tecnología es similar a la utilizada por las empresas que se mueven en los entornos de BAS (Breach and Attack Simulation), como Cymulate, Picus o Pentera, explica Ottavio Camponeschi que lo que hacen estas plataformas es simular ataques para verificar los controles de seguridad, "se comprueba que el firewall, el EDR o cualquier otra herramienta esté configurada correctamente moviendo malware de un lado a otro". La propuesta de Cyberbit es diferente. Lo que hace esta compañía es generar un ataque en un entorno virtual extremadamente realista, "y le pedimos a la gente que investigue ese ataque, que mitigue ese ataque, que detecte ese ataque". Es decir, las plataformas BAS ponen a prueba la tecnología, Cyberbit pone a prueba a las personas y los procesos para determinar "si dispongo de los recursos adecuados para hacer frente a un ciberataque".

La oferta de Cyberbit ha evolucionado desde que se creó en 2015. De ser un puro simulador de ejercicios se ha convertido en una plataforma de entrenamiento a la que Camponeschi se refiere como una "360 crisis management platform". Asegura el directivo que la tecnología es limitada y que necesitamos a personas con las habilidades adecuadas, por eso "la plataforma se ha convertido en

"Las plataformas BAS ponen a prueba la tecnología, Cyberbit pone a prueba a las personas y los procesos para determinar si dispongo de los recursos adecuados para hacer frente a un ciberataque"

una plataforma de evaluación, validación y desarrollo de habilidades, que abarca desde los técnicos hasta los ejecutivos, porque cada vez más los CEOS, CMOs, Chief Legal Officer… son críticos".

Plantea Ottavio Camponeschi qué hacer en caso, por ejemplo, de un ataque de ransomware. ¿hay que pagar o no? ¿Hay que comunicar el incidente a la prensa? ¿decir que se ha robado el número de tarjeta de crédito?... "necesitas comunicarte de manera oportuna" frente a un problema que no sólo hay que solventar desde la parte técnica, sino desde la sala ejecutiva", porque, aunque el objetivo principal sigue siendo el equipo técnico, hay una extensión de la plataforma que permite que el comité ejecutivo se capacite y comprenda qué debe hacer en caso de una crisis.



GET YOUR TEAM READY TO RESPOND WITH CYBERBIT

CLICAR PARA VER EL VÍDEO

Diferencial

"Somos extremadamente profundos en lo que hacemos", asegura Ottavio Camponeschi cuando le preguntamos por el diferencial de Cyberbit respecto a otros competidores.

Lo segundo, destaca el directivo es que el producto está muy enfocado a la parte superior de la cadena técnica de ciberseguridad; "estamos muy centrados en la ingeniería de seguridad del SOC, los arquitectos de seguridad y la seguridad de TI. Y obviamente ahora también la parte ejecutiva porque también es importante gestionar esos requisitos".

Respecto a los clientes tipo de Cyberbit, son grandes empresas, "y si tiene un SOC mejor, porque añade valor", dice Camponeschi, añadiendo que las grandes firmas de consultoría e integradores de sistemas son los grandes clientes de la plataforma, que la utilizan para asegurarse de que

"Vemos una adopción masiva de este tipo de plataformas en los próximos tres a cinco años"

pueden vender sus servicios “a los principales clientes con las personas adecuadas y el conocimiento adecuado. Para mí, esta es la tarjeta de presentación más valiosa que podemos presentar”. Una tarjeta de presentación en la que están presentes, entre otros, Deloitte, Accenture, KPMG, PwC o Infosys.

Expansión y filosofía

La compañía ha acelerado sus planes de expansión internacional, pero de una manera “pragmática”, reconoce el directivo. Cyberbit tiene una amplia presencia en Estados Unidos y Asia, y recientemente ha fijado su mirada en la región de EMEA.

La compañía ya tiene presencia en España, Francia, Alemania, Italia, Holanda, y Reino Unido, y se expande rápidamente en Oriente Medio, “pero somos muy pragmáticos. No vendemos soluciones típicas de seguridad. No vendemos firewalls, ni sistemas de prevención de intrusiones, ni EDR. Vendemos algo que es mucho menos tangible y más valioso. Estamos promoviendo un cambio cultural en el mundo: que la tecnología por sí misma no vale. Necesitas gente preparada”.

Asegura también el directivo que nos estamos enfrentando a un reto importante: no hay dinero para formación. En ciberseguridad, explica, todo es completamente diferente, y “tienes que asegurarte de que tu primer nivel de defensa contra el enemigo esté preparado”.

Es decir, que la mayoría de las empresas no saben que necesitan tu plataforma… “Creo que ese es el punto. Estamos entrando en una fase en la que vemos una adopción masiva de nuestra tecnología en los próximos tres a cinco años”, responde Ottavio Camponeschi. Asegura también el directivo que “nadie sabe cómo contratar a un profesional de seguridad”. En otros sectores se puede mirar el plan de estudios, y luego decidir si esa persona te gusta o no para el puesto, “pero cuando se trata de ciber, es muy complicado analizar si ese individuo es realmente bueno”.

Durante muchos años se ha confiado en la tecnología, “y es hora en que las empresas miren hacia las personas y se aseguren de convertirlas en el elemento central de lucha contra los ciberdelincuentes”, asegura Camponeschi, añadiendo que la magia no funciona sin la gente, que los clientes están recibiendo miles de millones de alertas y, “al final, son las personas quienes deberán decidir si son blancas o negras”.

Esta declaración, ¿es una llamada de atención a la Inteligencia Artificial? “Sí, tal vez, pero sigo siendo muy práctico. La inteligencia artificial es buena, pero las personas siguen siendo extremadamente valiosas. Creo que las empresas deben darse cuenta de que las personas son el activo más valioso y el activo más caro. Y que, a menos que los equipe con el back end adecuado, perderán dinero”.

España y canal de distribución

“We are channel friendly”, dice el directivo de Cyberbit. “No queremos vender en directo porque hay servicios que el partner puede proporcionar en nuestra plataforma. Y no somos una empresa de servicios. Somos un vendedor. Entendemos claramente lo que estamos haciendo, pero queremos que el socio

"Cuando se trata de ciber, es muy complicado analizar si ese individuo es realmente bueno"

"La inteligencia artificial es buena, pero las personas siguen siendo extremadamente valiosas"

Enlaces de interés...

- CyberbitPlatform
- Empowering the Enterprise CISO with SOC Team Readiness

brinde valor y servicios a través de nuestra plataforma", asegura también Camponeschi.

Sobre si la empresa española es lo suficientemente madura para la plataforma de Cyberbit, responde Blas Simarro, presente en la entrevista que "hay compañías con distinto nivel de madurez que lo entienden mejor que otras".

Añade que hay un factor común que les une: todas tienen problemas para reclutar gente, todas están pagando muy caros los perfiles que están reclutando, y aun así no cubren suficientemente las plazas. Explica Simarro que la plataforma de la compañía permite "reclutar de una manera eficiente a esos profesionales con una medición objetiva de lo que se está contratando, buscando los gaps y acomodando esos perfiles profesionales a las necesidades reales que tiene la empresa; y además crear un camino de mejora, una carrera profesional para esos profesionales". Añade el responsable de Cyberbit para la región de Iberia que son muchos los profesionales que no tienen medios de evolucionar en sus carretas, y que a través de la plataforma "les ofrecemos la posibilidad de estar siempre al día, haciendo que el entorno de trabajo sea más atractivo para ellos dentro de esa empresa en la que están trabajando".

Nos confirma también Blas Simarro que Deloitte y Accenture son partners en la región, y que "estamos en proceso de firmar otros acuerdos" que se irán anunciando.

Compartir en RRSS

Forcepoint ONE

Welcome to the power of ONE

ONE Platform

ONE Console

ONE Agent

Forcepoint

www.forcepoint.com

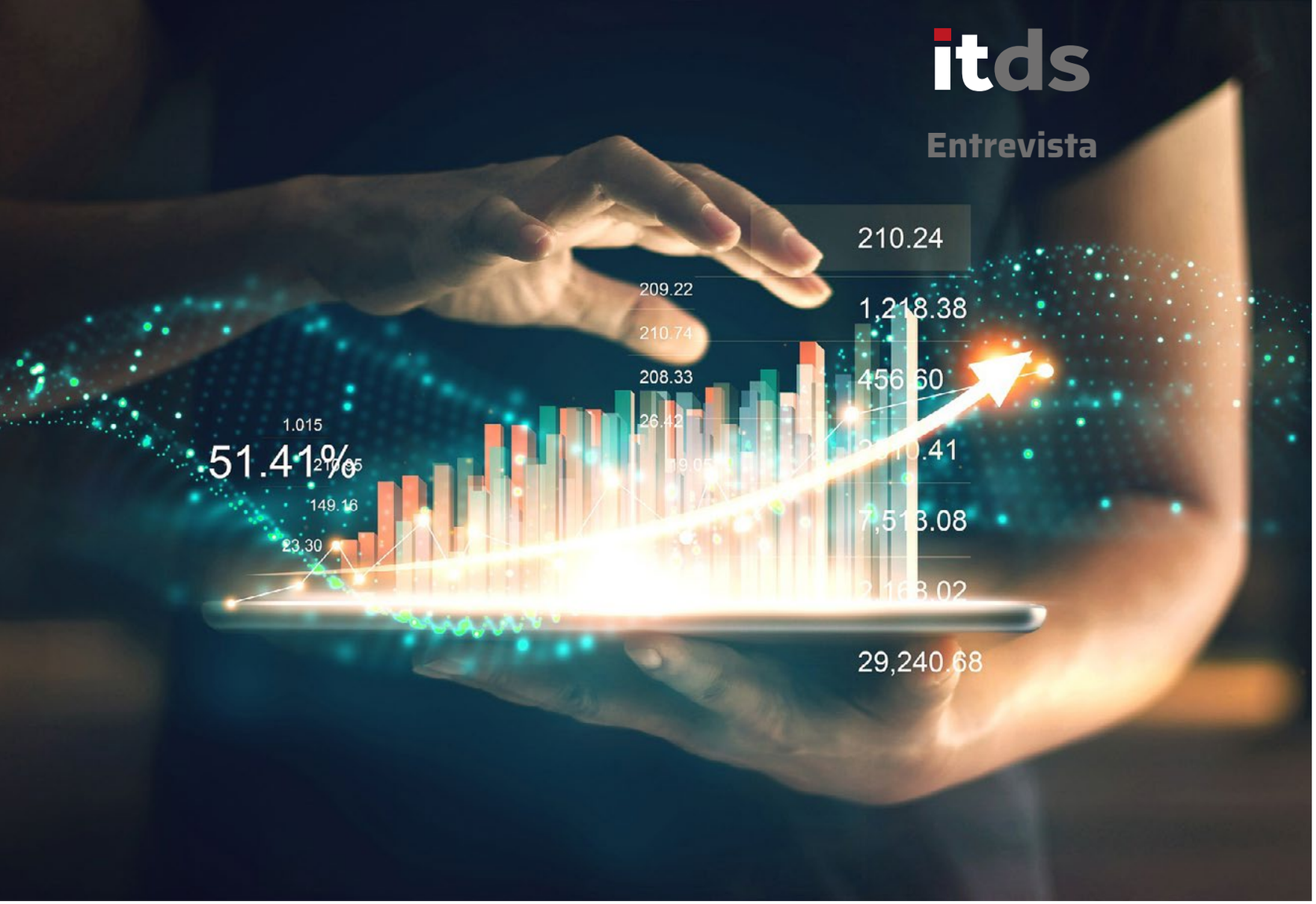
‘Ya sean en productos o servicios, el mercado de seguridad pide foco y flexibilidad’

(Javier Cazaña, Cynet)

Cynet es una empresa joven. Se fundó en 2015 en Tel-Aviv y hasta la fecha acumula 78 millones de dólares en diferentes fases de financiación. Con la sede instalada en Boston, la compañía, que proporciona una plataforma autónoma de protección que ayuda a identificar problemas de seguridad, y proporciona inteligencia de amenazas y gestión de la seguridad endpoint, hace unos meses abrió oficina en España de la mano de Javier Cazaña, un conocido del sector que hace unos años fue el responsable de abrir mercado en nuestro país con Carbon Black, comprada por VMware en agosto de 2019.

