it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Diciembre 2020 - nº 36

2021, el año de la consolidación

“El cloud no viene a resolver ni a empeorar la situación a nivel de seguridad” (Elena García)

TI Unificada y Neurons, o por qué Ivanti compra MobileIron y Pulse Secure

#EncuentrosITDS. De la continuidad de negocio a la resiliencia

#ITWebinars. Arquitecturas de seguridad, ¿qué ventajas ofrecen?

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 Favorit Comunicación, 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

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

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

2021: Más sorpresas no, por favor

Se cierra por fin 2020. El año de la pandemia lo ha revolucionado todo, ha impactado en nuestra vida y en la de todos los que nos rodean, en nuestro entorno personal y en el profesional, en la manera de comunicarnos y de hacer negocio. Hemos adoptado la resiliencia – nunca esta palabra ha cobrado tanto sentido, como un modo de vida.

Se cierra el año en el que se aceleró la transformación digital, en el que la ciberseguridad se puso en primer plano y la palabra ransomware se escuchó en el prime time televisivo; el año que pudimos irnos a teletrabajar a casa sin que fuera el privilegio de unos pocos; el año en el que el cloud, con su capacidad de escalabilidad y flexibilidad, cobró todo su sentido y terminó por convencer a los reacios.

Se cierra el año de la adopción de tecnologías que permitieran a las empresas hacer frente a una situación nueva y persistente en el tiempo; tecnologías de colaboración, de acceso remoto, de gestión de identidades, de protección más allá de un perímetro que, ahora sí, ha saltado por los aires.

De esta pandemia se han aprendido muchas cosas, entre ellas el papel vital que juegan los responsables de ciberseguridad de las empresas. En las siguientes páginas y a través de entrevistas y encuentros podréis leer diferentes declaraciones de lo que han aprendido los CISO, y también de lo que podemos esperar de 2021, un año que se centrará en la consolidación de todas las tecnologías que se adoptaron en semanas y de manera precipitada. Toca pulir y revisar, toca consolidar. Eso sí, más sorpresas no, por favor.

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

itds

Sumario

En Portada

2021, el año de la consolidación

Actualidad

TI Unificada y Neurons, o por qué Ivanti compra MobileIron y Pulse Secure

Entrevistas

"El cloud no viene a resolver ni a empeorar la situación a nivel de seguridad"

Elena García, Indra

Encuentros ITDS

Los servicios gestionados de seguridad a examen

De la continuidad de negocio a la resiliencia segura

#DesayunosITDS

No solo IT

Zero Trust ¿Quién le pone el cascabel al gato?

El Poder Judicial en la Nueva Sociedad Digital: ¿Evoluciona o no?

Índice de anunciantes

María Isabel Rojo, Enthec

#ITWebinars

Brechas de Seguridad, ¿hay opciones?

Arquitecturas de seguridad, ¿qué ventajas ofrecen?

TI UNIFICADA Y NEURONS,
O POR QUÉ IVANTI COMPRA MOBILEIRON Y PULSE SECURE

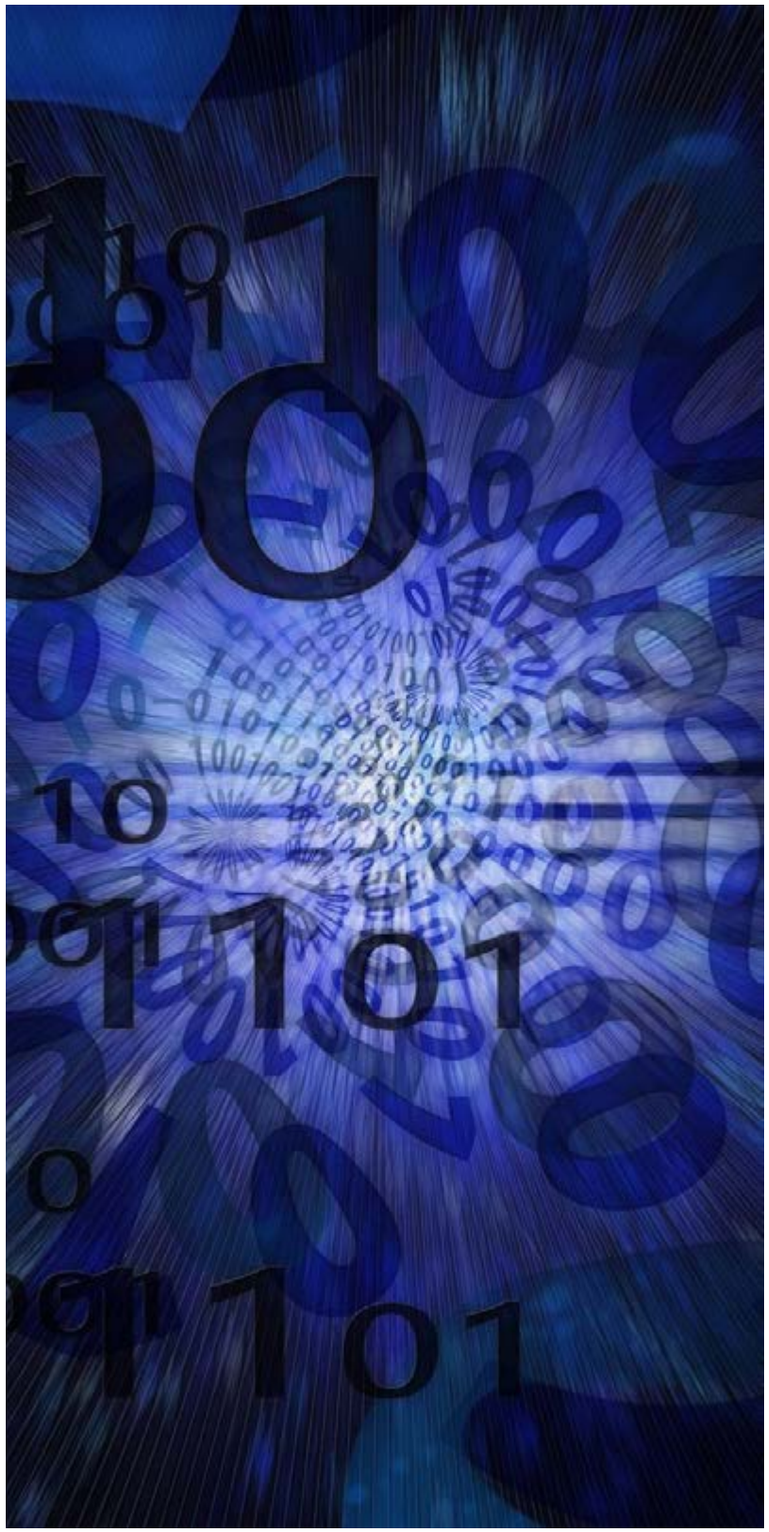
Apenas unas semanas antes de conocerse los últimos detalles de la compra de MobileIron y Pulse Secure, hablamos con Stefano Sardella, Channel Manager EMEA South de Ivanti, la empresa que ha comprado las dos primeras, en la misma semana y sin que los detalles financieros hayan trascendido.

Rosalía Arroyo

Ivanti no es un nombre que suene mucho en el mercado de seguridad. La compañía no es joven.

Sus orígenes se remontan a 1985 cuando nace LAN System, el germen de una empresa que actualmente tiene más de 27.000 clientes. En 1991 Intel compra esta compañía de software para formar Landesk, una división de negocio que en 1993 introduciría en el mercado la categoría de gestión del desktop. Landesk se escinde en 2002 como compañía independiente y es comprado por Avocent en 2006 por 416 millones de dólares, poco después de que añadiera tecnologías de gestión de procesos a su oferta. En 2010 la compañía cae en manos de Thoma Bravo, una conocida firma de capital, e inicia una etapa de adquisiciones que le lleva a comprar Wavelink, una empresas de software de cadena de suministro, in 2012; Shavlik, una empresa de evaluación de vulnerabilidades de red y gestión de parches, en 2013; Naurtech Corporation en 2014; Xtraction Solutions in 2015 o AppSense, proveedor de soluciones de gestión de entornos seguros de usuario en 2016.

Sobre todo este historial de compras, en el que habría que añadir a Enteo, Waveling, Frontrage y algunas otras, explica Stefano Sardella, Channel Manager EMEA South de Ivanti, que en 2017 se produce la fusión más grande de la compañía, la que une a Landesk con Heat Software, “una em-



"Ivanti Neurons es una herramienta realmente estratégica en nuestra visión de TI Unificada"

presa más enfocada en el Service Management"; la empresa resultante se llamará Ivanti y ya contará con más de 1.700 empleados en 23 países y un gran liderazgo en el mercado de software para la cadena de suministro. Bajo la marca Ivanti la compañía compra Concorde y RES en 2017 y Pulse Secure y MobileIron en 2020.

Sobre la tipología de las empresas que se han comprado, dice Stefano Sardella que son muy diferentes: algunas de seguridad, otras de business intelligence y analytics, empresas de gestión de activos o gestión del puesto de trabajo del usuario.

Neurons, el principio

Toda esta estrategia de adquisiciones se ha llevado a cabo "para llegar a lo que en los últimos años hemos definido como TI Unificada", que según el responsable de canal de Ivanti para el sur de Europa no es otra cosa que "ofrecer una herramienta única, una solución única para gestionar de forma unificada las operaciones de TI, las operaciones de seguridad y los procesos para ofrecer a los usuarios un entorno de trabajo securizado y gestionado".

En los últimos tres años ha compañía dio un

Stefano Sardella, Channel Manager EMEA South de Ivanti

respiro a su estrategia de adquisiciones. Un tiempo necesario para consolidar toda la tecnología acumulada en una herramienta totalmente integrada. Tres años después de las compras de 2017 suman 2020, el año de la pandemia, el año

en que Ivanti quiere seguir avanzando “porque el mercado está cambiando mucho. COVID-19 pone sobre la mesa un cambio, el de cómo gestionar el teletrabajo y los usuarios remotos; se necesita una nueva tecnología. La compañía lanza Neurons, “una herramienta realmente estratégica en nuestra visión de TI Unificada”.

Neurons, dice Stefano Sardella, es una herramienta de hiper-automatización que permite tener visibilidad completa de todos los activos de los usuarios, independientemente de dónde estén, desde la nube y a nivel central. “Esto es el principio, donde todo se ha iniciado, porque ya no se trata sólo de gestionar equipos sino del IoT”. Añade que las empresas están buscando herramientas para gestionar este tipo de dispositivos de forma unificada, y que el objetivo de Neurons es “gestionar el edge”.

Insite Stefano Sardella que es en este borde donde se enfoca realmente Neurons: “tener un descubrimiento total de lo que es el Edge y todo lo que está fuera de la empresa y los usuarios, porque es ahí que las mayoría de los datos serán creados en el futuro”. El hecho de que los datos se hayan convertido en el activo más importante de las empresas hace que sea vital gestionar este tipo de datos de forma segura”.

Seguridad adaptativa

Neurons, además, hace uso de la inteligencia artificial y el machine learning para ofrecer una herramienta de seguridad adaptativa, una herramienta capaz de “monitorizar el estado de los dispositivos e intentar auto reparar, auto corregir problemas”. La herramienta monitoriza algunos parámetros que pueden ser básicos, como CPU, RAM, disco duro, etc., o servicios críticos para la empresa como puede ser que un usuario haya desactiva el firewall de Windows, o el cifrado del disco. La herramienta sería capaz de reiniciar ese equipo en remoto y aplicar las correcciones oportunas

“Todo se enfoca en el concepto de inteligencia artificial que puede auto reparar, auto corregir y auto securizar el entorno de trabajo, también de un usuario remoto, o de un dispositivo”, dice Stefano Sardella, añadiendo que Neurons es la estrategia futura y la visión de Ivanti.

Pulse Secure y MobileIron

No es posible, por el momento, hablar de las dos últimas compras que ha realizado la compañía, y

Bajo la marca Ivanti la compañía compra Concorde y RES en 2017 y Pulse Secure y MobileIron en 2020

"Toda la estrategia de adquisiciones de Ivanti se ha llevado a cabo para llegar a lo que en los últimos años hemos definido como TI Unificada"

que han sido el objetivo inicial de una entrevista también enfocada en saber algo más de una empresa que ha optado por apostar fuerte y comprar dos grandes players del mercado de seguridad y no andar buscando startups.

Todo lo que nos puede decir Stefano Sardella es que "hace muchos años que empezamos a comprar empresas diferentes, siempre para complementar nuestra tecnología y para tener una oferta más amplia con el objetivo de gestionar todo el entorno del usuario". Un entorno, un puesto de trabajo, que está cada vez más lejos de las empresas y es cada vez más móvil, un entorno que habita en un mundo cloud y necesita acceder a los recursos empresariales de forma segura (Pulse Secure) y que necesita ser securizado y protegido de las ciberamenazas (MobileIron).

Escribíamos no hace mucho, fruto de una entrevista con Luis Miguel García, el director general de Pulse Secure en la región de Iberia, que el acceso seguro que Pulse lleva promoviendo desde sus inicios se ha convertido en el nuevo perímetro, un perímetro amorfo que cambia dependiendo de dónde esté la persona, qué dispositivos esté utilizando, desde dónde y a qué quiere acceder. La última gran actualización de la compañía ha sido llevar su servicio de acceso seguro al cloud, más cerca de ese edge en el que confluye todo y cuyo acceso tendrá que ser securizado bajo el nuevo modelo de Zero Trust. Mucho tiene que decir Pulse al respecto.

Experto en securizar los dispositivos móviles, la solución MobileIron Threat Defense (MTD), a que tendría acceso Ivanti tras el cierre del acuerdo, permite asegurar, controlar y gestionar todas las políticas de cumplimiento de PCs, portátiles, teléfonos inteligentes, tablets, etc. Es más, protege tanto el dispositivo, como las redes y las aplicaciones sin ninguna interacción por parte del usuario y sin interrupciones en su productividad.

Enlaces de interés...

- Ivanti
- Ivanti compra MobileIron y Pulse Secure
- Pulse Secure consolida los accesos con su nuevo Pulse Access Suite Plus

Para Ivanti, una empresa que desde sus comienzos ha trabajado la gestionar el desktop y más tarde el puesto de trabajo donde quiera que esté, las compras de Pulse Secure y MobileIron cobran todo el sentido.

Por el momento en el más estricto secreto, que no rompen ni las fuentes de mayor confianza, quedan por saber muchas cosas, entre ellas cómo se producirá la integración o qué pasará con las marcas; Ivanti pasa de no tener oficina en España a tener dos, las de MobileIron y Pulse Secure, y dos directores generales, Daniel Madero y Luis Miguel García respectivamente. Se trabaja con un único mayorista, Lidera Network, que no trabaja con ninguna de las dos recientes adquisiciones… las respuestas las sabremos al 'edge' de 2021. Estaremos atentos.

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 Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET Security Management Center ESET Cloud Administrator	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
RESPUESTA	**DETECCIÓN**

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Sophos Day 2020

“La ciberseguridad no es un deporte de espectador”

(Ricardo Maté, Sohos)

Por primer vez de forma 100% online, se ha celebrado el Sophos Day 2020, un evento que reunía más de 1.000 asistentes para hablar del panorama de ciberamenazas, del reto del ransomware, de lo que se ha vivido este año y de un futuro en el que la compañía busca hacer del threat hunting, la detección y la respuesta un servicio accesible a todo tipo de empresas.

Arrancaba el evento Kris Hagerman, CEO de Sophos, quien durante su discurso aseguraba que “ahora más que nunca la ciberseguridad debe ser una prioridad para todas las empresas”. Además de familiares, colegas o amigos, COVID-19 ha impactado en la vida y conducta de los cibercriminales, decía el directivo, para quien los ciberdelincuentes “nunca han estado más activos ni sido tan agresivos” que durante la pandemia.

En un momento en el que el panorama de amenazas está cambiando, recordaba el directivo que Sophos ha lanzado un nuevo servicio de respuesta rápida que proporciona a las organizaciones un equipo de respuesta ante incidentes 24x7, un equipo compuesto por cazadores de amenazas

Sophos Intecept X, el producto estrella de la compañía para la detección y respuesta en el puesto de trabajo, está creciendo un 50-60% anual

**SOPHOS:
CYBERSECURITY EVOLVED**

**CLICAR PARA
VER EL VÍDEO**

y analistas capaces “de detener rápidamente los ataques avanzados mientras ocurren y eliminar a los adversarios de sus redes”.

Como era de esperar casi el 85% de los ciberataques que ha investigado el equipo de Sophos Rapid Response han sido ransomware, una amenaza que lleva con nosotros un tiempo pero que se ha convertido en una de las propuestas “de más éxito jamás inventada por los ciberdelincuentes, y eso por una simple razón: funciona”, asegu-

raba el CEO de Sophos durante su intervención añadiendo que los ataques de ransomware están evolucionando hacia modelos más sofisticados y agresivos que añaden más presión a las empresas cuando la amenaza no es destruir los datos, sino filtrarlos, hacerlos públicos; también explicaba Hagerman que se está aumentando la cuantía de los rescates, que los atacantes “están siendo cada vez más audaces” y que, aunque los ciberdlincuentes lleven tiempo atentando contra las empresas grande, “esto no significa que las empresas pequeñas estén seguras”, sobre todo porque las propuestas de ransomware-as-a-service están creciendo.

El cloud, que continúa impulsando la modernización, la innovación y la velocidad en todas las industrias, se puede usar para bien o para mal, y los ciberdelincuentes están aprovechando la nube para mejorar sus capacidades y tomar ventaja, por lo que no es sorprendente, decía Kris Hagerman,

que el ransomware se haya convertido en uno de los delitos cibernéticos más denunciados en la nube pública.

Llegados a este punto, y asegurando que el debate de la ciberseguridad ha llegado a las directivas de prácticamente todas las organizaciones, planteaba el CEO de Sophos una serie de preguntas: las empresas, ¿entienden los riesgos para prevenir ataques? ¿son suficientemente resilientes? ¿han desarrollado un plan de respuesta bien definido y probado con anticipación para hacer frente a un incidente de seguridad? ¿han capacitado y probado a sus equipos y los recursos externos con los que se asociarán para asegurarse de que puedan reaccionar lo más rápido posible? Porque frente a un incidente lo que se produce "es una carrera entre los buenos y los malos", y lo que parece claro es que "para prepararte para el futuro necesitas invertir en ciberseguridad avanzada de próxima generación hoy".

El panorama es increíblemente amplio y cambia constantemente; "los atacantes adaptan, perfeccionan y orientan constante y rápidamente sus técnicas para que sean lo más eficaces posibles en cualquier situación determinada". Por eso el mensaje de Sophos es Sophos Evolved.

Sophos, empresa de ciberseguridad

Arrancaba Ricardo Maté su intervención en el evento Sophos Day 2020 asegurando que este es el año en el que nuestro modo de vida y nuestro modo de hacer negocios están cambiando, "y esto representa tanto una amenaza como una oportunidad", decía el director general de Sophos Iberia.

Asegurando que "las amenazas son activas y dinámicas", y que los datos, aplicaciones e infraestructuras están en constante evolución, mencionaba Ricardo Maté el compromiso de Sophos: proteger a las personas del cibercrimen desarrollando productos y servicios potentes e intuitivos que proporcionan la seguridad más efectiva del mundo para organizaciones de cualquier tamaño; "somos una empresa de ciberseguridad no de productos".

Dijo también el directivo que la estrategia sobre la que se basa Sophos tiene tres componentes: un

"El ransomware se ha convertido en una de las propuestas de más éxito jamás inventada por los ciberdelincuentes, y eso por una simple razón: funciona"

Kris Hagerman, CEO, Sophos

"Somos una empresa de ciberseguridad no de productos"

Ricardo Maté, Director General, Sophos Iberia

componente de analítica adaptiva, un componente de sistema interactivo y un componente de Threat Response integrado. Explicaba el directivo que el componente de analítica interactiva incorpora la inteligencia de amenazas, el threat Intelligence, y un conjunto de data science, de Data Analytics; el sistema interactivo es lo que la compañía denomina la plataforma de operación high utility; mientras que el Threat Response integrado incluye por un lado la inteligencia artificial con nuestros expertos "para garantizar que la ciberseguridad no es un deporte de espectador".

Ricardo Maté contó cómo ha evolucionado la seguridad sincronizada de Sophos, lanzada hace ya unos años, una seguridad sincronizada basada en una gestión centralizada de todos los productos, lo que representa una gran ventaja para los administradores porque, por un lado tienen una única consola para gestionar todos los dispositivos, y por otra "pueden añadir automatización en la detección y en la respuesta a poder responder de manera inmediata y proactiva".

El siguiente paso en la evolución fue incorporar una plataforma de datos, un Data Lake, que convierte en sondas a todos los controles de seguridad que van informando en cada instante de cualquier acontecimiento de forma que, incorporando inteligencia artificial, de puede analizar "para responder de manera automática ante cualquier amenaza". Recordaba Maté que la compañía ha abierto su plataforma y que a través de APIs se puede integrar con terceros, así como incorporar información de otros dispositivos y de otros fabricantes.

Destaca durante su intervención el director general de Sophos Iberia la propuesta de Managed Detection and Response (MDR) de la compañía, llamado Managed Threat Response (MTR), "uno de los componentes de los que Sophos está más orgulloso en estos momentos", un servicio de Threat Hunting, detección y respuesta 24x7 realizado por un equipo de expertos como servicio totalmente gestionado que en estos momento suma más de 1.400 clientes a nivel mundial.

Sophos Iberia

"En los últimos años no hacemos más que crecer en nuestro año fiscal", aseguraba Ricardo Maté, apuntando a que si en 2019 se creció un 18%, y en 2020 un 14%, durante los primeros seis meses del año fiscal 2021 ya se ha crecido un 23%, "un crecimiento muy saneado que demuestra que las personas cada vez confían más en Sophos".

La compañía también crece “de manera importante” en el número de clientes; también se incrementa el número de partners, mientas que Sophos Intecept X, identificado por Maté como el producto estrella de la compañía para la detección y respuesta en el puesto de trabajo, está creciendo un 50-60% anual. El nivel de aceptación de la solución EDR de Sophos “también es muy elevado”, aseguraba Maté añadiendo que durante el primer año se tuvieron 30 clientes, unos 160 clientes el segundo y en los primeros seis meses de su año fiscal ya hay más de 180 clientes. Crece también el negocio MSP de la compañía, un 60% en lo que llevamos de año con respecto al anterior.

Enlaces de interés...

- ‘Los servicios de threat hunting se van a convertir en una capacidad clave para las compañías’ (Álvaro Fernández, Sophos)
- Sophos lanza un servicio de respuesta remota frente a ataques activos

Sophos Day

El evento anual de Sophos contó además con la participación de Keren Elazari, Security Analyst & Ethical Hacker, quien compartio su investigación sobre cómo los ciberdelincuentes se están adaptando a las nuevas formas de vida como consecuencia del COVID-19.

Las últimas innovaciones tecnológicas en materia de ciberprotección de Sophos legaron de la mano de Alberto R. Rodas, Sales Engineer Manager de Sophos Iberia, quien mostró cómo detectar e investigar un ataque con tecnologías Next-Gen de Sophos. Por su parte, Iván Mateos, Sales Engineer de Sophos Iberia, tomando como referencia las principales amenazas en 2020 y usando casos de uso reales, explicó cuáles son las tecnologías y estrategias necesarias para protegerse frente a estas amenazas.

Compartir en RRSS

ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTIÓN DE LOS RIESGOS

Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES

Enthec:

“Nosotros somos los ojos de tu empresa”

Detectando una necesidad. Así nacen las empresas. Así nació Enthec hace unos años, con el objetivo de controlar qué información se filtra a la red. Lo hacen con Kartos, una plataforma que rastrea todo Internet, incluidas la Deep y la Dark Web, y determina cuán segura, o insegura, es una compañía monitorizando dominios. ¿El siguiente paso? El IoT.

“El problema está en el flujo inverso, en toda la información que generan los empleados y las máquinas y se expone al mundo”; este problema es lo que da vida a Enthec, una joven empresa española que nace de la necesidad de ir un paso más allá de las herramientas tradicionales de ciberseguridad. Explica María Isabel Rojo, CEO de esta empresa, que la mayoría de las compañías siguen un mismo patrón: establecer un entramado, una nube, que controla el flujo de entrada de información. Es decir, “controla todo lo que Internet envía a esta pequeña nube corporativa y todo lo que se mueve dentro de la misma”.

