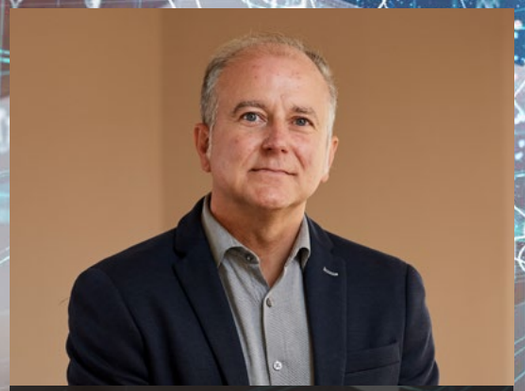
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Diciembre 2022 - nº 58

Grandes ciberataques en 2022

‘Lo más difícil de ser CISO es cuidar al equipo, formarlo y retenerlo’
Fabián Vidal, Ávoris



‘Queremos ofrecer a nuestros clientes resiliencia operacional’
Miguel Ángel Ordóñez, Kyndryl

Desayuno ITDS. De la gestión del riesgo al Incident Response

Encuentro ITDS. Mejorando tu seguridad con Servicios Gestionados

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

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

Controla y gestiona permisos de uso

Firma digitalmente documentos

Usa los certificados en cualquier lugar

Cumple con la normativa del sector

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

redtrust
a **KEYFACTOR** company

itds

Sumario

Entrevistas

‘Lo más difícil de ser CISO es cuidar al equipo, formarlo y retenerlo’

Fabián Vidal, Ávoris

‘Queremos ofrecer a nuestros clientes resiliencia operacional’

Miguel Ángel Ordóñez, Kyndryl

‘Los alumnos de ciber son muy vocacionales. Tienen una mentalidad muy analítica y una tendencia hacia la administración sistemas’

Javier García Algarra, U-tad

Desayuno ITDS

Encuentros ITDS

Índice de anunciantes

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

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

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

www.sophos.com/es-es

SOPHOS
Cybersecurity delivered.

Siete predicciones de ciberseguridad para 2023

Este ha sido otro año extremadamente ajetreado para los CISOs, y todo apunta a que 2023 será otro año complicado. Proofpoint anticipa en sus tendencias de ciberseguridad para el próximo ejercicio un mayor riesgo sistémico por las tensiones globales y un aumento de los ataques de ransomware, los robos de datos, las vulnerabilidades de la autenticación multifactor, el fraude de identidad provocado por los deepfakes, etc.

Según el análisis realizado por el equipo de CISOs residentes de Proofpoint, 2023 será un año más complejo en materia de ciberseguridad, a medida que se intensifiquen las tensiones globales, la economía mundial se vuelva más volátil y continúen los desafíos en el entorno laboral, por lo que deberán prepararse para ello. La compañía resume sus predicciones en estos siete puntos:

Los kits de hackeo para ejecutar ransomware han pasado a ser mercancía habitual de las redes clandestinas de la ciberdelincuencia

1. Las tensiones globales por la recesión y los conflictos agravarán el riesgo sistémico.
Nuestro ecosistema digital, cada vez más complejo e interconectado, empeora las preocupaciones existentes y suscita nuevos temores en torno al riesgo sistémico, en el que las debilidades de cualquiera de sus componentes amenazan la fortaleza de todo el conjunto. Según un reciente estudio de Proofpoint, el 75% de los consejos de administración cree que entiende claramente el riesgo sistémico de sus organizaciones. Aun así, la inestable situación mundial hace muy difícil comprender el alcance total de las amenazas, por lo que, en consecuencia, el riesgo sistémico exigirá una atención constante.

2. La comercialización de herramientas de hackeo en la 'dark web' aumenta la ciberdelincuencia.
En los últimos años, los kits de hackeo para ejecutar ransomware han pasado a ser habitual mercancía dentro de las redes clandestinas de la delincuencia. Ese ransomware como servicio se ha convertido en un negocio lucrativo en la dark web y ha hecho que proliferen estos ataques con poca o ninguna sofisticación técnica, abriendo la puerta de la ciberdelincuencia a cualquier persona con un navegador Tor y algo de tiempo.

Mientras que el comercio por la dark web siga en auge, habrá oleadas de ataques también de smishing o de control de dispositivos móviles.

3. Los ataques exitosos de 'ransomware' incluirán el robo de datos, ya que el negocio de los atacantes se mueve hacia la doble extorsión
El ransomware es endémico, y ninguna organización en el mundo es inmune a esta amenaza. El

68% de las empresas ha sufrido al menos una infección de este tipo, de acuerdo con el informe State of the Phish de Proofpoint en 2022. Lo más preocupante, sin embargo, es la evolución que ha tenido en los últimos tres años el cifrado de datos hasta llegar a esquemas de doble extorsión que cifran y exfiltran datos. Solo una banda había utilizado esta táctica de doble extorsión en 2019, pero, en el primer trimestre de 2021, el 77% de los ataques incluía amenazas de filtración de datos. Asimismo, la última tendencia es la triple extorsión, en la que los atacantes buscan pagos no solo de la organización objetivo, sino también de cualquier entidad que pueda verse afectada por la fuga de datos.

El ransomware es endémico, y ninguna organización en el mundo es inmune a esta amenaza

4. Crecerán los ataques para eludir la autenticación multifactor (AMF) a medida que los ciberdelincuentes exploren nuevas vías para vulnerar las defensas y explotar las debilidades del comportamiento humano

Los atacantes siguen innovando mientras aprenden acerca de las personas y cómo obtener de manera más fácil sus credenciales. Ante esto, el sector de la ciberseguridad ha respondido impulsando la AMF, que se ha convertido en una práctica estándar y una especie de juego del gato y el ratón: si las organizaciones añaden una capa de seguridad con la AMF, más ciberdelincuentes explotan sus debilidades y se aprovechan de los usuarios. Esto empieza a ser tendencia, aunque no se trata en sí de una amenaza nueva. Los investigadores de Proofpoint verificaron hace dos años vulnerabilidades que eludían la AMF, pero se están viendo más herramientas para ejecutar estos ataques, como kits de phishing para robar tokens.

5. La cadena de suministro será un arma cada vez más poderosa, aprovechando la confianza depositada en vendedores y proveedores

Puede que los casos de SolarWinds y Log4j hayan sido llamadas de atención, pero lo cierto es que todavía se está muy lejos de tener las herramientas adecuadas para protegerse frente a las vulnerabilidades en la cadena de suministro digital. Una encuesta del Foro Económico Mundial revela que casi el 40% de las organizaciones sufrió efectos negativos tras incidentes de seguridad relacionados

Los atacantes siguen innovando mientras aprenden acerca de las personas y cómo obtener de manera más fácil sus credenciales

con su cadena de suministro, y prácticamente todas mostraron su preocupación por la resistencia de pequeñas y medianas empresas dentro de su ecosistema.

Estas preocupaciones aumentarán en 2023, ya que la confianza en partners y proveedores de terceros se convertirá en uno de los principales canales de ataque.

6. La tecnología 'deepfake' tendrá un papel más destacado en los ciberataques, aumentando el riesgo de fraude de identidad, engaño financiero y desinformación

La tecnología deepfake es cada vez más accesible para las masas. Gracias a los generadores de IA entrenados con enormes bases de datos de imágenes, cualquiera puede generar deepfakes con pocos conocimientos técnicos. Aunque el resultado no esté exento de fallos, la tecnología está mejorando constantemente, y los ciberdelincuentes la utilizarán para sus narrativas.

Tradicionalmente, los deepfakes se han empleados para fraudes con correos empresariales, pero se prevé que vayan más allá de estos engaños. Solo hay que imaginar el caos que produciría en el mercado financiero si, mediante esta tecnología, el supuesto CEO o CFO de una importante empresa hiciese unas declaraciones con las que, acto seguido, las acciones subiesen o experimentasen una fuerte caída. Los ciberdelincuentes también podrían aprovechar la autenticación biométrica y los deepfakes para fraudes de identidad o control de cuentas. Estos son algunos ejemplos, pero la creatividad de los atacantes siempre sorprende.

7. El papel del CISO

A medida que haya más requisitos de transparencia en las empresas, se mejorará la supervisión y aumentará la experiencia de ciberseguridad dentro del propio consejo de administración, cambiando el papel tradicional del CISO. Pero, con solo la mitad de estos viéndose cara a cara con sus juntas directivas, unido a las crecientes expectativas y el estrés por la responsabilidad de un potencial ataque, aumentará la tensión en las relaciones entre ambos con enormes implicaciones para la ciberseguridad de la organización. it

Enlaces de interés...