El mercado de ciberseguridad es uno de los más dinámicos. Bien es cierto que es más joven que otros, y hay bastantes más empresas que en el resto. Si hace unos años el término de moda para proteger el endpoint era el EDR, ahora se avanza hacia el XDR. Para la mayoría es una evolución natural que muchos fabricantes de EDR han seguido, pero en general lo que importa es que los clientes recurren a la detección y respuesta extendidas (XDR) para obtener un amplio conjunto de capacidades de seguridad automatizadas y totalmente integradas.

Recordamos que Carbon Black fue uno de los pioneros del mercado de EDR junto con Cylance, comprado por Blackberry en noviembre de 2018,



El nacer como una compañía de respuesta ante incidentes convierte a Cynet en experta en análisis forense e investigaciones

Sentinel One y Crowdstrike. Cazaña se mueve al compás del mercado con Cynet, que destaca por su plataforma todo en uno de protección que utiliza aprendizaje automático, inteligencia artificial y automatización para administrar vulnerabilidades, inteligencia de amenazas, analizar el comportamiento del usuario y brindar protección de punto final dentro de un sistema unificado.

Destaca Javier Cazaña durante una entrevista concedida a IT Digital Security que Cynet nace bajo la marca de Eyal Gruner, un joven de 27 años muy dinámico que con 21 ya lanzó Versafe, comprada por F5 en 2013, para darse cuenta años después de que “solamente tienen acceso a tecnología de alto nivel las mismas compañías de siempre. Las grandes”. De forma que Cynet nace bajo la idea de poner a disposición de todos los clientes, independiente de su tamaño, tecnologías de protección de alto nivel. La propia idiosincrasia del mercado español, con un tejido empresarial marcado por empresas de tamaño reducido, parece perfecta para una empresa que ofrece tecnología de seguridad gestionada.

“El hecho de gestionar esa seguridad de nueva generación hace que todas las inversiones realizadas en los últimos años, que genera mucha información, se puedan explotar y permita mejorar la postura de seguridad del cliente final y anticiparse a potenciales amenazas complejas”, explica Javier Cazaña.

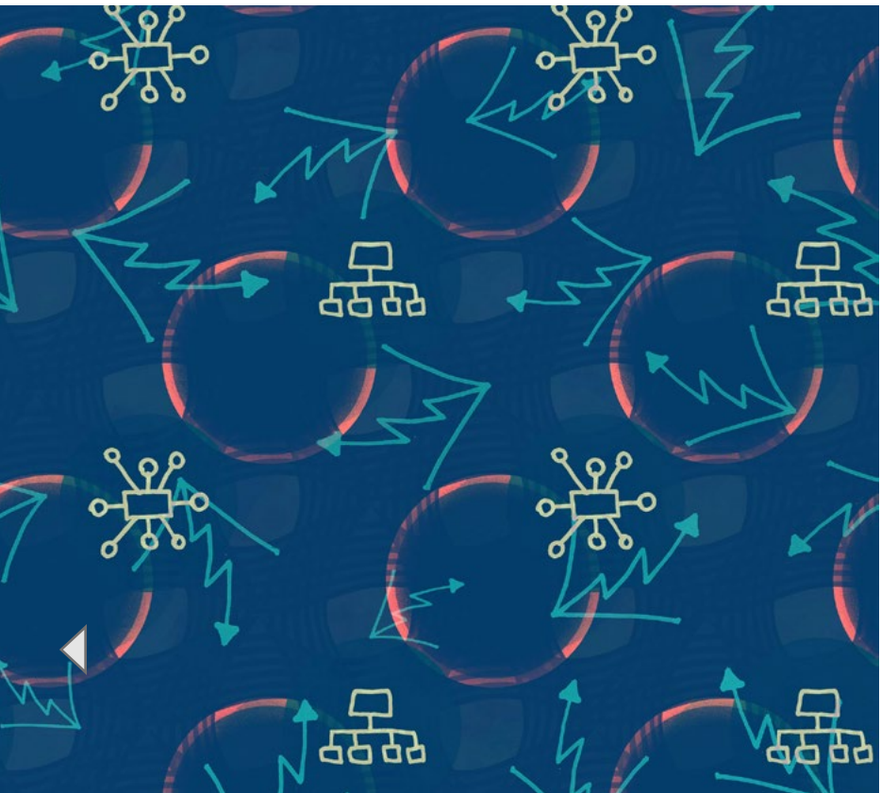
Define el directivo la propuesta de Cynet como un XDR automatizado en el que “tienes todo tipo de sensores para recabar información, no solamente a nivel de endpoint con su EDR, sino análisis de comportamiento, incluso el análisis de la postura de seguridad de las aplicaciones más usadas”. Nacer como una compañía de respuesta ante incidentes convierte a Cynet en experta en

Destacados del mercado XDR

XDR es una tecnología emergente que puede ofrecer capacidades mejoradas de prevención, detección y respuesta de amenazas para los equipos de operaciones de seguridad. Según el Market Guide for Extended Detection and Response de Gartner publicado en noviembre de 2021:

- Continúa la tendencia de buscar proveedores de seguridad y consolidación de productos para administrar los riesgos y mejorar la productividad de las operaciones de seguridad. La detección y respuesta extendidas (XDR) está evolucionando para brindar estos beneficios.
- Se espera que la adopción de XDR aumente por parte de organizaciones de seguridad más pequeñas que probablemente no cuenten con soluciones de administración de eventos e información de seguridad (SIEM)/automatización de orquestación de seguridad y respuesta (SOAR) implementadas en la actualidad. Actualmente, ningún XDR satisface todas las necesidades de las operaciones de seguridad maduras de grandes empresas porque XDR no desplazará la funcionalidad SIEM para todos los casos de uso.
- XDR será una capacidad cada vez más crítica para los compradores. Las soluciones XDR se basan en varios productos diseñados para proporcionar una solución más completa para la seguridad del espacio de trabajo, la seguridad de la red o los dominios de seguridad de la carga de trabajo.

- La seguridad moderna necesita de gran cantidad de datos, y los proveedores de XDR competentes tendrán capacidades amplias y rentables de almacenamiento de datos, análisis y aprendizaje automático (ML).



análisis forense e investigaciones, añade también Cazaña.

Destaca el directivo el alto perfil técnico y de ingeniería de la compañía, que ocupa una excelente posición en detección y respuesta siguiendo la metodología MITRE.

MDR

Decíamos al comienzo que el mercado tiende hacia el XDR. Sería más correcto decir que se busca el MDR, es decir, la detección y respuesta gestionada, sea extendida o no. ¿Por qué? Porque las amenazas son cada vez más complejas, las herramientas de detección recogen cada vez más información y la falta de personal provoca que no se puede dar una respuesta ágil si no es un partner adecuado.

Cynet ofrece detección y respuesta administradas las 24 horas (MDR) como parte de su plataforma XDR. Según la compañía, a diferencia de las ofertas de la competencia que requieren varios empleados a tiempo completo para administrar todos los diferentes componentes de XDR, la plataforma XDR de Cynet puede ser administrada por una sola persona.

Reconoce Javier Cazaña que todos los fabricantes están haciendo un grandísimo esfuerzo, que existen soluciones de calidad y que cada

"Somos los aspirantes a todo"

uno tiene su hueco. ¿Qué oportunidades tiene Cynet? “El punto fuerte es la flexibilidad. Tenemos el tamaño adecuado para podernos adaptar más rápidamente a las necesidades de un cliente”, asegura Cazaña, añadiendo: “La verdad es para nosotros es un reto. Somos los aspirantes a todo”.

Continúa diciendo el directivo de Cynet que “el mercado de seguridad pide foco y flexibilidad, ya sean productos o servicios”. Recordando la escasez de personal, de recursos técnicos, espera como clientes a aquellas empresas que quieran cubrir sus necesidades de ciberseguridad “con una metodología un poco diferente”, además de “realizar alguna técnica de contra vigilancia”, porque la propuesta de Cynet incluye Threat Hunting, higiene de IT o incluso técnicas de deception, o engaño.

Es más, donde Cynet se diferencia es al incluir la tecnología de engaño como parte de su plataforma XDR. La mayoría de las herramientas de engaño que existen en mercado están destinadas a empresas medianas o grandes y requieren de alto conocimiento y especialización.

Cynet también va más allá del análisis del comportamiento del usuario que ofrecen muchos competidores para analizar también el comportamiento de las entidades, lo que puede ayudar a identificar comportamientos fuera de lo normal en PowerShell o en aplicaciones que aprovechan las configuraciones incorrectas para evadir los firewalls, etc.

La palabra automatización se ha hecho tan popular como Inteligencia Artificial. Y en ambos casos, demostrar que se tiene es complicado. En Cynet la automatización está basada en un servicio gestionado por ingenieros de alto nivel capaz de avisar y entender lo que está sucediendo en una compañía. El XDR de Cynet está preparado para absorber toda la telemetría de todas esas fuentes diferentes, colocarla en un solo panel y abordar la consolidación.

Canal

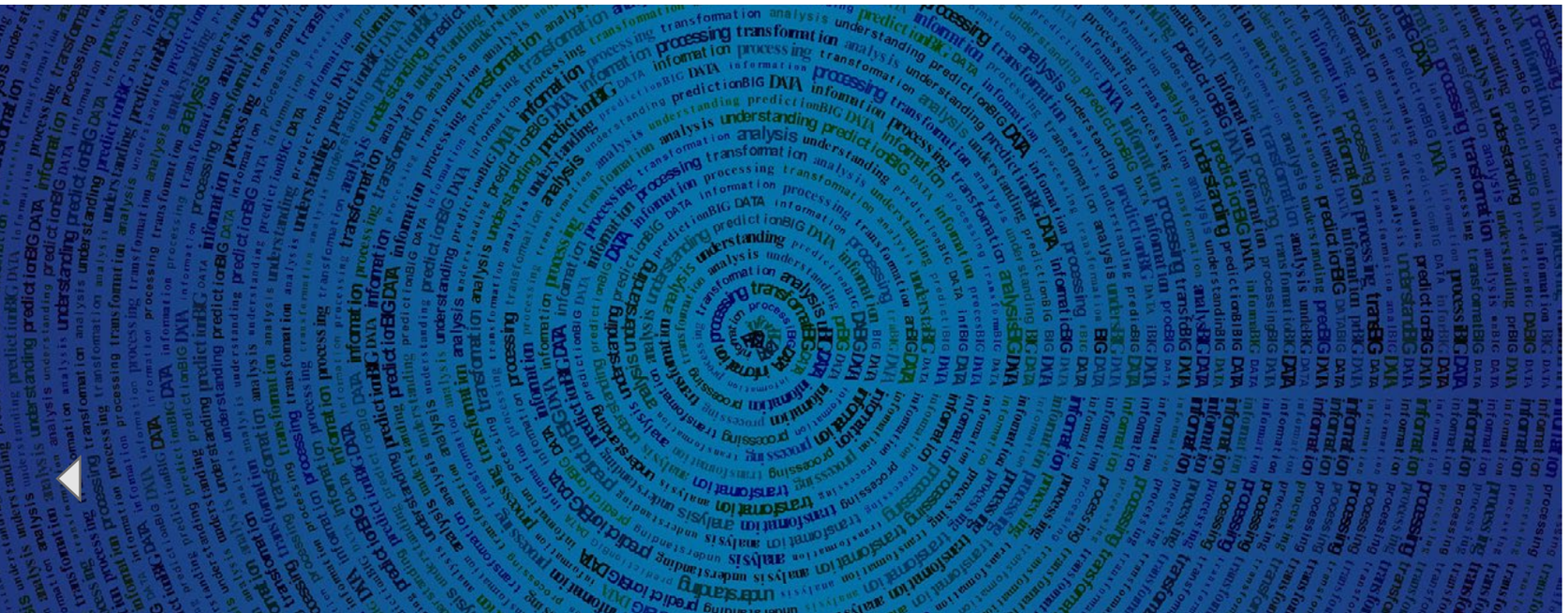
Explica Javier Cazaña que el programa de canal de la compañía está en constante mejora, pero

"El XDR de Cynet está preparado para absorber toda la telemetría de todas esas fuentes diferentes, colocarla en un solo panel y abordar la consolidación"

que de momento se trabaja con Satinfo como mayorista en exclusiva. Con más de treinta años de experiencia, Satinfo busca consolidarse como uno de los mejores mayoristas enfocados a la seguridad para todo tipo de empresas.