Su experiencia en varias compañía, desde Banco de Santander a Airbus pasando por Minsait le llevó a ver, en entornos reales, ataques que se estaban ejecutando porque las herramientas daban por bueno un tráfico que permitía que “toda esa información –credenciales o número de máquina, se vertiera fuera”.

Añade María Isabel Rojo que, viendo lo que estaba pansando, “empezamos a investigar y surgió el producto que tenemos”, y que no es otro que Kartos.

En este punto, ¿sabían las empresas lo que les estaba ocurriendo? No. Recuerda María Isabel Rojo que el feedback que recibieron cuando se lanzó la primera versión del producto “fue curioso”. Enthec llevó su producto a cien empresas, tanto posibles proveedores de ciberseguridad como clientes finales, pensando en que les iba a encantar, “pero se frustraban bastante con lo que encontrábamos. En internet estaban expuestos desde código fuente a correos, datos de usuarios y de todo tipo que pueden suponer un incumplimiento de GDPR”. También se encontraron en aquella primera fase de pruebas con gente que les ayudaron a avanzar, que fueron “el germen de la herramienta como la conocemos hoy en día; les gustaba la herramienta pero decían era excesivamente técnica”, de forma que sus creadores añadieron una interfaz de usuario más amigable de forma que “con unos semáforos rojos y unos candados, cualquiera puede entender lo que hay”.

A partir de ahí, se trata de vender la herramienta, de llamar a la puerta de diferentes departamentos, como el de Recursos Humanos. Explica la CEO de Enthec que ahora que el teletrabajo se ha extendido Kartos es muy útil porque por ejemplo puede “detectar empleados que utilizan sus ordenadores corporativos y sus cuentas corporativas para fines totalmente personales”. Saberlo permitiría a las empresas indicar a esos empleados, a través de algunos cursos de concienciación, “por qué no tienen que hacer todo lo que están haciendo”.

Enthec nace “con la mirada muy puesta en los feeds de información, sobre todo documental y el tema de correos y comportamiento de los empleados de las empresas, y ahora hemos crecido”, dice

"El caso de uso que más está creciendo, sin ninguna duda, es la gestión de proveedores, la gestión de terceros"

"Podemos saber muchísimo sobre su empresa y no somos intrusivos"

la responsables de Enthec. Después de agregarse una capa de UX (user experience) para que cualquiera pueda entender todo lo que encuentra la herramienta, "ahora estamos entrando en temas de IoT, estamos entrando en temas de honeypots, incluso empezamos a hacer rastreos de criptomonedas para ver de dónde vienen transacciones y detectar si alguna empresa está haciendo minería sin saberlo" y, como no podía ser de otra manera, "se está trabajando con inteligencia artificial "porque como tenemos una base de documentos tan grande estamos haciendo unos motores de inteligencia artificial para que avisen si alguno de estos documentos incumple GDPR".

Kartos

Kartos lo único que necesitas es que le metas una URL, "y automáticamente todo nuestro entramado de robots se pone a monitorizar toda la red, tanto internet como Deep Web y Dark Web, para encontrar todas las filtraciones de información que hay alrededor de ese dominio y alrededor de esa empresa".

Respecto al tamaño de cliente, "tenemos de todo", desde grandes cuenta que además son las que más se asustan con el resultado, a empresas más pequeñas.

Menciona María Isabel Rojo el caso de un cliente con apenas 30 empleados que no hacía más que cambiar las tarjetas de crédito porque llegaban cargos de compras de consolas de juegos y similares; al final se dieron cuenta que uno de los empleados con acceso a esas tarjetas había metido sus credenciales corporativas en un foro que había sido hackeado, "y daba igual cuantas veces cambiaran las tarjetas porque tenían acceso a su correo y a esa información".

IoT

Volvemos al mundo del Internet de las Cosas, o Cosas Conectadas, o, como quiso bautizarlo sin éxito una compañía, el Internet of Everything. Se trata de un mercado enorme, con un valor

"Estamos empezando a crear una base de datos enorme donde meter motores de patrones y de inteligencia artificial con el fin de detectar en qué casos hay un elemento de IoT expuesto detrás de esas IPs"

que alcanza los 82.400 millones de dólares en 2020, según datos de Quince Market Insights, y en el que se prevé un crecimiento medio anual del 21,3% hasta 2028. Y si nos centramos en el mercado de seguridad del IoT, crecerá desde los 12.500 millones de 2020 a los 36.600 previstos para 2025 gracias, entre otras cosas, a una mayor preocupación de seguridad en infraestructuras críticas, incremento de los ataques contra dispositivos IoT, el riesgos de fuga de datos en redes IoT o las crecientes regulaciones de seguridad, según la consultora Markets and Markets.

Consciente de la situación, Enthec trabaja para incorporar la monitorización del Internet de las Cosas. Explica María Isabel Rojo que cuando trabajan con el espectro de IPs de una empresa "podemos saber si tienes una base de datos expuesta, si tienes un servicio FTP… Podemos saber muchísimo sobre su empresa y no somos intrusivos", y el siguiente paso, pensando en el IoT, es: "estamos empezando a crear una base de datos enorme donde meter motores de patrones y de inteligencia artificial con el fin de detectar en qué casos hay un elemento de IoT expuesto detrás de esas IPs".

Esta evolución de producto está atrayendo muchos clientes de sectores como puertos marítimos o de transporte "que son empresas que están yen-

do por completo a IoT", porque es muy interesante para ellos saber qué exposición tienen cuando, por ejemplo, un barco lleno de dispositivos IoT está entrando en un puerto, o una furgoneta de reparto, "porque si no lo tienes muy bien controlado, a lo mejor estás expuesto y no lo sabes", dice la directiva añadiendo: "Nosotros somos los ojos de tu empresa, pero que miran a toda la red en vez de a tu empresa, nosotros sabemos lo que sabría toda la red sobre tu empresa".

Pasar a monitorizar las IP del IoT, de miles de millones de cosas conectadas, es dar un paso enorme. Dice María Isabel Rojo que por ello se cuenta con "una infraestructura gigantesca por detrás, dispuesta a aguantar terabytes". Dice también la CEO de Enthec que la compañía nació con la idea de monitorizar entre dos y cuatro millones de dominios y que durante un año el trabajo fue "crear una arquitectura lo suficientemente sólida y poner tecnologías punteras para que soporten toda esta carga. Tenemos cientos de robots monitorizando 24/7 toda la red que te están haciendo una ingesta enorme de datos dentro de la plataforma, y todo esto tiene que ir funcionando como un engranaje".

Canal

Cuando hablamos de canal nos cuenta María Isabel Rojo que se ha afrontado teniendo en cuenta que son herramientas nuevas en el mercado y que el primer paso que se está dando es "elabora un entramado de partners de seguridad que ven que nosotros aportamos valor a sus clientes", para lo que se ha puesto en marcha una amplia campaña "para darnos a conocer".

De los casos de uso de la tecnología de Enthec, que varían entre gestión del riesgo de terceros, gestión de riesgos empresariales, GDPR, protección de la imagen pública, cumplimiento, etc., el que más está creciendo es, "sin ninguna duda, la gestión de proveedores, la gestión de terceros", dice María Isabel Rojo, añadiendo que durante 2019 el 70% de los ataques a las empresas se produjeron a través de los proveedores.

Enlaces de interés...

- Enthec
- Guía de ENISA para blindar la cadena de suministro de IoT

Compartir en RRSS

STORMSHIELD

Primer cortafuegos en obtener ambas certificaciones del CCN.

Producto Cualificado y Producto Aprobado

Stormshield, filial participada al 100 % de Airbus CyberSecurity, propone soluciones de seguridad completas e innovadoras para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security). www.stormshield.com/es/

“El cloud no viene a resolver ni a empeorar la situación a nivel de seguridad”

(Elena García, Indra)

Dice abordar el cloud con naturalidad, como una evolución tecnológica más; asegura que los usuarios están mucho más preparados para el cambio de lo que pensamos; prefiere no hablar de tecnologías imprescindibles, sino de pilares del marco de control; sobre los servicios de seguridad gestionada dice que son una oportunidad de hacer las cosas de manera diferente; si tuviera un cheque en blanco no pediría tecnologías, sino personas. Hablamos con Elena García, CISO de Indra, para quien 2021 será el año de la consolidación de todos los proyectos e iniciativas que se han generado este año.

Texto: Rosalía Arroyo • Fotos: Ania Lewandowska

"El buen CISO será aquél que lleve a cabo la estrategia que necesita su compañía y el negocio que defiende". Lo dice Elena García Díez, CISO de Indra desde hace más de dos años, con casi once de experiencia en Inteco y algunos más en otras compañías. Añade que la visión y las exigencias que tiene ahora mismo la ciberseguridad, cada vez más visible, están impactando en esas cualidades del buen CISO, están traspasando el conocimiento técnico para añadir capacidades más comunes a otros entornos, como los de liderazgo, comunicación con el fin de que "todos entiendan la necesidad de la seguridad y la estrategia de seguridad para que puedan participar activamente en ella".

Añade Elena García que hay que encontrar el sitio en el que tiene que estar el discurso del CISO "dependiendo de la situación, dependiendo de la compañía y dependiendo del objetivo del reporte, de la comunicación y de la estrategia que estemos siguiendo en cada momento".

Hacer que seguridad sea una prioridad dentro de las empresas es un camino que están recorriendo cada vez más compañías y que se ha visto impulsado por el contexto COVID. Asegura Elena García que no es un camino nuevo, que hace años que a nivel de política pública, tanto a nivel europeo como a nivel español, "se viene trabajando en sensibilizar al tejido empresarial en la necesidad de mejorar su seguridad para mejorar la calidad del servicio y su progresión".

"El cloud se aborda con naturalidad, como una evolución tecnológica más, como un cambio en un sistemas de gestión más"

De la pandemia hemos aprendido mucho, dice la CISO de Indra, añadiendo que lo importante "es quien lo ha aprendido". Entre las cosas buenas que se han aprendido este año destaca "que los usuarios están mucho más preparados para cambio, que podemos cambiar más rápido de lo que pensamos, que podemos trabajar o impulsar proyectos y adaptarlos de manera más rápida", recoge refiriéndose a esos proyectos que las empresas tenían previsto implantar en años y se han visto acelerados, implantados en meses debido a la situación.

La pandemia también nos ha enseñado que los riesgos están ahí; "sabíamos que hay un fuerte mercado de ciberdelincuencia, pero con la llegada de la pandemia el número de ataques dirigidos y generalizados se ha incrementado exponencialmente, y hemos aprendido que el riesgo es real y que el incidente se produce y se materializa".

Que el riesgo de los ciberataques es real ya lo sabían los responsables de ciberseguridad. Al fin y al cabo es para lo que preparan a sus empresas, y

pocos son los que no han sufrido algún incidente, grande o pequeño. Ese riesgo, a menudo obviado u olvidado por alta dirección de las empresas, se ha puesto sobre la mesa, se ha colado en el prime time de las televisiones, en las portadas de la prensa generalista. Sobre lo que han aprendido los CEO, explica Elena García que durante la pandemia los CEO han pedido a sus empleados cambiar la forma de trabajar, el lugar de trabajo "sin que se redujese la productividad y sin que se redujese ninguna de las condiciones que nos pedían cuando estábamos aquí, y que lo hiciéramos en tiempo récord". Y han aprendido que sí, que podemos hacerlo, "pero que la seguridad tiene que estar desde el principio".

Cloud

"El cloud se aborda con naturalidad, como una evolución tecnológica más, como un cambio en un sistemas de gestión más", dice Elena García. Tiene claro la CISO de Indra que el cloud "no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad", porque "el marco de seguridad es el mismo, las políticas son las mismas, los controles son los mismos".

Añade la directiva que cuando se habla de cloud se habla de un proveedor más, "un proveedor que también está ofreciendo los servicios de seguridad que acompañan a toda su infraestructura cloud", lo que convierte en "una oportunidad el poder llevar el marco de seguridad que ya tienes a otro entorno, estableciendo unos parámetros claros, unas responsabilidades claras, unas obligaciones de comunicación, de coordinación, e integrando esa nueva realidad o ese nuevo entorno –que ya no es sólo nuestro CPD".

Servicios de Seguridad

Hablar con la CISO de Indra de la importancia de los servicios de seguridad gestionados es excesivamente obvio. Salva la situación Elena García asegurando que lógicamente son fundamentales y que "yo como CISO tengo un colaborador de lujo muy cerca, como es SIA, la empresa líder en ciberseguridad en España y Portugal que adquirimos a comienzos de este año". El disponer de un equipo así "en casa" es una oportunidad que permite, por ejemplo "tener unas capacidades de escalabilidad en mis necesidades muy rápidas".

"2021 será el año de la consolidación de todos los proyectos, de todas las iniciativas y de todas las necesidades"

En todo caso asegura también Elena García que "la experiencia y la demanda es, al fin y al cabo, la misma que cualquier compañía" y que los servicios de seguridad gestionada es como el cloud: una oportunidad de hacer las cosas de manera diferente. Si consigues que te dé eficiencia, que mejore tu capacidad de rendimiento y el nivel de seguridad que ofreces al entorno de la compañía, fenomenal".

Los imprescindibles

Preguntamos a Elena García cuál sería la capa básica de seguridad sin la cual no puede estar una compañía. La respuesta genera un debate en sí mismo; "No entiendo una capa básica tecnológica", dice añadiendo que lo que entra en debate no es tanto la tecnología sino "¿cuáles son los procesos o las personas a los que no podría renunciar?".

De la pandemia los CEO han aprendido... "que la seguridad tiene que estar desde el principio"

El planteamiento de la CISO de Indra es: "pensemos en cuáles tienen que ser los pilares del marco de control y con eso veamos qué tecnología la tienen que acompañar. No hay una tecnología imprescindible per se. Y además, el mundo de las soluciones de seguridad ahora mismo es tan amplio, está evolucionando tanto… No hay una tecnología, lo que se tiene que tener claro es cuál es el objetivo y cuáles son los marcos de control que resultan imprescindibles".

Si tuviera un cheque en blanco Elena García no buscaría una solución tecnológica. Si pudiera escribirle una carta a los Reyes Magos "lo que pido no es tecnología, pido personas". Explica que los equipos de seguridad tienen que ser capaces de aprovechar más la información y que toda la tecnología que ayude a automatizar, a liberar a los equipos de cierta capa de operación y dedicar mayor esfuerzo a la inteligencia, es fundamental hoy en día. Pero, "el problema ahora mismo no es la tecnología, son los profesionales".

Añade que si CISO tiene que evolucionar "el equipo tiene que evolucionar con él, le tiene que ayudar", y que ese profesional de la seguridad que estaba muy centrado en la tecnología "tiene que proyectarse también a comunicar mejor, a reportar mejor, a construir mejor el discurso, a explicarle directamente mejor al usuario cuál es la su parte de responsabilidad, a combinar la tecnología de una manera flexible...". Dice Elena García que "el profesional del producto no nos vale" sino que se necesitan "verdaderos profesionales de seguridad que acompañan la función de seguridad en todos sus niveles".

En 2021 no se esperan más cambios. 2021 será "el año de la consolidación de todos los proyectos, de todas las iniciativas y de todas las necesidades" que se han planteado en 2020. Añade que la visibilidad de la ciberseguridad que se ha producido este año ha llevado a muchos responsables empresariales a tener una actitud más proactiva con lo que se estaba haciendo en sus organizaciones y que este 2021 también será el año de "asentar cuánta información sobre la seguridad, el nivel de riesgo e incidentes y peripecias de nuestra función quieren seguir viendo o no. Ese es el único cambio que habrá que ver".

Enlaces de interés...

- 'Los CISO somos ciberresilientes desde hace mucho tiempo' (Javier Sánchez Salas - HAYA Real Estate)
- 'No tiene sentido ver la seguridad como un gasto' (Rubén Fernández, Grupo DIA)
- 'Está demostrado que cada vez que inviertes en educación el nivel de fraude baja' (Iker Osorio, Cetelem)
- 'El Shadow IT sigue siendo un grandísimo problema hoy en día y con cloud todavía más' (Globalia)
- "Un servicio gestionado puede ser tan bueno como estés dispuesto a hacerlo" (Iván Sánchez, Sanitas)
- "La figura del CISO ha evolucionado bastante, y más que tiene que evolucionar" (Mónica de la Huerga, Sopra Steria)

La aniquilación del ransomware

No permitas que un ransomware paralice tu negocio.

it Digital Security

Los Servicios Gestionados de Seguridad a examen

Diciembre 2020

Los servicios gestionados de seguridad a examen

Si una cosa ha quedado clara durante la pandemia es que el perímetro de seguridad ha dejado de existir como consecuencia de la adopción masiva del teletrabajo y una aceleración en la adopción de la nube. Se le une una creciente complejidad de los procesos de las organizaciones, de la confluencia entre la IT y la OT, un incremento de las ciberamenazas, una mayor profesionalización de los ciberdelincuentes, que no dudan en utilizar, ellos también, tecnologías de inteligencia artificial para garantizar el éxito de sus ataques.

Los entornos IT también se hacen más complejos. Se habla ahora de microarquitecturas, de contenedores, de desarrollo ágil, de computación en el Edge, de moverse en entornos cada vez más complejos que hay que asegurar con la misma diligencia que se ponía en proteger un servidor de correo on-premise… en aquellos años.

Se suma una enorme falta de profesionales que hacen necesario el compartirlos. Se hace necesario un soporte de seguridad integral que permita a las organizaciones mantenerse seguras y

itds

Encuentros ITDS

LA VISIÓN DE LAS EMPRESAS **LA VISIÓN DE LA INDUSTRIA IT**

LOS SERVICIOS DE SEGURIDAD GESTIONADA A EXAMEN **CLICAR PARA VER EL VÍDEO**

además alejarse de la primera línea de defensa para prestar atención al cliente y al crecimiento de su empresa.

Los proveedores de servicios de seguridad gestionados, o MSSP, se han convertido en un recurso de incalculable valor para las empresas que desean incrementar sus niveles de seguridad.

A nivel global, el mercado de servicios de seguridad gestionada crecerá de 31.600 millones de dólares en 2020 a 46.400 millones de dólares en 2025, lo que representa un tasa de crecimiento anual del 8,0% durante el periodo.

Con el objetivo de saber a ciencia cierta cuál es la situación a la que se enfrentan los responsables de ciberseguridad de las empresas, qué debe esperar debe esperarse de los servicios de seguridad gestionados, qué elementos se echan en falta, o cómo saber escoger la mejor entre una enorme oferta, se ha celebrado una mesa redonda bajo el título “Los Servicios de Seguridad Gestionada a examen”, que ha reunido a Javier Sánchez, CISO de Haya Real Estate; Daniel Zapico, CISO de Globalia; Manuel Barrio Paredes, CISO de Solvia; Carlos Asún, CISO de Food Delivery Brands y Rafael Luque, CISO de INECO, de una parte y a Francisco Valencia, Director General de Secure&IT; Álvaro Fernández, Enterprise Account Executive de Sophos Iberia y Carlos Tortosa, Director de grandes cuentas de ESET, de otra.

A continuación, podrán leer un resumen de las intervenciones de cada uno de los participantes.

SOPHOS

Managed Threat Response

Tome medidas contra las ciberamenazas

Un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

Más información

LA VISIÓN DE LAS EMPRESAS

GLOBALIA. Daniel Zapico, CISO

"De los servicios gestionados espero que sean servicios gestionados, y no recursos cedidos"

Daniel Zapico, CISO, Globalia

Retos tenemos muchísimos dice Daniel Zapico, CISO de Globalia. En relación a los servicios gestionados plantea este directivo que quizá la pregunta sería ¿qué nos lleva a los servicios gestionados? Una de las razones es la dificultad de encontrar perfiles, "no hay gente, y menos aún gente lo suficientemente cualificada", dice, añadiendo que si además hablamos de tareas de seguridad ofensiva suelen ser gente muy inteligente, a los que es difícil mantener motivados y son difíciles de retener.

¿Qué papel juegan los servicios gestionados de seguridad? Explica el CISO de Globalia que la compañía cuenta con personal interno muy cualificado y con experiencia, pero que "en una parte importante" los procesos de seguridad están sustentados sobre proveedores de servicios, que "tienen una visibilidad muy extensa de lo que pasa en otras empresas y sectores".

"No elijo el mismo tipo de proveedor para desarrollar la capa de gobierno, de control interno, o desarrollar el plan director de seguridad que un proveedor para gestionar una tecnología. Creo que son proveedores distintos y no creo que todo el mundo valga para todo, ni muchísimo menos", asegura Daniel.

Plantea el directivo que trabajar con proveedores de servicios hace que te pongas en sus manos, que tengas que transferir mucho de tu conocimiento tácito y que se llegue a tener riesgo de concentración y de perder conocimiento por transferir excesivas partes a un proveedor; "al final tienes que poner en la balanza y elegir".

"Yo de los servicios gestionados esperaría que sean servicios gestionados", dice Daniel Zapico de manera contundente, explicando que "en España estamos acostumbrados al outsourcing: te pongo una persona y me desentiendo". Dice el CISO de Globalia que un servicio gestionado es un servicio donde se han definido procesos, actividades, SLA, interfaces… "y no es te pongo gente y me la gestinas tú".

Por otra parte, menciona Zapico el riesgo de que se creen silos cuando se trabaja con diferentes proveedores y se tienen que integrar diferentes tecnologías, algo que "ni es trivial ni es sencillo". Añade que en ocasiones es difícil asegurarse que "tus proveedores conocen tus procesos y servicios de verdad; no sobre el papel; no sólo ponerlo en marcha sino mantenerlo y conseguir una mejor continua según va avanzando el servicio.

Además de las pertinentes consultas a otros colegas, a la hora de escoger un proveedor Daniel Zapico apuesta por contar con unas RFPs muy bien hechas, con todo claramente definido, incluidas fases de entrega, devolución del servicio o penalizaciones en caso de que se quieran imponer. Apuesta el CISO de Globalia por contratos relativamente cortos en el tiempo (1 o 2 años), "lo cual en determinadas cosas será un poco problemática, y es verdad que incrementa el coste, pero al mismo tiempo te da flexibilidad".

FOOD DELIVERY BRANDS GROUP (Telepizza, Pizza Hut, Jeno´s, Apache). Carlos Asún, CISO

Dice Carlos Asún, CISO en Food Delivery Brands, que identificar los niveles de riesgo y de gestión es muy importante para "establecer un entorno seguro con los servicios gestionados". Añade que "nos apoyamos mucho en el outsourcing y en los servicios gestionados", y que es importante que estos servicios estén alineados con el negocio, conozcan los diferentes entornos críticos y den una respuesta ágil, porque en el caso de Food Delivery Brands, "cualquier inconveniente impacta mucho en un plazo muy corto de tiempo".

"Aunque hacemos todos los procesos de investigación del proveedor, de la documentación que contestan en las RFPs que emitimos, y se analiza a nivel técnico los niveles que pueden llegar a tener… Hay veces que se nos escapa algún detalle", apunta Carlos Asún. Dice también el CISO de Food Delivery Brands que, de un servicio gestionado, lo que espera es que la experiencia y el conocimiento sea lo más alto posible.

> "De un servicio gestionado espero que la experiencia y el conocimiento sea lo más alto posible"
>
> Carlos Asún, CISO, Food Delivery Brands

También espera que los proveedores "sean muy ágiles en ciertos procesos y en ciertas circunstancias, y totalmente proactivos en temas de amenazas, vulnerabilidades, etcétera". Entender el negocio y sus riesgos es algo que también demanda Carlos Asún a los proveedores. Así como "el saber gestionar las necesidades bidireccionalmente entre todos los proveedores que están dando servicios a un mismo cliente; trabajar en equipo".

> "A la hora de escoger el mejor servicio gestionado hay que tener bien claro qué es lo prioritario para tu compañía"
>
> Rafael Luque, CISO, Ineco

Sobre lo que echa en falta de un proveedor de servicios, lo resumen Carlos Asún con dos palabras: cercanía y exclusividad.