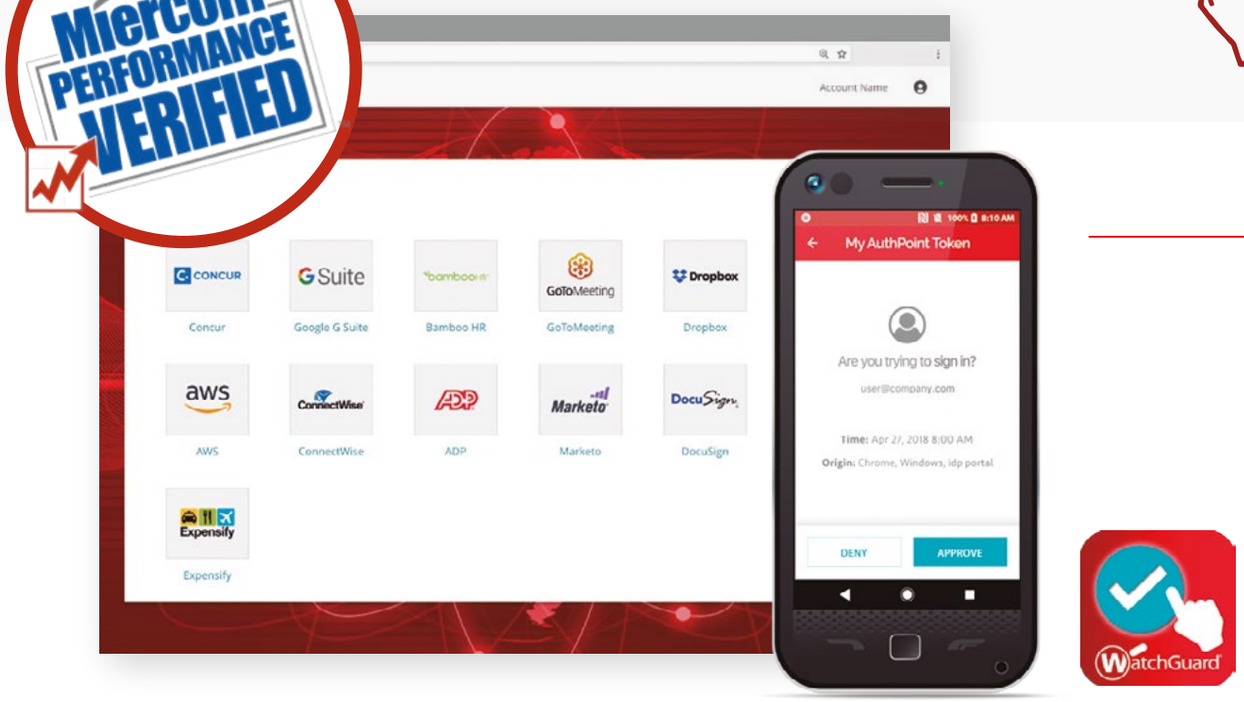
- ¿Qué esperar en la segunda mitad del año en materia de ciberamenazas?
- Estos serán los retos de seguridad de las organizaciones a corto plazo
- Esto es lo que nos deparará 2023 en materia de ciberseguridad

Compartir en RRSS

WatchGuard AuthPoint

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

¿Cuántas de estas personas trabajan en su organización?



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

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

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

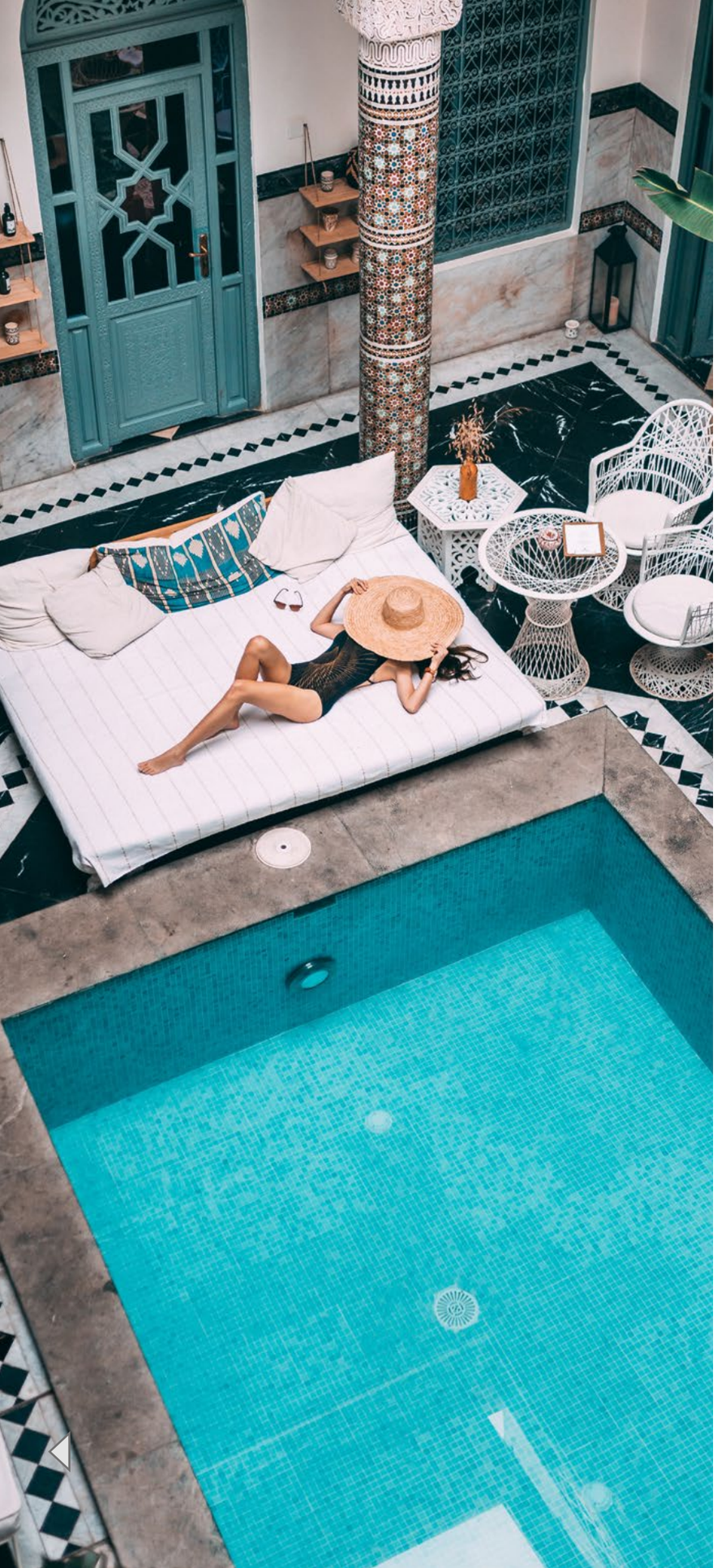
‘Lo más difícil de ser CISO es cuidar al equipo, formarlo y retenerlo’

(Fabián Vidal, Ávoris)

Tener capacidad de liderazgo es, en opinión de Fabián Vidal CISO de Ávoris, una de las principales habilidades que debe tener un buen CISO, además ser una persona calmada. Está de acuerdo con quienes plantean que es necesario convertir a los empleados en firewalls humanos, y apuesta por las herramientas de descubrimiento de activos y el XDR como herramientas de seguridad imprescindibles en un futuro.

Texto: Rosalía Arroyo
Fotos: Ania Lewandowska

Fabián Vidal de la Fuente es el CISO de Ávoris, una corporación que desde 1931 tiene al viajero en el centro de su actividad y que, en la actualidad, es responsable de marcas como B travel, Halcón Viajes, Viajes Ecuador, RACC Travel by Ávoris, Geomon, Business Travel, Congresos y Wäy. Antes de ser CISO, Vidal de la Fuente fue el responsable de Riesgos y Gobierno de la Información para Europa y Latinoamérica de



"Sí a los servicios gestionados de seguridad, pero de una manera mixta"

Sanitas durante más de seis años, después de dedicar otros tantos en tareas de auditoría en Deutsche Bank y Grupo Banco Popular.

Ser CISO es un camino que se recorre desde diferentes orígenes. Las ingenierías de Informática, Telecomunicaciones o Industriales son algunos. Llegar a ser CISO es, en opinión de Fabián Vidal, recorrer un itinerario "que te permita coger conocimientos técnicos y no técnicos, que son de gobierno, estrategia o liderazgo". Asegura que muchos proceden del mundo de las auditorías y consultorías, que tiene como ventaja que "puedes ver un montón de empresas y un montón de tecnologías"; también de la segunda o tercera línea de defensa, "que es un salto quizá menos cómodo pero que tiene sentido"; también los hay que proceden del área de infraestructura "porque en la seguridad de la información y la parte de infraestructura nos necesitamos unos a otros".

Sobre la evolución de la figura del CISO, asegura Fabián Vidal que se ha ganado en visibilidad y presencia en los órganos directivos de la empresa, sobre todo en los últimos cinco años. Y reconoce al mismo tiempo una evolución del propio CISO, que empezó siendo una persona puramente técnica hasta convertirse, con la llegada de más tecnologías, normativas y riesgos "en una parte clave de las empresas, incluso miembro del comité de dirección". Aunque no hay un modelo perfecto, en opinión de este directivo, lo más sano es que el CISO dependa del CEO porque "es donde más independencia se genera".