"Estamos muy contentos con los primeros pasos que estamos teniendo, tanto en distribución como en todas las conversaciones que estamos manteniendo con grandes integradores que obviamente ven algo especial en una marca como Cynet", asegura el directivo.

En opinión de Javier Cazaña la empresa española necesita empresas que les puedan ayudar a mejorar su postura de seguridad de una manera bastante automatizada y que una opción que un partner pueda asociarse con Cynet para "proteger a sus clientes de una manera muy segura, con garantías". it



Enlaces de interés...

- ¿Qué es MDR? Beneficios de seguridad de detección y respuesta administrada
- XDR, redefiniendo el juego para los MSSP
- La escala de los ciberataques aumenta la demanda de soluciones y servicios XDR

Compartir en RRSS

STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

www.stormshield.com

‘Saber separar el trigo de la paja requiere gente muy preparada’

(Pedro David Marco Llorente, Iberlayer)

Fundada en 2012 por ingenieros españoles, Iberlayer es una compañía española que nació, literalmente, en la Pedriza, un área de la sierra de Guadarrama, dentro del municipio madrileño de Manzanares el Real. En plena escalada, Pedro David Marco Llorente, Main Account Manager y Fundador de la compañía, tuvo una idea, imaginó una tecnología que no existía, que era necesaria y que el mercado ha terminado validando. Pedro David Marco ideó un algoritmo, la manera de conocer, con una probabilidad muy alta, si un correo electrónico es válido, o no.

Diez años después aquel germen forma parte del motor actual de la solución, que no ha dejado de crecer. “Es algo que no existía y que, hasta donde yo sé, sigue sin utilizar nadie”, dice el directivo en referencia a la manera de tiene Iberlayer de hacer frente a la seguridad del correo electrónico, uno de los vectores de ataque más utilizados por lo ciberdelincuentes.

Actualmente el 60% de la facturación del negocio viene de fuera. Los clientes europeos de la compañía están repartidos en países como Finlandia, Grecia, Alemania, Francia, Portugal o Grecia. Se le suman cuentas en Turquía, Estados Unidos y Latinoamérica

Previendo hacia dónde se dirigía el mercado, Iberlayer decidió fabricar la tecnología y operarla como un servicio porque “hoy en día nueve de

“NO MUCHOS DIRECTIVOS SON CONSCIENTES DEL DAÑO QUE LE PUEDE OCASIONAR A SU COMPAÑÍA UN CIBERATAQUE”, PEDRO DAVID MARCO, IBERLAYER

CLICAR PARA VER EL VÍDEO

"Que los servidores de correo de las empresas estén on-premise o en la nube nos da un poco igual porque lo nuestro es un filtro previo"

cada diez incidentes de seguridad empiezan por un correo electrónico”, explica Pedro David añadiendo que el email es la manera más fácil de llegar a un usuario; “si a un usuario le dices que tiene un paquete de Amazon pendiente, o un cargo en Hacienda, o una multa no pagada, lo más probable es que pinche”.

La cantidad de los mensajes de correo que se reciben, la mayor profesionalización de los ataques, que además son dirigidos en muchos casos, hace que la complejidad del filtrado de correo sea alta.

Sí, sí, te lo decía porque en realidad hoy en día la complejidad de las horas del email o de de la complejidad del filtrado de correo es tan alta.

“Saber separar el trigo de la paja requiere gente muy preparada, no sólo en ciberseguridad, sino en esa tecnología. Al operarla como un servicio permitimos a las empresas abstraerse de esa necesidad porque ya no tienen que estar preocupándose de que acaba de aparecer un Zero Day o tu equipo ha configurado el sistema para prevenirte contra esa nueva amenaza.

Aunque durante un tiempo se han ofrecido dos servicios diferentes, Email Guardian y Domain Guardia, Iberlayer ha decidido unificarlos en uno solo que se ofrece como tarifa plana, una de las diferencias de Iberlayer frente a otros fabricantes que cobran en función de las características o funcionalidades que se utilizan del producto. “Nosotros ofrecemos una tarifa plana en la que se incluye

El modelo de negocio de Iberlayer es por número de usuarios protegidos, y no por buzones

todo, incluso las nuevas funcionalidades que sacamos, porque siempre estamos liberando motores o ideas nuevas", explica Pedro David. Nos cuenta también que el modelo de negocio es "por número de usuarios protegidos, y no por buzones", lo que simplifica mucho el modo de licenciamiento, "lo hace más sencillo".

Diferencial

Reconoce Pedro David que en el mercado hay soluciones muy buenas, y que son muchos los que pueden presentar una estadística o informe que dice que son los mejores; "tenemos competidores haciéndolo muy bien, eso es innegable, pero hay diferencias", asegura cuando le preguntamos por el diferencial de la compañía.

La primera gran diferencia que quiere destacar el fundador de Iberlayer es el soporte; "si tú llamas a un soporte porque tienes un problema no es lo mismo hablar español que hablar inglés, por muy buen inglés que tengas; además, nuestro soporte es directamente con gente de la compañía". Y es que empieza a convertirse en tendencia el contar con empresas más pequeñas capaces de dar servicios más cuidados y donde la responsabilidad no se diluye hasta el infinito.

Hay un antes y un después en la adopción de la nube. Lo que parecía un cambio lógico a tenor de las ventajas que se asociaban con el cloud, no lo era tanto en la realidad. El impulso realizado por Microsoft con el lanzamiento de Office 365, fue un desencadenante en procesos de migración. ¿Cómo

"Tenemos competidores haciéndolo muy bien, eso es innegable, pero hay diferencias"

impactó en Iberlayer? Explica pedro David que el hecho de que los servidores de correo electrónico de las empresas estuvieran en la nube o en on-premise "nos daba un poco igual porque lo nuestro es un filtro previo".

Volvemos al correo electrónico como principal vector de ataque. La experiencia lleva al fundador de Iberlayer a decir que es muy fácil suplantar dominios. Cuando los motores específicos de la compañía detectan la suplantación avisan al cliente y le ayudan a arreglar el problema "porque es parte del servicio"; en ocasiones se lanzan avisos a empresas que no son clientes, pero por experiencia, "cuando son empresas muy grandes no suelen hacerte caso".

Sobre si la empresa española protege el correo adecuadamente, asegura Pedro David que la aumentado la concienciación y que se nota mucho entre países. Aunque en España "nos queda mucho por avanzar, en general estamos bastante mejor que otro países europeos", asegura el directivo.

Comenta también que más que del país depende también de las empresas. "A la empresa pequeña o mediana le cuesta, pero escucha", asegura, mientras que en la grande "aunque sepan que está mal, nadie toca nada".

Respecto al canal de distribución, Iberlayer ha empezado a trabajar este año con Cefiros y se trabaja en la firma de un acuerdo con V-Valley. Se busca también ampliar el número de partners.

Enlaces de interés...

- La invasión rusa de Ucrania dispara los ciberataques
- El 25% de los usuarios de email reconoce haber abierto un correo de phishing
- El email despunta como principal punto de entrada de los ciberataques

Compartir en RRSS

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Sharepoint Security ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET PROTECT	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Secure SharePoint Server ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
RESPUESTA	**DETECCIÓN**

Digital Security
Progress. Protected.

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

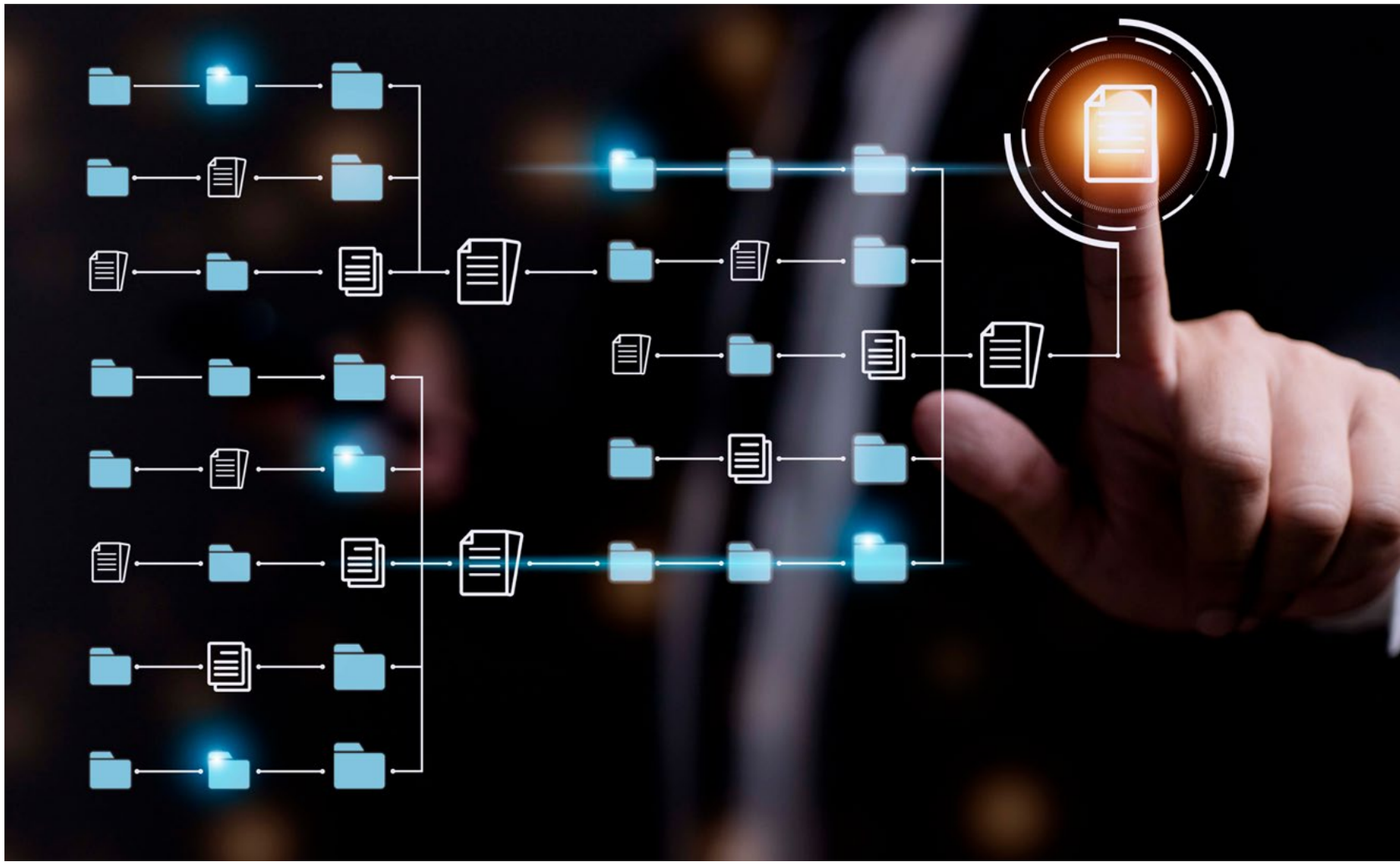
MADE IN EU

Directorio Activo, se enciende el botón de alerta

E. Frechoso Muñoz

El Directorio Activo, o Active Directory, es el corazón de la infraestructura de TI de más del 90% de las organizaciones. En tanto que proporciona autenticación y autorización para cada recurso crítico en todo el entorno corporativo, es un objetivo principal para los atacantes que buscan acceder a los datos sensibles de la empresa. En consecuencia, debe gestionarse como un activo de seguridad, no solo como infraestructura.

La seguridad del Directorio Activo es un objetivo en movimiento y, aunque las auditorías periódicas son esenciales, la supervisión diaria es igual de importante. Pero ¿cómo se puede proteger contra los ataques?