Para el CISO de Food Delivery Brands Carlos Asún, a la hora de escoger el mejor proveedor de servicios, se deben tener en cuenta muchos factores. No sólo hay que hacer mucho análisis, sino preguntar también entre los compañeros y conocer sus experiencias, así como ver cómo responden los proveedores a las RFPs y reuniones de defensa de las mismas. Añade que para evitar posibles errores hay que contar con una serie de contramedidas, como es no ligarse mucho a un único proveedor y cerrar muy bien los contratos.

INECO. Rafael Luque, CISO

Uno de los problemas a los que se enfrentan los responsables de seguridad es el propio perfil de los CISO, dice Rafael Luque, CISO de INECO. Explica este directivo que no sólo hay que "mantener un

conocimiento de la tecnología, que va evolucionando bastante rápido", sino que hay que gestionar un equipo, así como servicios vinculados a la seguridad para completar las necesidades de protección sin tener que incrementar el coste de personal propio de la compañía, lo "obliga a delegar parte del control de la seguridad en proveedores"

¿Qué papel juegan los servicios gestionados de seguridad? Un servicio gestionado de seguridad te ofrece más calidad y ayuda en todo lo relacionado con la seguridad de tu empresa; "tú puedes enfocar toda tu inversión en seguridad en una compañía que te ofrezca garantía y calidad, con personal formado y capacitado", lo que resulta mucho eficiente para una empresa.

Lo que se espera es ofrecer más calidad a la hora de cubrir el ámbito de la seguridad respecto a lo que se podría hacer de forma interna porque los proveedores tienen una visión un poco más global, tienen la experiencia de haber trabajado con distintos clientes y con distintas tecnologías.

En cuanto a lo que se echa en falta, uno de los problemas importantes que tienen los proveedores de servicios gestionados de seguridad es que el papel lo aguanta todo, pero en la práctica se pierde un poco el control del desempeño de ese servicio.

A la hora de escoger el mejor servicio gestionado hay que "tener bien claro qué es lo prioritario para tí". Depende, por tanto, "de lo que tú tengas ya en tu casa, del conocimiento que tengas en tu casa" y de los recursos que tenga cada uno.

SOLVIA. Manuel Barrio Paredes, CISO

"De algunos proveedores de servicios, se echa en falta que sienta la empresa del cliente como suya"

Manuel Barrio Paredes, CISO, Solvia

Uno de los principales retos a los que nos enfrentamos cuando hablamos de servicios gestionados es "encontrar un socio tecnológico que entienda ese servicio como parte de su empresa", dice Manuel Barrio Paredes, CISO de Solvia. Añade que es difícil encontrar proveedores que sientan como suyos los procesos y tecnologías, "sobre todo cuando son proveedores que dan servicio muchas empresas".

"Tenemos casi el 100% de los servicios externalizados, tanto a nivel de IT como de seguridad", dice, mencionando la falta de talento o la dificultad de encontrar personal muy especializado en ciertas tecnologías, lo que lleva recurrir a los proveedores de servicios de seguridad gestionados.

"Lo que más echamos falta a veces cuando contratamos servicios gestionados son perfiles realmente especialistas para determinados sistemas o aplicaciones. Las empresas de servicios no siempre pueden poner las empresas a gente senior", dice Manuel Barrio. Añade que, por desgracia, en casi todos servicios gestionados al final entre lo que se redacta en la oferta por parte del proveedor cuando se presenta a un RFP y el servicio finalmente prestado suele haber bastantes "Claro oscuros" ya que después suele pasar que no es la gente realmente especializada quien atiende ese servicio.

Dice también el CISO de Solvia que se ha encontrado con casos en los que el proveedor de servicios no conoce bien el negocio, que se centra mucho en la parte técnica, pero no en el negocio que sustenta esa parte técnica; "se echa en falta que sienta esa empresa como suya y conozca hasta el último detalle y cómo afecta a negocio cualquier incidente o que pueda ocurrir en los sistemas que está gestionando".

A la hora de escoger un servicio gestionado generalmente se consulta primero a otros responsables de ciberseguridad, y también a los propios

"Del proveedor de servicio demando una actitud más proactiva"

Javier Sánchez, CISO, HAYA Real Estate

fabricantes, a quien se les pregunta que empresa es la que tiene más experiencia en un producto, o el que tiene menos problemas. Añade Manuel Barrios que "intentamos hacer los menos experimentos posibles con productos o soluciones nuevas, e intentamos en la mayor medida posible, optar por tecnologías y soluciones ya con experiencia en el sector".

HAYA REAL STATE. Javier Sánchez, CISO

"Retos tenemos todos", dice Javier Sánchez, CISO, Haya Real Estate, cuando se plantean cuáles son los desafíos a los que se enfrentan los responsables de ciberseguridad. Buscar perfiles es complicado, y aparte de que no los hay "tampoco nos interesa", ya que si está muy especializado en una tecnología o producto y este cambia, tienes un problema, "y esta es la principal ventaja de un servicio gestionado", junto con la experiencia que aporta a la hora de saber escoger una tecnología determinada.

Sin tener externalizada toda la seguridad, dice Javier Sánchez que los servicios gestionados de seguridad se consideran, dentro de los planes de la compañía, "como proveedores críticos" porque "tenemos gran parte de nuestra protección de seguridad delegada en ellos y en el caso que ellos estuvieran una caída, podríamos tener un gran problema".

"Yo siempre espero de un servicio gestionado, y lo que demando además, es que nos acompañen en esta evolución hacia un mundo en el que podamos considerar que tenemos los suficientes controles para dormir tranquilos", dice Javier Sánchez. Menciona el directivo que esta demanda implica una actitud más proactiva, que sea el proveedor de servicio el que proponga, como expertos en seguridad, qué podría hacerse, nuevas ideas. "Lo que a mí me aportaría valor es que me diga hacia dónde vamos, qué tendencias hay, novedades, cuál es el siguiente paso. Eso es lo que yo demando ahora de un servicio gestionado".

A la hora de escoger entre los diferentes servicios de seguridad gestionados se parte "de la experiencia que hayamos tenido con ese proveedor; en ocasiones porque nos preguntamos entre nosotros, y otras veces es e intuición y suerte", dice Javier Sánchez Salas, que, para empezar, opta por pedir opinión a colegas.

Necesitas un

PLAN

DE CONTINUIDAD

DE NEGOCIO

B

Secure&IT by LKS

www.secureit.es

LA VISIÓN DE LA INDUSTRIA IT

SECURE&IT. Francisco Valencia, CEO &IT

"El principal reto de un proveedor de servicios es dar respuesta a los retos a los que se enfrentan los responsables de seguridad", asegura Francisco Valencia. El problema con la rotación y la retención del talento que tienen las empresas, y para lo cual contratan a proveedores no hace sino "trasladarnos el problema a nosotros, porque efectivamente hay un problema increíble de falta de recursos".

Otro reto es ayudar a los CISOs a socializar el riesgo, porque cuando existe un incidente y tenemos que responder al mismo tenemos que hablar no solo con IT, sino con recursos humanos, con asesoría jurídica, con la dirección financiera o con la dirección general… El CISO tiene un rol muy transversal y nosotros tenemos que dar soporte a esa transversalidad.

Secure&IT cuenta actualmente con unos 200 clientes aproximadamente, todos del rango de 400, 500 o 600 empleados, más o menos, explica Francisco Valencia. Añade el directivo que justo en este nivel de empresa se produce una frontera muy interesante: "por debajo lo que buscan es rellenar el check que tienen que poner los consejos de administración cuando dicen si han hecho ya seguridad en su casa o no. Para poner el check contrata un servicio de seguridad gestionada, y como no tienen muy claro, a ese nivel, qué es lo que te están

FRANCISCO VALENCIA, CEO &IT

CLICAR PARA VER EL VÍDEO

"El CISO tiene un rol muy transversal y nosotros tenemos que dar soporte a esa transversalidad"

Francisco Valencia, CEO &IT

"Un servicio tiene que ser transparente, medible, y el dueño tiene que ser el cliente"

Álvaro Fernández,
Enterprise Executive, Sophos Iberia

ÁLVARO FERNÁNDEZ,
ENTREPRISE EXECUTIVE, SOPHOS IBERIA

CLICAR PARA VER EL VÍDEO

contratando, al final te piden un llave en mano y ahí desarrollamos un servicio que se llama Gold Security", donde la compañía se encarga de la seguridad desde distintos ámbitos: legales, con protección de datos o propiedad intelectual o industrial o código penal, hasta el forense de hacking ético pasando por el SIEM o toda la monitorización y en general todos los servicios que una empresa necesitan.

"Hasta ese nivel es todo muy sencillo porque nos constituimos como responsables de seguridad de las organizaciones", dice el CEO de Secure&IT. Lo que ocurre por encima de ese tamaño de empresa es que todo se segmenta muchísimo, unos quieren la monitorización, o solo la respuesta ante ataques… y en ese punto se producen un reto que es muy importante que es la interrelación con otros proveedores y otros departamentos que gestionan los sistemas.

Dice Francisco Valencia que el mismo problema que tiene un CISO a la hora de seleccionar un proveedor de servicios "lo tengo yo como proveedor a la hora de seleccionar un fabricante. Con qué producto marcas toda tu estrategia para defender al cliente". Añade el directivo que "una empresa como la nuestra vive de vuestra seguridad" y que Secure&IT no vende tecnología sino seguridad.

Añade este proveedor de servicios que en el caso de su compañía no se tiene a ningún empleado en outsourcing y que cada cliente cuenta con tres perfiles, el abogado, el ingenio y el experto en procesos, "que forman parte, o invitamos a que formen parte, del Comité de Seguridad y Cumplimiento".

SOPHOS. Álvaro Fernández, Enterprise Executive

Fabricante de seguridad, explica Álvaro Fernández, Enterprise Executive de Sophos Iberia que Sophos ha sido muy meticuloso a la hora de desarrollar productos que puedan ser gestionados por terceros, y que el reto es escuchar al mercado, entender cuá-

les son las necesidades de los partner y plasmarlo en la tecnología.

En ciberseguridad hay que alinear tres cosas: personas, procesos y tecnología. Para las empresas es muy complicado poder alinearlas por sí solas, y los proveedores de servicios pueden ayudarles. Destaca también Álvaro Fernández que un servicio tiene que ser transparente por lo que, por un lado, los proveedores tenemos que ser muy claros, y por otro los clientes tienen que preguntar y ser muy meticulosos a la hora de entender qué es lo que pueden esperar de este servicio.

Uno de los gap que ha detectado su compañía, y donde Sophos ha hecho una propuesta de servicio importante, es en la detección y respuesta. Explica el ejecutivo de Sophos que las soluciones EDR (endpoint detection and response) ofrecen mucha capacidad de ver cosas para poder responder a las amenazas, pero se necesita poner recursos que estén formados, recursos que es complicado conseguir y que nosotros ofrecemos como servicio.

"El servicio por excelencia en seguridad es la gestión", asegura Álvaro Fernández cuando se le pregunta por los servicios de seguridad que más de demandan. Añade que hay dos tipos de servicios, por un lado, la gestión de la detección y el dar una respuesta ante las amenazas que se encuentran, "y que no deja de ser el tener a expertos por detrás haciendo un threat hunting a través de nuestro EDR", y un segundo tipo de servicios de respuesta rápida ante incidente "que desgraciadamente se

> "Nosotros entendemos un servicio sí gestionado y con un proveedor que sea cercano"
>
> Carlos Tortosa, responsable de grandes cuentas, ESET

demanda mucho" y que ayudan a las empresas a afrontar un incidente a restablecer el servicio.

"Un servicio tiene que ser transparente, medible, y el dueño tiene que ser el cliente", dice Álvaro Fernández. Añade que, para escoger bien un servicio, un cliente debe "preguntar, comparar, ver exactamente lo que propone cada uno de los servicios y pensar cuál es el servicio que tú necesitas". Además, "los servicios deben tener un objetivo y hay que cumplirlo, y si no, pues tendrá que haber penalizaciones".

Es importante trabajar desde el primer momento de manera muy cercana con el fabricante e integrador para entender bien cuál es el servicio y poder tener diferentes alternativas para decidir la más idónea.

ESET. Carlos Tortosa, responsable de grandes cuentas, ESET

Refiriéndose a cómo las siglas acuñadas por algunas consultoras en ocasiones añaden complejidad a las tecnologías existentes en el mercado, dice Carlos Tortosa, responsable de grandes cuentas de ESET, que "tenemos que ser capaces de poner en valor el producto no por el nombre, sino por cómo te va a proteger". Para nosotros, continúa este directivo, es un reto "facilitar al proveedor servicios una herramienta concreta que te proteja ante una amenaza concreta. Y el nombre que nosotros le vamos a dar no tiene importancia".

Entre los retos a los que se enfrenta ESET, destaca el directivo el hacer llegar al proveedor de servicios "cuál es la herramienta completa que se tiene que utilizar en cada situación, en cada cliente y cómo hacerla funcionar". No tanto un reto como una obligación es que los proveedores de servicios que trabajan con nuestros productos tengan conocimiento suficiente para que la capa de protección os

cubra al cien por cien lo que realmente está diciendo. “Pero creo que es el reto principal en nuestro caso es dar formación al proveedor de servicio y darles las herramientas necesarias para ese nivel de protección”, añade el responsable de grande cuentas de ESET.

Dice Carlos Tortosa que se está rebajando muchísimo el nivel de cliente que está solicitando un servicio gestionado. La empresa pequeña no es capaz de contratar un especialista en ciberseguridad, y lo más lógico es contratar un especialista en ciberseguridad, y si además tiene la capacidad de realizar un servicio de monitorización y de respuesta, muchísimo mejor.

Con las propuestas de servicios gestionados lo que estamos haciendo es llegar prácticamente a cualquier tipo de cliente, y lo que más se demanda es seguridad endpoint, que es lo mínimo, además de monitorización. Y después, en empresas un poco más grandes, lo que se solicita es una respuesta inmediata de un incidente, una resolución de manera remota.

ESET facilita a sus partners un servicio de monitorización de sus productos, con sus herramientas y acceso a la capacidad del departamento de soporte de la compañía. Se trata de una herramienta que “facilitamos a aquel distribuidor o partner que no tiene capacidad a nivel profesional y que sí tiene capacidad de llegar a una cantidad concreta de clientes, sean del tamaño que sea, porque hemos puesto un precio ajustado de servicios”.

CARLOS TORTOSA,
RESPONSABLE DE GRANDES CUENTAS, ESET

CLICAR PARA VER EL VÍDEO

“Nosotros entendemos un servicio sí gestionado y con un proveedor que sea cercano. Para nosotros eso es lo lógico”, asegura Carlos Tortosa, añadiendo que su compañía trata en todo momento que la formación que tenga el proveedor del servicio sea la máxima posible.

¿Cómo se tiene que elegir un servicio gestionado? Primero, el proveedor tiene que ser de garantías; otra cosa serán los productos que incluyan dentro de este servicio, dice Carlos Tortosa. Asegura en directivo que “la necesidad de que el proveedor conozca las herramientas que os está facilitando y que no nos tengamos que fijar ya tanto en el nombre de las herramientas que utiliza, sino en la robustez y el conocimiento que tiene de las mismas, creo que debería de ser algo primordial para cualquiera de los responsables de seguridad”.

ENCUESTA

El dato en la toma de decisiones:

haciendo la empresa hiperinteligente

¿Tienes toda la información que necesitas para tomar decisiones en tu empresa?

¿Es sencillo acceder a la información empresarial?

¡PARTICIPA!

it User
TECH & BUSINESS

De la continuidad de negocio a la resiliencia segura

it Digital Security

CISCO

Diciembre 2020

De la continuidad de negocio a la resiliencia segura

2020 se ha convertido en el año que ha puesto a prueba la resiliencia empresarial. Conectar gente, asegurar los negocios y automatizar procesos, a veces de manera urgente y en ocasiones de manera diferente, son las claves de la resiliencia empresarial, tan necesaria para mantener el negocio a pleno rendimiento.

Cisco es un testigo de excepción para hablar de lo que ha ocurrido durante la pandemia. Como proveedor de soluciones de colaboración, la compañía ha podido ver el crecimiento que se producido en relación con este tipo de herramientas y los problemas de seguridad que han generado algunas de ellas. Durante un encuentro con varios responsables de ciberseguridad, recordaba Eutimio Fernández, Director de Ciber-seguridad de Cisco España, que la compañía también es experta en el tema de comunicaciones y "también somos proveedores de una arquitectura muy amplia de ciberseguridad", lo que le permite estar muy involucrado en las necesidades de los clientes.

La experiencia durante la pandemia lleva a Eutimio Fernandez a decir que no estábamos preparados y que "nos está obligando a cambiar la forma de hacer IT"; sobre la situación de la ciberseguridad durante los primeros meses de este año dice el director de Ciber-seguridad de Cisco España que si bien no ha habido innovación en los ataques, sí que ha habido un gran incremento.

"Desde el punto de vista de tecnología y de ciberseguridad está siendo un momento muy entretenido", apuntaba el directivo. Los negocios se redefinen por los cambios de hoy y por las incertidumbres del futuro. Cambios e incertidumbres que establecen nuevas prioridades, como empoderar a los empleados para que trabajen desde cualquier sitio y con cualquier dispositivo, pero de una mane-

DE LA CONTINUIDAD DE NEGOCIO A LA RESILIENCIA SEGURA. CONCLUSIONES

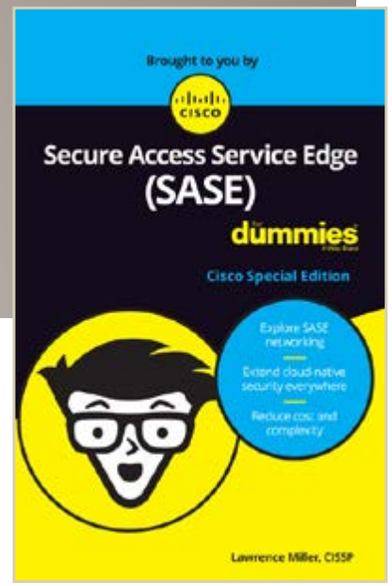
CLICAR PARA VER EL VÍDEO

ra segura, de forma que el rendimiento empresarial llegue al hogar.

¿Cuáles han sido los retos a los que se han enfrentado los responsables de ciberseguridad de las empresas?, ¿qué se ha aprendido de la pandemia?, ¿cómo se ha afrontado la aceleración de la transformación digital vista en los últimos meses? Estas son algunas de las preguntas que se han debatido en un Encuentro ITDS patrocinado por Cisco y en el que han participado Jesus Alonso Murillo, CISO de Ferrovial Servicios; Mónica de la Huerga, CISO de Sopra Steria; Josep Bardallo, CISO del Grupo Recoletas; Carlos Manchado CISM CISSP, CISO de Naturgy; Jorge Arrufat Tejera, Head of Security de BBVA Next Technologies; Ruben Fernandez Nieto, CISO de DIA Group y Eutimio Fernández García-Donas, Director de Ciber-seguridad en Cisco España.

SASE PARA DUMMIES, BY CISCO

Los equipos de TI de hoy se enfrentan a un desafío común: cómo habilitar de forma segura el creciente universo de usuarios, dispositivos y aplicaciones SaaS sin agregar complejidad o reducir el rendimiento del usuario final, todo ello mientras aprovechan sus inversiones de seguridad existentes. Este libro examina el panorama cambiante de la red y la seguridad, y los pasos que puede tomar para mantener su organización segura y protegida a medida que evoluciona su red.



LA VISIÓN DE LA INDUSTRIA IT

Jesús Alonso, CISO, Ferrovial Servicios

"Nos hemos dado cuenta de que la tecnología existe"

Jesús Alonso, CISO, Ferrovial Servicios

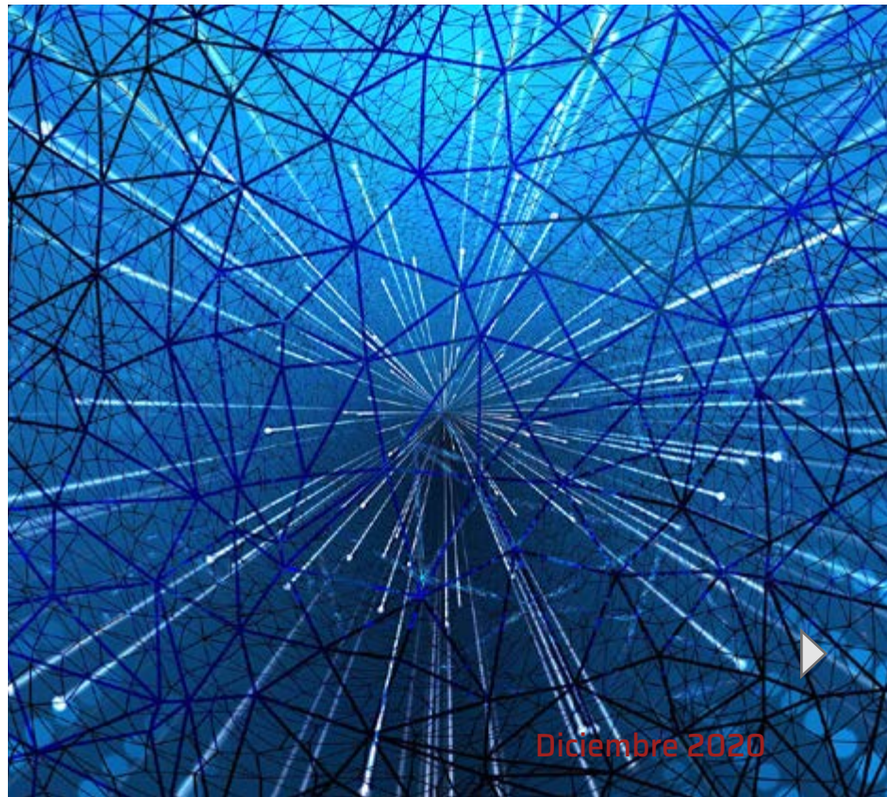
Explicando que en Ferrovial Servicios, donde ocupa el puesto de CISO, se ofrecen diferentes servicios, algunos públicos y de especial criticidad, como servicios de IT y todo lo que tiene que ver con seguridad en Hospitales, explicaba Jesús Alonso que uno de los retos a los que se ha tenido que enfrentar este año de pandemia ha sido el enviar a los empleados a casa a trabajar, que si bien es un reto per se, se complica cuando el que se ve afectado es un call center. "Nos hemos dado cuenta de que la tecnología existe, que permite establecer las conexiones de forma segura, el problema ha sido hacerlo de una manera excesivamente rápida", dice Jesús Alonso.

No hay mal que por bien no venga, porque lo que está ocurriendo es que las nuevas licitaciones o proyectos que se están viendo ahora ya incluyen el tema del acceso seguro de empleados remotos, lo que permite "desde el inicio, establecer los procesos para poder trabajar de una manera más segura".

"Hemos aprendido de la pandemia es que se pueden seguir operando y trabajando desde casa, o desde donde queramos, con tal de que tengamos una conexión medianamente razonable", dice el CISO de Ferrovial. Hace años que se habla de la pérdida de perímetro, y la pandemia ha terminado por eliminarlo definitivamente.

El objetivo ahora es "proteger el dato, la información, y cómo se accede a esa información". Ahora bien, este un binomio del dato y la autenticación, a lo que hay que añadir la trazabilidad y comportamiento del usuario, "no se puede aplicar absolutamente a todo porque podemos paralizar ciertos procesos, ciertos proyectos, ciertos servicios", dice Jesús Alonso. Asegura el directivo que hay que centrarse en el dato que de verdad sea importante, que de verdad sea crítico; "hay que intentar decidir qué es crítico y quitar el grano de la paja" y apostar por modelos SASE.

Durante su intervención Jesús Alonso decía también que en plena transformación digital, acelerada durante la pandemia sanitaria, "hay que alejarse un poco de hierro para externalizar cosas, e irnos al cloud, a un concepto de seguridad como servicio".