La primera de las cualidades que debe tener un buen CISO es "el liderazgo, porque el reto, a día de hoy, son las personas" asegura Vidal de la Fuente. "Lo más difícil de ser CISO es cuidar al equipo, formarlo y retenerlo", añade. También tiene que tener un buen CISO habilidades financieras, porque los recursos humanos son caros, y hay que contratar tecnologías y servicios conforme a unos presupuestos. Menciona también el tener capacidades de networking, porque "si estás metido en tu despacho intentando proteger a tu organización, casi seguro no lo vas a conseguir; tienes que estar a la última, tienes que estar muy al día de lo que le está sucediendo al vecino para adelantarte". No se le olvida añadir a Fabián Vidal que un buen CISO debe ser un buen comunicador "porque explicar la ciberseguridad es muy complejo" y que debe tener cierta madurez; "poner un CISO muy junior no tiene sentido, aunque sea el mejor técnico del planeta, incluso el mejor financiero del mundo".

No siendo imprescindible, "merece la pena" que un buen CISO sea, además, "una persona calmada

"Un buen CISO debe ser un buen comunicador porque explicar la ciberseguridad es muy complejo"

porque en un incidente puede que hagas más gordo algo que no lo es".

¿Qué tipo de amenaza le quita el sueño a Fabián Vidal? "En el mundo en el que vivo ahora uno de los problemas graves es el fraude", responde el responsable de la ciberseguridad de una organización con diferentes portales, y una cantidad importante de proveedores, empleados y usuarios registrados. Añade que la respuesta varía dependiendo de la empresa en la que se esté y pone como ejemplo que en una empresa de comercio electrónico un ransomware puede tener mucho más impacto, y en empresas de innovación es peor una fuga de datos.

Seguridad y evolución tecnológica

El mercado tecnológico vive una evolución constante. Si bien ya se asumen aspectos como la virtualización o el cloud, el Edge avanza al ritmo de los contenedores, mientras el Security Mesh va asomando la cabeza. ¿Cómo se afronta esta evolución de manera segura? "Se afronta con persona del seguridad integrado en los equipos que se dedican a la innovación de las empresas", responde Fabián Vidal añadiendo que en general la situación se afronta de una manera insuficiente, "o no se afronta".

Explica el CISO de Ávoris que mientras que lo equipos de gestión de riesgos, o cumplimiento normativo se incorporaron hace tiempo a los departamentos de ciberseguridad, el equipo de arquitectura, que es quien define "cómo va a ser la seguridad cuando nos vamos a la nube o el que diseña más la seguridad en ese container o de cualquier otro tipo de nueva tecnología, está un poco menos rodado, no por los profesionales que lo integran, que son buenísimos, sino porque realmente se han incorporado más tarde", aclara. Añade además que estos arquitectos tienen que conocer muy bien la organización y la infraestructura que se tiene y que "están verdaderamente demandados".

En un mercado tan saturado de fabricantes, soluciones y propuestas, ¿cómo escoger? Para Fabián Vidal el factor determinante es saber qué objetivos

"Por mucho piloto que hagas con tres soluciones no hay nada como que alguien que lleve tres años utilizando el producto me cuente su experiencia"

de seguridad se tienen. Aquí entra en escena el riesgo que cada compañía está dispuesta a asumir porque "dependiendo del riesgo que quiere asumir, tendrá que invertir más o menos".

El segundo punto a tener en cuenta es decidir qué tipo de solución se necesita. A la hora de decidir por una u otra "tiro de networking. Por mucho piloto que hagas con tres soluciones no hay nada como que alguien que lleve tres años utilizando el producto me cuente su experiencia".

Un tercer factor tiene que ver con el "cómo de cómodo estás con el comercial. Si tienes una confianza absoluta en que esta persona te va a responder cuando algo vaya mal, es un factor. No es el primero ni el segundo, pero sí uno a tener en cuenta".

Concienciación

Cuando hablamos de concienciación, está de acuerdo Fabián Vidal con quienes creen que hay que convertir al empleado en el firewall humano. "Da igual la tecnología que pongas. No hay nada que te pueda salvar de un ataque si tus empleados tienen acceso a la información, porque la tienen que tener, y el ataque te entra por ahí", asegura, añadiendo que la concienciación es una de las partes más creativas de la seguridad, y que tiene que ver "con la imagen que damos a la empresa".

En una empresa grande las píldoras de formación/concienciación que llegan a los empleados terminan siendo la imagen que les llega desde el departamento de ciberseguridad. Estos mensajes terminan formando parte de toda una estrategia de comunicación, normalmente muy amigable, "que no sólo sirve para concienciar o para formar a los empleados, sino también para transmitir la importancia de la seguridad y de la información y de todo el área". Añade que además de ayudar a la empresa, "ayudas a las personas en sus casas y en sus familias porque alguien que aprende a no caer en un fraude o en un phishing en el trabajo, tampoco cae en su casa".

Tecnologías

Sí a los servicios gestionados de seguridad, pero de una manera mixta. "Hay partes que merece mucho la pena tenerlas dentro, porque al final el conocimiento de la empresa lo tienes que tener. Y hay

Para afrontar la evolución tecnológica de una manera segura es necesario que haya personal del seguridad integrado en los equipos que se dedican a la innovación de las empresas

partes que, en mi opinión, casi casi merece mucho la pena tenerlas fuera", asegura Fabián Vidal, especificando que SOC y CSIRT son candidatos indiscutibles a un servicio gestionado.

Respecto a las tecnologías de seguridad que deberían ser imprescindibles en cualquier empresa, asegura Vidal de la Fuente que "el EDR sí o sí", el NAC para controlar la red y el firewall para la seguridad perimetral; considera también que la parte de fuga de datos es imprescindible, así como la concienciación y el SIEM para recoger todos los eventos, correlarlos y aprender de ello.

Hay dos tecnologías de seguridad que Fabián Vidal considera que serán necesarias en un futuro: las que permiten hacer descubrimiento de activos y el XDR como una evolución del EDR.

Enlaces de interés...

- "Las herramientas de detección y validación continua de vulnerabilidades son ya fundamentales" (José Manuel Beltrán, Hermanas Hospitalarias)
- 'Hay muchas de empresas de seguridad, pero nuestra experiencia en redes nos da una habilidad única' (Dhrupad Trivedi, A10 Networks)
- 'Somos el sueño del operario de las herramientas' (Álex López, Gigamon)
- 'La concienciación del usuario es un pilar básico de una buena estrategia integral de seguridad' (Roberto Alunda, Mediapro)
- "Seguimos trabajando con passwords, y esto en algún momento se tendrá que acabar", (Enrique Solís, Aguas de Añarbe)

Compartir en RRSS

utimaco®

SOLUCIONES de CIBERSEGURIDAD

Remote Key Load

PKI

HSM en la Nube

Blockhain&IoT

Sellado de Tiempo

Criptografía Post Cuántica

Firma Digital

Cifrado

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

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

Síguenos en:

www.realsec.com

realsec
by utimaco

Entrevista

‘Queremos ofrecer a nuestros clientes resiliencia operacional’