La investigación "El aumento de los exploits de Active Directory: ¿Es hora de dar la voz de alarma?" realizada por la firma de analistas Enterprise Management Associates (EMA) en 2021 y en la que se analiza el impacto en las organizaciones de las vulnerabilidades de seguridad del Directorio Activo (AD, por sus siglas en inglés), revelaba que el 50% de las empresas había sufrido un ataque a AD en los últimos uno o dos años, y más del 40% afirmó que los atacantes habían logrado vulnerar su implementación de AD. Asimismo, indicaba que el 86% de las compañías encuestadas afirmó que estaba planeando aumentar su inversión en la protección de AD. Esto muestra el nivel de preocupación por las amenazas a la seguridad de AD y como dice el título del estudio ¿conviene hacer sonar las alarmas?

Está claro, AD se ha convertido en un objetivo codiciado para los ciberatacantes, que no piensan en listas y hojas de cálculo, sino que buscan las rutas de ataque para encontrar la más fácil hacia los activos críticos de las organizaciones. Active Directory es a menudo uno de los caminos más rápidos para llegar a las joyas de la corona de las empresas: sus recursos e información. ¿Por qué? La respuesta es sencilla: AD es el proveedor de identidades más extendido dentro de las infraestructuras tecnológicas empresariales. Adicionalmente, podemos considerar la identidad como el nuevo perímetro, de este modo, el simple compromiso de una identidad puede suponer una parada total en la actividad de una empresa, previa escalada de privilegios, movimientos laterales, persistencia y, finalmente, cifrado de los controladores de dominio.

"Si unimos las premisas anteriores al intrínseco funcionamiento de AD con protocolos legacy, se crea el caldo de cultivo perfecto para que los cibercriminales abusen de las debilidades de estos protocolos para pertrechar ataques con mucho impacto en el negocio casi exclusivamente robando identidades", explica Carlos Manchado, responsable de ciberseguridad de Microsoft en España.

La principal razón por la que los ciberdelincuentes atacan a AD es porque sirve de puerta de entrada al resto de la red como servicio para gestionar,

"Hay empresas que, por tener un perfil tecnológico más avanzado, ven con mayor claridad la necesidad de inversión en soluciones de seguridad para el AD, pero todas tienen esa necesidad"

César Moro,
senior sales consultant, Quest

conectar en red, agrupar, autenticar y proteger a los usuarios en las redes de dominios corporativos. "Los usuarios y ordenadores dependen de AD para acceder a diversos recursos de la red. Por ello, los ciberdelincuentes saben que los ataques de ransomware a AD pueden causar estragos en cualquier organización, lo que lo convierte en un excelente mecanismo de extorsión", apunta Shweta Khare, senior product marketing manager de Delinea.

El hecho de que AD proporcione una función crítica -autenticar a los usuarios para que puedan acceder a los servicios y aplicaciones- y de que tenga muchas vulnerabilidades de seguridad que los atacantes pueden explotar, lo convierte en un blanco de ataques. AD fue desarrollado para ser un sistema de directorio empresarial altamente resistente y fiable para autenticar a los usuarios y gestionar el acceso, y está diseñado para ser abierto. "Hoy en día, esa apertura es también su talón de Aquiles", señala el director de ventas de Semperis en España, Ray Mills, para quien "una vez que los atacantes consiguen meter su pie en la puerta hacia AD, suelen intentar elevar sus privilegios. Las organizaciones de ransomware como servicio (RaaS), entre las que se encuentran Conti, BlackCat, LockBit y otras, han construido su negocio a partir de la explotación de AD (entre otras tácticas) porque la variedad de vías de ataque al AD es casi infinita".

Ante este panorama, la siguiente pregunta lógica que cabe hacerse es si son conscientes las empresas de lo importante que es la protección de AD. Si atendemos a los datos de la encuesta de EMA anteriormente expuestos, podría decirse que el grado de concienciación con la seguridad de AD debería ser alto. Lo mismo ocurre si tenemos en cuenta que, solo en 2021, Microsoft analizó 24 billones de señales diarias, bloqueando 24 billones de amenazas de correo y 31 billones de identidad, según refleja el informe anual de defensa digital de la

compañía. Estos datos resultan. cuando menos. inquietantes.

Pero la realidad es bien distinta, pues “muchas empresas no son conscientes de la importancia del AD. Es el servicio que normalmente siempre funciona, no se queja, es estable, y por lo tanto no le prestamos toda la atención que se merece. Solo nos acordamos de él cuando surge un problema. Y eso aplica a su gestión, a su gobierno y por supuesto a su protección”, opina César Moro, senior sales consultant en Quest, que es tajante al puntualizar que se trata de un problema de filosofía y compresión de su importancia en los niveles directivos de las compañías. “Se invierte gran parte de los presupuestos en innovaciones tecnológicas que apoyen al negocio, pero no se dan cuenta que la base que permite que el negocio siga corriendo es AD”, dice.

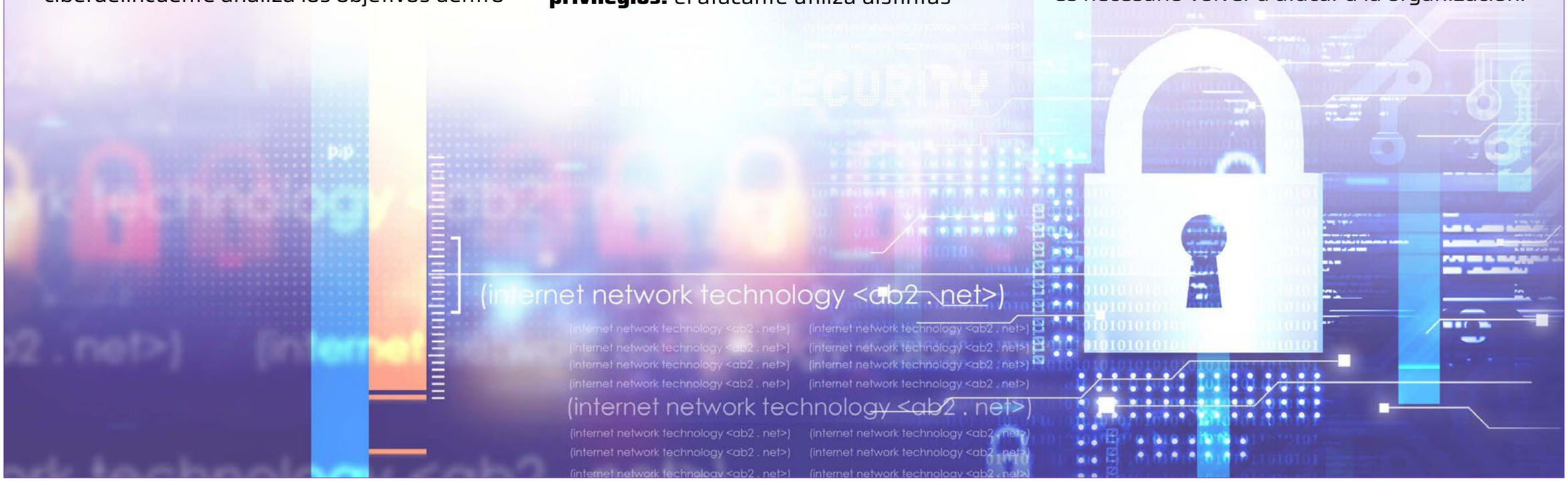
La gran mayoría de las organizaciones utilizan AD on-premise como su principal almacén de identidades. De hecho, aproximadamente el 90% de las empresas de la lista Global Fortune 1000 lo usan como método principal para proporcionar autenticación y autorización sin fricciones. Aunque no hay que olvidar que los ataques sufridos por la naviera Maersk, SolarWinds y Colonial Pipeline empezaron todos con la vulneración de AD.

Tipos de ataques son los más frecuentes en Active Directory

De acuerdo con César Moro, senior sales consultant en Quest, hay una serie de ataques tipificados muy comunes que se podrían resumir de la siguiente forma: Mapeo de los caminos de acceso al Tier 0, Explotación de Políticas de Grupo, Ataques basados en replicación, Explotación de la autenticación NTLM y Explotación de la autenticación Kerberos. Cada uno de estos grupos se compone de distintos tipos de ataques como podrían ser: "Pass the Hash", "Golden Ticket", "Kerberoasting" o "DCSync". Lo importante es disponer de soluciones que permitan protegerse ante esa diversidad de ataques.

Es más, la mayoría de los ataques al AD se componen de varios de los ataques expuestos, pero ejecutados en distintas fases. Si nos adentramos en la anatomía de un ciberataque, descubriríamos que cada fase tiene sus propios tipos de ataque. Y las fases son realmente lógicas y están muy establecidas:

- **Reconocimiento:** fase en la que el ciberdelincuente analiza los objetivos dentro de la organización y recolecta información sobre la misma.
- **Planificación:** en esta fase el ciberdelincuente determina el vector de ataque que va a usar para la infiltración
- **Intrusión:** se utiliza el vector de ataque seleccionado para romper el perímetro de red y acceder a los sistemas de la organización
- **Movimiento lateral y escalada de privilegios:** el atacante utiliza distintas técnicas para realizar movimientos laterales e ir adquiriendo mayores privilegios que le den acceso a los objetivos seleccionados
- **Exfiltración y limpieza:** se produce el robo de datos o la corrupción de los mismos (dependiendo del objetivo del ataque) y en algunos casos, se realiza la limpieza de pistas para evitar que se detecte el ataque y que posteriormente pueda ser utilizado de nuevo si es necesario volver a atacar a la organización.



"La seguridad del AD implica un proceso continuo de evaluación, supervisión y respuesta a las amenazas según sea necesario. Este esfuerzo requiere tiempo y recursos, pero es fundamental para la viabilidad de la organización"

Ray Mills, director de ventas, Semperis España

"Estos incidentes han supuesto que cada vez más líderes empresariales y de seguridad sean conscientes de que el AD es un importante vector de ataque", añade Mills. "En los últimos meses, varios analistas -incluido Gartner- han señalado la necesidad de contar con soluciones de seguridad y recuperación específicas para AD. Sin embargo, muchas organizaciones no protegen adecuadamente sus entornos de AD, lo que fomenta más ataques relacionados con la identidad".

En este sentido, Manchado destaca que "las actividades de los ciberdelincuentes cada vez son más oportunistas, constituyendo un modelo de negocio en sí mismo". Este incremento del número de incidentes, con un especial impacto en la identidad, afecta de forma directa a todo el tejido empresarial. "Los ataques, cada vez más extendidos y agresivos, han conducido a los responsables de ciberseguridad y el C-Level a tener cada vez más claro que AD se postula como un objetivo de gran valor, siendo el elemento clave y estructural para el funcionamiento de la infraestructura y comunicaciones tecnológicas on-premise".

Adiós perímetro tradicional. Hola seguridad de la identidad

La pérdida del perímetro tradicional, que ha puesto foco en la seguridad de la identidad, ha ayudado también a fomentar esa concienciación sobre la necesidad de proteger AD. Todos los directivos consultados están de acuerdo en esto. De hecho, "la identidad es el nuevo perímetro de seguridad. Dado que AD controla el acceso a las aplicaciones críticas y a los activos digitales, debe protegerse en todo su ciclo de vida ante un ataque", dice Khare.

Por su parte, Moro hace hincapié en que era importante que se produjera este cambio de filosofía. "La seguridad perimetral es totalmente necesaria, pero el mercado nos ha enseñado desde hace años que el 50% de los ataques que se producen en las compañías son por amenazas internas. Si solo se presta atención a la seguridad perimetral, estás

perdido. Y más con el cambio tecnológico que han supuesto los nuevos entornos de trabajo y la apertura al uso de servicios en la nube".

Las amenazas internas están ahí desde empleados descontentos, espionaje industrial, administradores no capacitados… ninguna empresa está exenta de sufrirlas. "Esta situación entronca con la filosofía de ciber-resiliencia. Independientemente de que una organización cuente con las mejores tecnologías de seguridad y un excelente equipo de profesionales, tarde o temprano será víctima de un ataque, pues es complicado tener todo controlado. Esta mentalidad debe regir en las empresas. Partiendo de esta base, las compañías deben contar con planes de recuperación rápida sin sufrir pérdidas", continua el directivo de Quest.