Carlos Manchado, CISO, Naturgy

"La movilidad del endpoint no es algo trivial"

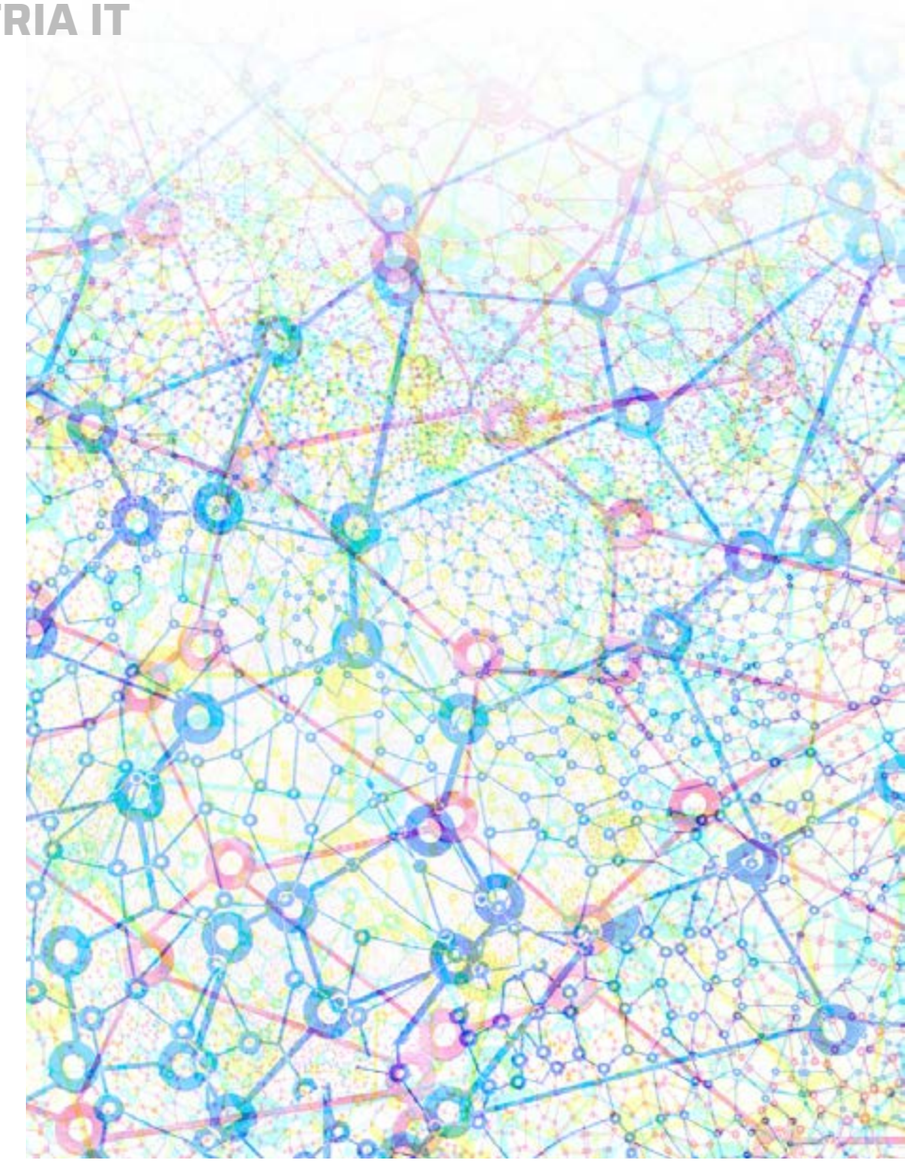
Carlos Manchado, CISO, Naturgy

Ser una empresa de servicios esenciales y sometida a la Ley de Infraestructuras críticas llevó a Naturgy a trabajar con cuidado y contrarreloj para poder establecer una arquitectura que de manera segura permitiese conectar de forma remota con las instalaciones, explica Carlos Manchado, CISO de esta compañía, mencionando el primer reto al que tuvo que enfrentarse en los primeros momentos de pandemia. Otro de los grandes desafíos ha sido "tener equipos que habitualmente estaban bajo el perímetro y bien custodiados y parcheados y pasar a gestionar equipos que no están en ese perímetro, que a veces son personales y que se conectan desde redes domésticas que no ofrecen ninguna garantía", explicaba el directivo.

Mientras que algunas empresas tenían experiencia en la movilidad del endpoint, en otras empresas o sectores "esto no era trivial", dice Carlos Manchado cuando se le pregunta por las lecciones aprendidas durante la pandemia. "Hemos aprendido a que no es lo mismo tener un equipo de sobremesa detrás de un perímetro que no es que se haya difuminado, es que ha saltado por los aires, por mucho que se hubiera hablado del tema", explica el CISO de Naturgy añadiendo que "también te das cuenta de que las VPN están muy bien a nivel IT y para un primer momento, pero que tienen muchos riesgos".

Añade el directivo un tercer aprendizaje: "las grandes suites de colaboración y compartición nos han hecho un gran favor, pero tienen unos riesgos terribles porque ninguna está securizada desde el comienzo".

Una de las formas de afrontar el perímetro es con concienciación, algo que para Carlos Manchado es clave pero que "no es tan fácil como montar un appliance o hacer una integración de tecnologías. La formación de los empleados es un tema mucho más costoso". Si nos centramos en el tema tecnológico "tenemos que cambiar el paradigma totalmente," dice el CISO de Naturgy poniendo sobre la mesa los conceptos Zero Trust y SASE y asegurando que en su compañía se tiene claro que es hacia estos paradigmas hacia donde hay que ir; "creo que tiene que haber un elemento central por el que en todas las conexiones, ya sea en terceros y de personal interno o externo, se apliquen los mismos controles".



Jorge Arrufat, Head of Security, BBVA Next Technologies

El reto, o retos, a los que se han enfrentado los responsables de ciberseguridad durante este año de pandemia "va muy en línea con el punto en el que te encuentres de tu transformación digital", dice Jorge Arrufat, Head of Security de BBVA Next Technologies. Añade el directivo que la pérdida de perímetro ha hecho que la confianza se haya tenido que reevaluar y que el mayor beneficio de la pandemia ha sido su impulso en la transformación digital de las empresas, un impulso que en muchos casos no se ha visto acompañado de seguridad.

"De la pandemia hemos aprendido que esto no va de comprar una solución y darle a un botón, sino de plantear una estrategia de seguridad para que todo nazca seguro", dice Jorge Arrufat. De los empleados siempre se ha dicho que son el eslabón más débil porque están en el otro lado de ese túnel que les permite acceder a la información y al dato, y durante este año también se ha aprendido que estos usuarios "tienen que entender esos riesgos de seguridad, y no sólo sobre el papel"

> "Esto no va de comprar una solución y darle a un botón"
>
> Jorge Arrufat, Head of Security, BBVA Next Technologies

Para Jorge Arrufat, la identidad es clave. Dice el Head of Security de BBVA Next Tehnologies que una vez que el perímetro ha desaparecido, igual ocurre con la confianza, que ha de re-evaluarse siempre para cada identidad, tanto de humanos como de dispositivos, así como de los sistemas de información". Es lo que persigue Zero Trust, una filosofía que no es nueva y que requiere de unas tecnologías para poder hacerse realidad; "ahí la clave está en que todas las tecnologías se hablen y se complementen, que sepamos sacar provecho de ellas". Menciona de manera específica las técnicas de inteligencia artificial "que nos pueden ayudar a analizar el comportamiento de la identidad o el comportamiento del usuario en el acceso a estos datos".

Josep Bardallo, CISO, Grupo Hospitalario Recoletas

"Estar preparados para la contingencia de las personas" es uno de los retos a los que se ha enfrentado Josep Bardallo, CISO del Grupo Hospitalario Recoletas. Con 22 centros hospitalarios, los planes de contingencia de la compañía estaban preparados para los sistemas, "pero no para que un médico se ponga enfermo, esté en su casa y tenga que dar servicio". En apenas unos días se puso sobre la mesa cómo acelerar todos los proyectos de transformación digital, que en el caso de Grupo Recoletas eran proyectos de telemedicina.

Otro gran reto que no estaba contemplado fue el de las integraciones: "todos los hospitales privados

"Se apuesta por todo tipo de tecnologías que ayuden a garantizar quien está accediendo al dato"

Josep Bardallo, CISO, Grupo Hospitalario Recoletas

se tuvieron que integrar con la sanidad pública, y desde el punto de vista de la seguridad es una pesadilla".

"Básicamente nosotros lo que hemos aprendido es que desde seguridad tenemos que trabajar asumiendo riesgos y en silencio", dice Josep Bardallo, explicando que durante los últimos meses se han tenido que dar soluciones e implementar tecnologías "pero sin molestar al usuario y sin dejar de dar servicio".

Durante la pandemia sanitaria ha quedado claro que la nueva situación de telemedicina y el tener que abrir los sistemas a terceros ha obligado a poner herramientas de visibilidad y control "alrededor de nuestros datos sanitarios para ver por dónde llegan, como protegerlos, etc.".

Poniendo el perímetro en el dato, y siendo los datos que gestiona extremadamente sensibles, dice Josep Bardallo que se apuesta por "todo lo que sean tecnologías para identificar correctamente a la persona que acceda a los datos para protegerlos, temas de reconocimiento por patrones o temas de comportamientos inusuales (UEBA). En definitiva, se apuesta por todo tipo de tecnologías que ayuden a garantizar quien está accediendo al dato".

Mónica de la Huerga, CISO, Sopra Steria

"Dar soluciones de continuidad a nuestros clientes y sobre todo acelerar los procesos en los cuales estábamos trabajando con ellos", es el principal reto al que se tuvieron que enfrentar en Sopra Steria ante el contexto generado por la pandemia. Para Mónica de la Huerga, CISO de esta empresa, también supuso un reto la pérdida de perímetro y de control al tiempo que mantenían los servicios y los niveles de seguridad.

Sobre lo aprendido en la pandemia menciona Mónica de la Huerga varias cosas. Por un lado los CISO han ganado visibilidad a nivel de las empresas; "la seguridad tiene que estar ahí, sigue siendo una pieza clave y fundamental". Al mismo tiempo "hemos aprendido con la pandemia que no somos ni invencibles ni inmortales" y que puede haber flexibilidad en la tarea de un responsable de ciberseguridad, "que somos capaces de plantear alternativas, que gustan más o gustan menos, lógicamente, pero que sí, que tenemos esa capacidad de improvisación, de innovación, que al final es lo que necesita la compañía". Añade la CISO de Sopra Steria que nada está escrito y "hay que evolucionar, hay que adaptarse al ambiente, hay que tener en cuenta los nuevos riesgos, como por ejemplo el riesgo de pandemia".

En un mundo sin perímetro coincide Mónica de la Huerga en que es igual de importante proteger el dato, y, lógicamente, controlar quién puede acceder y cómo puede acceder al mismo. El problema,

"Nada está escrito, hay que evolucionar y adaptarse al ambiente"

Mónica de la Huerga, CISO, Sopra Steria

añade la CISO de Sopra Steria, ya no es sólo que la seguridad perimetral haya desaparecido, sino que se ha fundido con el perímetro personal y del ámbito del domicilio de cada uno, “lo cual lo hace todavía más difícil de gestionar”. Cree que, al final, el foco sigue siendo “concienciar a los usuarios, ya no sólo a nuestros trabajadores, sino a la sociedad en general, de la importancia del dato, de la importancia de las conexiones, de la importancia de tener bien configurados nuestros equipos…”.

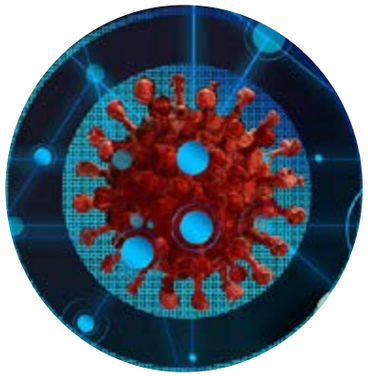
Rubén Fernández, CISO, Grupo Dia

Para Rubén Fernández, CISO de Grupo DIA, las empresas sí que estaban preparadas para las diferentes situaciones que se generaron durante la pandemia, “lo que no estábamos es dimensionados”. En caso del teletrabajo, estaba pensado para el 20% de la plantilla, pero en pocos días el 100% de las personas tiene que tener la capacidad de teletrabajar, “y obviamente hay que dimensionar de una manera correcta esta nueva situación”.

Sí está de acuerdo es que se ha acelerado mucho la transformación digital y que el principal reto en ese sentido es acompañar correctamente esta aceleración que tenemos en el proceso de digitalización de las empresas con las opciones de seguridad que consideramos que son necesarias.

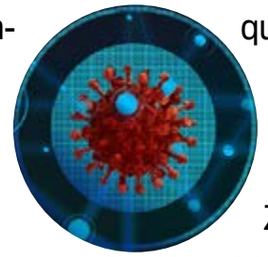
La pandemia ha provocado “un cambio más cultural que de seguridad”, dice Rubén Fernández. Hace referencia al teletrabajo, que muchas más empresas de las que estarían dispuestas a reconocerlo no veían con buenos ojos, un teletrabajo que se disfrutaba como un privilegio y que ahora es necesario para evitar contagios.

Además, la pandemia ha enseñado que “tenemos que reforzar mucho la parte de concienciación y la seguridad de los endpoints”, entre otras cosas por-



"La pandemia ha provocado un cambio más cultural que de seguridad"

Rubén Fernández, CISO, Grupo Dia



que al no estar en la oficina impactan en temas como la política de parcheo.

Afrontar un mundo sin perímetro de seguridad pasa por enfocarnos en modelos Zero Trust, en patrones de comportamiento, en herramientas tipo EDR que no se fijan tanto en firmas, o en herramientas de monitorización basadas en el comportamiento de un usuario, dice el CISO de Grupo DIA. Insiste Rubén Fernández en que “deberíamos utilizar más ese tipo de herramientas para intentar identificar patrones anómalos y posibles compromisos, tanto a nivel aplicación como a nivel de usuario porque ya no tenemos al empleado en la oficina”.

LA VISIÓN DE CISCO

“Hay que cambiar la forma de hacer IT para dar soporte al teletrabajo y que éste sea seguro”

PROPUESTA TECNOLÓGICA CISCO SEGURIDAD

CLICAR PARA VER EL VÍDEO

No se sorprende Eutimio Fernández, Director de Ciber-seguridad de Cisco España, por ninguna de los retos que han planteado los seis CISO invitados al debate. Coincide con que la tecnología está, pero que no se estaba utilizando “pensando en que mis trabajadores son ahora tele-trabajadores”. El siguiente paso después de los primeros meses de pandemia ha sido empezar a pensar en cómo rehacer la IT antes de que llegue una tercera oleada, para lo que se ponen sobre la mesa conceptos como Zero Trust que faciliten que el teletrabajo esporádico sea algo habitual o que un PC se gestione de la misma manera estando fuera o dentro de la red.

De la pandemia “hemos aprendido de las experiencias de todos vosotros”, decía Eutimio Fernández a los CISOs participantes en un debate que, según el directivo, ponía sobre la mesa que la VPN no es el futuro porque “al menos para lo que son conexiones de usuarios hacia la compañía es inmanejable”; que se ha producido un cambio cultural que lleva a la adopción de la nube “porque es lo que me permite tener acceso desde cualquier sitio”; que la protección tiene que estar en el dato teniendo en cuenta que “en entornos cloud el dato es responsabilidad del cliente, no del proveedor de la aplicación”; o que realmente el perímetro de seguridad “está en la propia identidad”.

Teniendo en cuenta que la seguridad del dato y la identidad se han vuelto cruciales, y que la estrategia a la hora se securizar puede ser prácticamente la misma pensando que el trabajador puede estar en cualquier parte; “la idea es conseguir que plataformemos una vez, que nuestras medidas de se-

guridad sean lo más transparentes posibles y que la experiencia de usuario sea la misma esté donde esté".

Durante el debate surgen de manera recurrente conceptos como Zero Trust o SASE, modelos que en la empresa española han tenido una "aceleración muy fuerte", ya que prácticamente todas las compañías con las que se está hablando "están moviéndose a entornos SASE".

Propuesta tecnológica

Sobre la propuesta tecnológica de la compañía, explica Eutimio Fernandez en el vídeo, que está muy alineada con las necesidades que están demandando las empresas y que se ha "realizado una fuerte inversión en el modelo SASE", que ha evolucionado desde Cisco Umbrela.

La compañía ofrece, desde la nube, protección DNS, "que es la primera línea de defensa", así como firewall, proxy, DLP, CASB… y con un modelo bajo servicio. Se añade toda la estrategia SD-WAN de Cisco para ofrecer "una solución SASE que puede ir a todo tipo de cliente".

Desde el punto de vista de Zero Trust, explica Eutimio Fernández que gracias a una arquitectura que "es la más amplia del mercado" se garantizar una implementación de Zero Trust en todo tipo de entorno: Zero Trust para usuario remoto, Zero Trust para entorno de oficina y Zero Trust para entorno de Datacenter.

De esta forma, "desde el punto de vista de SASE y desde el punto de vista de Zero Trust tenemos arquitecturas completas para implementar en todo tipo de compañías"

"Se ha producido un cambio cultural que lleva a la adopción de la nube porque es lo que me permite tener acceso desde cualquier sitio"

Todo lo que necesita para asegurar su nube.

Simplifique su seguridad en la nube con Trend Micro Cloud One™, la plataforma de servicios de seguridad para desarrolladores líder en el mundo.

Cloud One™
Cloud Security simplificada

La infraestructura global evoluciona con el tiempo pero Trend Micro va por delante optimizando la protección. Creado con datos reales por el artista **Andy Gilmore**

Descubra Cloud One en este video:

Conozca más en www.trendmicro.es

TREND MICRO™

La Seguridad de la Identidad

La identidad digital es una de las tendencias tecnológicas más importantes del planeta no sólo en el ámbito personal, porque cambia la manera con la que interactuamos con las instituciones públicas, sino a nivel profesional porque nos permite acceder a los recursos empresariales de una manera más sencilla. También tiene un riesgo porque el robo de esa identidad podría generar una brecha de seguridad.

Desayuno ITDS

Para hablar de identidad digital, cómo protegerla, cómo está avanzando celebramos uno de nuestros DesayunosITDS en el que nos acompañan Guillermo Martín Soto, Regional Sales Manager, Spain, Portugal & North Africa - IAM (Identity & Access Management) de Thales; Raúl D'Opazo, Solutions Architect de One Identity y Samir Zerizar, Channel Account Manager de Okta.

Arrancamos el debate preguntando si las empresas españolas son conscientes de la importancia de proteger la identidad digital y cómo lo están haciendo. Para Guillermo Martín Soto, el COVID "ha acentuado la necesidad de las empresas de proteger los accesos", debido a que los empleados han salido de la oficina, "y ese paradigma de que la identidad es un nuevo perímetro cobra más sentido que nunca". En todo caso, asegura también el directivo de Thales que queda mucho camino por recorrer si tenemos en cuenta que desde principios de 2019 ha habido más de 40.000 reportes a la Unión Europea de fugas de información "y alrededor del 80 por ciento de estas fugas se han debido a la suplantaciones de identidad".

Para Raúl D'Opazo durante los últimos tres años sí que ha habido una mayor concienciación de que la identidad hay que protegerla; "ahora bien, esa conciencia no siempre deriva desde un proyecto estratégico para realmente tener un concepto de seguridad orientado a esa identidad". Añade el directivo de One Identity que se sigue tratando la seguridad de la identidad como parte de la seguridad perimetral, "pero todavía cuesta adoptar el concepto de centralizar la identidad porque las empresas siguen utilizando métodos muy tradicionales para proteger la identidad, como utilizar una contraseña tanto si estoy en mi casa como en mi oficina".

Dice Samir Zerizar que con el COVID se ha tomado más conciencia de la importancia de proteger la identidad, de proteger los accesos, "porque las empresas se dan cuenta de que si se protege

"Las empresas son conscientes de la importancia de la seguridad de la identidad, pero todavía no han sabido implementar las medidas necesarias"

Guillermo Martín Soto, Regional Sales Manager, Spain, Portugal & North Africa - IAM, Thales

El 80% de las fugas de información se deben a suplantaciones de identidad

#DESAYUNOSITDS.
LA SEGURIDAD DE LA IDENTIDAD

CLICAR PARA VER EL VÍDEO

la identidad se van a proteger los datos empresariales". Otra cosa es que las empresas apuesten por la integración de plataformas que puedan focalizarse en la identidad, añade el directivo de Okta.

El uso de tecnologías de biometría en la protección de la identidad digital es "fundamental", dice Raúl D'Opazo a pesar de que su compañía, One Identity, no se dedique a ello. Habla de evolución para conseguir una identificación y un acceso seguro a través del uso del móvil como plataforma de identificación o que las aplicaciones integren detección facial o de iris.

Para Samir Zerizar el uso de tecnologías de biometría para la protección de la identidad digital es "primordial", entre otras cosas porque "evita al usuario utilizar credenciales y contraseñas, y puedes tener un acceso rápido con un acierto del cien por ciento". De forma que la biometría hace que el usuario sea más productivo, porque no hay fricciones y al mismo tiempo da la seguridad máxima.

Recuerda Guillermo Martín que antiguamente la biometría se utilizaba para usos muy específicos y que ahora ha avanzado mucho. "Para Thales la biometría es un factor más, e importante, porque en tanto en cuanto es un dato inequívoco de las personas, es un factor de autenticación fuerte más", y añade que en la división de Banking & Payment de la compañía ya están implementando esta tecnología.

Passwordless

Hemos pasado de las contraseñas, más o menos simples, a la autenticación multifactor. ¿Se puede vivir sin contraseñas? Dice El responsable de

caso no deben ser el único método de autenticación.

"Mucha gente no está preparada para vivir sin contraseñas", dice el directivo de One Identity, añadiendo que se está avanzando en los métodos de autenticación multifactorial. "Al final para mí es importante que las empresas tengan muy claro cómo quieren que sus usuarios accedan a sus sistemas desde esos tres puntos de vista: qué es lo que el usuario sabe, qué es lo que puede tener y qué es lo que es", explica, añadiendo que también es importante para las empresas "saber diferenciar la criticidad de los empleados, y que en base a esa criticidad sea capaces de tomar decisiones".

La experiencia de usuario se ha convertido en un elemento clave en el mundo tecnológico. Planteamos cómo se está gestionando esa buena ex-

"Las empresas siguen utilizando métodos muy tradicionales para proteger la identidad"

Raúl D'Opazo,
Solutions Architect, One Identity

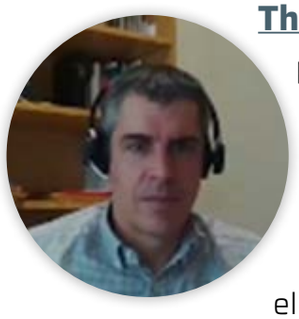
canal de Okta que las empresas están intentando poner a disposición de los clientes plataformas que permitan eso, el fin de las contraseñas. La idea, añade, es facilitar el acceso a los usuarios a diario y con las tecnologías de autenticación multifactor, que recogen lo que uno sabe, lo que uno tiene y lo que uno es, y que permiten "un acceso seguro sin fricciones".

Por el momento las contraseñas son el método de autenticación más común y más expandido, dice Guillermo Martín, quien asegura que sí, se puede vivir sin contraseñas "y es incluso aconsejable, pero para eso queda muchísimo". En todo

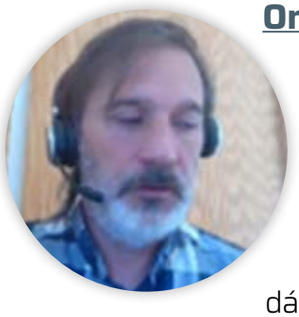
A grandes retos, grandes soluciones

Para finalizar el debate pedimos a los expertos en seguridad que hagan sus propuestas para ayudar a las empresas a hacer frente a la seguridad de la identidad.