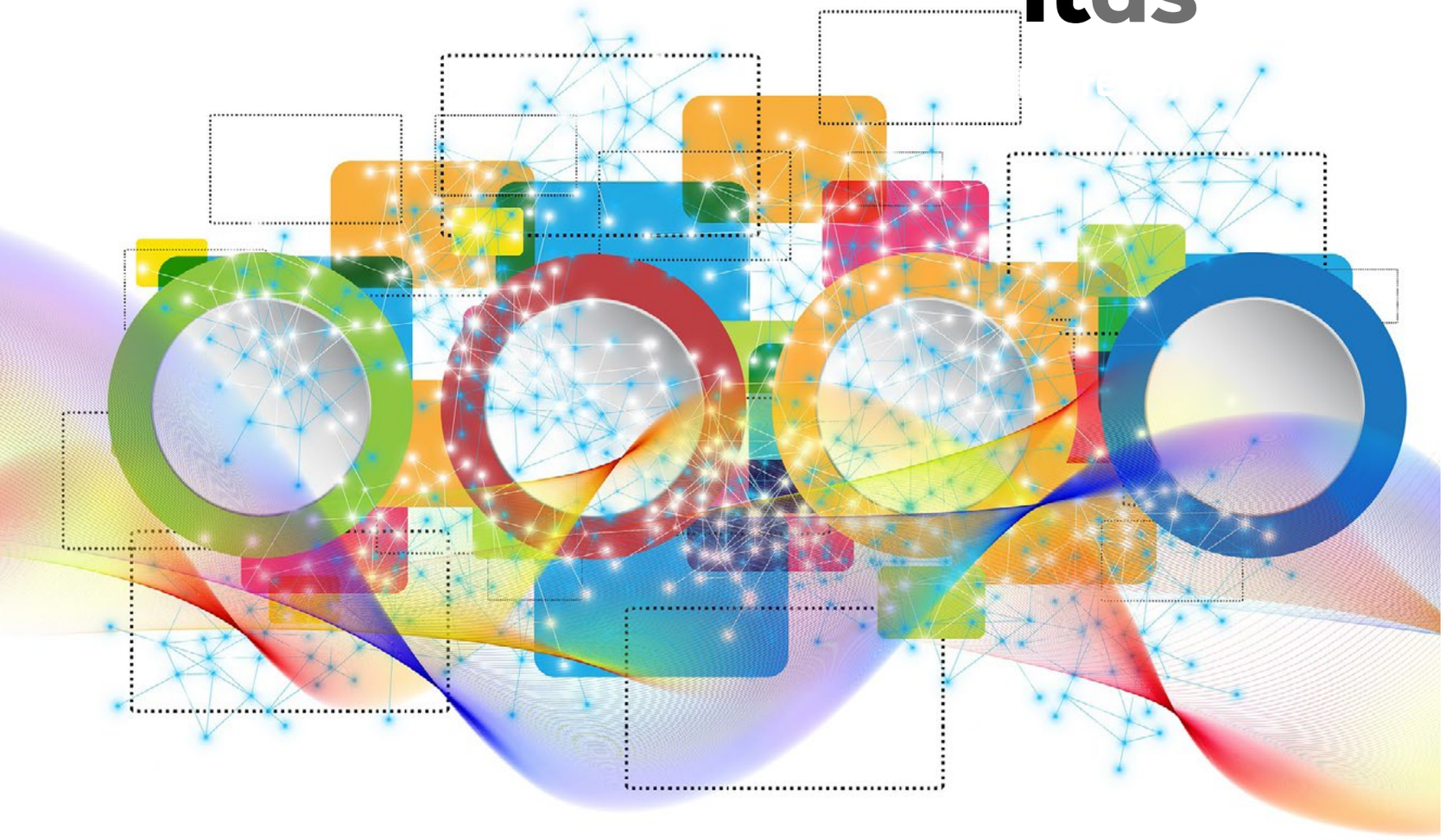
(Miguel Ángel Ordóñez, Kyndryl)

Texto: Rosalía Arroyo

En octubre de 2020 IBM anunció la división de su negocio en dos para impulsar el cloud desde la matriz y controlar la división de infraestructuras de manera independiente. Apenas un año después, el 3 de noviembre de 2021, IBM escindió su negocio de centro de datos, un negocio de ingresos decrecientes y bajo margen y lo llamó Kyndryl. Ahora, libre de IBM, Kyndryl busca su hueco en el mercado con la idea de crecer en áreas como seguridad y resiliencia, IA, datos y análisis, o automatización inteligente.

Podría decirse que Kyndryl es una joven compañía nacida en noviembre de 2022. Que sea una escisión de IBM, un gigante nacido en 1911 como Computing Tabulating Recording Corporation, que cambiaría su nombre por el de IBM (International Business Machines) en 1924, nos hace olvidar una juventud que solo se refleja sobre el papel.

Kyndryl es la parte de servicios de centro de datos de TI de IBM que anteriormente comprendía la mayor parte de IBM Global Technology Services. Tradicionalmente operaba y diseñaba centros de datos para grandes corporaciones y gobiernos, y fue un negocio de gran crecimiento para IBM en la década de 1990 hasta la década de 2000. Pero esto terminó hace aproximadamente una década,



"El cliente tipo es aquel que está en algún proceso de transformación digital y que quiere hacer esa transformación de manera segura"

cuando surgió la nube y muchas grandes corporaciones trasladaron sus centros de datos de TI a proveedores de nube como Amazon Web Services y Microsoft Azure.

La compañía divide su portfolio en seis prácticas, según nos cuenta Miguel Ángel Ordóñez, responsable de la parte de Seguridad y Resiliencia para la región de Iberia. Nos cuenta que hay una parte ligada a gestión de servicios de tecnología que ya se llevaba en IBM, Core Enterprise and zCloud, que incluye también la migración de unas tecnologías a otras "dado que ya no tenemos un producto al que asociarlo". Existe también una práctica de redes, Network and Edge; otra relacionada con la protección del dato, Data and AI; la de Digital Work Place, dedicada a tecnologías del puesto de trabajo; Aplicaciones, y el gran área de Cloud que es la que mejor recoge la filosofía de Kyndryl, que no es otra que "abordar cualquier proyecto de transformación en cualquier cloud de una manera totalmente agnóstica e imparcial".

La práctica de Seguridad, de la que es responsable Miguel Ángel Ordóñez, ya era una unidad de negocio en IBM "y lo sigue siendo ahora", explica el directivo, añadiendo que, si bien antes estaba ligado a una oferta concreta en la que se vendían productos y servicios de seguridad, "ahora nos ajustamos a muchos productos, el más idóneo en cada caso".

Reconoce el directivo que en los meses que Kyndryl lleva funcionando como empresa independiente "nos hemos tenido que poner al día, pero el negocio de seguridad no ha parado y lo hemos unido al de resiliencia".

El peso de que tiene esta práctica de Seguridad y Resiliencia dentro de Kyndryl es "importante", porque, como comenta Ordóñez, la trayectoria en gestión de infraestructuras de la matriz, y por lo que ha sido conocida, siempre ha incluido la resiliencia y tenido en cuenta la seguridad. Asegura también que actualmente cualquier contrato de Kyndryl de gestión, desde lo más sencillo al outsourcing completo, "siempre suma seguridad y

"Lo que el cliente demanda es continuidad de negocio y continuidad de las operaciones"

resiliencia", incluyendo servicios de recuperación, de backup, de alta disponibilidad, etc.

¿Por qué se agrupa seguridad y resiliencia? Explica el directivo que la razón viene de escuchar a los clientes, que lo que demandas es "continuidad de negocio y continuidad de las operaciones, y nos parecía que nuestro framework, nuestro marco de trabajo, unía ambas cosas". El objetivo, asegura Ordóñez, es ofrecer a nuestros clientes, resiliencia operacional, "y eso significa que tus operaciones sean continuas en todo momento, independientemente del riesgo que tengas que abordar".

Para Miguel Ángel Ordóñez hace unos años la necesidad de continuidad estaba más asociada a negocios críticos o entornos de banca, pero ahora "cualquier negocio tiene necesidad de continuidad, y queremos ser lo líderes para ellos en resiliencia operacional, y hablarles tanto de seguridad como de respuesta y recuperación cuando lo necesiten".

La práctica de Seguridad y Resiliencia engloba todo lo que una empresa pueda necesitar, desde ayudar a una empresa a definir políticas de seguridad a temas de cumplimiento, seguridad perimetral, gestión de identidades y accesos y privilegios, tecnologías Zero Trust… En la parte de Seguridad Gestionada se trabaja con múltiples herramientas de monitorización y se están incorporando Inteligencia de Amenazas al tiempo que se intenta ser

"La filosofía de Kyndryl es abordar cualquier proyecto de transformación en cualquier cloud de una manera totalmente agnóstica e imparcial"

más proactivo. En este sentido, aclara Ordóñez, "si antes con IBM estábamos gestionando una herramienta, ahora estamos gestionando cinco en los meses que llevamos, lo que demuestra que no nos atamos a un producto". Aclara también el directivo que el objetivo no es la reventa ni asociarse a una marca, sino "dar el servicio más completo posible alrededor de la tecnología que mejor se adapte en ese momento. En la parte de servicios de recuperación se da mucha importancia a los planes de respuesta.

Clientes

"En Kyndryl abordamos todos los mercados y todos los tamaños" de clientes, asegura Miguel Ángel Ordóñez, añadiendo que ahora el cliente tipo es aquel que está en algún proceso de transformación digital y que quiere hacer esa transformación de manera segura, que es algo "que se ha acentuado desde la pandemia".

Es, además, "un cliente que quiere dejarse aconsejar por un socio que conozca su segmento, su regulación… y que requiere de unos altos niveles de servicio".

La tradición heredada de IBM les lleva a moverse en segmentos de gobierno, banca, seguros, pero se refuerza la presencia en retail o el cliente industrial, que está creciendo mucho y es muy variopinto, porque puede ser desde una eléctrica a una fábrica.

Partners

"No trabajamos con una única marca, y eso ha sido una liberación", dice Migue Ordóñez cuando le preguntas qué productos, qué fabricantes, están por debajo de los servicios que ofrecen. Asegura el directivo que la nueva aproximación está dando más confianza a los clientes porque para una necesidad se contará con la solución más adecuada.