Coincide con esta idea Manchado, que explica que proteger el perímetro es necesario, pero no suficiente. Este paradigma está muy interiorizado ya por la mayoría de los responsables en el ámbito de seguridad TI. Es necesario no solo proporcionar a los usuarios los mínimos privilegios de acceso y verificar el cumplimiento de las condiciones de acceso de forma explícita y de manera continua, pero también las organizaciones deben estar preparadas para defenderse de un ataque en cualquier momento, especialmente si se dirige a la base de su defensa. "Todo esto, de forma adaptativa, dinámica y basada en riesgos y en el contexto de los usuarios, su comportamiento y sus dispositivos", comenta el directivo de Microsoft.

Impacto del cloud y el teletrabajo

La sombra de la pandemia también toca a AD. Por todos son conocidos ya los efectos que provocó el Covid-19 y cómo las organizaciones tuvieron que transformar su gestión de identidades y accesos, adoptando modelos híbridos o la modernización total de sus identidades. Algunas compañías ya contaban con protocolos de trabajo remoto y estaban acostumbradas a autenticar a los usuarios y a gestionar los permisos de los empleados que trabajaban en cualquier lugar, pero la realidad es que a muchas otras se les hizo complicado poner en marcha estrategias de acceso seguro, incluidas las mejores prácticas, como la aplicación de la autenticación multi-factor (MFA).

Recordemos que AD es un sistema complejo y existen múltiples desconfiguraciones comunes

"Este incremento del número de incidentes, con un especial impacto en la identidad, afecta directamente a todo el tejido empresarial. Los ataques, cada vez más extendidos y agresivos, han conducido a los responsables de ciberseguridad a tener cada vez más claro que AD es un elemento clave y estructural para el funcionamiento de la infraestructura y comunicaciones tecnológicas on-premise"

Carlos Manchado, responsable de ciberseguridad, Microsoft Iberia

Buenas prácticas a seguir por las empresas

A la hora de proteger el AD, desde Delinea se aconseja tener en cuenta lo siguiente:

1. Evitar añadir usuarios del dominio al grupo de administradores locales y, en su lugar, implementar controles de acceso de mínimo privilegio o just-in-time. Esto garantiza que los administradores estén estrechamente controlados y que solo se les concedan más privilegios cuando sea necesario.

2. Debido a que es común que los atacantes intenten forzar credenciales débiles en los endpoints, las empresas deben implementar siempre un sistema robusto de MFA y seguridad de los accesos privilegiados.

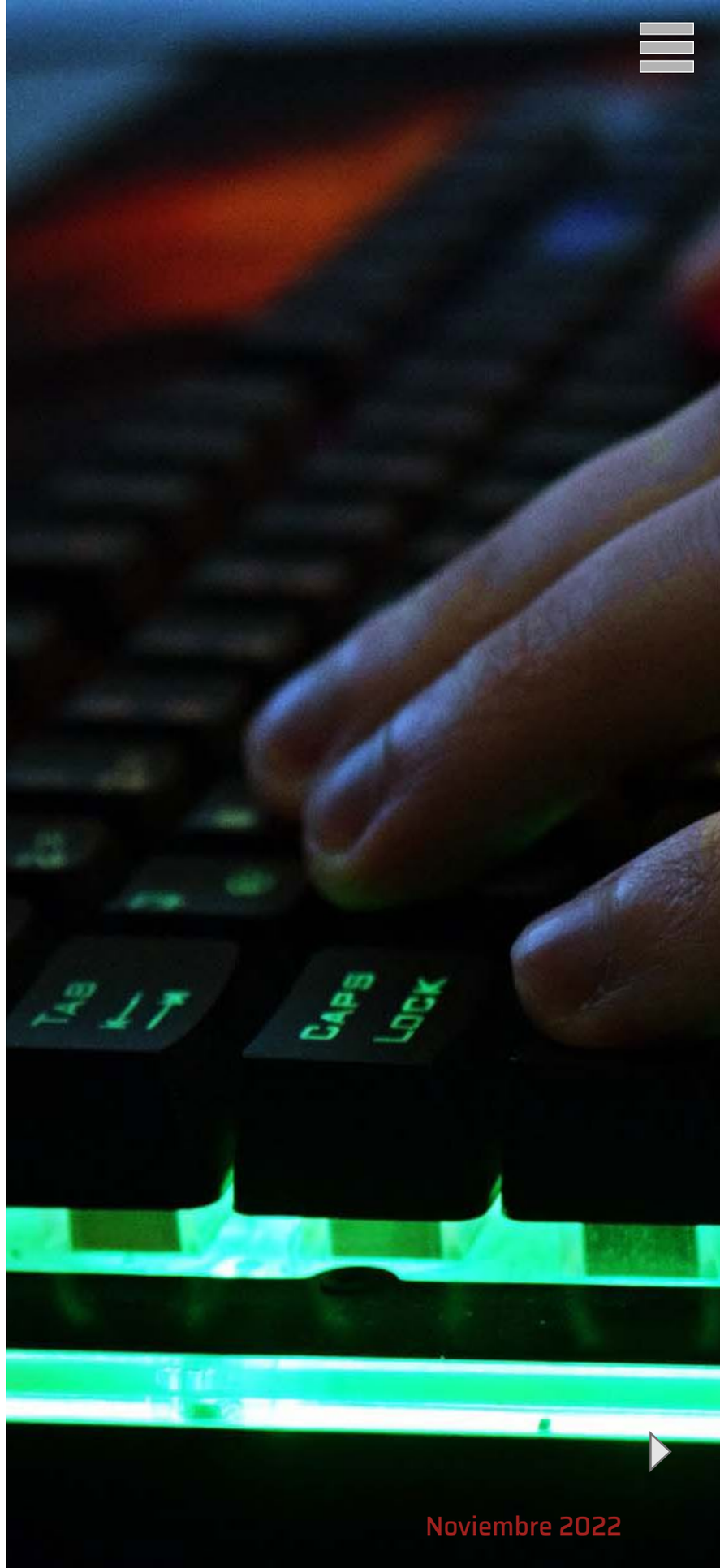
3. Impedir que los usuarios con demasiados privilegios tengan derechos de administrador local en todos los sistemas y, al mismo tiempo, asegurarse de que existen controles para evitar que se ejecuten aplicaciones no autorizadas en endpoint.

"En este sentido, las soluciones de gestión de accesos privilegiados (PAM) desempeñan un papel fundamental, ya que permiten a las empresas aplicar estas medidas de seguridad y, sobre todo, rompen la cadena de ataque de AD, elevando el nivel de validación, autenticación, autorización y auditoría de los usuarios", señala Shweta Khare, de Delinea.

que los hackers buscan para vulnerar. "El aumento exponencial y no planificado del trabajo a distancia provocado por la pandemia ha añadido aún más complejidad y ha ejercido una enorme presión sobre los equipos de TI", puntualizan desde Delinea.

"La buena noticia es que esta situación aceleró el enfoque en la seguridad de las aplicaciones en la nube para apoyar el escenario de trabajo híbrido que ahora es común", señala el ejecutivo de Semperis. "Dicho esto, la mayoría de las organizaciones todavía tienen trabajo que hacer para asegurar el acceso a las aplicaciones en la nube, incluyendo la realización de evaluaciones de vulnerabilidad a través de AD on-premise y Azure AD, la supervisión continua del entorno de identidad para los cambios maliciosos, y la remediación automática de los ataques".

Lo mismo piensa Moro, que dice que muchos han comprendido que la gestión y la seguridad de la identidad es clave. La mayoría de las compañías que empiezan a abarcar los servicios en la nube no se desprenden de su AD on-premise. Al revés, ese repositorio de identidades es el que se sincroniza con la nube y permite usar esos servicios. "Se puede estar muy avanzado tecnológicamente, tener servicios en la nube, etc. pero si se produce un problema en el AD local y los cambios se replican, todos esos servicios pueden verse afectados",



"La identidad es el nuevo perímetro de seguridad. Dado que AD controla el acceso a las aplicaciones críticas y a los activos digitales, debe protegerse en todo su ciclo de vida de un ataque"

Shweta Khare, senior product marketing manager, Delinea

explica mientras recalca la idea que de AD es el pilar sobre el que se montan el resto de servicios. "Sería la base de nuestro castillo de naipes. Si falla por la base, todo se desploma", sentencia el portavoz de Quest.

AD, común denominador en todos los sectores y negocios

AD es transversal a los sectores de negocio de las empresas. Así, encontramos que decenas de miles de empresas utilizan Microsoft Active Directory, incluyendo alrededor del 90% de las empresas de la lista Fortune 1000. La mayoría de estas empresas se encuentra en los sectores de tecnología y fabricación, sin embargo, también en el ámbito de la industria, que es amplio y diverso.

Al final, vemos que es un servicio común que todas las organizaciones utilizan de la misma forma, con mayor o menor implicación sobre el resto de servicios que tenga la compañía. "Podemos resumirlo en que cualquier empresa que tenga AD y una red on-premise, necesita adoptar una solución de seguridad. Ahora bien, más que una solución de seguridad sería un plan de seguridad con distintos elementos que configuren una defensa efectiva", recalca el ejecutivo de Microsoft.

"Más del 90% de las empresas basan su servicio de autenticación y autorización sobre AD", aclara Moro. "Por tanto, si no quieren correr riesgos han de montar soluciones para aumentar la seguridad del AD. Hay empresas que por tener un perfil tecnológico más avanzado ven con mayor claridad la necesidad de inversión en soluciones de seguridad para el AD, pero todas tienen esa necesidad".

El alto impacto de explotar vulnerabilidades

A la hora de hablar del impacto que pueden tener las vulnerabilidades de seguridad de AD en las organizaciones y ver cómo están respondiendo ante ellas, se deber partir de la base de que "las vulnerabilidades de seguridad por sí solas no tienen mucho impacto", tal y como explica Mills, que argumenta que es cuando las vulnerabilidades son atacadas con éxito cuando empiezan los problemas. "La seguridad del AD implica un proceso continuo de evaluación, supervisión y respuesta a las amenazas según sea necesario. Este esfuerzo requiere tiempo y recursos, pero es fundamental para la viabilidad de la organización", continua Mills.

Por tanto, "es evidente que el impacto puede ser muy alto, y más si consideramos al AD una de las joyas de la corona de nuestra infraestructura tecnológica", según afirma Manchado, que explica que habitualmente, cuando se informa de una vulnerabilidad crítica en AD, las compañías suelen tratar de priorizarlo y encajarlo en una ventana de

Aplicar una estrategia de defensa en capas que proteja AD antes, durante y después de un ataque es clave

intervención creada ad-hoc. Por supuesto, esto hace que las empresas tengan que poner a prueba sus procesos de parcheo, no solo para la propia intervención en producción, sino para asegurar en un entorno de pruebas que no habrá afectación en su entramado tecnológico. Lamentablemente, no existe una solución mágica para las vulnerabilidades de software. Por eso, desde Microsoft apuestan por un completo ecosistema, que combina profesionales altamente cualificados y algoritmos de Inteligencia Artificial con el fin de afinar y optimizar cada proceso de parcheo y gestión de vulnerabilidades, exponen desde la compañía.

Así, sufrir un ataque que comprometa AD puede tener consecuencias devastadoras, llegando a producir incluso la parada total del negocio de una compañía. Se trata de un servicio crítico. “Si un atacante consigue obtener los derechos de gestión de accesos y comprometer un controlador de dominio, sería esencialmente el dueño de la red, ya que tiene el control completo y puede acceder a todos sus diversos servidores y datos”, apunta Khare. “Por eso, los ciberdelincuentes se dirigen cada vez más a Microsoft AD con ataques de ransomware. Lamentablemente, a pesar de la clara amenaza, muchas empresas siguen careciendo de planes de seguridad y recuperación de AD, lo que dificulta enormemente la recuperación de un ataque de ransomware”.