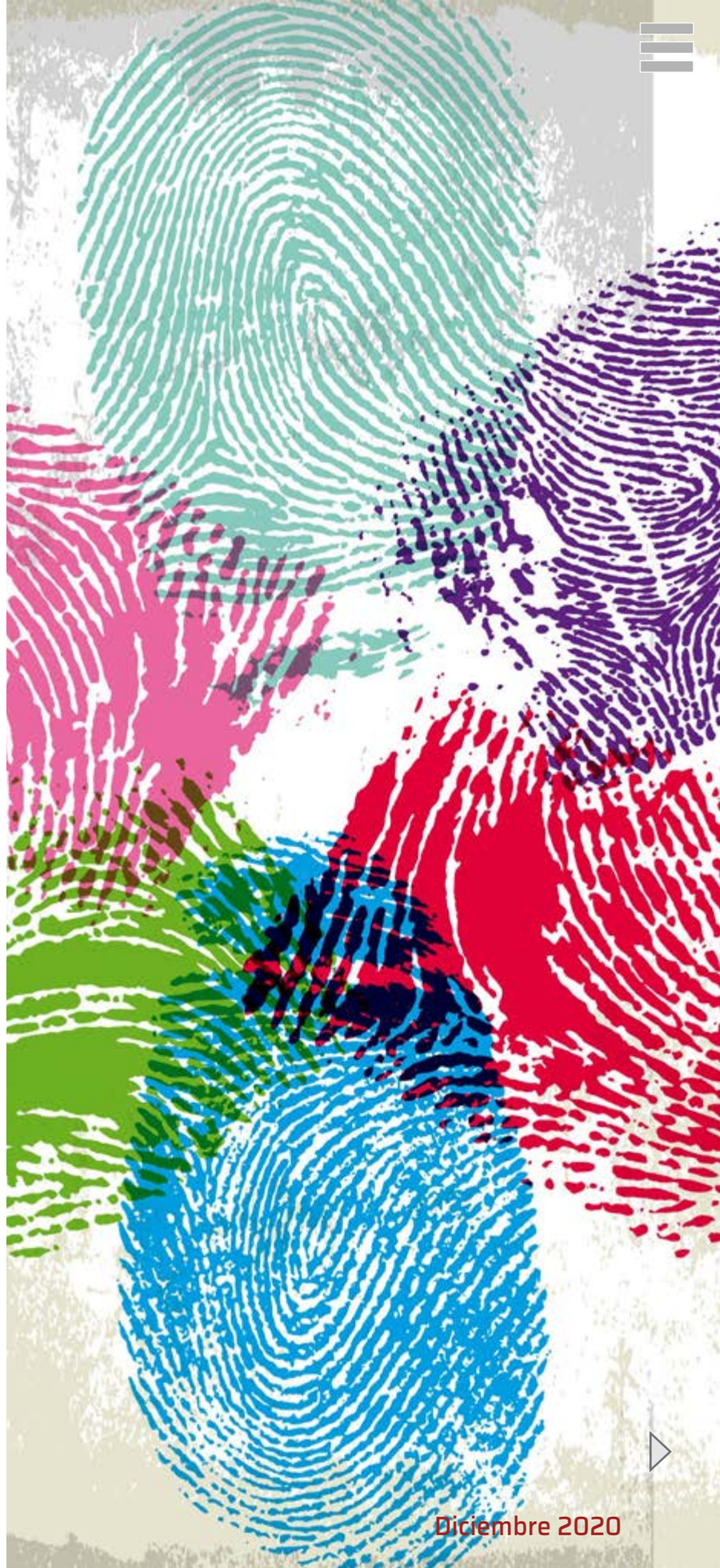
Okta. Desde hace once años Okta propone una plataforma centralizada que permite gestionar la identidad del usuario a todos los niveles. Hablamos de inicio de sesión único, la entrada a todas las aplicaciones que necesita un empleado para trabajar sin tener que introducir credenciales para cada aplicación; de un modelo de autenticación multifactor adaptativo que permite, con factores contextuales, verificar las credenciales del usuario incluyendo factores de comportamiento de riesgo que tiene en cuenta desde qué dispositivo, IP o lugar geográfico accede; también se propone a las empresas el poder automatizar el aprovisionamiento de los usuarios; dar acceso seguro a los servidores para usuarios privilegiados; establecer un repositorio central con todos los datos de los usuarios y la gestión de las APIs para el mundo de los desarrolladores.



Thales. Desde Thales lo que se propone es una manera fácil de autenticación de usuarios pero al mismo tiempo ser capaces de proteger la información y la seguridad de la empresa. Para ello se implementa por defecto un sistema de Single Sign-On para el acceso a todos los recursos de la empresa a través de un portal. A partir de ahí, la gran ventaja es que cada conexión a cada recurso, a cada aplicación, es monitorizada y se va a subir o se va a bajar el nivel de seguridad en función de quién se esté conectando, desde dónde y a qué información. Resaltar además que la compañía cuenta con la mayor gama de tokens de seguridad del mercado.



One Identity. El objetivo de la compañía es proteger ese nuevo perímetro de seguridad que es la identidad desde la base, desde la gestión del ciclo de vida de esa identidad, dándole una capa muy importante de gobierno para que no sólo pueda darse esa capa de aprovisionamiento sino esa capa de certificación de los accesos, de gestión de riesgos y de segregación de funciones que muchas veces es fundamental para minimizar los riesgos de los accesos inapropiados a las aplicaciones. Y desde ese prisma del gobierno de la identidad, se puede extender a identidades de entornos robóticos, de aplicaciones y servicios. One Identity es, además, una empresa especializada en entornos Microsoft para la gestión y securización del directorio activo.



"Durante la pandemia las empresas han tomado más conciencia de la importancia de proteger la identidad porque se dan cuenta de que, si se protege la identidad, se van a proteger los datos de la empresa"

Samir Zerizar,
Channel Account Manager, Okta

periencia de usuario con una buena protección de su identidad de forma que el proceso sea sencillo y transparente. Apunta Guillermo Martín que desde Thales "nuestra idea es implementar sistemas que permitan por defecto hacer la vida fácil al usuario con federación de aplicaciones y de recursos y el Single Sign-On (SSO), pero implementando sistemas de password de un solo uso, de forma que el usuario no tiene que recordar nada, para el acceso a determinados recursos".

Hace referencia Raúl D'Opazo a un estudio realizado por su compañía que recogía que una de las mayores preocupaciones de los departamentos de seguridad respecto a proyectos de gestión de identidades y accesos es la experiencia usuario final; "es decir, es una preocupación real y de las más importantes cuando nos embarcamos en este tipo de proyectos".

La experiencia de usuario, la facilidad de acceso y la seguridad, "se tienen que complementar", dice Zerizar. La tecnología de Okta verifica la identidad del usuario que se va a conectar pero con una experiencia de usuarios muy positiva, sin fricciones, "porque si el usuario puede acceder de manera muy simple, podrá ser mucho más productivo".

Identidad Digital y Blockchain

Hace mucho que se habla de blockchain, de la tecnología de bloques, y más recientemente en el uso de esta tecnología para garantizar la identidad digital. Hay un ambicioso proyecto europeo para crear una ID soberana apoyada en blockchain, la Identidad Digital que dará a los ciudadanos el poder sobre sus datos. ¿Se está utilizando blockchain para proteger la identidad de los usuarios en el mercado empresarial?

Explica Raúl D'Opazo que hace tres años surgió en One Identity la iniciativa de evaluar la tecnología blockchain para implementarla en los produc-

tos de la compañía. Asegurando que se trata de una tecnología muy útil para dar fiabilidad de una identidad, su uso lo ve más asociado a proyectos gubernamentales o de la Unión Europea, pero no tanto en torno a las identidades corporativas, foco de su compañía, porque genera algunos hándicaps relacionados con la experiencia de usuario o de rendimiento que hacen que el uso de blockchain en estos entornos sea más complejo.

"Desde Okta entendemos que blockchain es una tecnología muy interesantes para el usuario porque le permite controlar su identidad, también para el mercado de Smart Contract, por ejemplo", dice Samir Zerizar.

Explica el responsable del negocio de gestión de identidades y empresas de Thales que su objetivo son los usuarios empresariales, pero que a nivel gubernamental la tecnología Blockchain "sí que me parece útil y creo que es una tendencia que irá desarrollándose en cuanto se puede tener la certeza de que quien se identifica de tal manera es quien dice ser".

Enlaces de interés...

- España podría situarse a la vanguardia en gestión de identidades con el Proyecto Dalion
- El mercado de verificación de identidades crecerá a un ritmo superior al 15% hasta 2025
- 224.000 millones de dólares: es el impacto económico de blockchain en la gestión de identidades en 2030

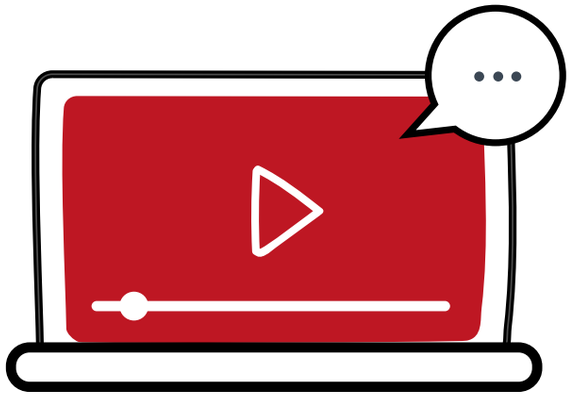
Compartir en RRSS

11
DICIEMBRE
10:00 CET

REGISTRO

Generando confianza en la cadena agroalimentaria con blockchain: descubre IBM Food Trust

Conoce de la mano de Ibermática todas las capacidades de IBM Food Trust, basada en IBM Blockchain, y cómo la cooperativa aceitera Conde de Benalúa ha comercializado 12 millones de litros de aceite durante la temporada 2019/2020, llegando a expandirse a consumidores de todo el mundo que adquieren su aceite con total confianza conociendo todos los detalles de su producción, gracias a esta plataforma.



#ITWEBINARS

2021, ¿el año de la ciberdefensa?

Únete a nosotros en este Encuentros IT Trends sobre Ciberseguridad en 2021 y descubre qué ocurre en el mundo del cibercrimen, qué tipos de ataques se están produciendo y cómo pueden afectar a tu empresa. Y sobre todo, qué nos espera en 2021.

REGISTRO

15
DICIEMBE
11:00 CET

IT Trends 2021. La TI salva el negocio

En 2021 continuaremos viendo cómo aumenta la penetración de modelos tecnológicos alrededor de cloud; se perfeccionan las estrategias de puesto de trabajo digital iniciadas a marchas forzadas en 2020; se buscan nuevos planteamientos para garantizar la continuidad del negocio y para reducir costes y optimizar la TI empresarial; se replantean la seguridad de los datos y aplicaciones... ¡Únete a este Encuentro IT Trends y descubre más!

REGISTRO

17
DICIEMBRE
11:00 CET

Webinar Arquitecturas

#ITWebinars

Arquitecturas de Seguridad,

¿qué ventajas ofrecen?

CIPHER IS NOW ENTRUST

Check Point SOFTWARE TECHNOLOGIES LTD.

SONICWALL

Diciembre 2020

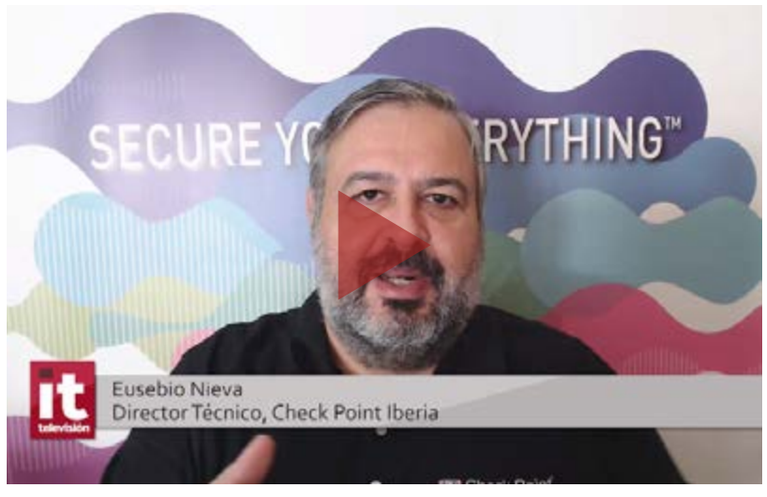
Arquitecturas de seguridad, ¿qué ventajas ofrecen?

Ataques cada vez más sofisticados, aumento del número de vectores de ataque, cientos de herramientas de seguridad, y diferentes entornos que proteger hacen que las arquitecturas de seguridad se hayan vuelto imprescindibles para dar cohesión a la seguridad empresarial.

Arquitecturas integradas, colaborativas y adaptativas diseñadas para ofrecer seguridad distribuida para empresas ofreciendo protección frente a amenazas, desde IoT a dispositivos remotos, y a través de las redes, nube o dispositivos móviles.

Acompáñanos en este IT Webinar en el que diferentes expertos de seguridad explicarán las ventajas de contar con una plataforma unificada de seguridad capaz de orquestar diferentes elementos y automatizar las operaciones para conseguir una seguridad más coherente y flexible.

A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados. También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la sesión completa aquí.



Eusebio Nieva, Director Técnico, Check Point

"La seguridad tiene que estar automatizada"

"No debemos confiar por principio en nadie, ni siquiera aunque sea de dentro de nuestra compañía", asegura Eusebio Nieva, Director técnico de Check Point en la sesión online Arquitecturas de Seguridad, ¿qué ventajas ofrecen?. Se trata del modelo Zero Trust, que se antepone a un modelo anterior que confiaba en lo que ocurría en las redes internas, un modelo que propone verificar "absolutamente todo porque en ocasiones la amenaza está dentro".

Para Eusebio Nieva verificar y contrastar todos y cada uno de los accesos con respecto a los permisos que se deben y pueden tener es fundamental no solamente desde el punto de vista de aplicar ese Zero Trust, sino que es fundamental tener en cuenta que todas estas arquitecturas de seguridad, cualquiera que queramos implementar, tiene que estar automatizada, "porque la nube es uno de los mayores condicionantes que van a venir".

Explica que además de tender hacia arquitecturas híbridas, hay cambios importantes en el desarrollo de aplicaciones, "especialmente cuando hablamos de nube". Dice Eusebio Nieva que cuando hablamos de nube "estamos pasando de un modo de entender las aplicaciones a otro completamente diferente, basado en mucha mayor resiliencia y mucha mayor escalabilidad, y si no somos capaces de escalar y de automatizar la seguridad tal y como hacemos con las aplicaciones, olvídate. Es la hora de DevSecOps", de acercar lo más posible la seguridad y los controles de seguridad al propio desarrollo.

La propuesta CloudGuard de Check Point es el paraguas bajo el cual estamos implementando todos los controles que tenemos que poner para que la seguridad en la nube sea de facto "como la arquitectura de la nube nos está exigiendo", una nube

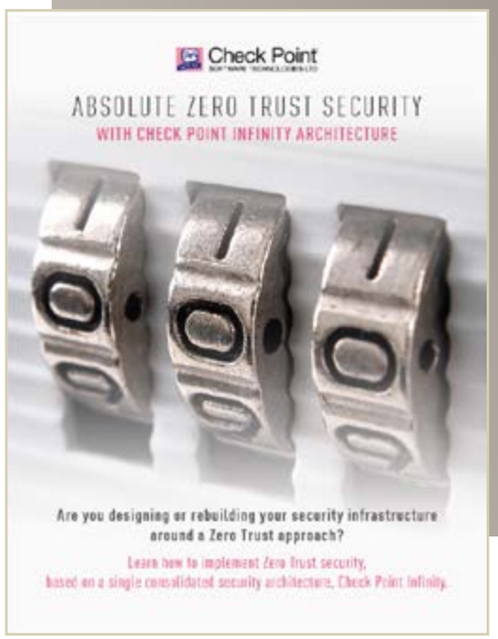
**EUSEBIO NIEVA,
DIRECTOR TÉCNICO, CHECK POINT**

**CLICAR PARA
VER EL VÍDEO**

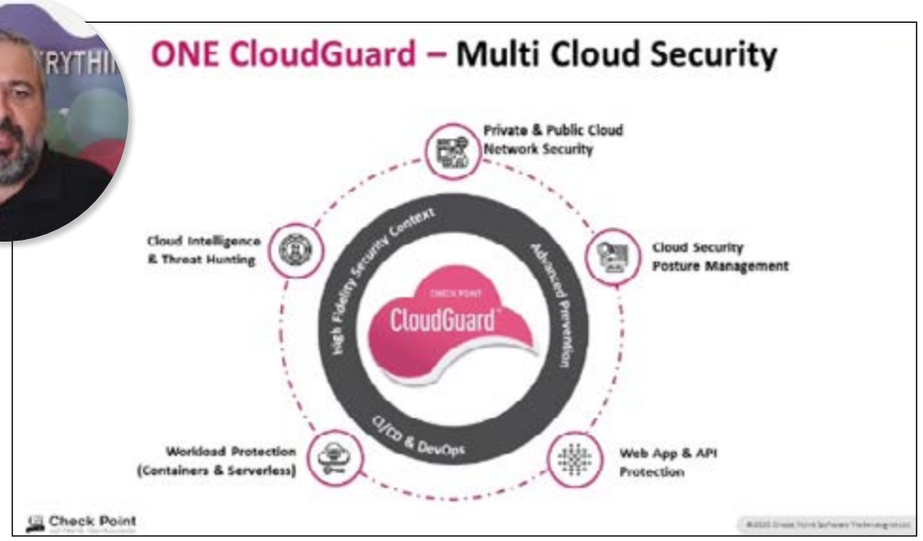
it whitepapers

SEGURIDAD ZERO TRUST ABSOLUTA CON CHECK POINT INFINITY

La reconstrucción de su infraestructura de seguridad en torno a un enfoque de Confianza Cero utilizando tecnologías dispares puede generar complejidades y brechas de seguridad inherentes. La arquitectura de seguridad de Check Point Infinity permite a las organizaciones implementar completamente todos los principios Zero Trust.



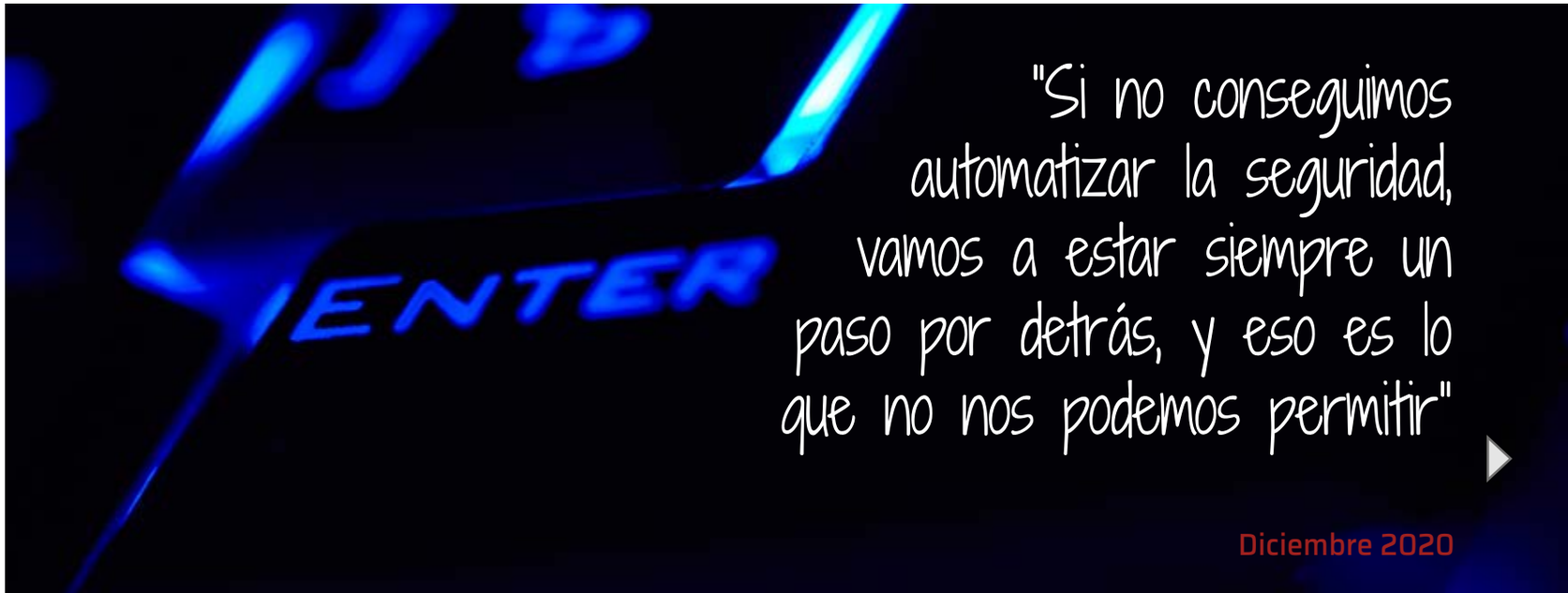
que exige escalabilidad, ir a la misma velocidad que los cambios que se producen y aplicar múltiples controles.



CloudGuard establece una serie de protecciones que ayudan a implementar esos cambios en la nube. No sólo se protege el tráfico, norte-sur y este-oeste, sino la gestión automatizada de la postura de seguridad, aplicaciones en la nube, cargas de trabajo y todo ello con la inteligencia necesaria para responder a una amenaza mediante técnicas de threat hunting. Añade Eusebio Nieva que el elemento común, importantísimo, de todas estas protecciones es la automatización; “si no conseguimos automatizar todo esto, vamos a tener un problema muy grave a la hora de ser capaces de adaptarnos desde el punto de vista de seguridad a lo que implementan nuestros departamentos de desarrollo. No vamos a ser capaces de poner una seguridad efectiva en la nube”.

Explica el directivo que la arquitectura de Check Point automatiza la seguridad mediante una gestión única que simplifica la forma de aplicar la seguridad mediante políticas dinámicas.

Vea aquí la intervención de Check Point en Arquitecturas de Seguridad, ¿qué ventajas ofrecen?



Sergio Martínez, Regional Manage, SonicWall Iberia

"Hay que cambiar de arquitectura"

Al mismo ritmo que COVID-19 se expandía por todo el mundo, la digitalización se aceleraba y lo que debería haber ocurrido en años, ocurrió en semanas. Lo dice Sergio Martínez, director general de SonicWall Iberia, en la sesión online Arquitecturas de Seguridad, ¿qué ventajas ofrecen?, añadiendo que esto suponía un reto para la supervivencia de las empresas, "para los ciberdelincuentes ha sido una bendición".

La superficie de exposición ha crecido muchísimo como consecuencia del teletrabajo, rompiendo definitivamente el perímetro de seguridad, incrementando el uso de aplicaciones cloud. Toda esta situación ha creado lo que SonicWall denomina un "Business Gap" entre lo que tienen las compañías y lo que efectivamente necesitan, explica Sergio Martínez.

"Estamos en una ciberguerra", dice el directivo de SonicWall cuando le preguntamos por lo que está sucediendo en el mercado. A destacar también un fuerte incremento de los ataques de intrusión y de ransomware, "el gran caballo de batalla del cibercrimen", que se ha disparado desde el pasado mes de junio. La necesidad de más ancho de banda, un mayor número de dispositivos inalámbricos, la necesidad de integrar todas las soluciones o tener que añadir nuevas capacidades está añadiendo más complejidad al mercado de ciberseguridad.