No significa que se empiece de cero. Explica el directivo que ya saben qué partner se ajusta a cada caso y que hay un grupo de Alianzas encargado de contactar con gran parte del mercado… "y nuestra lista de partners ha crecido muchísimo". Al respecto, y sin dar nombres concretos, la lista incluye tanto nombres tradicionales como otros más de nicho.

Enlaces de interés…

- 'Hay muchas de empresas de seguridad, pero nuestra experiencia en redes nos da una habilidad única' (Dhrupad Trivedi, A10 Networks)
- 'Somos el sueño del operario de las herramientas' (Álex López, Gigamon)
- 'Muchas organizaciones tienen todavía programas de seguridad de APIs inmaduros, o carecen de ellos' (Salt Security)
- 'Con la aparición de la computación cuántica la infraestructura debe evolucionar para proteger las claves criptográficas' (Utimaco)

Compartir en RRSS

Forcepoint ONE

Welcome to the power of ONE

ONE Platform

ONE Console

ONE Agent

Forcepoint

www.forcepoint.com

‘Los alumnos de ciber son muy vocacionales. Tienen una mentalidad muy analítica y una tendencia hacia la administración sistemas’

(Javier García Algarra, U-tad)

Dentro de lo que se conoce como “Máster de FP”, el Centro Universitario U-tad ha estrenado este curso una formación en ciberseguridad que el próximo año se ampliará a Big Data y realidad Virtual. De esto y otras cosas hablamos con Javier García Algarra, director académico en U-tad.

U-tad es un Centro Universitario adscrito a la Universidad Camilo José Cela, aunque autónomo en la configuración académica de los programas de educación. Nació hace once años en torno a la industria de la animación y el videojuego, cuando “no se encontraban profesionales formados en esos terrenos”. Nos lo cuenta Javier García Algarra, director académico en

U-tad, un ingeniero en Telecomunicación y Doctor en Física de los Sistemas Complejos, Doctor en Historia, y que ha sido responsable durante más de 20 años de analítica y reporting de la Operación de Servicios Globales (Video, IoT, Cloud) del Grupo Telefónica.

De esa pasión por la animación y los videojuegos U-tad se expandió hacia otras dos áreas: ingeniería y diseño. Una de las cualidades que diferencian a U-tad de otras universidades es su cercanía con la industria, y si algo hace falta en la industria es talento en torno a las TI y, de manera más específica, en ciberseguridad. Javier García Algarra se hizo cargo de la dirección del área de ingeniería hace tres años y desde el verano es el director académico de U-tad, que cuenta con 1.800 alumnos.

Dentro del área de Ingeniería el grado con más historia es el de Ingeniería del Software. Se trata de un grado de cuatro años que U-Tad quiso especializar en software porque “pensábamos que un grado más especializado podía colocar mejor a los alumnos para lo que demanda ahora mismo la empresa”.

Dentro del grado de Ingeniería del Software hay tres especialidades, o menciones, que se escogen a partir del tercer curso: Ciberseguridad, Ciencia de Datos e Inteligencia Artificial y un tercero de programación gráfica, realidad virtual y desarrollo de videojuegos

La mención en ciberseguridad, con 90 créditos, cubre todas las áreas básicas de la ciberseguridad,

"En casos como desarrollo software y la especialización de ciberseguridad, o estás en la industria o cualquier cosa que cuentes de hace tres o cuatro años ha quedado obsoleta"

incluido hacking ético, bastionado, análisis forense, desarrollo de aplicaciones seguras… “básicamente lo que debería conocer cualquier especialista generalista de la ciberseguridad”.

La mitad de los alumnos de Ingeniería Software eligen ciberseguridad; “es la que más demanda tiene y la empleabilidad es del 100%. Ahora mismo están terminando la promoción entre 25 y 30 alumnos”, comenta Javier García Algarra añadiendo que todos los que han acabado en los últimos años “están trabajando en empresas especializadas en ciber, consultoras o el sector financiero, que tira bastante de profesionales de ciberseguridad”.

Especializaciones

Además del grado de formación universitaria de cuatro años, este curso U-tad ha estrenado un nuevo programa, que son las Especializaciones “para alumnos que han terminado un ciclo formativo de grado superior”; es lo que algunos conocen como los “Máster de FP”, que no es otra cosa que una formación de post grado para alumnos ciclo formativo de Grado Superior de FP.

Esta formación, presencial y de 700 horas, cumple con los planes educativos de la Comunidad de Madrid para el establecimiento del programa de especialización de FP. Curiosamente, este programa de especialización apuesta por las tres menciones que establece U-tad en su Ingeniería del Software: Ciberseguridad, Big Data y Realidad Virtual.

El programa de esta especialización cubre los tres grandes ejes de la ciberseguridad: la parte de ataque, o hacking ético; la parte de defensa, que se centra en el bastionado y desarrollo de

"La mitad de los alumnos de Ingeniería Software eligen ciberseguridad. Es la que más demanda tiene y la empleabilidad es del 100%"

U-tad nació hace once años en torno a la industria de la animación y el videojuego, cuando no se encontraban profesionales formados en este terreno

aplicaciones seguras; y tiene una parte de desarrollo forense y normativa de seguridad.

Con el fin de dar la opción a los alumnos universitarios a este tipo de cursos de especialización, el centro universitario U-tad trabaja en un programa, que estará activo el próximo curso, y que será “una versión reducida y más adaptada a alumnos que hayan podido usar un grado universitario y lo ofreceremos como título propio”.

En ese afán de estar lo más cerca de la industria posible con el objetivo de ofrecer a los alumnos una formación totalmente adaptada a las demandas y necesidades del tejido industrial prácticamente todos los profesores “están trabajando también en el sector. Tratamos de que la mayoría de nuestros profesores, en todos los cargos que tenemos, tengan experiencia en la industria”, de forma que están muy al tanto de lo que está ocurriendo en el mercado. “En casos como desarrollo software y la especialización de ciberseguridad, o estás en la industria o cualquier cosa que cuentes de hace tres o cuatro años ha quedado obsoleta”, asegura Javier García Algarra.

Ciberseguridad manda

Comenta el director académico de U-tad que los alumnos de Ingeniería del Software tienen claro lo que escogen en tercero. La mitad, como ya hemos comentado en el artículo, escogen Ciberseguridad y a Javier García Algarra “que soy más de la parte de datos e inteligencia artificial, a veces me da un poco de rabia que algún alumno brillante tire más para la parte de ciber”. Añade que los alumnos de

ciber “son muy vocacionales. Tienen una mentalidad muy analítica y una tendencia hacia la administración y herramientas de sistemas”, mientras que los más creativos tienden hacia programación gráfica o datos.

Planteado si se colaboran con fabricantes de ciberseguridad, nos cuenta el directivo que existe un Comité Industrial que se reúne una o dos veces al año con representantes de la industria para preguntarles qué es lo que necesitan, “qué tipo de perfil o formación”; además, existen convenios para hacer prácticas. Destacar en este punto que se mantiene la independencia de herramientas concretas trabajando con productos opensource.

Enlaces de interés...

- U-tad
- Los cinco ciberataques que te pueden estropear el verano
- SilentForce, el arte de la ciberseguridad

Dentro del grado de Ingeniería del Software hay tres especialidades, o menciones, que se escogen a partir del tercer curso: Ciberseguridad, Ciencia de Datos e Inteligencia Artificial y un tercero de programación gráfica, realidad virtual y desarrollo de videojuegos

Sobre la visión que se tiene de un profesional de ciberseguridad, comenta el director académico de U-tad que se les suele ver como frikis con poca vida social, “un poco lo que han presentado las películas que, por una parte, les da cierto aire romántico y aventurero porque lo que hacen es algo mágico”. En la vida real, “son ingenieros tan normales como puede ser cualquier otro”. Este comentario, quizá obvio para los que nos movemos, de una manera más o menos profunda, en el mundo cíber, está más dirigido a muchos padres que en las jornadas de puetas abiertas que se celebran en U-tad, descubren la realidad.

Una realidad, por cierto, en la que la brecha de género es enorme. “hacen falta mujeres en el campo de la ciberseguridad porque necesitamos muchos puntos de vista, muchas maneras de pensar para adelantarte a los ciberdelincuentes”.

Compartir en RRSS

STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

www.stormshield.com

it Digital Security

Desayunos ITDS

Estrategias de seguridad, de la gestión del riesgo al Incident Response

Diciembre 2022

Desayunos ITDS

Está claro por qué una empresa debe invertir recursos y establecer un programa de respuesta a incidentes. Sólo hay que pensar en el impacto en una corporación que sufre un desastre sin haberse preparado para ello. La respuesta a incidentes es un proceso continuo, un ciclo de vida que requiere una estrategia de mitigación de riesgos que cubra los riesgos operativos, legales y de reputación. ¿Por dónde empezar?