Recordemos que los ataques de ransomware a través de AD supusieron a Colonial Pipeline pagar 5 millones de dólares de rescate para recuperar sus activos y poder reanudar sus operaciones, mientras que el ataque a Maersk costó a la empresa al menos 300 millones de dólares en 2017. Así, asegurar el AD no es simplemente una opción deseable, “a día de hoy, y ante el panorama actual de amenazas, es vital para la salud y la longevidad de un negocio: si AD no es seguro, nada lo es”, insisten

Directorio Activo es un sistema complejo y existen múltiples desconfiguraciones comunes que los hackers buscan vulnerar

desde Semperis. El problema es que no todas las organizaciones son conscientes de ello. “La mayoría adoptan unas medidas preventivas mínimas, pero no tienen una visión general de los múltiples tipos de ataque, los objetivos de los mismos y cómo estar protegidos ante ellos. Y mientras siga existiendo una vía de ataque, la organización estará expuesta”, añade Moro.

Las empresas deberían…

Visto todo esto, y teniendo en cuenta los peligros a los que AD está expuesto, desde Microsoft tienen claro que es muy importante acometer un bastionado y sanitización del AD (AD hardening), así como la adopción de un Modelo de Acceso Empresarial, incluyendo el modelo de tiers AD y el uso de PAWs, tal y como comparte la compañía en su plataforma Microsoft Learn. Igualmente, aconsejan desplegar tecnología que aporte proactividad en la línea de defensa para prevenir, detectar, investigar y responder frente a potenciales compromisos o ataques.

“De este modo sumamos una pieza más a un puzle que tiene como objetivo contrarrestar los incidentes y acelerar la respuesta ante ellos”, puntualiza Manchado, que también recomienda incluir algunos de los eventos y logs generados por Windows en su solución SIEM nativa en la nube, acumulando así un conocimiento que permita reforzar la identificación de sucesos sospechosos y tendencias de ataque. “Esto puede eliminar las necesidades de configuración y mantenimiento de la infraestructura de seguridad, permitiendo reducir los costes hasta en un 48% en comparación con los SIEM tradicionales”.

Evidentemente, aplicar una estrategia de defensa en capas que proteja AD antes, durante y después de un ataque, es clave. “Las organizaciones necesitan soluciones que aborden cada etapa del ciclo de vida del ataque, incluyendo la identificación y mitigación de vulnerabilidades, la detección de ataques avanzados, la corrección automática de cambios maliciosos y la garantía de una recuperación de AD libre de malware en caso de un ciberataque”, explica Mills. Puesto que muchos ataques al AD tienen éxito, el directivo insiste en que “las organizaciones deben prepararse para lo peor teniendo un plan de recuperación de AD testado y probado para poder reanudar las operaciones de negocio lo antes posible después de un ataque”.

No obstante, y aunque ahora la seguridad del AD es un tema de conversación muy candente, en 2013 ya se definió el framework de ciberseguridad

AD fue desarrollado para ser un sistema de directorio empresarial altamente resistente y fiable para autenticar a los usuarios y gestionar el acceso, y está diseñado para ser abierto

NIST (National Institute of Standards and Technology) que muestra una serie de buenas prácticas que ayudan a reducir los riesgos de un ciberataque a infraestructura crítica. En este sentido, desde Quest recomiendan que cualquier empresa que quiera aumentar la seguridad de su AD se fije en este framework y aplique las medidas sobre cada uno de los puntos que expone. Así, se trata primero de Identificar y tener visibilidad de todos los activos de la organización y saber si los sistemas son vulnerables, controlar los permisos a recursos y la pertenencia a grupos. En segundo lugar, se habla de Proteger, fase en la que se deben ver las medidas de defensa que se tienen implementadas y si estas cubren todos los escenarios o si se están utilizando adecuadamente. El tercer paso sería Detectar las acciones indebidas sobre los sistemas, o si se es capaz de identificar en tiempo real los incidentes que se están produciendo. Responder y ver qué medidas se pueden tomar para limitar el impacto de un incidente y cómo mitigar la situación, sería el cuarto paso a seguir. Mientras que Recuperar y comprobar si las medidas de recuperación con las que se cuenta han sido ya probadas con anterioridad, sería la última de las fases.

Enlaces de interés...

- Las principales vulnerabilidades de la infraestructura heredada de Active Directory y cómo las detectan los atacantes
- La seguridad del directorio activo sigue en entredicho
- El Directorio Activo en el punto de mira

Compartir en RRSS

FORO it Digital Security

PROTEGIENDO EL NUEVO PERÍMETRO

Patrocinadores Platinum

COMMVAULT

ESET

SONICWALL

SOPHOS

Patrocinadores Gold

Bitdefender BUILT FOR RESILIENCE

citrix

CyberRes A Micro Focus Line of Business

Cynet

proofpoint.

Secure&IT www.secureit.es

STORMSHIELD

WatchGuard

yubico

it Digital Security

Active Directory, protegiendo el corazón de la empresa

anadat technology

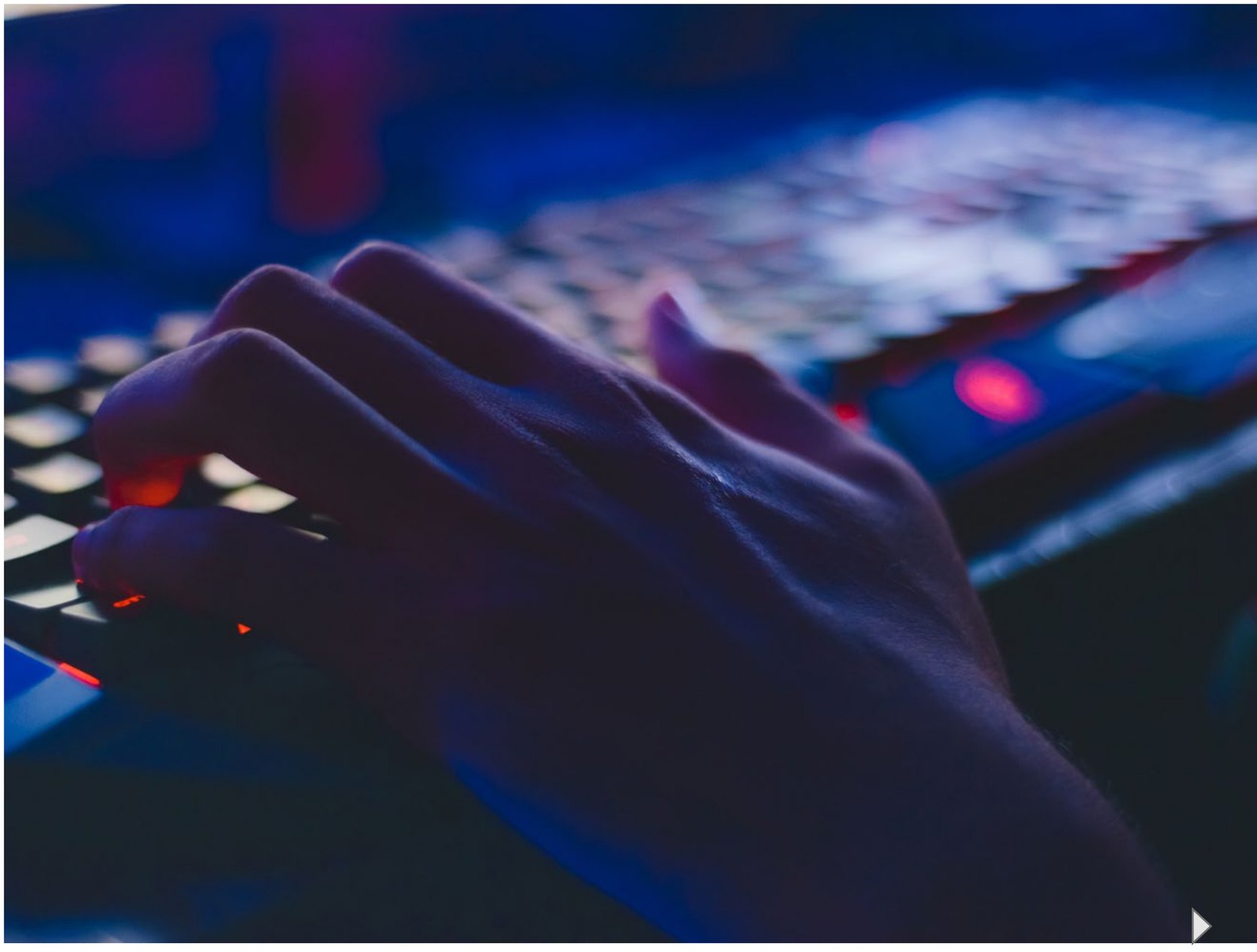
semperis

Noviembre 2022

¿Quién no ha oído hablar del Directorio Activo? Existe desde Windows 2000 y es una pieza fundamental para autorizar usuarios, accesos y aplicaciones en toda una organización, lo que le convierte en un objetivo prioritario para los atacantes. Si un ciberdelincuente es capaz de acceder al Directorio Activo podrá acceder a todas las cuentas de usuario, bases de datos, aplicaciones y todo tipo de información. Por lo tanto, un compromiso del Active Directory, particularmente cuando tarda en detectarse, es, sencillamente, un desastre.

La identidad se ha convertido en algo problemático de proteger. Recuerda Nuno Antunes Ferreira, director para España y Portugal de Semperis, que la razón por la cual la identidad llama la atención de los ciberdelincuentes es “porque vivimos en un mundo sin muros físicos ni lógicos, sin muros que nos defiendan”. El trabajo híbrido, que muchas organizaciones han mantenido después de la pandemia, o el fenómeno de los nómadas digitales, es una constante, dice también el directivo, añadiendo que los usuarios esperan poder trabajar y ser productivos en cualquier momento y en cualquier lugar, “de ahí la necesidad de saber quién es quién, dónde está, lo que puede hacer y desde qué dispositivo y red está trabajando”. Y por eso es importante proteger los sistemas de identidad de las empresas, Active Directory y Azure Active Directory, “porque si controlas al Directorio Activo de una organización, controlas la organización”.

Semperis es una compañía fundada en 2014 con el objetivo de ayudar a las empresas a proteger su directorio activo, detectando vulnerabilidades, interceptando ciberataques y recuperándose rápidamente del ransomware y otras



Uno de los sectores más críticos de las infraestructuras y de los clientes es el directorio activo

“LA INTERRUPCIÓN DEL DIRECTORIO ACTIVO NO ES UNA OPCIÓN” (ANADAT)

CLICAR PARA VER EL VÍDEO

emergencias de integridad de datos. Y lo hace a través de dos herramientas: Directory Service Protector (DSP) y Active Directory Forest Recovery, sobre los que nos habla David Carbonero, Cloud Arquitect Specialist de Anadat, partner de referencia de Semperis en España con más de 20 años en el mercado y cuyo objetivo es “ayudar a los clientes con la operación de sus entornos más críticos”.

Lo primero que destaca David Carbonero es que uno de los sectores más críticos de las infraestructuras y de los clientes es el directorio activo. Las aplicaciones empresariales locales y en la nube se basan en Active Directory y Azure Active Directory, lo que las convierte en una pieza fundamental de su infraestructura de TI. Su flujo constante, gran cantidad de configuraciones y un panorama de amenazas cada vez más

“LAS EMPRESAS DEBEN REALIZAR URGENTEMENTE UNA EVALUACIÓN DE LOS ENTORNOS DE AD” (SEMPERIS)

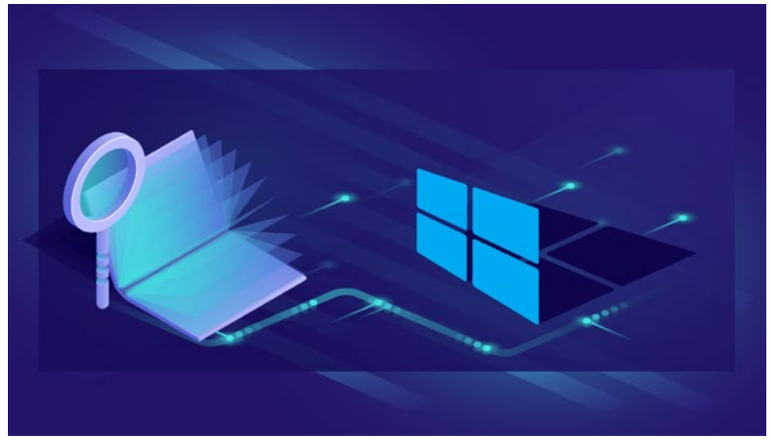
CLICAR PARA VER EL VÍDEO

La tecnología patentada de Semperis desacopla Active Directory del sistema operativo subyacente para evitar la reinfección de malware

sofisticadas hace que proteger el Directorio Activo no sea fácil. “Entendemos que la interrupción del servicio de validación de identidades no es una opción”, asegura el ejecutivo explicando que Semperis Directory Services Protector (DSP) es “un radar”, una herramienta “que me va a permitir monitorizar y ver los eventos que se pueden producir en el directorio activo cuando esté sufriendo un ataque. La solución supervisa continuamente AD y Azure AD en busca de indicadores de exposición y proporciona una vista única de las actividades, tanto en las instalaciones como en la nube.