SERGIO MARTÍNEZ, REGIONAL MANAGE, SONICWALL IBERIA

CLICAR PARA VER EL VÍDEO

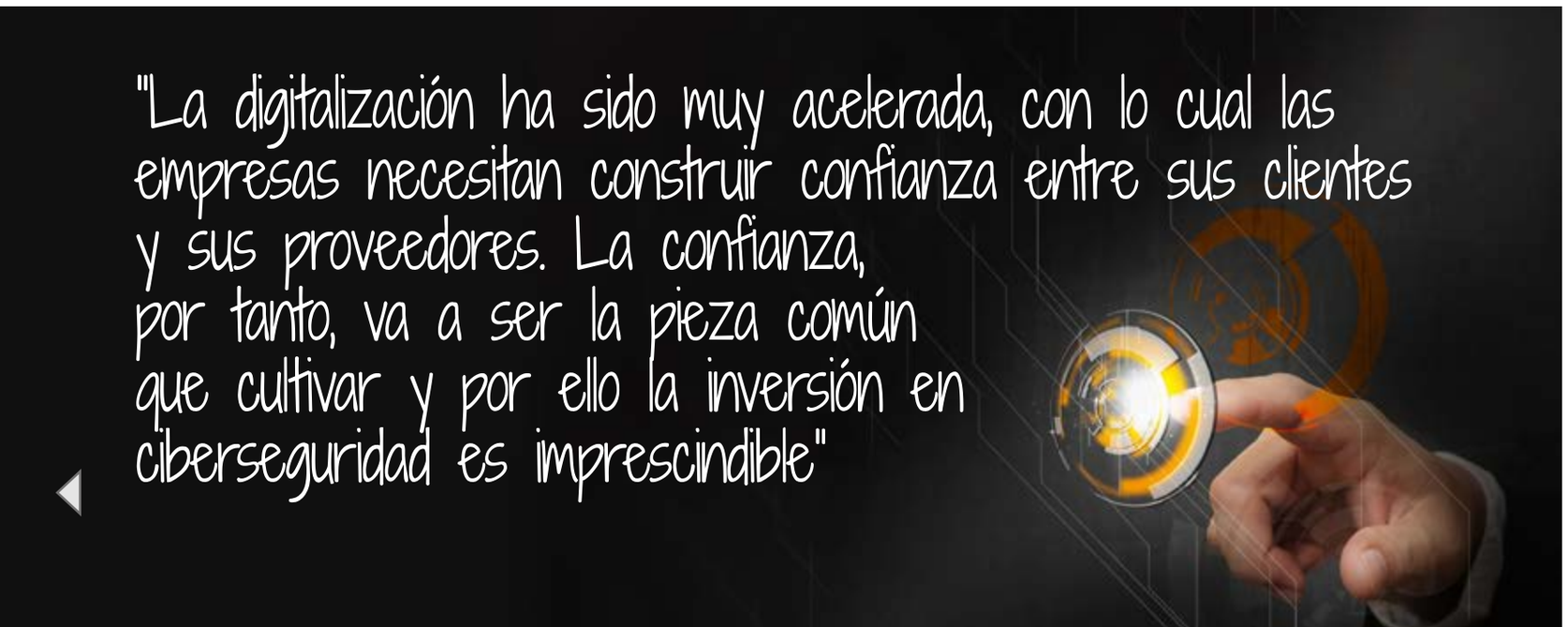
Asegurando que hay que cambiar de arquitectura, menciona Sergio Martínez la estrategia Boundless Cybersecuity lanza a primeros de año y que propone una plataforma que "proporciona seguridad en cualquier momento, en cualquier lugar e independientemente de los dispositivos con una serie de pilares", dice el directivo de SonicWall. El primer pilar es poder conocer lo desconocido, y

le siguen el poder establecer una defensa por capas, con una visión unificada Para saber lo que está ocurriendo en tu red, un TCO disruptivo, con una inteligencia artificial que va a aprendiendo y una adaptación continua ante cualquier tipo de amenaza.

Detrás de esta plataforma está la oferta de la compañía, compuesta por los firewalls de nueva generación, Secure WiFi, acceso remoto seguro, seguridad del email, firewalls virtuales, seguridad para Office 365 y Google Suite, y seguridad del IoT. “La integración de todas las soluciones es la clave”, asegura el directivo de SonicWall, mencionando el Capture Security Center

Con Cloud Edge Secure Access Sonicwall pone en marcha el paradigma Zero Trust. Se trata de un producto diseñado para proporcionar acceso remoto de todo tipo a las compañías, con un despliegue en minutos, con un control muy potente de los privilegios de acceso y un acceso directo a Cloud.

Vea aquí la intervención de SonicWall en Arquitecturas de Seguridad, ¿qué ventajas ofrecen?



it whitepapers

SONICWALL
CLOUD EDGE SECURE ACCESS

SonicWall Cloud Edge Secure Access es un potente servicio de red-as-a-service para conectividad de sitio a sitio y de nube híbrida a AWS, Azure, Google Cloud y más. En el proceso, combina enfoques de seguridad Zero-Trust y Least-Privilege en una oferta integrada.

El enfoque de acceso con privilegios mínimos restringe el acceso de un usuario en particular a solo lo que se necesita y nada más. Al limitar la exposición a otras áreas sensibles de la red, las organizaciones pueden asegurar sus recursos sin sacrificar su flexibilidad operativa.

José Perez, Sales Engineer, nCipher

"Security World es una arquitectura de protección de claves criptográficas"

Las soluciones criptográficas de nCipher Security, que a partir del 30 de noviembre de 2020 se convierte en Entrust, protegen las tecnologías y ayudan a cumplir con las nuevas exigencias en materia de cumplimiento. Dice José Pérez, Sales Engineer de nCipher, en la sesión online Arquitecturas de Seguridad, ¿qué ventajas ofrecen?, que en temas de cifrado su compañía trabaja con los HSM (Hardware Security Module) y que este tipo de dispositivos ofrecen muchas ventajas, "como el escalado, la flexibilidad y la resistencia a fallos que puedas ver en la operativa de diaria".

JOSÉ PEREZ
SALES ENGINEER, NCIPHER

CLICAR PARA VER EL VÍDEO

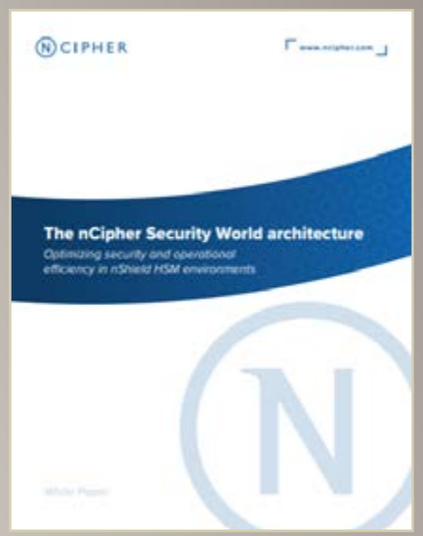
Explica este experto que cuando se habla de protección de claves de cifrado siempre hay un servidor de aplicación que le demanda criptografía al HSM; esa clave se genera dentro del HSM y, en teoría, nunca sale de ese HCM. "El problema que tiene esta aproximación es que si trabajas con un número de claves alto, la memoria del HSM muy probablemente se te acabe llenando", lo que lleve a comprar más HSM, y se termine ignorando la regla de que la clave nunca abandone el módulo, algo que también sucedería en el caso de que se quiera hacer un backup del material criptográfico.

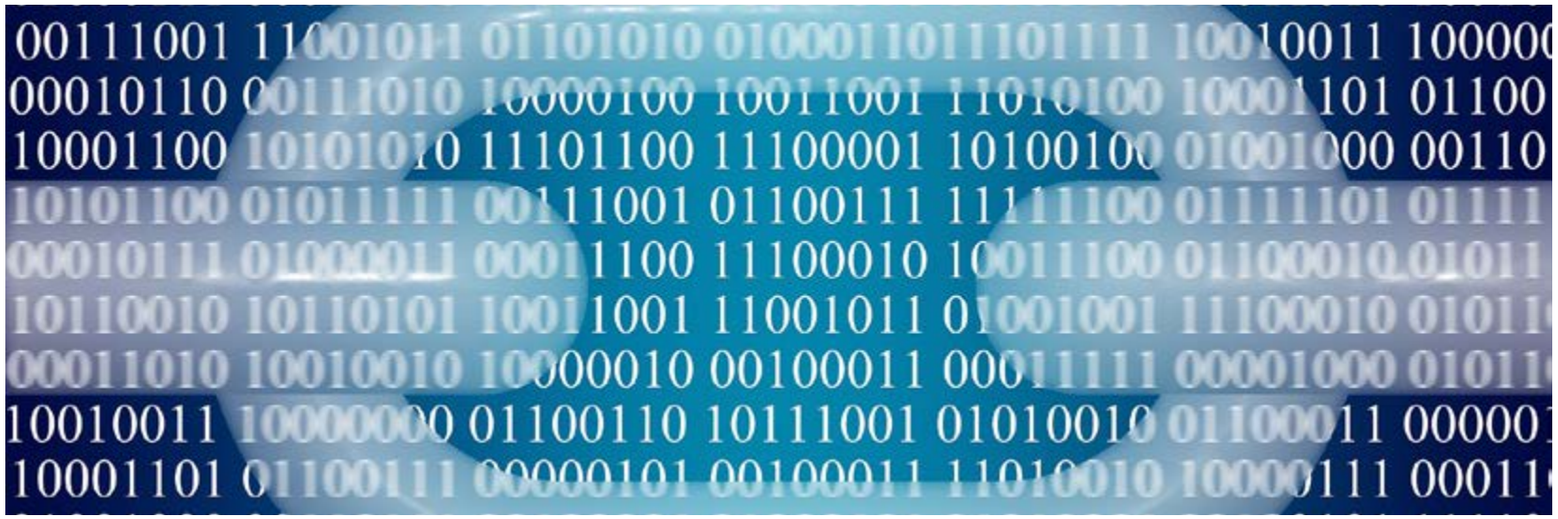
"Nosotros pensamos que esta no es la mejor aproximación a la hora de proteger tus claves y lo que proponemos es nuestra arquitectura Security World", donde al final se tiene lo mismo, un servidor de aplicación y un HSM. En este caso, explica

it whitepapers

THE NCIPHER SECURITY WORLD ARCHITECTURE

La arquitectura nCipher Security World admite un marco de gestión de claves especializado que abarca toda la familia nShield de HSM de propósito general. Esta arquitectura proporciona una experiencia unificada de administrador y usuario e interoperabilidad garantizada ya sea que el cliente implemente uno o cientos de dispositivos.





"Nuestra arquitectura Security World supone una ventaja en estos despliegues cloud en los que los HSM ya no son un appliance, sino que son un servicio"

José Pérez, el servidor de aplicaciones no va a empezar a generar claves sin más, "sino que va a generar una clave muy importante, la Clave Module, dentro del HSM", de forma que cuando se necesiten claves de aplicación, estas se crean dentro del HSM con su generador de números aleatorio, se cifran con la Module Key y se guarda fuera del HCM en el sistema de ficheros.

De esta manera "solo hay una clave dentro del HSM, lo que evita el peligro de quedarnos sin memoria" y que, en caso de tener que hacer un backup de las claves criptográficas, esas claves cifradas no son más que archivos de poco peso que si se abren están cifrados.

A la hora de utilizar esas claves cifradas "solo cuando están dentro de los límites seguros del HSM, se descifra con la Module Key se utilizan". El secreto, asegura el ejecutivo de nCipher, "es que la clave nunca está en claro fuera del HSM".

"El hecho de que sólo hagamos HSM no quiere decir que esos HSM no se puedan poner en el cloud", dice José Pérez apuntando a otra de las ventajas que tiene la arquitectura de la compañía, cuyos clientes pueden acceder a esos HSM en modo servicio.

Vea aquí la intervención de nCipher en Arquitecturas de Seguridad, ¿qué ventajas ofrecen?

La documentación TIC, a un solo clic

it whitepapers

Ciberseguridad orientada al futuro

La ampliación del acceso externo y la falta de conocimientos internos sobre cómo protegerse son las razones clave por las que los ataques a la industria pesada están creciendo en número y gravedad. En este documento se exploran seis tendencias clave asociadas al actual sector de la industria pesada como el auge de la digitalización, mayores objetivos, el aumento del acceso a TI y OT, el sector industrial de las cosas, el internet industrial de las cosas y algunos de los riesgos que representan.

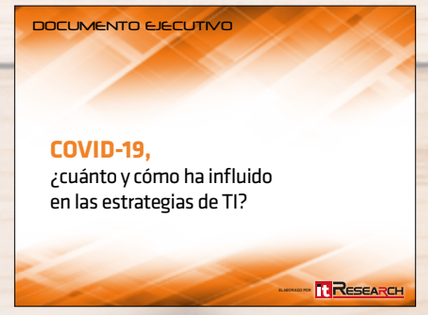
Threat Hunting Report 2020: así son las campañas de intrusiones hoy en día

Solo en la primera mitad del año 2020 los ataques de intrusión han superado en un 17% el número total de intrusiones llevadas a cabo durante 2019. Este informe de CrowdStrike recoge los datos de la herramienta de threat hunting Falcon OverWatch analizados por los equipos de inteligencia y servicios de la compañía. En el estudio se muestran las tendencias de intrusión entre enero y junio de 2020 y se ofrece un análisis del entorno actual de las tácticas de los ciberdelincuentes, que han visto reforzada su actividad debido al incremento del teletrabajo como consecuencia de la COVID-19.

Tecnologías que impulsan el cambio en el sector de la construcción

Las megatendencias sociales, económicas y ambientales del siglo XXI harán que cada vez sea más urgente la transformación de la industria de la construcción. Sin embargo, son los resultados claros y notables de los innovadores digitales los que transformarán esa urgencia en demandas concretas por parte de inversores, aseguradores, propietarios, ocupantes y reguladores.

COVID-19, ¿cuánto y cómo ha influido en las estrategias de TI?



La pandemia causada por el COVID-19 ha tenido consecuencias en todos los ámbitos que han ido produciéndose en cascada: la necesidad de preservar la salud de los ciudadanos produjo el confinamiento de los mismos, con el consiguiente efecto en el ámbito económico. Las empresas han tenido que reaccionar ante esta situación para evitar la parada de su actividad, y apoyarse en las posibilidades que las diferentes soluciones tecnológicas les brindaban para mantener sus negocios.

#ITWebinars

Brechas de seguridad, ¿hay opciones?

FORCEPOINT mobileiron okta sealpath

Diciembre 2020

Brechas de seguridad, ¿hay opciones?

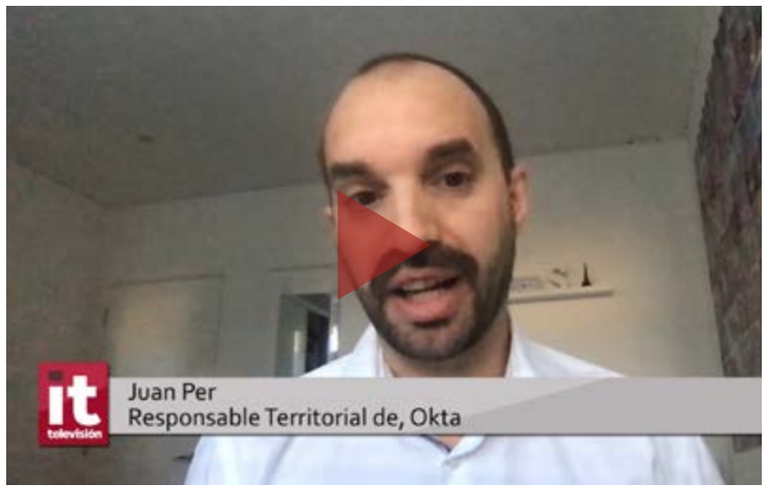
Las fugas de datos no discriminan. Adif, Mapfre, Tesla, Honda, EasyJet... son algunas de las empresas protagonistas este año de una brecha de seguridad que ha dejado expuestos los datos de miles de sus clientes. Sólo en España y hasta julio de 2020 se comunicaron a la Agencia Española de Protección de Datos (AEPD) más de 800 brechas de seguridad, 200 más que en el mismo periodo de hace un año.

Hacer frente a una brecha de seguridad no es tarea fácil. En este ITWebinars podrás conocer varias propuestas para afrontar a una brecha de seguridad.

Una de las empresas participantes es Forcepoint, para quien el nuevo perímetro de seguridad está en el ser humano y que con su Human Centric Security protege datos y usuarios allí donde estén.

Experto en gestión unificada de endpoints, lo que MobileIron propone es que información corporativa fluye libremente y de manera segura por los dispositivos y servidores en la nube.

También veremos, a través de Okta, cómo las soluciones de gestión de identidades ayudan a proteger el acceso a la información conectando de forma segura a las personas adecuadas con las tecnologías adecuadas en el momento adecuado.



Por último contaremos con la visión de Sealpath, un experto en IRM cuya tecnología permite a profesionales y empresas proteger sus documentos críticos dondequiera que se encuentren, acompañándoles en todo momento.

A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados. También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la sesión completa aquí.

Luca Livrieri, Sales Engineer Manager Italy & Iberia, Forcepoint

“La seguridad debe cambiar de manera dinámica y ser un habilitado del negocio”

La protección de los datos es el principal reto al que se enfrentan las empresas, dice Luca Livrieri, Sales Engineer Manager Italy & Iberia de Forcepoint, en la sesión online Brechas de seguridad, ¿hay opciones?. Añade el directivo que los datos están en todas partes y que no sólo hay que proteger la oficina principal, sino las remotas; además, la pandemia sanitaria ha añadido el problema de proteger a los empleados en casa.

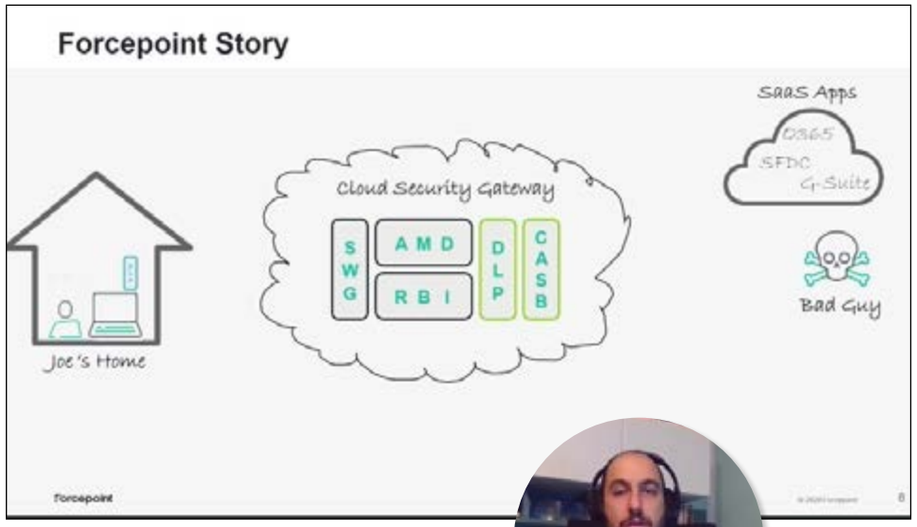
Para hacer frente a esta situación “se ha producido una convergencia de dos paradigmas: SASE y Zero Trust”, y si uno explica qué hay que proteger y el otro dice cómo hay que protegerlo en un mundo sin perímetro donde todo se mueve hacia la nube y los datos están disgregados. “Tenemos que cambiar el paradigma porque el nuevo perímetro es el usuario”, dice Luca Livrieri.

Explica el directivo de Forcepoint que el camino hacia la nube partió de una seguridad distribuida en silos, con una oferta muy fragmentada en diferentes soluciones, para pasar a una propuesta basada en la integración de productos que se hablan unos con otros y, finalmente, en la seguridad convergente, basada en servicios cloud y con un enfoque Zero Trust que valida los accesos y, muy importante para Forcepoint, verifica el comportamiento humano de manera constante.

Human Centric Cybersecurity es la propuesta de Forcepoint para los modelos Zero Trust y SASE y en la que convergen un cloud security gateway para

LUCA LIVRIERI, SALES ENGINEER MANAGER ITALY & IBERIA, FORCEPOINT

CLICAR PARA VER EL VÍDEO

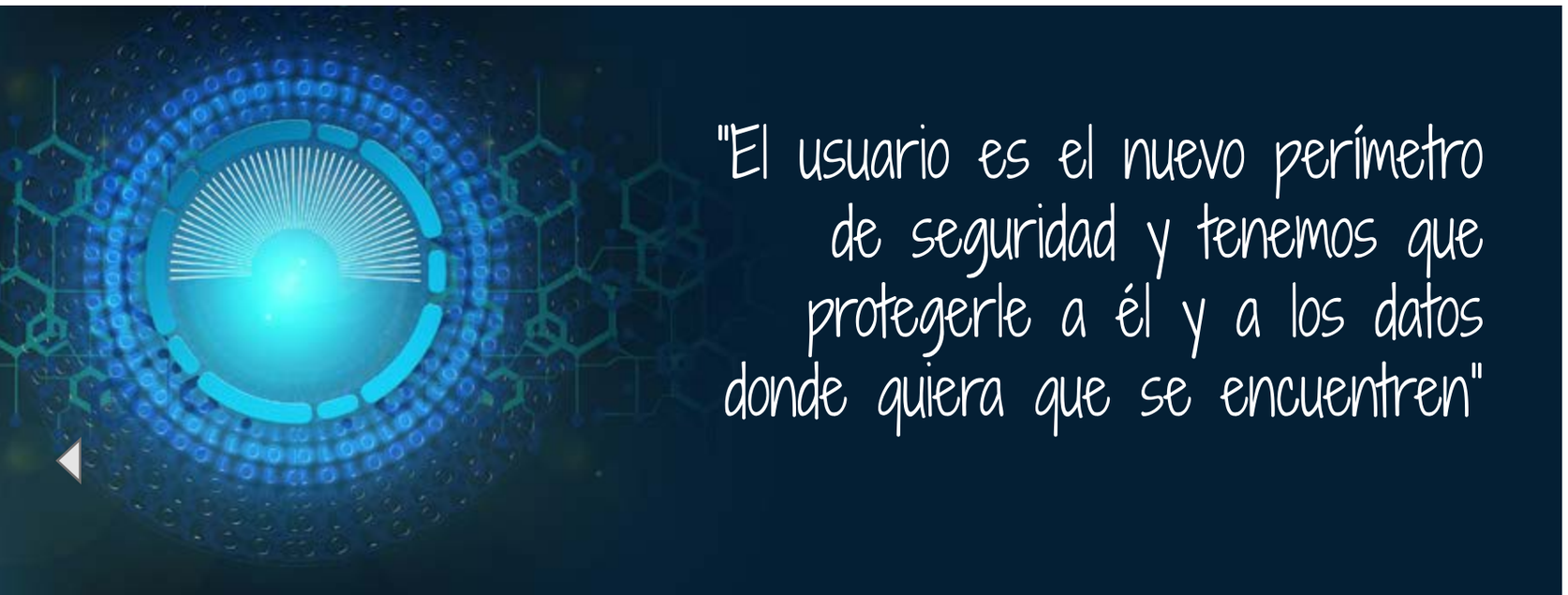


el tema de los accesos, una propuesta de DLP (Data Lost Prevention) y una oferta de protección de usuario basado en la verificación constante del comportamiento para aplicar una seguridad dinámica.

Con el objetivo de proteger los datos allá donde se encuentren, Luca Livrieri asegura que no se debe trabajar a nivel de perímetro y que una de las mejores prácticas para hacer frente a una brecha de seguridad es proteger el punto en el que los usuarios acceden a los datos, teniendo en todo momento un control sobre su comportamiento y pudiendo ofrecer una respuesta dinámica en función de este comportamiento para que la seguridad se convierta en un habilitador del negocio.

La propuesta Human Centric Cybersecurity de la compañía provee una visibilidad muy rica de la actividad del usuario para identificar y mitigar comportamientos; ofrece para las empresas de nube híbrida una protección de datos unificados y protege la red con un mejor costo-beneficio y mantiene seguro a los usuarios remotos de las ciberamenazas.

Vea aquí la intervención de Forcepoint en Brechas de Seguridad, ¿hay opciones?



Joaquín Malo de Molina, Responsable de canal, MobileIron

"Los códigos QR se han convertido en una creciente amenaza para los dispositivos móviles"

JOAQUÍN MALO DE MOLINA, RESPONSABLE DE CANAL, MOBILEIRON

CLICAR PARA VER EL VÍDEO

"Para los cibercriminales es el momento ideal, es la tormenta perfecta", asegura Joaquín Malo de Molina, responsable de canal e MobileIron, en la sesión online Brechas de seguridad, ¿hay opciones?, cuando le preguntamos qué es lo que está pasando en el mercado. Menciona el directivo que los hackers son cada vez mejores en lo que hacen y que las empresas suelen relegar a segundo plano la seguridad móvil "a pesar de que los empleados trabajan con estos dispositivos para acceder al correo electrónico, aplicaciones, etc.".

El phishing, circunscrito habitualmente al ordenador, también campa a sus anchas en los móviles. Existen muchos tipos de phishing, aunque todos buscan engañar al usuario para que pinche en un enlace externo que llevará a descargar malware, o ceder sus credenciales. Los móviles se han convertido en un objetivo muy atractivo para el phishing porque, según explica Joaquín Malo de Molina, el tamaño de su pantalla limita la informa-

PROTEGIENDO LOS DATOS EN MOVIMIENTO EN DISPOSITIVOS MÓVILES

La VPN sigue siendo un componente integral para proteger todos los datos en movimiento cuando los usuarios de dispositivos móviles y PCs requieren acceso al correo electrónico, contenido y recursos de colaboración de la empresa que residen detrás de un firewall en las oficinas centrales locales o en la nube. MobileIron tiene una sólida solución de tecnología de túnel VPN para dispositivos móviles y plataformas de escritorio.

ción que puede ver el usuario; porque es difícil determinar si un SMS es auténtico o no, “y por la prácticamente imposibilidad de revisar cualquier web que el usuario vaya a visitar”. Soluciones como las de MobileIron protegen a los móviles de estas amenazas.