Con el objetivo de saber que está impulsando el mercado de gestión de riesgos, que impacto tuvo la pandemia en los planes de respuesta ante incidentes o si el cloud es reto o aliado en los planes de respuesta ante incidentes se ha celebrado un nuevo Desayuno ITDS en el que han participado Sergio Martínez, Regional Manager de SonicWall Iberia; José Luis Paletti, Senior Sales Engineer de WatchGuard y Borja Pérez, Country Manager Iberia de Stormshield.

Arrancamos el encuentro pidiendo a nuestros invitados cuáles son los principales riesgos a los que se enfrenta una empresa. En opinión de Sergio Martínez, aunque se está percibiendo una disminución en el ransomware a consecuencia de que los ataque son más dirigidos, “por el contrario, vemos un incremento bastante interesante de las amenazas encriptadas”. Ello es consecuencia de que el 70% del tráfico en las empresas está encriptado. Por ello, opina Sergio Martínez que hay que reforzar las estructuras y desarrollar una nueva por si el firewall, siendo el elemento más importante de la ciberdefensa, fallase en el análisis del tráfico posterior.

Siguiendo con la opinión de su compañero, dice Borja Pérez, Country Manager Iberia de Stormshield que las organizaciones no solo van a tener el cifrado en las comunicaciones, “sino que quieren también cifrar los datos, correro, etcétera, pues esas comunicaciones VPN no son tan seguras”. En cuanto a los riesgos, para Borja Pérez el principal es desconocer tus propios activos.

José Luis Paletti, Senior Sales Engineer de WatchGuard, comentaba que a raíz de la pandemia y la descentralización del trabajo fuera de la oficina, el riesgo de los ataques se centró en gran medida en los endpoint que estaban fuera de la red.

Continuamos el encuentro preguntando a los invitados qué es lo que deben hacer las organizaciones para impulsar la gestión de riesgos, y por dónde tendrían que empezar. Borja Pérez, conectando con su anterior respuesta, reitera que es imprescindible conocer qué activos tiene esa

"La estrategia para minimizar los riesgos es una defensa por capas"

Sergio Martínez,
Regional Manager, SonicWall Iberia

organización, y cuáles son más importantes para el negocio. Entender dónde están los activos, cuales son más valiosos, el procedimiento para protegerlos y recuperarlos, es esencial. No pasa por verlo solo desde un punto de vista técnico, sino desde un punto de vista de negocio y de operativa del mismo".

Continúa José Luis Paletti comentando que esta identificación de los activos no es tan sencilla, dada la gran cantidad de equipos en la nube. Efectivamente y como apuntaba el directivo de WatchGuard para Iberia, unos son más críticos que otros. Por ello, crear políticas adecuadas alrededor de esos entornos, aplicando las metodologías y configuraciones adecuadas es importante. Resume José Luis Paletti los tres puntos más importantes: identificación, creación de políticas y una correcta configuración que funcione.

Sergio Martínez, enfocó su respuesta de manera diferente a la de sus compañeros, compartiendo que la nueva gestión de riesgos ha cambiado, porque el nuevo entorno, como consecuencia de la pandemia, y la digitalización acelerada, ha cambiado todo, y los riesgos se están incrementando, los que según Sergio "cambia el paradigma de ciberseguridad". Se ha pasado de tener un entorno muy controlado, a "estar todos en la calle con portátil y smartphones recibiendo mails de todo tipo". Para Sergio Martínez, la mejor estrategia es una defensa con diferentes barreras y por capas.

Continuamos el encuentro lanzando una nueva pregunta a nuestros invitados, esta vez pedimos que compartan el papel que juega el empleado, normalmente catalogado como el eslabón más débil. Comienza José Luis Paletti esta ronda de respuestas diciendo que en muchas ocasiones el empleado carece de la formación adecuada como para distinguir un ataque de un correo correcto. Por ello, la concienciación y formación al empleado en diferentes entornos es esencial. Añade Sergio Martínez que, en este nuevo modelo de trabajo híbrido, hemos pasado a tener unas empresas muy distribuidas, y por ello la defensa del endpoint es tan importante, donde el empleado con una formación apropiada debe gestionar los riesgos.

DE LA GESTIÓN DEL RIESGO AL INCIDENT RESPONSE

CLICAR PARA VER EL VÍDEO

Añade Borja Pérez que, efectivamente, es esencial darle una correcta formación al empleado, que incluya no solo conceptos, sino incluso soluciones. No obstante, reconoce que sigue siendo un punto de riesgo.

Se plantea también durante el debate que para muchos la transformación digital debe de ir de la mano de una gestión correcta de riesgos, y se les pregunta a nuestros invitados si eso se está viendo reflejado en el mercado, o todavía va desacompasado. Sergio Martínez reitera que la transformación digital de la que hablamos está siendo muy rápida. Menciona el gap que existe entre la transformación acelerada y los recursos de las empresas para afirmar que hay mucho por hacer, mucho por construir.

Añade Borja Pérez a la respuesta de su compañero que “aunque se haya elevado el nivel de concienciación, sigue siendo complicado sacar presupuestos de ciberseguridad en las empresas”. José

"Los diferentes proveedores de servicios en cloud tienen sus propias medidas de seguridad"

José Luis Paletti,
Senior Sales Engineer, Watchguard

"Entender dónde están los activos, cuáles son más valiosos, el procedimiento para protegerlos, y recuperarlos, es esencial"

Borja Pérez, Country Manager Iberia, Stormshield

Luis Paletti coincide en que los presupuestos varían dependiendo del tamaño de la empresa.

Sobre el impacto de la pandemia en la respuesta ante incidentes, comenta Borja Pérez que todo pasa por tener un backup correcto y, en el caso de ataque, poder recuperarlo. José Luis Paletti aporta que esa concienciación de necesidad de mejora tras la pandemia, se quedó en intento; "aunque es cierto que muchas empresas han tomado nota de lo vivido y aprendido con la pandemia, globalmente lo que se aprendió principalmente fue a reconocer el nuevo perímetro".

Para Sergio Martínez a nivel de comunicación si ha habido mejoras en lo que a la comunicación de los incidentes se refiere.

Igual que la seguridad pasó de ser una barrera para la adopción del cloud a un habilitador, se plantea a los habilitadores si la nube es barrera o habilitador de la respuesta ante incidentes. José Luis Paletti, no duda en contestar que para él es un reto, "porque además los diferentes proveedores de servicios en cloud tienen sus propias medidas de seguridad". Según el directivo de WatchGuard falta mucho para poder avanzar en ese sentido.

Para Sergio Martínez las credenciales "son la joya de la corona en el cloud". Asegura además que la nube es un reto porque, entre otras cosas, no te puedes fiar de la seguridad de los proveedores. En cuanto a Borja Pérez, también opina que la nube, aunque aporta algunos valores, es un reto ya que añade superficie de ataque.

Enlaces de interés...

- De la gestión del riesgo al incident response

Compartir en RRSS

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

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

Digital Security
Progress. Protected.

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Grandes ciberataques en 2022. La ciberseguridad no puede dejarse de lado

Ciberseguridad, ciberseguridad y ciberseguridad. Para bien o para mal, ha sido y es uno de los conceptos protagonistas en el ranking de términos tecnológicos de 2022, y con mucha probabilidad seguirá siendo una de esas palabras que formará parte de nuestro vocabulario habitual en el futuro.

Texto: E. Frechoso Muñoz

Ya sea porque las empresas están invirtiendo más en proteger sus infraestructuras y datos, porque hay mayor concienciación, porque la ciberseguridad está relacionada con todos y cada uno de los ámbitos de nuestro día a día -tanto en los negocios como en la vida del usuario de a pie-, porque es un sector que genera empleo, o porque se habla de ciberseguridad en lo que respecta a la falta de profesionales, o cómo no, porque los incidentes, las amenazas, la explotación de vulnerabilidades y los ciberataques a todo tipo de entidades y organizaciones han crecido de una forma brutal y no ha habido un solo mes del año en que no hayamos sido testigos de titulares que se hacían eco de estos incidentes. Por todo esto y mucho más, la ciberseguridad es, en opinión de muchos expertos, protagonista indiscutible en el sector TIC y en tantos otros.

En un mundo digital e hiperconectado, en el que los avances tecnológicos se suceden de forma tan rápida, el número de ciberataques no deja de aumentar. La explicación es obvia: el radio de acción cada vez es mayor y la superficie de ataque no deja de crecer. Y es que estos ataques pueden comprometer todo tipo de información, poniendo en jaque a empresas, particulares y gobiernos. Las amenazas bloqueadas por los fabricantes de seguridad y entidades gubernamentales ya no se cuentan por miles, sino por miles de millones. Esto se traduce en mayor riesgo de sufrir un ataque. Según el informe anual de ciberseguridad de 2021 de Trend Micro, las amenazas bloqueadas por la compañía aumentaron un 42% respecto al año anterior, hasta superar los 94.000 millones. Cifras como estas resultan difíciles de imaginar, de digerir y, por supuesto, de

El ritmo al que las empresas, sin importar su tamaño, están experimentando violaciones de ciberseguridad, resulta alarmante

gestionar, y solo ponen de manifiesto la espiral de riesgos para la infraestructura digital y los trabajadores remotos a medida que los actores de amenazas aumentan su ritmo de ataque a organizaciones e individuos.