Semperis Directory Services Protector puede escanear una implementación de Active Directory o Azure AD en busca de vulnerabilidades y configuraciones erróneas, priorizando los fallos de seguridad en función de su gravedad para ayudar a los administradores a abordar primero los problemas más importantes. La herramienta detecta cambios maliciosos que se haya podido producir durante un ciberataque y los notifica a los administradores. Opcionalmente, puede revertir las modificaciones automáticamente tan pronto como se detecten, lo que permite a las empresas responder a las infracciones con mayor rapidez.

“La recuperación del directorio activo es siempre, siempre la primera operación que hay que realizar o nada funcionará”, explica Nuno Antunes. Aquí



Los secretos de Semperis Active Directory Forest Recovery (ADFR)

Respondidas por David Carbonero, Cloud Arquitect Specialist de Anadat, las siguientes preguntas desvelan las características más destacadas de Semperis ADFR

- **¿Es necesario dar de alta el servidor ADFR en el Dominio?** No, no hace falta. El Servidor ADFR es una máquina que debe estar siempre configurada en un grupo aparte.
- **¿Se puede gestionar con el servidor ADFR más de un bosque?** Sí. Si tienes distintos bosques necesitas varias licencias, una para cada bosque, y con el producto puedes crear un plan de backup diferente para cada bosque o dominio que tengas
- **¿Se puede restaurar el Directorio Activo en los mismo Controladores de dominio o necesito es necesario desplegar nuevos servidores?** La herramienta nos permite restaurar el Directorio Activo sobre los mismos DCs, pero en el caso de que los DCs estén infectados, la herramienta me permite restaurar el AD sobre máquinas nuevas recién instaladas. Una de las grandes ventajas del producto es que desacopla el sistema operativo del directorio activo, por lo que al hacer el backup del AD, solamente se copian los objetos, y mediante esos objetos es capaz de restaurar el AD sobre las máquinas recién instaladas.
- **¿Para el ADFR se necesita algún servidor de BBDD? N**o. Semperis ADFR integra un SQL Server Express, que es una versión gratuita de Microsoft, y no necesitamos licenciar ningún servidor.
- **¿Cómo conecta el servidor ADFR con los Controladores de Dominio?** Mediante unos agentes. Por eso es muy importante instalar el servidor ADFR en una red independiente que solamente tenga conexión con los controles de dominio mediante estos agentes. De esta manera los backups van a estar siempre protegidos y seguros ante un ataque de tipo ransomware y me va a garantizar el poder levantar las máquinas.

es donde entra Semperis Active Directory Forest Recovery, que promete ayudar a las empresas a restaurar rápidamente las implementaciones de AD y Azure AD después de un ciberataque. El producto puede reducir el tiempo de inactividad hasta en un 90%. Cuando un ataque de ransomware o de limpieza (wiper attack) elimina los controladores de dominio, la recuperación de su bosque puede prolongarse durante días o incluso semanas, con el riesgo de que el malware vuelva a impactar durante el proceso. Pero con Active Directory Forest Recovery (ADFR) de Semperis, puede recuperar el directorio activo con unos pocos clics de ratón y menos de una hora.

Active Directory Forest Recovery (ADFR) permite restaurar la copia de seguridad más reciente, incluso si los controladores de dominio estaban infectados cuando se realizaron las copias de seguridad. La tecnología patentada de Semperis desacopla Active Directory del sistema operativo subyacente para evitar la reinfección de malware.

Los secretos de Semperis Directory Services Protector (DSP)

David Carbonero, Cloud Arquitect Specialist de Anadat, responde a algunas preguntas clave sobre Semperis DSP

- **¿Con DSP puedo crear reglas automatizadas para deshacer un cambio en el AD?** DSP Me permite crear reglas automatizadas para responder a ciertos ataques basadas en cambios de atributos u objetos. Es decir, si un atacante, por ejemplo, se quiere añadir como administrador de dominio al grupo domain admin y quitar a los administradores actuales, el DSP puede deshacer esa operación de forma automática.
- **¿Con DSP puedo comprobar el nivel de seguridad de mi AD?** La herramienta de DSP incorpora un módulo que valida tu infraestructura de AD, chequea el directorio activo y proporciona visibilidad e información sobre cómo solventar esas vulnerabilidades que tienes en el directorio activo
- **¿Se pueden enviar los eventos encontrados a un SIEM?** Semperis DSP genera muchísimos eventos y tienes dos formas de recopilarlos. Bien mirando el log del propio servidor o bien enviando todos los datos a un SIEM
- **¿Puedo enterarme si una regla creada ha detectado algo en el sistema?** Sí. La herramienta tiene un panel de monitorización que muestra por pantalla cualquier cambio que se produzcan en el AD. Como decíamos antes, podemos crear reglas automatizadas, pero también tenemos la posibilidad de deshacer un cambio de forma manual.
- **¿DSP necesita de un SQL Server?** Sí. Si Son tantos eventos los que se generan que necesitamos un SQL Server Express para almacenar todos los cambios que se realicen en la configuración de la propia herramienta, y además un SQL server aparte para almacenar todos los datos que se cambien en el Directorio Activo.
- **¿Necesito desplegar agentes en los DCs?** Efectivamente, necesitamos desplegar unos agentes en los DCs (controladores de dominio)
- **¿DSP conecta con Azure?** Con DSP existe la posibilidad de monitorizar en la misma herramienta nuestro DA y el Azure AD. Si el cliente tiene configurado que el AD esté replicado su director activo con Azure, tengo tiene un módulo, mediante una máquina virtual, que puedo conectar a la parte de Azure y así poder ver y observar los cambios que se puedan producir en Azure.

"La interrupción del servicio de validación de identidades no es una opción

David Carbonero,
Cloud Arquitect Specialist, Anadat

Enlaces de interés...

- 2021 Semperis Active Directory Security Halftime Report
- Purple Knight Proves Essential in Securing AD for Southern Utah University
- Anadat Insights

No es necesario realizar restauraciones de prueba y error en busca de copias de seguridad limpias. No es necesario reconstruir AD desde cero.

Las joyas de la corona

Los sistemas de identidad son las joyas de la corona de cualquier organización. Así lo asegura Nuno Antunes, añadiendo que la recuperación del directorio activo tras un ciberataque "es siempre la primera operación que hay que realizar, o nada funcionará. Explica que no ayuda el hecho de que el AD tenga 22 años y se creara sin tener en cuenta la seguridad y que gracias a la tecnología de Semperis se pueden ir un paso más allá del backup tradicional al lograr recuperaciones automatizadas, muy rápidas y con garantías de que no hay malware.

La experiencia de muchos años en el mercado lleva a Nuno Antúnez a pedir a las empresas una evaluación "urgente" de los entornos de AD; "en términos prácticos, esto significa actualizar y corregir muchas vulnerabilidades identificadas en los últimos años", para lo que la empresa ofrece Purple Knight una opción gratuita que ayuda a las organizaciones "a priorizar su remediación urgente de identidades tanto para AD como para Azure AD". La versión comercial de esta herramienta es DSP, que incorpora enormes capacidades en lo que respecta a la supervisión proactiva y continua de los directorios de las organizaciones, no sólo en lo que respecta a los vectores de ataque comunes, sino también a los cambios reales que se producen casi en tiempo real".

"Las empresas deben realizar urgentemente una evaluación de los entornos de AD"

Nuno Antunes,
Director España y Portugal, Semperis

Compartir en RRSS

Consigue la herramienta comunitaria nº 1 para la evaluación de la seguridad de AD

- Informe diagnóstico sobre la seguridad de Active Directory y Azure AD
- Indicadores de seguridad antes y después de un ataque
- Asesoramiento prioritario y práctico
- Modelos de amenazas definidos por la comunidad de usuarios
- Correlación con el marco MITRE ATT&CK

purple knight

Desarrollado por Semperis

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.

it Digital Security

Tribuna Tecnología y Negocio

La Red como plataforma para hacer realidad Web3 y Metaverso

Cuando leí, en 2016, "The Network Imperative: How to Survive and Grow in the Age of Digital Business Models", de Barry Libert, Megan Beck y Jerry Wind, tuve la sensación de que tanto énfasis en "la red" era desproporcionadamente excesivo, por comparación con otras tecnologías de la digitalización, también muy importantes, como cloud computing, edge computing, machine learning, big data, ciberseguridad y otras tecnologías que hacen posible la transformación digital.

JORGE DÍAZ-CARDIEL

SOCIO DIRECTOR GENERAL DE ADVICE STRATEGIC CONSULTANTS

Economista, sociólogo, abogado, historiador, filósofo y periodista. Autor de más de veinte mil de artículos de economía y relaciones internacionales, ha publicado más de una veintena de libros, cinco sobre Digitalización. Ha sido director de Intel, Ipsos Public Affairs, Porter Novelli International, Brodeur Worldwide y Shandwick Consultants.

Compartir en RRSS

Seis años más tarde, en 2022, he leído las dos obras magnas (hasta hoy) sobre Metaverso y Web3, publicadas el pasado mes de julio/agosto, por lo que son bastante actuales en su contenido: “THE METAVERSE: And How it Will Revolutionize Everything” de Matthew Ball y “Navigating the Metaverse: A Guide to Limitless Possibilities in a Web 3.0 World”, de Cathy Hackl, libros que citan, respectivamente, dos conceptos poco utilizados en 2016: Metaverso y Web3. Ambos libros vuelven a poner foco en “el imperativo de red”.

No se trata de hacer un ranking de tecnologías de la digitalización para discernir cuáles son más importantes. Pero, el análisis de los saltos (eras) en Tecnologías de la Información, desde 1939 (año de fundación de Hewlett-Packard, punto de referencia para al nacimiento del sector TIC que hoy conocemos, incluidas BigTech), muestra que fue necesario ampliar la conectividad de red…

- 1) Cuando utilizábamos mainframes;
- 2) Cuando pasamos a la informática distribuida con workstations en empresas y ordenadores en casas;
- 3) Cuando en 1993 aparece la primera versión popular de Internet, Web.1, que algunos conocimos desde su nacimiento y dio lugar a un concepto que utilizábamos mucho en Intel Corporation: HCI (Hogar Conectado a Internet).

- 4) Cuando la Web.2 e Internet son ubicuas y móviles, gracias a billones de dispositivos andando por la calle, viajando en aviones y trenes, con el sustrato de las tecnologías de la digitalización arriba mencionadas y que World Economic Forum, en 2016 y 2018 agrupó en el concepto de la Cuarta Revolución Industrial.

El siguiente paso exige también “el imperativo de la red”. Para que Web3 y Metaverso sean realidad, mucho hay que aumentar el poder de la red, que habrá de ser “una plataforma fuerte, sólida y robusta” para sustentar que, entre 2022 y 2032, el tráfico de datos en la red se multiplicará por 20 y que la necesidad de computación

Entre 2022 y 2032, el tráfico de datos en la red se multiplicará por 20 y la necesidad de computación (procesamiento) habrá de multiplicarse por 1.000

(procesamiento) habrá de multiplicarse por 1.000, lo que posiblemente requiera la computación cuántica de que ya hemos hablado en IT User en varias ocasiones, pero no ahora. Estos dos últimos datos los proveyó Irene Bernal, directora de Innovación en Conectividad en Telefónica, en el lanzamiento de la propuesta de valor de Metaverso y Web3 de Telefónica, el pasado 29 de septiembre. También supimos que, por primera vez, Telefónica nombraba a Yaiza Rubio su Chief Metaverse Officer.