Además del phishing, los códigos QR se han convertido también en una creciente amenaza para los dispositivos móviles. Utilizados por la inmensa mayoría de los usuarios, escanear uno de estos códigos puede desatar una auténtica debacle de la que la mayoría de los usuarios no son conscientes. Los código QR maliciosos pueden ser utilizadas por los hackers para espiar un teléfono, realizar un pago, hacer una suplantación de identidad, coger tus contactos, etcétera.

Para hacer frente a todas las amenazas propone Miguel Malo de Molina la solución MobileIron Threat Defense (MTD), que incorpora varias capas para “proteger y corregir amenazas conocidas y de día cero en dispositivos móviles sin interacción del usuario, lo que ayuda a impulsar la adopción al 100%”, y que está integrada en la solución UEM (Unified Endpoint Management) de la compañía. Desde una consola unificada la solución permite asegurar, controlar y gestionar todas las políticas de cumplimiento de PCs, portátiles, teléfonos inteligentes, tablets, etc.

En definitiva, MobileIron Threat Defense ofrece una seguridad móvil integral que permite a las empresas monitorizar, administrar y proteger los dispositivos móviles contra ciberataques de dispositivos,

"Nuestro MobileIron Threat Defense (MTD) permite implementar protección y correción de phishing multi vectorial para todo el tráfico basado en Internet independiente del navegador"

redes y aplicaciones, y sin ninguna interacción por parte del usuario y sin interrupciones en su productividad.

Vea aquí la intervención de MobileIron en Brechas de Seguridad, ¿hay opciones?

Juan Per, Responsable Territorial Iberia, Okta

"Con un doble factor de autenticación se conseguiría reducir gran parte de las brechas de seguridad"

Nueve mil clientes, más de 2.000 empleados y una facturación anual de 560 millones de dólares convierten a Okta en una de las empresas líderes del mercado de gestión de accesos e identidades (IAM), dice Juan Per, responsable territorial de Okta, en la sesión online Brechas de seguridad, ¿hay opciones?. Añade el directivo que una de las grandes ventajas de su compañía es que "somos capaces de gestionar el área tradicional en la que se han focalizado las soluciones de IAM, que son los empleados, pero también el área de lo que definimos como colaboradores necesarios", que pueden ser los proveedores, los partners, colaboradores, etc., a los que también hay que darles cierto acceso a ciertas aplicaciones o infraestructuras.

Hace tiempo que hablamos de cloud, ¿cómo ha impactado en la empresa y en todo lo que tiene que ver con la gestión de identidades? Para Juan Per, "la nube lo ha cambiado todo. Ha sido la gran revolución en el mundo IT". Explica el directivo que Okta nació en la nube y que se está viendo

JUAN PER, RESPONSABLE TERRITORIAL IBERIA, OKTA

CLICAR PARA VER EL VÍDEO

"Para que una empresa no sufra una brecha lo que tiene que securizar es la identidad de los usuarios"

cómo sectores que antes eran reacios a migrar a la nube, como la banca o los organismos gubernamentales, están yendo al cloud en todos sus proyectos de transformación digital, y añade que la gran mayoría de los proyectos que lleva a cabo su compañía compañía son híbridos porque los clientes están en una fase de transición y aún mantienen recursos on-premise.

La identidad ha evolucionado, explica el directivo de Okta. Si hace unos años era parte de un stack y hoy se apuesta por una plataforma independiente y neutral capaz de integrarse con el resto del ecosistema de IT, a lo que se va es "a gestionar la autenticación y la identidad, no de dispositivos o personas físicas, sino de cosas, a gestionar el IoT".

Okta Identity Cloud es la solución global de gestión de identidades de la compañía, una solución que está compuesta por siete módulos o productos, a los que los clientes pueden optar de manera independiente. El primero es Okta Single-Sing On, una herramienta de sesión de inicio único; le sigue Okta Adaptative MFA, o de múltiple factor de autenticación basada en contexto; con API Access Management se securizan todas las conexiones y la creación de APIs en las empresas; Okta Directory Universal permite consolidar diferentes directorios; Life Cicle Management es la herramienta de gestión de acceso de usuarios a aplicaciones; Okta Advanced Server Access y Okta Advanced Gateway se centran en la gestión de usuarios con privilegios y en las conexiones entre infraestructura on-premise y cloud.

Vea aquí la intervención de Okta en Brechas de Seguridad, ¿hay opciones?

LA IDENTIDAD EN EL CENTRO DEL PLAN DE SEGURIDAD

En la última década, empresas de todo el mundo han adoptado aplicaciones basadas en la nube, han reducido su infraestructura informática, han disminuido sus costes de adquisición y han permitido a sus empleados trabajar a distancia en cualquier lugar del mundo y en cualquier momento, pero eso ha complicado el tener una visión general única de todos los usuarios, terminales y aplicaciones. Por lo tanto, necesitan una plataforma de identidad unificada.

Joaquín de la Torre, Director de Desarrollo de Negocio, Sealpath

"La información es uno de los activos más valiosos de cualquier organización"

Siendo la información uno de los principales activos de las empresas, solo en el 2,2% de las fugas de datos la información estaba protegida de algún modo, dice Joaquín de la Torre, Director de Desarrollo de Negocio de Sealpath en la sesión online Brechas de seguridad, ¿hay opciones?, lo que quiere decir que en el 98% de los casos los ciberdelincuentes que se llevan la información de las empresas "pueden hacer con ella lo que les dé la gana".

JOAQUÍN DE LA TORRE, DIRECTOR DE DESARROLLO DE NEGOCIO, SEALPATH

CLICAR PARA VER EL VÍDEO

Recuerda Joaquín de la Torre que las fugas de datos no sólo se producen por ataques externos, sino internos, y que los ataques no se producen sólo contra gente de la organización, sino contra colaboradores "con los que compartimos información". De lo que se deduce que la información debe estar protegida "frente a las amenazas externas, pero también frente a las internas. Y también cuando sale de nuestra organización, cuando la compartimos hacia afuera".

Lo que aporta Sealpath es "una protección persistente del documento", es "ir más allá del cifrado", es "poder controlar lo que la gente puede hacer con la información, aunque esta salga de nuestra organización", explica Joaquín de la Torre. Añade el directivo que la clave de la oferta de su compañía es que la información va a ser siempre del cliente, esté donde esté, porque la información va a seguir siempre las órdenes del dueño de la información, no del dueño del dispositivo en el que está la información, "con lo cual siempre se va a mantener un

MANTENER EL CONTROL SOBRE NUESTROS DOCUMENTOS, ¿POR QUÉ ES TAN IMPORTANTE?

SealPath te permite asignar permisos sobre los documentos de forma que sólo quien tú decidas tendrá acceso a la documentación independientemente de dónde se encuentre. También te permite poner fechas de caducidad sobre los documentos para que pasada la misma determinadas personas dejen de tener acceso a la documentación. La documentación viaja siempre con la protección y está cifrada. Es una protección persistente que sólo quien la ha aplicado puede quitar.

Compartir en RRSS

"Podemos hacer una auditoría completa del acceso a la información en cualquier momento, y en cualquier momento vamos a poder revocar, modificar o cambiar completamente los permisos de acceso a la misma"

control completo sobre la información sensible de la organización".

Explica también el Director de Desarrollo de Negocio de Sealpath que lo que se propone es un nuevo modelo de protección basado en círculos de confianza "donde desaparece ese anonimato, tanto del receptor como del emisor, de la información y donde se puede controlar lo que la gente pueda o no puede hacer con la información, incluso modificar o revocar completamente los permisos de acceso a la misma si alguien abandona ese círculo de confianza".

Insiste Joaquín de la Torre que con Sealpath se puede controlar qué es lo que esa persona va a poder hacer con la información y también durante cuánto tiempo, independientemente del formato. Se puede decidir que no pueda modificarla, que no pueda imprimirla, que no pueda copiar su información de una documentación nuestra y llevársela a otro sitio, impidiendo la fuga de información.

Vea aquí la intervención de Sealpath en Brechas de Seguridad, ¿hay opciones?

it User
TECH & BUSINESS

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

2021, el año de la consolidación

Diciembre 2020

2020 se va quedando atrás. No es probable que olvidemos el año de la pandemia, del teletrabajo, de las clases en remoto, de la telemedicina, de una aceleración tecnológica nunca vista. Una aceleración que ha impulsado la transformación digital, la adopción del cloud, el reconocimiento de la de ciberseguridad como elemento imprescindible que debe acompañar cada paso; una aceleración que está impulsando tecnologías como SASE o Zero Trust, las nuevas niñas bonitas del mercado.

2021 será el año de más ransomware, eso seguro, y de que el mundo se convierta en el campo de batalla; la seguridad del IoT, pero también del OT y de la 5G saltarán a primer plano; la masiva adopción de la nube de este 2020 impactará en las estrategias de ciberseguridad de las empresas; el perímetro de seguridad se ha trasladado definitivamente, aunque no terminamos de definir dónde recolocarlo; las tecnologías de acceso remoto seguro van a cambiar y se reforzará la seguridad móvil; la inteligencia artificial cobrará más protagonismo y los servicios de seguridad gestionados se harán imprescindibles.

Acompáñanos en nuestras previsiones, fruto de decenas de conversaciones y recopilaciones y prepárate para 2021, el año en el que todas las tecnologías adoptadas, las decisiones tomadas tendrán su tiempo de respiro, de consolidación, de remate.

1. El ransomware sigue adelante

Se ha convertido en una de las amenazas más peligrosas, más rentables y que mejor funcionan para los ciberdelincuentes, y seguirá siendo la estrella en 2021. En su nueva modalidad ya no es suficiente con cifrar los datos, porque ahora lo que hacen es robarlos y amenazar con publicarlos. Cuando lanzan este tipo de ataques, los cibercriminales primero extraen grandes cantidades de datos sensibles antes de cifrar el equipo infectado. Tras esto, amenazan a su víctima con publicar esta información a no ser que se pague el rescate. Para demostrar que su amenaza es veraz, publican una pequeña cantidad de datos en la dark web, aumentando así el nivel de presión.

Los rescates por ransomware ya han alcanzado las decenas de millones de dólares y se espera que la cifra se incremente en 2021

COVID-19, protagonista también en 2021

Los atacantes seguirán explotando la pandemia sanitaria. Los ciberdelincuentes supieron explotar el interés que despertó un coronavirus que puso partas arriba el mundo, nuestra forma de vida y nuestra forma de hacer negocio. COVID-19, coronavirus o pandemia se convirtieron en los señuelos perfectos en todas las campañas de ingeniería social y seguirán siéndolo el próximo año.

Como COVID-19 seguirá dominando los titulares, las noticias sobre el desarrollo de vacunas o nuevas restricciones seguirán utilizándose en campañas de phishing, como lo han sido durante 2020. Las empresas farmacéuticas que desarrollan vacunas también seguirán siendo blanco de ataques maliciosos que buscan explotar la situación.

Es una táctica que ya hemos visto y que se convertirá en un problema mayor en el espacio de la atención médica, donde los atacantes pueden usar registros de pacientes robados para chantajear a las empresas, que tendrán que decidir si es mejor pagar la extorsión o una multa de GDPR. Los rescates, por cierto, ya han alcanzado las decenas de millones de dólares y se espera que la cifra se incremente.

Una tendencia preocupante es que los atacantes se están moviendo cada vez más hacia el ransomware-as-a-service, que incluye ofrecer malware y las habilidades para implementarlo de forma única o continua. Por otra parte, si bien muchas organizaciones pagan rescates y recuperan el acceso a sus datos, a menudo olvidan que los atacantes todavía tienen sus datos y que se recomienda no pagar.

A medida que aumenta el volumen y el coste de las infracciones, las organizaciones tenderán a contratar un ciberseguro integral para reducir los riesgos contractuales

2. Los ciberseguros serán casi obligatorios

A medida que aumenta el volumen y el coste de las infracciones, las organizaciones que procesan datos en nombre de sus clientes se verán obligadas a contratar un ciberseguro integral para reducir los riesgos contractuales.

El aumento en la frecuencia y el coste de los incidentes de ransomware, las consecuencias de violaciones de datos y una regulación más sólida está impulsando un mercado de 4.500 millones de

dólares que se espera que crezca hasta los 21.400 millones para 2025. Según los últimos estudios, la proliferación de compañías de tecnología de seguros tecnológicos que llegan al mercado, junto con la competencia entre aseguradoras establecidas desde hace mucho tiempo, continúa ampliando la disponibilidad de cobertura y manteniendo los precios de las primas relativamente bajos.

Naturalmente, esto tendrá un costo para la organización, pero también proporcionará a los atacantes una nueva fuente de ingresos. Los ciberdelincuentes apuntarán a las grandes marcas con pólizas de seguro que pagarán para liberar datos robados en lugar de enfrentar el pago de la póliza para cubrir cualquier acción correctiva.

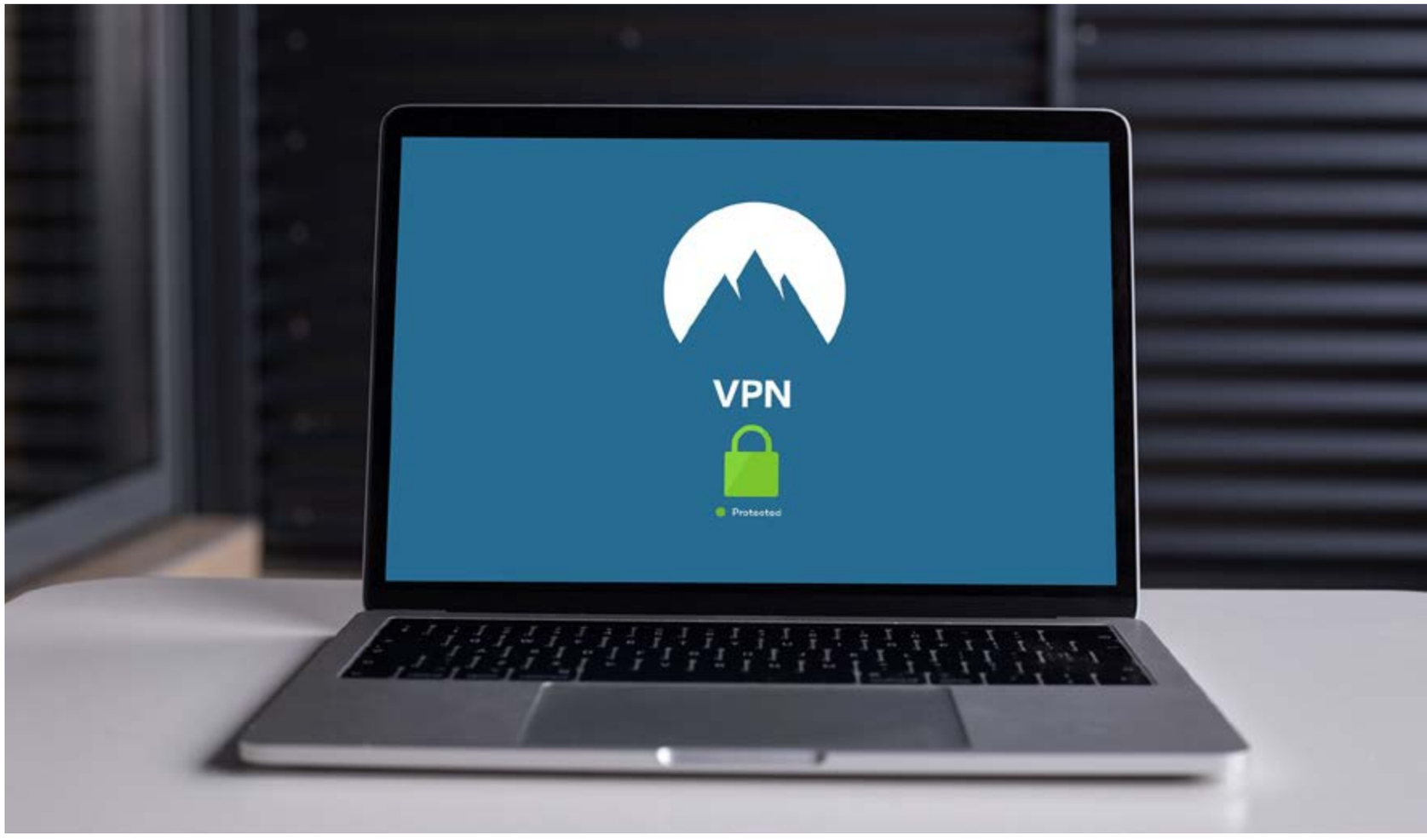
3. En plena ciberguerra

Los ciberataques entre países están creciendo y seguirán haciéndolo en el futuro. La guerra Fría que se instauró tras la Segunda Guerra Mundial hasta la caída del muro de Berlín, triunfa ahora en las redes, y los ataques informáticos entre países en entornos virtuales, ya sea para espiar o para influir en determinados acontecimientos, seguirán al alza. Los principales actores de amenazas de los Estados-nación que continuarán sus esfuerzos en 2021 incluirán a Rusia, China, Irán y Corea del Norte; además, se está viendo un aumento en la actividad de Vietnam y el sur de Asia, por lo que se espera que esas naciones aumenten sus operaciones el próximo año.

Los principales actores de amenazas de los Estados-nación que continuarán sus esfuerzos en 2021 incluirán a Rusia, China, Irán y Corea del Norte

Según datos del equipo de investigación de FireEye, el spear phishing seguirá siendo es uno de los vectores de infección más populares en lo que respecta a la actividad de amenazas del Estado-nación. Al mismo tiempo se están viendo técnicas de

Para 2021 se espera un incremento de los ataques no sólo contra las VPN, sino contra el protocolo de desktop remoto, o RDP (Remote Desktop Protocol)



intrusión que no requieren interacción del usuario, como la explotación de aplicaciones web y la difusión de contraseñas, tácticas que se han observamos en varios grupos iraníes, rusos y chinos en 2020, y que continuarán en 2021.

4. Los antiguos mecanismos de acceso remoto desaparecerán

Las primeras semanas de pandemia llevó a la adopción rápida de tecnología que pudiera dar servicio a una plantilla que se marchaba a su casa a trabajar. En el fragor de la batalla se optó por arquitecturas heredadas, las VPN, que han demostrado que no son una solución suficiente a largo plazo; las VPN introducen latencia, obstaculizan la productividad, pueden ser difíciles de escalar y pueden otorgar a los empleados un acceso excesivo a los recursos internos. Además, son fácilmente explotables por los ciberdelincuentes.

Para 2021 se espera un incremento de los ataques no sólo contra las VPN, sino contra el protocolo de desktop remoto, o RDP (Remote Desktop Protocol), que ya se ha convertido en uno de los servicios más atacados en Internet. Utilizando credenciales robadas, exploits y la fuerza bruta, se espera que los ataques contra RDP, VPN y servidores de conexión remota se duplicarán en 2021.

El futuro, por tanto, se verá marcado por la adopción de modelos Zero Trust, que garantiza que los usuarios sólo accedan a lo que necesitan para realizar su trabajo. De hecho, se espera que el 60% de las empresas eliminarán gradualmente las VPN en favor de accesos de confianza cero para 2023.

5. Los Deepfake se extienden

No son nuevos, pero su calidad mejora, como se ha visto durante 2020, y todo hace suponer que en 2021 se verá una nueva oleada de falsificacio-

La IA es una de las herramientas más poderosas que tenemos para combatir los ataques generados por inteligencia artificial

nes de harán dudar de si lo que hay al otro lado de una vídeo conferencia es humano o no.

Los investigadores lo tienen claro: los deepfakes se infiltrará en nuestra vida diaria, tanto como para poder mantener conversaciones con famosos o políticos, o incluso con nuestros seres queridos fallecidos.

Pensar que estás hablando con un superior sobre la situación financiera o las últimas innovaciones pueden comprometer a las empresas. Los expertos insisten, irónicamente, la IA es una de las herramientas más poderosas que tenemos para combatir los ataques generados por inteligencia artificial. La inteligencia artificial puede comprender patrones y detectar automáticamente patrones y anomalías inusuales más rápido y con mayor precisión que un humano.

6. La inteligencia artificial y el aprendizaje automático en el punto de mira

A medida que el aprendizaje automático se generaliza dentro de las empresas para tomar decisio-

El mercado de ciberseguridad en España

Según previsiones de IDC, el mercado de la ciberseguridad generará este año en España un volumen de negocio de 1.381 millones de euros, lo que supondría un crecimiento del 6% con respecto a 2019. En este contexto, los servicios de seguridad gestionada representarán un 27%; los servicios de integración, un 25%; el software de integración end-point, un 17%; los servicios de consultoría, un 15%; la seguridad para redes, un 12%; y el software de identidad y confianza digital, un 4%.

De cara a 2021 la consultora apunta a que el 50% de los consultores de los centros de operaciones de seguridad (SOC) elevarán su productividad gracias a la Inteligencia artificial y al aprendizaje automático. En esta línea también cabe reseñar que para 2022 el 35% de los clientes de servicios de seguridad gestionada (MSS) serán atendidos por proveedores de MSS en la nube debido a las cargas de trabajo que exigen los entornos cloud.

De hecho, con el aumento de la apuesta empresarial por la confianza digital, IDC Research España considera que para 2025 el 25% del gasto en servicios de seguridad se dedicará a desarrollar, implementar y mantener "frameworks de confianza digital".

Los ciberdelincuentes aprovecharán técnicas de machine learning para acelerar los ataques a redes y sistemas

nes automatizadas, los atacantes tienen un nuevo vector que considerar. Explican desde Beyond-Trust que después de que un actor de amenazas roba una copia de los datos de entrenamiento originales, comenzará a manipular los modelos generados al inyectar datos envenenados en el grupo de entrenamiento, creando un sistema que ha aprendido algo que no debería. Esta manipulación tendrá un efecto multiplicador debido al procesamiento automático de las aplicaciones posteriores, destruyendo la integridad de los datos procesados legítimamente.

Por otra parte, hay que tener en cuenta que los cibercriminales conforman una industria rentable y activa que hace uso de herramientas y tecnologías que pueden impulsar su negocio, que no son otras que el cloud, o la inteligencia artificial. De forma que no será raro ver en 2021 cómo los ciberdelincuentes aprovecharán técnicas de machine learning para acelerar los ataques a redes y sistemas; estos motores de ML se entrenarán con datos de ataques exitosos y podrán identifique patrones en las defensas para identificar rápidamente las vulnerabilidades que se han encontrado en sistemas/entornos similares.

Este enfoque permitirá a los atacantes concentrarse en los puntos de entrada en entornos de manera mucho más rápida y sigilosa, ya que apuntarán a menos vulnerabilidades con cada ataque, evadiendo herramientas que necesitan un volumen de actividad para identificar irregularidades.

7. Convergencia Zero-Trust y SASE

Zero Trust se ha promocionado durante años como el futuro de la seguridad de la red aunque no ha sido hasta hace poco cuando ha comenzado a ganar tracción como un marco práctico de seguridad empresarial. Su protagonismo ha aumentado a medida que las aplicaciones y los recursos de red migran a la nube y difuminan el perímetro de la red tradicional, poniendo en entredicho la seguridad en firewalls, puertas de enlace seguras, VPN y proxies.

Al mismo tiempo, Secure Access Service Edge, o SASE, está obteniendo mucho reconocimiento en la industria de la ciberseguridad porque representa

Gartner espera que al menos el 40% de las empresas cuenten con estrategias para adoptar SASE para 2024

una transformación que se adecúa a la nueva realidad: un entorno de trabajo en constante cambio, con aplicaciones que se trasladan a la nube y trabajadores que se conectan desde ubicaciones distribuidas utilizando todo tipo de dispositivos.

Desde Netskope prevén una convergencia de ambos modelos, una arquitectura SASE que se apoye en una implementación de confianza cero como piedra angular para un entorno de teletrabajo como el que tenemos, y que no desaparecerá, proporcionando una visibilidad, control y habilitación totales para una transformación segura de la nube.