Los atacantes siempre están trabajando para aumentar su número de víctimas y sus beneficios, ya sea a través de cantidad o de la eficacia de los ataques que lanzan. Identificar los cambios en la forma en que los actores maliciosos se dirigen y atacan a sus víctimas en todo el mundo se ha convertido en una ardua labor.

Pero ¿por qué ocurren los ciberataques?

Las motivaciones pueden variar. Además de la ciberdelincuencia, los ciberataques también suelen estar asociados a la guerra cibernética o al ciberterrorismo, aunque podríamos clasificar estas motivaciones en tres grupos principales: delictivas, políticas y personales. Otros motivos detrás de los ciberataques incluyen el espionaje para obtener una ventaja indebida sobre los competidores, y el desafío intelectual.

Organizaciones delictivas, actores estatales y grupos particulares pueden estar detrás de los ciberataques, quienes recurren a un sinfín de técnicas como el robo de credenciales, el phishing, ransomware, ingeniería social, business email compromiso (BEC), mala configuración de la nube, explotación de vulnerabilidades en el software de terceros, el aprovechamiento de sistemas no parcheados adecuadamente, etc. para perpetrar estos ciberataques.

Veamos a continuación algunos de los mayores ataques, brechas de datos e incidentes de ciberseguridad más sonados de 2022. No se trata de una

lista exhaustiva, pero sí puede ayudar a hacerse una idea de lo que sufrir un ataque supone y el colapso que esto puede crear.

Enero de 2022

Brecha en Crypto.com

El modelo blockchain ha sido considerado durante mucho tiempo como una de las formas más seguras de procesamiento de transacciones. Sin embargo, esto no ha impedido que los hackers intenten comprometer las transacciones basadas en cripto. Esto es evidente en el ataque del 17 de enero de 2022 que tuvo como objetivo las carteras de 483 usuarios en Crypto.com.

Como parte de este hackeo, los quienes estaban detrás de este robo se hicieron con alrededor de 18 millones de dólares en Bitcoins y 15 millones de dólares en Ethereum, además de otras criptomonedas. Esto fue posible principalmente gracias a la capacidad de los hackers para saltarse la autenticación de doble factor y acceder a las carteras de los usuarios.

Crypto.com, que en un principio lo calificó como un mero “incidente”, se retractó más tarde, confirmando que el dinero había sido robado y que los usuarios afectados habían sido reembolsados. La empresa también declaró que había auditado sus sistemas y trabajado para mejorar su postura de seguridad.

Las empresas deben ser conscientes de los riesgos asociados al robo de criptomonedas. La mejor manera de protegerse contra este tipo de fraude es asegurarse de que todos los datos sensibles están cifrados.

Brecha de datos en Cruz Roja

En enero de 2022, unos hackers atacaron los servidores que albergaban la información personal de más de 500.000 personas que recibían servicios del Movimiento de la Cruz Roja y de la Media Luna Roja. Los servidores hackeados contenían datos relacionados con los servicios de Restablecimiento del Contacto entre Familiares de la organización, que trabaja para reconectar a personas separadas por la guerra, la migración y la violencia. La Cruz Roja desconectó los servidores para detener este presunto ataque de un Estado nacional, aunque no se ha identificado definitivamente al culpable.

¿Cuánto cuesta una brecha de seguridad en los datos en 2022?

Los costes de las brechas de seguridad en los datos aumentaron un 13% de 2020 a 2022, según queda reflejado en el informe anual "Cost of a Data Breach 2022" de IBM Security y realizado por Ponemon Institute

Entre las principales conclusiones del estudio se encuentran las siguientes:

- El coste medio de una vulneración de datos fue de 4,35 millones de dólares en 2022, un récord histórico. Esta cifra representa un aumento del 2,6% con respecto al año pasado, cuando el coste medio fue de 4,24 millones de dólares. El coste medio ha aumentado un 12,7% con respecto a los 3,86 millones de dólares del informe de 2020.
- El 83 % de las organizaciones estudiadas han sufrido más de una vulneración de datos y tan solo el 17% dijo que fue la primera. El 60% de las organizaciones estudiadas afirmó que aumentaron el precio de sus servicios o productos como consecuencia de dichas vulneraciones.
- El coste medio de una vulneración de datos para las empresas de infraestructura crítica analizadas fue de 4,82 millones de dólares, un millón más que el coste medio para las organizaciones de otros sectores. Entre las empresas de infraestructura crítica se incluyeron las de servicios financieros, industriales, tecnología, energía, transporte, comunicación, sanidad, educación y sector público. El 28% experimentó un ataque destructivo o de ransomware, mientras que el 17% experimentó una vulneración al verse comprometido uno de sus socios.
- Las brechas en organizaciones que emplean IA y herramientas de automatización, cuestan 3,05 millones de dólares menos que en aquellas que carecen de estos recursos.
- Las organizaciones que cuentan con un equipo de respuesta de incidencias y que revisan su plan de respuesta con regularidad, se ahorraron una media de 2,66 millones de dólares.
- Las organizaciones que han implantado una arquitectura zero trust, se gastan un millón menos de media en brechas.
- Las tecnologías de detección y respuesta ampliada, contribuyen a ahorrar una media de 29 días en tiempo de respuesta.
- El 45% de los ataques del estudio ocurrieron en el cloud. Los ataques que ocurrieron en un ambiente de cloud híbrido costaron una media de 3,80 millones de dólares, frente a los 4,24 millones de los ataques en clouds privados y los 5,02 millones en clouds públicos.

Febrero de 2022:

Brecha en GiveSendGo

El reciente secuestro de un sitio cristiano de recaudación de fondos, GiveSendGo, tuvo lugar en respuesta a las protestas de los camioneros de Ottawa, y tuvo como resultado que los datos personales de quienes donaron a sus fondos se vieran comprometidos.

Los hackers redirigieron el sitio de recaudación de fondos a una página que condenaba las protestas de Freedom Convoy, un caso de ataque de denegación de servicio distribuido (DDoS). A continuación, publicaron los datos personales de los 90.000 donantes que habían contribuido a la iniciativa a través del sitio web de GiveSendGo.

¿Qué revela este incidente? Esta brecha pone de manifiesto lo importante que es asegurarse de que las empresas emplean métodos y plataformas de pago seguros. Si no es así, los datos de sus clientes podrían verse fácilmente comprometidos.

UpdateAgent: el malware para Mac se sofistica

El dicho de que los productos de Apple son los más seguros volvió a cuestionarse. De hecho, ya cuentan con diversas amenazas que los hackers cada vez sofistican más. UpdateAgent, lo que empezó siendo un ladrón de información bastante básico, ganaba en peligrosidad para convertirse en un distribuidor de carga útil de segunda etapa. Inicialmente se encargaba de recopilar nombres de productos, números de versión y otra información básica del sistema. Además, su capacidad de ejecución cuando se iniciaba un Mac era muy rudimentaria.

El equipo de inteligencia de amenazas de Microsoft 365 Defender alertaba de que UpdateAgent ahora era capaz de mandar una suerte de 'latidos' que permitían a los atacantes cerciorarse de si el malware seguía funcionando. En la última campaña, el malware instaló el evasivo y persistente adware Adload, pero la capacidad de UpdateAgent para obtener acceso a un dispositivo teóricamente

Países enteros pueden quedar paralizados si no se han invertido los recursos adecuados en la preparación para los ataques de ransomware

puede aprovecharse aún más para obtener otras cargas potencialmente más peligrosas, tal y como aseguraban los investigadores.

Guerra Rusia-Ucrania

Redes eléctricas, infraestructuras de Internet, bancos… No es un secreto que Rusia lleva muchos años lanzando ataques digitales contra infraestructuras ucranianas provocando apagones eléctricos, tratando de sesgar las elecciones, robando datos y utilizando malware para atacar al país y al mundo. A finales de febrero los ataques pasaron al plano físico y con el estallido de la guerra la dinámica digital de ciberataques se intensificó entre los dos países poniendo el foco en los sistemas relacionados con el gobierno y el ejército. Esto significa que mientras Rusia ha seguido atacando las instituciones e infraestructuras ucranianas con ciberataques, Ucrania también ha reaccionado. Aunque hablar de ciberguerra no es nuevo, si es cierto que los conflictos cibernéticos ofrecen la oportunidad de tomar el pulso y medir la eficacia de las estrategias y tácticas, así como de las propias armas técnicas.