Para conseguir que la red sea plataforma de Web3 (o que se conciba la “red como plataforma”) Irene Bernal se apoyó en tres pilares: explotar el valor potencial de las redes de telecomunicaciones, como 5G o Wifi 6; el Edge Computing; y extender la softwarización a la forma en la que se crean los nuevos servicios de conectividad. Dicho de otra manera, para que una “Telco” pueda convertir la red en plataforma para la creación, desarrollo y crecimiento de Web3 y Metaverso, son necesarios tres conceptos: Tecnologías de baja latencia; Edge Computing y Programable Network que significa esa “softwarización”, por la que se concibe la “Network as a Service” (NaaS). Chema Alonso, CDO de Telefónica afirmó rotundamente que su empresa tiene listos y preparados esos tres pilares.

Lo es cual es esencial, ya que el área que dirige Chema Alonso en Telefónica es el back end, es un laboratorio de ideas y tecnologías. Pero es el front end quien tiene que crear la propuesta de valor de Web3 y Metaverso para empresas y sectores económicos de actividad.

Telefónica Tech es el front end para el mercado B2B, empresarial y sector público. La empresa que José Cerdán Ibáñez dirige como CEO es el área de Telefónica que más crece del grupo y en la presentación de resultados del primer semestre de 2022, Telefónica Tech creció +72% en ingresos.

Evidentemente, ya lo tiene todo, en lo que a la transformación digital se refiere: 5,5 millones de clientes, presencia en 24 mercados internacionales de primer nivel y Equipo, 6.000 empleados, agrupados en dos grandes negocios, según las tecnologías que proveen: Telefónica Tech Cybersecurity & Cloud, que dirige la CEO María Jesús Almazor; y Telefónica Tech AI of Things (IOT, BigData), que dirige el CEO, Gonzalo Martín-Villa.

La provisión de todas las tecnologías de la digitalización que ofrece Telefónica Tech es necesaria para el desarrollo y crecimiento de la nueva era de Internet, Web3 & Metaverso que, por cierto, no son lo mismo. Y, junto a todo ello, “la Red como Plataforma”.

Antes he citado varios libros, y, en la vida de la empresa se vive lo que se dice en esos libros. Este verano pasado estuve dos meses trabajando en Estados Unidos. Parte de mi trabajo fue llevar a cabo encuestas electorales cara a las elecciones legislativas norteamericanas del próximo 8 de noviembre. Y, también, visitar BigTech en Silicon Valley, Seattle, Texas, Arizona y Florida. Es decir: Meta (Facebook), Oracle, Apple, Alphabet-Google, Amazon, Microsoft, Cisco, Intel Corp. Dell Tecnologies y Tesla, entre otras empresas.

El caso de Tesla es curioso porque su fundador y dueño, Elon Musk, no cree en Web3 ni en Metaverso. Tampoco Jack Dorsey, fundador de Twitter.

Pero el resto de empresas BigTech mencionadas han avanzado mucho en Web3 y en Metaverso, aunque algunos no lo sepan y otros no quieran verlo. Cuando alguien se toma en serio el desarrollo de un negocio o tecnología, lo primero que hace es (además de tener un objetivo y un plan para conseguirlo) invertir dinero: en 2021, BigTech invirtió 27.000 millones de dólares en el desarrollo de Web3, 7.000 millones más de los invertidos ese año en Ciberseguridad, tecnología y negocio establecidos, maduros y con mucha generación de ventas, por su necesidad. Muchas empresas son conocidas en el ámbito de la ciberseguridad: Fortinet, CheckPoint, Palo alto Networks, Telefónica Tech Cybersecurity & Cloud; Symantec, McAfee y muchas más.

¿Cuántas empresas conocidas -diríase- son reconocidas por estar en el Metaverso y en We3? A priori, ninguna. En última instancia, sí lo están

La provisión de todas las tecnologías de la digitalización que ofrece Telefónica Tech es necesaria para el desarrollo y crecimiento de la nueva era de Internet, Web3 + Metaverso que, por cierto, no son lo mismo

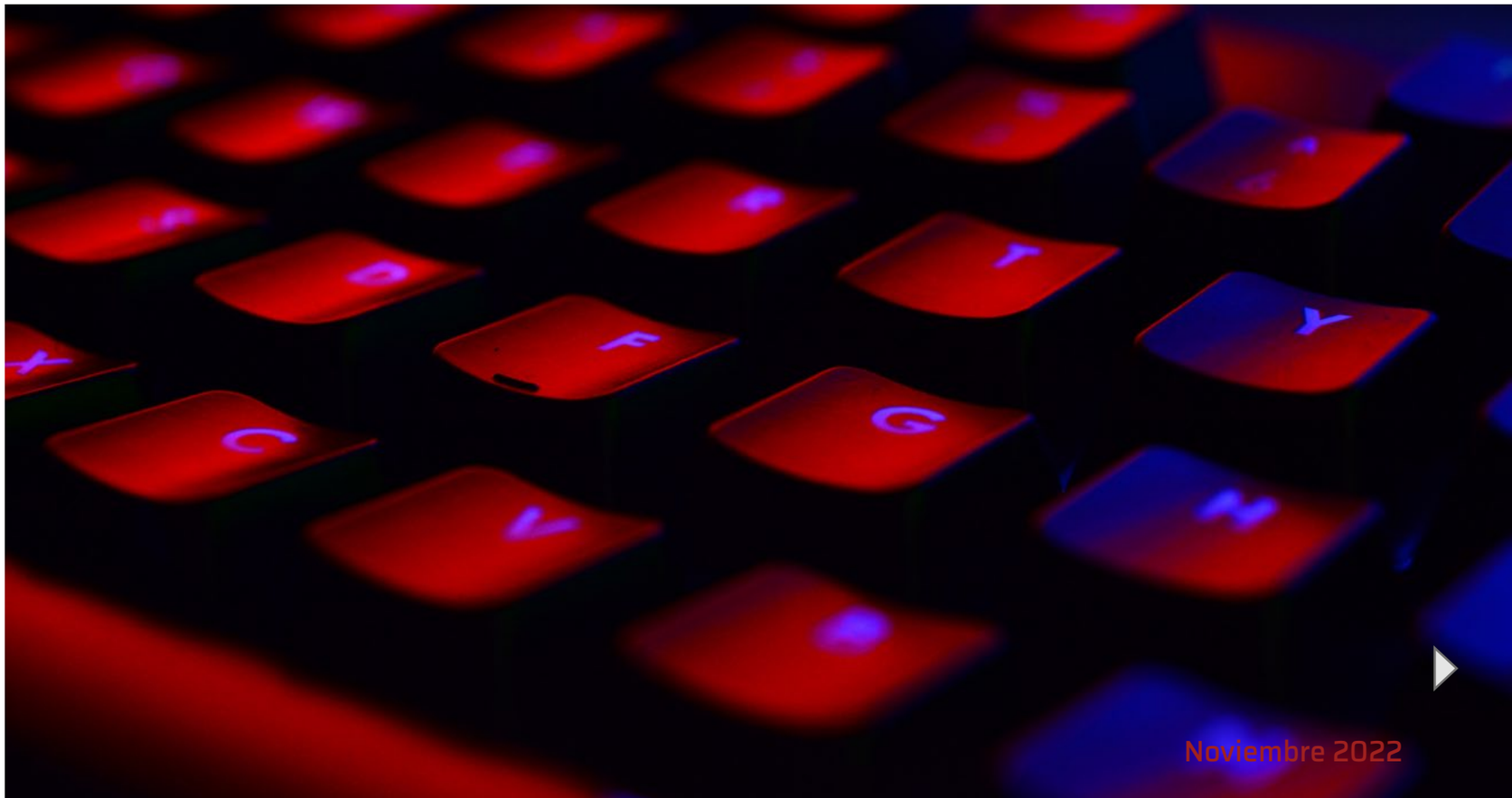
casi todas las firmas tecnológicas grandes, que, en desarrollo del Metaverso, llevan invertidos 200.000 millones de dólares en 2022. Las tecnológicas grandes son BigTech (Meta, Oracle, Apple, Alphabet-Google, Amazon, Microsoft, Cisco, Intel, Dell Tecnologies…), en torno a las cuales hay cientos de miles de empresas pequeñas que desarrollan aplicaciones para Web3.

Y, en lo que todas esas grandes empresas tecnológicas coinciden es en la necesidad de la una red muy fuerte sea con fibra, 5G, o 6G. La "gracia del asunto" es que BigTech no pone las redes y, en EE.UU., usan las de las operadoras de telecomunicaciones (Verizon, AT&T, Comcast, T-Systems…), como en Europa usan las redes de Telefónica y otros operadores. Sigue sin cerrarse la reclamación justa de las Telcos, de que BigTech pague por el uso de las redes. Lo que requiere legislación y, por tanto, regulación.

Cara al futuro inmediato de Web3, en que estructuras descentralizadas (DAO) funcionan autónomamente, sin un poder centralizado o concentrado en unas pocas empresas, como sucede en Web.2 con BigTech, que lo domina todo… con DEFI (Decentralized Finance), que elimina a los bancos como intermediarios y el universo de TOKENS, NFT, Blockchain, cryptomonedas (Ethereum y Bitcoin, sobre todo) … es obvio que está naciendo un nuevo mundo tecnológico, con una nueva Internet. Los que empujan Web3 dicen que "se trata de devolverle el poder a la gente frente a las inmensas corporaciones".

Jack Dorsey (fundador de Twitter) es tan directo como sarcástico: "Web.3 es una fachada de marketing que vende `poder para el pueblo en Internet´, pero la realidad es que, de nuevo, solo servirá para que los billonarios y las grandes empresas tecnológicas se hagan aún más ricas y tengan más poder". Supongo que "el sabrá", porque es billonario y ha dado a luz varias empresas grandes tecnológicas poderosas.

Como escribió George Orwell en "Rebelión en la granja", tras las revoluciones, el poder acaba volviendo siempre a los poderosos, sean los de



Enlaces de interés...

- The Network Imperative: How to Survive and Grow in the Age of Digital Business Models; de Barry Libert, Megan Beck y Jerry Wind
- The Metaverse: And How it Will Revolutionize Everything; Matthew Ball
- Navigating the Metaverse: A Guide to Limitless Possibilities in a Web 3.0 World; Cathy Hackl

Para que una "Telco" pueda convertir la red en plataforma para la creación, desarrollo y crecimiento de Web3 y Metaverso, son necesarios tres conceptos: Tecnologías de baja latencia; Edge Computing y Programable Network

siempre o sean otros nuevos. Pero, también es cierto que, las llamadas Revoluciones Tecnológicas de los siglos XX y XXI no sólo se hicieron un hueco, sino que lo impregnaron todo. Igualmente, pensamos que, con el impulso de BigTech y sus ecosistemas; con la oferta de integradores de tecnologías de nueva generación como Telefónica Tech, que ha invertido comprando muchas empresas para el desarrollo de Web3 y Metaverso (Bit2me, Imascono, Helium, Metasoccer, Gamium, Crossmint, Rand…, y acuerdos con Niantic y con Unity, entre otros), si Web3 quiere hacerse paso, lo hará y no habrá nada ni nadie que puedan impedirlo.

Otra cosa es que Tokens, NFT, DEFI, DAO, Crytomonedas, BlockChain… estén sometidos al escrutinio de una posible-futura regulación (que, por ejemplo, los bancos exigen con vehemencia y de la que no para de hablarse) para proteger a los consumidores y, también para proteger el Antiguo Régimen económico, establecido con web2, antes de que Web3 tome definitivamente La Bastilla…

it Reseller
TECH&CONSULTING

Fidelización
El negocio basado en la cercanía del cliente

El futuro de la seguridad pasa por los servicios SOC, y el canal lo sabe

Cada mes en la revista,
cada día en la web.