Por cierto que Gartner espera que al menos el 40% de las empresas cuenten con estrategias para adoptar SASE para 2024.

8. La seguridad del IoT sigue sin despegar

Llevamos tiempo hablando de la inseguridad del IoT, bautizado por muchos con el Internet of Threats o el Internet of Troubles, y no parece que en 2021 vayamos a ver grandes cambios, salvo por un aumentos de los problemas. Y es que la llegad de 5G ayudará a incrementar la cantidad de dispositivos conectados, lo que incidirá directamente en la seguridad de las redes.

Los pequeños dispositivos de IoT seguirán siendo vulnerables y sin posibilidad de parches, a medida que se vuelvan ubicuos. Los actores maliciosos encontrarán usos nuevos y más creativos para estos dispositivos; los equipos con funciones de bienestar recogerán información sobre el usuario (ritmo cardiaco, etc.), los coches incluirán funciones para controlar el movimiento de otros vehículos o peatones y las ciudades inteligentes podrán recabar información sobre los hábitos de sus ciudadanos. Este volumen de datos tan masivo necesita altos niveles de seguridad para evitar robos o filtraciones. Algo que podemos esperar o, más bien, preocuparnos, son los ciberataques contra la última generación de vehículos conectados.

funciones internas, y no todas han sido diligentes a la hora de asegurar el cloud. En 2020, además, se ha acelerado su adopción debido a la necesidad de tomar decisiones rápidas impuestas por la pandemia.

Se espera por tanto que muchas empresas se pongan al día con la seguridad de la nube el próximo año, reforzando los métodos de acceso a los datos mediante tecnologías de gestión de identidades y accesos privilegiados.

Las organizaciones también deben ser más conscientes de su relación con los proveedores de la nube. Una de las cosas que muchas organizaciones malinterpretan es que no pueden traspasar el riesgo cuando subcontratan o se trasladan a la nube porque, si bien el proveedor de la nube es responsable de proteger la nube, el cliente sigue siendo responsable de determinar quién tiene acceso a la nube y cómo lo ha hecho, así como de la protección de sus datos en la nube. La organización debe determinar qué proteger y cómo protegerlo, y asegurarse de que esas protecciones se implementen correctamente.

Por lo pronto se espera que los ataques a la nube continúen ejecutándose a través de: credenciales robadas, generalmente mediante phishing; explotación de configuraciones incorrectas de la nube; piratería de aplicaciones.

En este contexto, y según WatchGuard, todo servicio que no incluya un sistema de autenticación multifactor (MFA) sufrirá una brecha de seguridad. Dice la compañía que las bases de datos con nom-

> Todo servicio que no incluya un sistema de autenticación multifactor (MFA) sufrirá una brecha de seguridad

No sólo es difícil obtener una visibilidad completa de los dispositivos y tienen requisitos de seguridad complejos que hace necesario un enfoque más holístico de la seguridad de IoT, con una combinación de controles nuevos y tradicionales para proteger estas redes en constante crecimiento en todos los sectores industriales y comerciales.

9. La seguridad cloud necesita un impulso

Alrededor del 95% de las empresas tienen algún tipo de presencia en la nube, aunque solo sea para

La adopción masiva del teletrabajo ha difuminado definitivamente el perímetro de seguridad

bres de usuario y contraseñas dispobibles en foros clandestinos, junto con la facilidad de automatizar los ataques de autenticación, significa que ningún servicio expuesto a Internet está a salvo de la intrusión si no utiliza la autenticación multifactor (MFA). Por eso, aun reconociendo que es una predicción audaz, la compañía dice que en 2021 todos los servicios que no tengan MFA habilitado sufrirán una infracción o un compromiso de cuenta.

10. Las personas, los usuarios, son el nuevo perímetro

Los ciberdelincuentes llevan años atentando contra los usuarios, haciendo uso de técnicas de ingeniería social para lanzar ataques que explotan sus hábitos y comportamientos. Es algo que quedó claro cuando miles de empleados se marcharon a trabajar a casa y los ciberdelincuentes aprovecharon para lanzar phishing, vishing, ransomware como si no hubiera un mañana.

Lo que parece cierto es que aunque los empleados volverán a la oficina, no lo harán a tiempo completo, y tampoco de forma masiva. Según datos de un informe de MobileIron más del 80 % de la gente no quiere volver a la oficina, nunca más, lo que supone la desaparición definitiva del perímetro de seguridad. Esta pérdida de perímetro, de la que se habla desde hace un tiempo, ha llevado a buscar un nuevo elemento en el que colocarlo. Algunos hablan del dato, otros de identidad, o personas.

Pensamos que las personas se convertirán en el nuevo perímetro porque garantizando su identidad se garantiza la integridad del dato al que se accede. Garantizar la identidad de los usuarios, de los empleados, definirá a qué se les permite acceder, tanto dentro como fuera de la red corporativa. Incluso cuando estén conectadas a la red, tendrán un acceso mínimo a los recursos hasta que la persona y el dispositivo que esté utilizando hayan sido autenticados y autorizados. Este modelo, que no es otro que el modelo Zero Trust del que tanto se habla, llegará a todos los ámbitos, abarcando no solo a los empleados, sino también a clientes, contratistas y otros socios comerciales.

Enlaces de interés...

- La ciberseguridad será protagonista del gasto en tecnología el año que viene
- Predicciones para las Everywhere Enterprises en 2021
- Diez claves a tener en cuenta en las estrategias de ciberseguridad de 2021
- El cryptojacking tiende a desaparecer, según las predicciones de Acronis

Compartir en RRSS

it Reseller
TECH&CONSULTING

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

SANTIAGO MORAL RUBIO

EXPERTO EN CIBERSEGURIDAD

Actualmente es el VP de Innovación y Ciberseguridad de OpenSpring y codirector y uno de los fundadores del Instituto DCNC Sciences de la Universidad Rey Juan Carlos, así como Presidente de la Asociación HITEC en España y miembro de su sede norteamericana. Moral Rubio, quien ocupó el cargo de CISO del Grupo BBVA entre 2000 y 2018, también ha participado en la creación del Grupo de Ciberseguridad del Laboratorio de Informática e Inteligencia Artificial (CSAIL) del MIT.

Zero Trust

¿Quién le pone el cascabel al gato?

En la fábula de "Los ratones y el gato" de Esopo, estos proponían poner un cascabel al gato para saber cuándo se acercaba y tener así tiempo de huir. El final de fábula es que no lo consiguieron. Disculpen el spoiler.

Unos interpretan que por cobardía. No hubo ningún ratón lo suficientemente valiente como para abordar el reto imposible de colocarle un cascabel al gato.

Si lo analizamos desde una perspectiva actual, esta fábula se parece mucho a un patrón de comportamiento que se produce de manera repetitiva a la hora de determinar cómo han de resolverse problemáticas que afectan a colectivos.

¿Qué sucede cuando dentro de un colectivo, para resolver un problema común, se plantea una solución aparentemente buena pero imposible de alcanzar? El auténtico problema real llega cuando todos dan por buena una solución, que de alcanzarse es francamente buena, pero que desde el punto de vista operativo es simplemente imposible de lograr. Según va pasando el tiempo el colectivo va entrando en una especie de melancolía en la que nadie consigue explicarse cómo no pueden alcanzar la solución que han ideado.

En ese momento tienes dos problemas: el que tenías originalmente, que no has empezado a resolver, y el nuevo que es convencer a un colectivo de que el esfuerzo que están haciendo es inútil porque la estrategia utilizada no es la adecuada.

Este tipo de dinámicas se producen especialmente cuando se dan modelos de relación de adversarios, como las que tenemos en ciberseguridad entre atacantes y víctimas. Cualquier solución que unos piensen, los de enfrente se esforzarán en superarla.

Para evolucionar nuestras arquitecturas actuales a modelos Zero Trust no es necesario hacer más inversiones en tecnologías de seguridad

ZTA. Sólo otro modelo más que intenta resolver este problema.

Los modelos Zero Trust vienen a plantearnos soluciones radicalmente distintas a los mismos problemas de seguridad que llevamos intentando evitar los últimos 35 años.

¿Por qué sabemos que necesitamos aproximaciones radicalmente distintas a las actuales?

Porque las que estamos utilizando ahora no están funcionando. Sólo hay que leer la prensa para ver que el número de incidentes y su impacto no para de crecer. La opinión generalizada es que lejos de mejorar, estamos en una espiral en caída libre.

El NIST ha sacado recientemente (agosto 2020) la primera versión final del “NIST Special Publication 800-207. Zero Trust Architecture”. Es una apuesta decidida del NIST y de la Cybersecurity & Infrastructure Security Agency del Departamento de Homeland Security de USA por forzar a todas las agencias que dependen de la Administración Federal a evolucionar hacia modelos Zero trust.

¿En qué están basados los modelos Zero Trust? En que no puede haber ningún tipo de comunicación entre dos programas, entre dos máquinas o entre dos usuarios que no esté expresamente aprobado en el momento en el que se produce.

Zero Trust es una forma de diseñar la ciberseguridad basada en principios, no en guías de implantación

¿Por qué Zero Trust es una aproximación radicalmente distinta? Porque la forma actual de diseñar los sistemas de información, las comunicaciones y las tecnologías es que hay zonas de confianza. Si dos aplicaciones, si dos máquinas están dentro de una zona de confianza pueden acceder la una a la otra relajando mucho los mecanismos de control. Con los modelos Zero Trust desaparecen las zonas de confianza.

Las Zero Trust Architectures (ZTA) son por ende arquitecturas tecnológicas diseñadas siguiendo los principios Zero Trust.

Empresas reales con personas reales

¿Por qué podría funcionar este nuevo paradigma? Uno de los aspecto que más me hace pensar que puede ser el siguiente gran modelo de seguridad es que está pensado para que funcione en “empresas reales”. En las “empresas reales” las personas de distintos departamentos de informática colaboran muy poco entre sí, cuando no mantienen posiciones de enfrentamiento permanente entre ellos. Además, esta falta de alineamiento de objetivos entre personas y colectivos de las empresas es un tipo de comportamiento fractal. Se produce de manera recursiva en todos los niveles y tamaños de grupos humanos.

Cuantas más campañas del tipo “¡Somos un equipo!!!” observo en las empresas más pienso que sus departamentos internos están completamente enfrentados.

¿Por qué se produce esta falta de sintonía entre los departamentos de las empresas?

Supongo que los antropólogos tienen mucho que decir al respecto. Cuanto más veo documentales de chimpancés con sus luchas de castas, guerras territoriales y posicionamientos en sus jerarquías, más entiendo las dinámicas internas de las empresas.

Son muy clarificadores. ¿Qué tiene que ver Zero Trust con la falta de colaboración entre departamentos? Los modelos Zero Trust parecen estar pensados no sólo para que se puedan crear arqui-

tecturas tecnológicas de confianza cero, sino para que sean diseñadas, implementadas y gestionadas por personas que entre ellos van a tener "Colaboración Cero". Parecen estar pensadas para que puedan generar un avance muy importante en materia de seguridad dentro de "empresas reales" donde los niveles de colaboración interdepartamentales son escasos y puntuales.

Es la primera vez que veo un modelo de ciberseguridad que, naciendo de una organización de estandarización, no supone que todo el mundo en la empresa va a dejar todas sus tareas diarias y cogidos de mano todas las mañanas, cantando canciones dominicales, van a dedicar todos sus esfuerzos a implantar interminables listas de controles de seguridad.

En las "empresas reales" todas las áreas técnicas tienen una presión enorme por hacer que los sistemas funcionen todos los días, todos los minutos, todos los segundos, lo hagan bien y cada vez con menos presupuesto y menos personal. Y las Áreas de Negocio no se escapan a esta presión. Tienen que conseguir, por ejemplo, que la rotación diaria de personal en los Contact Centers se haga rápido a pesar de sus usuarios y sus contraseñas.

En las "empresa reales" todo el mundo tiene mucho que hacer y mucha presión para cumplir los objetivos que le ponen a cada uno, como para estar dedicándole ni un minuto a estas zarandajas de la Cyber. Lo normal es que piensen ¡Que se encarguen l@s chic@s de Cyber!!! ¡Que para eso les pagan!!!

¿Por qué puede ser una solución el concepto Zero Trust?

En los siguientes artículos iremos desgranando las virtudes de los modelos Zero Trust. Lo de no confiar en nada ni en nadie parece un poco paranoico, pero es tan fácil de construir técnicamente que es muy difícil explicar a los Comités de Dirección de las empresas cómo es que no lo tenemos ya todos completamente instalado. La respuesta es políticamente incorrecta y nadie va a darla: "No lo hemos hecho ya porque no nos "ponemos de acuerdo" dentro de la empresa".

Creo que una imagen vale más que mil palabras. Voy a utilizar dos ejemplos reales de dos empresas que han tenido sendos incidentes de ransomware durante esta pandemia para explicar el modelo y algunos de los principios Zero Trust.

Primer ejemplo: Accesos externos basados en usuario y contraseña.

En el modelo Zero Trust das por sentado que todos nuestros usuarios y contraseñas, nuestras direcciones de correo, nuestros números de tarjetas, nuestros PINes… se pueden comprar en el mercado negro.

Ningún mecanismo de acceso externo a la organización debería estar basado en usuario y contraseña, ya que estas se pueden adquirir fácilmente en el mercado negro.

Los grupos de delincuencia organizada están escaneando permanentemente todo el perímetro externo de las organizaciones buscando accesos

abierto tipo VPN o RDP que estén habilitados con usuario y contraseña.

Si tu empresa tiene un acceso externo al que puedas entrar con usuario y contraseña, puedes tener la garantía (casi absoluta) que vas a tener un incidente de ransomware en breve. ¿Por qué? Muy fácil: la probabilidad que un atacante pueda comprar algún usuario y contraseña tuyo es muy alta y la probabilidad de que tengas parcheados TODOS los sistemas internos a las últimas vulnerabilidades conocidas con algún exploit disponible es CERO!!!

Conclusión: Si tienes expuestas conexiones (VPN, RDP…) con usuario y contraseña vas a tener un ransomware próximamante.

Después de tener el incidente la Alta Dirección va a preguntar si el problema era conocido.

La respuesta suele ser que sí. Que el departamento de Seguridad lo conocía. La siguiente pregunta de la Dirección es evidente: ¿Por qué no se había corregido ya? Las respuestas serán variopintas, pero el fondo de todas es el mismo: “No nos hemos puesto de acuerdo los departamentos internos para hacerlo”. Muchas veces nadie se atreverá a decirlo.

Segundo ejemplo: Hemos tenido un ransomware y sólo se han salvado los PCs que estaban en teletrabajo.

Uno de los patrones repetitivos en los incidentes de ransomware durante la pandemia es que los PCs que estaban en teletrabajo no son cifrados en el ataque. Este tipo de comportamiento, si bien era conocido por los expertos, nunca se había evidenciado antes ante la Alta Dirección de las empresas, ya que el número de PCs en teletrabajo era infinitamente menor.

La causa es obvia para los expertos en Cyber. La probabilidad de que un ataque de ransomware se propague desde el interior de una empresa a sus PCs que están en teletrabajo es menor que a los PCs internos. La razón es que las empresas se protegen habitualmente de sus PCs cuando estos están en teletrabajo, utilizando lgún cortafuegos o IPs. Esta protección usualmente es bidireccional. Los PCs que están en teletrabajo han quedado protegidos accidentalmente del ransomware que se ha propagado desde el interior de la organización.

Llegado este punto la pregunta de la Dirección es evidente ¿Por qué no tenemos a todos los PCs como si estuvieran en Teletrabajo? Como en el ejemplo anterior, las respuestas de los Departamentos de Seguridad a sus Direcciones serán variopintas. Incluso es posible que algunos indiquen que es imposible, que es muy caro de mantener o que generaría incomodidades para los usuarios. Los que nos dedicamos a este oficio sabemos que nada de eso es cierto. Como en el ejemplo anterior la única respues-

Los modelos Zero Trust parecen estar pensados no sólo para que se puedan crear arquitecturas tecnológicas de confianza cero, sino para que sean diseñadas, implementadas y gestionadas por personas que entre ellos van a tener "Colaboración Cero"

Enlaces de interés...

W Tu camino hacia Zero Trust

I Solo un tercio de las empresas posee una infraestructura de acceso remoto segura

ta honesta es que “No nos hemos puesto de acuerdo los departamentos internos para hacerlo”.

¿Cómo se diseñan arquitecturas “basadas en principios”?

Zero Trust es una forma de diseñar la ciberseguridad basada en principios, no en guías de implantación. Se van haciendo diseños arquitectónicos que se “someten” a la validación de los principios. De esta manera se debe verificar, por ejemplo, que una arquitectura técnica concreta impide el acceso a la organización desde el exterior de la misma utilizando simplemente un usuario y contraseña.

Para evolucionar nuestras arquitecturas actuales a modelos Zero Trust no es necesario hacer más inversiones en tecnologías de seguridad. Habitualmente con las que ya tenemos son suficientes. Hay que usarlas de otra manera y empezar a configurar todas las tecnologías (no sólo las de seguridad) de manera que cumplan los principios Zero Trust.

Estos son los dos mayores inhibidores para la implantación de Arquitecturas Zero Trust:

1. **Los fabricantes/proveedores de seguridad** no tienen ningún interés en recomendarte que no compres más cacharrería de Cyber. Supongo que esto no hay que explicarlo.
2. **Los departamentos técnicos** (no de seguridad) tienen que trabajar muy duro y durante mucho tiempo para implementar Arquitecturas Zero Trust. Sirva como ejemplo el esfuerzo que tienen que hacer los Departamentos de Comunicaciones y de Microinformática si, como describíamos en un ejemplo anterior, quieres que los PCs no puedan verse entre ellos, para reducir drásticamente la probabilidad de que puedan propagarse un malware.

Para evolucionar hacia arquitecturas de confianza cero no necesitas comprar más tecnologías. No hay que hacer más inversiones. Sólo hay que usar de otra manera las que ya estamos haciendo. ¿Vamos a conseguir solucionar un problema en el que todos los fabricantes/proveedores actuales pierden y en el que las áreas técnicas y de negocio de las empresa tienen que dedicarle mucho tiempo y esfuerzo en objetivos que no son los suyos?

¿Quién le pone el cascabel al gato?

Ahí queda la pregunta.

Profundizaremos en los principios Zero Trust en próximos artículos.

¿CÓMO INVERTIRÁ TU EMPRESA EN TI EN 2021?

it TRENDS

Ayúdanos a conocer la realidad digital de nuestras empresas

ENCUESTA
IT TRENDS 2021

¡PARTICIPA!

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

Con más de 20 años en el sector de la CyberSeguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Calculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.

El Poder Judicial en la Nueva Sociedad Digital: ¿Evoluciona o no?

Me repito una vez más, ya no se discute si estamos llegando a la Era Digital de la Humanidad, ESTAMOS YA en esta nueva Era, y tal vez la pandemia del Covid 19 está dejando todavía más claro no solo por el incremento de relaciones digitales personales , educativas, sanitarias, comerciales, con las administraciones del Estado…

Simplificando la teoría de los 3 poderes del Estado democrático, se asigna a cada uno de ellos una labor fundamental que establece un equilibrio. Nadie discute este principio del siglo 18 que nos ha dado ya dos siglos y medio de un gran avance de la humanidad.

El Poder Judicial es el más técnico y menos político de los 3 poderes del Estado y, por tanto, el más difícil de imaginar cómo podría evolucionar digitalmente manteniendo los principios básicos de la Justicia y mejorando la eficiencia, eficacia, transparencia y claridad de lo que ha llegado a ser en el siglo XXI.

El poder judicial del siglo XVIII tenía que dar respuesta a las necesidades de la sociedad

preindustrial, simple y básica, fundamentalmente agrícola, con apenas unos de centenares de millones de ciudadanos. Utilizando la herencia del Derecho Romano, de hace muchos siglos, fue capaz de ser uno de los pilares sobre los que se construyeron los Estados democráticos modernos.

Durante los siglos XIX y XX, con el apoyo de un Poder Legislativo vibrante y que mantenía el ritmo de modernización de las 3 Revoluciones Industriales, fue capaz de adaptarse a una Sociedad Moderna y con 7.500 millones de habitantes en el planeta.

Lamentablemente, con la llegada de la Cuarta Revolución que trajo consigo la Digitalización de la Sociedad y la aparición de los Ciudadanos Digitales se ha producido un estancamiento en esta capacidad de adaptación y no se producido ninguna Evolución Digital del Poder Judicial.

Se culpa al Poder Ejecutivo por no facilitar los recursos económicos para realizar esta Evolución Digital, que ya en esta segunda década del siglo XXI ve que ni siquiera la documentación de la administración de justicia ha abandonado el papel como soporte de la información para la administración de justicia. Cómo vamos a pedir que se aprovechen las nuevas plataformas digitales actuales para mejorar y hace más eficiente y eficaz el sistema judicial.

Está claro que el Poder Judicial necesita evolucionar digitalmente con urgencia para dar un mejor servicio a su Ciudadanos Digitales contemporáneos

Se culpa al Poder Legislativo por la lentitud de evolución de las leyes para adecuarse a la nueva realidad digital de la sociedad en el siglo XXI, obligando a administrar justicia a problemas actuales, digitales por cierto, con leyes en muchos casos obsoletas que obligan a una gran imaginación de los jueces para interpretar situaciones no conocidas por esas leyes.

El inmovilismo tecnológico del Poder Legislativo tiene el efecto de entorpecer el mejor funcionamiento del poder judicial obligándole, a enfrentarse a situaciones donde no existen leyes que regulen nuevas situaciones y, por tanto, los jueces se ven obligados a tomar decisiones en ausencia de leyes apropiadas y así suplir las carencias causadas por esta situación.

Aceptemos estas reclamaciones, son justas y tanto el Poder Ejecutivo como el Poder Legislativo no pueden negarlas, pero seamos críticos al expresar que parece que en el último tercio del siglo XX y dos décadas iniciales del siglo XXI, el Poder Judicial ha mostrado una autocomplacencia con la situación y no hemos visto ningún movimiento de evolución.

Los Ciudadanos Digitales exigen una Justicia transparente, eficaz y eficiente, como todos los otros servicios digitales a los que están acostumbrados.

Enlaces de interés...

- Separación de poderes
- Poder Judicial en España

Cómo vamos a pedir que se aprovechen las nuevas plataformas digitales actuales para mejorar y hace más eficiente y eficaz el sistema judicial

Pero ante todo exigen una justicia rápida, no conciben que pueda haber problemas judiciales que duren años o incluso décadas, permitiendo situaciones donde responsables de delitos no son castigados porque mueren de viejos o acusados absueltos después de procesos judiciales de muchos años de duración ven como es casi imposible recuperar la reputación perdida por acusaciones que resultaron ser falsas y sostenidas durante largos períodos de tiempo.

Un pequeño ejemplo. La aparición del Big Data y la Inteligencia Artificial, que permite el aprovechamiento de la información histórica acumulada, podrían ayudar a analizar esta ingente información de dos siglos de casos judiciales para acelerar la toma de decisiones. No, es mejor usar un ejército de pasantes y la inteligencia (¿experiencia?) de un abogado/juez para escribir una nueva pieza de brillantez intelectual individual en vez de usar la inteligencia colectiva de jueces y abogados de muchas generaciones anteriores que demostraron una brillantes intelectual al menos igual al de los actuales.

Está claro que el Poder Judicial necesita evolucionar digitalmente con urgencia, la Justicia tiene muchos elementos técnicos que los profesionales nuevos de la abogacía, jueces, fiscales, procuradores y abogados, por su nueva formación digital son capaces de cambiar para dar un mejor servicio a su Ciudadanos Digitales contemporáneos. No olvidemos que todos los días nacen nuevos Ciudadanos Digitales, y muchos de ellos serán juristas, que vienen a reemplazar a generaciones que por ley de vida van abandonando esta sociedad.

Y los Ciudadanos Digitales quieren soluciones inmediatas, rápidas, eficientes; ya se sabe, con la digitalización, o evolucionas o desapareces.

¿Cuál es la situación de la empresa española en relación con la digitalización?

¿Qué tecnologías son las que están impulsando la transformación digital?

Descubra las últimas tendencias en el Centro de Recursos IT User

Tecnología para tu Empresa

Con la colaboración de:

NFON
Cloud Telephone System