Así, Ucrania formó un "Ejército de TI" voluntario al comienzo de la guerra, que se centró en los ataques DDoS y los ataques disruptivos contra las instituciones y los servicios rusos para causar el mayor caos posible. Igualmente, hacktivistas de todo el mundo también han puesto su foco en el conflicto. Y como Ucrania utiliza otros métodos de piratería contra Rusia, incluidos los ataques con malware personalizado, los rusos han sufrido brechas de datos e interrupciones del servicio en una escala sin precedentes.

Marzo de 2022

Violación de datos de Microsoft

El 20 de marzo de 2022, Microsoft fue el objetivo de un grupo de hackers llamado Lapsus$. El grupo publicó una captura de pantalla en Telegram indicando que habían hackeado a Microsoft y, en el proceso, comprometieron Cortana, Bing y algunos otros productos. Pero el 22 de marzo Microsoft anunció que había detenido rápidamente el intento de hackeo y que solo una cuenta había sido comprometida. Microsoft también declaró que no se habían robado datos de clientes. En este caso, Microsoft se benefició de la publicidad que recibió por su eficaz respuesta de seguridad. Lapsus$ había atacado anteriormente a Nvidia, cuando consiguieron sustraer 1 TB de información confidencial al colarse en el sistema de servidores de correo electrónicos de la compañía y los interceptaron. Después de esto, fue la propia NVIDIA quien contraatacó a los criminales con un ransomware que cifró sus discos duros tras infectar sus ordenadores, y así la información robada quedó encriptada y completamente inaccesible para ellos. Samsung y a muchas otras organizaciones, también habían sido víctimas de Lapsus$ por

lo que el equipo de seguridad de Microsoft estaba preparado.

Suceso en Toyota

Otro incidente destacado es el que afectó a Toyota: entre febrero y marzo de 2022, tres proveedores de Toyota fueron hackeados, lo que demuestra que, por muy segura que sea una organización, un actor de amenaza decidido puede encontrar, y encontrará, la forma de entrar.

Cuando el proveedor de Toyota, Kojima Industries, sufrió un ciberataque (no necesariamente un ataque de ransomware), el gigante tuvo que detener las operaciones en 14 de sus plantas japonesas. Se dice que este hackeo causó una enorme caída del 5% en la capacidad de producción mensual de la empresa.

Abril de 2022

Ronin

Uno de los atractivos de las criptomonedas es que no se "guardan" en un banco tradicional, sin embargo, muchas redes de criptomonedas no tienen la seguridad necesaria para protegerse de una brecha de datos. En abril de 2022, Ronin informó que fueron hackeados por 540 millones de dólares. No solo perdieron ese dinero, sino que también tuvieron que reembolsar a sus clientes la cantidad que perdieron.

Este es el segundo mayor hackeo de criptomonedas de todos los tiempos, y seguramente no será el último. Aunque la perspectiva de acumular más riqueza en criptomonedas y de que los tokens no fungibles aumenten su valor es atractiva, es importante evaluar los protocolos de ciberseguridad de la red de criptomonedas para asegurarse de que los activos no se vean afectados por una brecha de datos.

Desarticulación de Zloader

La Unidad de Crímenes Digitales de Microsoft (DCU) llevó a cabo una operación junto a ESET, Black Lotus Labs y la Unit 42 de Palo Alto Networks que dio como resultado la desarticulación de una red cibercriminal llamada ZLoader. El malware que daba nombre a la red empezó su vida como un troyano bancario inspirado en Zeus, pero evolucionó con el tiempo y los ciberdelincuentes comenzaron a utilizar la técnica de malware como servicio para distribuir varias familias de ransomware, entre ellas el peligroso Ryuk. Durante los últimos

Debemos asegurarnos de que las empresas emplean métodos y plataformas de pago seguros

El 20 de marzo de 2022, Microsoft fue el objetivo de un grupo de hackers llamado Lapsus$

tres años atacó a empresas, hospitales, colegios y usuarios particulares.

Tras conseguir una orden judicial, Microsoft eliminó docenas de dominios utilizados como servidores de comando y control por la notoria botnet ZLoader, también confiscó 65 dominios codificados utilizados para controlar la botnet y otros 319 dominios registrados utilizando el algoritmo de generación de dominios utilizado para crear canales de comunicación alternativos y de respaldo.

Mayo de 2022:

Ransomware Conti: el Gobierno de Costa Rica declara el estado de emergencia

Con toda probabilidad este ha sido el ataque del que más se ha hablado en 2022, ya que es la primera vez que un país se vio abocado a declarar una emergencia nacional en respuesta a un ciberataque. El primer ataque de ransomware al país comenzó a principios de abril y tumbó al Ministerio de Hacienda, afectando no solo a los servicios del gobierno sino también al sector privado dedicado a la importación/exportación.

El grupo de ransomware Conti asumió la responsabilidad del primer ataque, pidiendo al gobierno el pago de un rescate de 10 millones de dólares, que posteriormente aumentó a 20 millones.

El 31 de mayo, un nuevo atentado desestabilizó el sistema sanitario del país. Este ataque, vinculado al grupo de ransomware Hive, afectó a la caja de la seguridad social costarricense. Este ataque afectó directamente al ciudadano de a pie, ya que dejó fuera de servicio los sistemas de salud del país.

Si bien los matices políticos y las implicaciones de este ataque son muchos y la cronología de la forma en que se desarrolló el ataque puede llenar páginas, la idea de incluir este ataque en esta lista es mostrar los resultados profundos y perjudiciales que un ataque de ransomware puede tener en los organismos gubernamentales.

Queda demostrado lo peligroso que puede ser un ataque de ransomware. Países enteros pueden quedar paralizados si no se han invertido los recursos adecuados en la preparación para los ataques de ransomware, si no se cuenta con las soluciones de protección y la formación en ciberseguridad de los empleados, miembros del personal, etc. para responder a estos ataques.

Junio de 2022:

Filtración de datos de Shields Health Care Group

El proveedor de servicios médicos con sede en Massachusetts, Shields Health Care Group (Shields), sufrió una brecha de datos que expuso

los datos de aproximadamente dos millones de pacientes en Estados Unidos después de que los hackers violaron su red y robaron datos. La información extraída se puede utilizar con fines de ingeniería social, phishing, estafas e incluso extorsiones, según el caso, y está considerada como información extremadamente sensible.

> Las amenazas bloqueadas por los fabricantes de seguridad y entidades gubernamentales ya no se cuentan por miles, sino por miles de millones

Una vez más Marriott

En 2014, Marriott sufrió una brecha de datos y se expusieron casi 340 millones de registros de clientes. Este incidente no se detectó hasta septiembre de 2018 y provocó una multa de 14,4 millones de libras de la Oficina del Comisionado de Información del Reino Unido. En enero de 2020, Marriott fue hackeado de nuevo, afectando a 5,2 millones de registros de huéspedes.

En junio de 2022, los hackers afirmaron haber conseguido más de 20 GB de datos confidenciales, incluidos los datos de las tarjetas de crédito de los huéspedes. Los atacantes recurrieron a la ingeniería social para engañar a un empleado de una propiedad de Marriott en Maryland para que les diera acceso a su ordenador. Marriott niega que los datos hayan afectado a más de 300-400 personas,

aunque se estaba poniendo en contacto con los afectados por el incidente.

Julio de 2022:

Ataque al CSIC

El Consejo Superior de Investigaciones Científicas (CSIC), fue víctimas en julio de un ciberataque masivo de tipo ransomware. El rasomware ha permitió a los ciberdelincuentes encriptar de forma compleja parte de la información que manejan tanto la sede central del CSIC como de sus centros e institutos repartidos por España. El ataque, además de paralizar la actividad de las 149 entidades bajo su paraguas, provocó robo de datos personales sensibles. Su delegado de protección de datos admitió que hubo filtración de datos, ya que el ciberataque afectó a expedientes con datos identificativos y de contacto.

Dos comunicados del CSIC y del Ministerio de Ciencia señalaban que fue un ransomware de origen ruso, sin concretar más nombres, ni añadir explicaciones sobre cómo se determinó la atribución a Rusia.

Días después de que el CSIC comunicara que no habían detectado pérdida de datos sensibles o confidenciales, Vice Society se atribuyó la autoría del ataque de ransomware y expuso centenas de documentos para su descarga en la deep web.

MaliBot

Un nuevo malware para Android se estaba dirigiendo a los clientes de banca online de España e Italia, y que tenía capacidad para robar las credenciales y cookies de los usuarios y eludir los códigos de autenticación multifactor (MFA). El malware MaliBot intenta pasar desapercibido tomando la apariencia de diferentes aplicaciones, como son las aplicaciones de minería de criptomonedas “Mining X” o “The CryptoApp”, así como de otro tipo de aplicaciones, como “MySocialSecurity” y “Chrome”.

Además de robar información financiera, credenciales, monederos de criptomonedas y datos personales (PII), MaliBot tiene capacidad para controlar de forma remota los dispositivos infectados utilizando una implementación de servidor VNC, tal y como informaban desde F5.

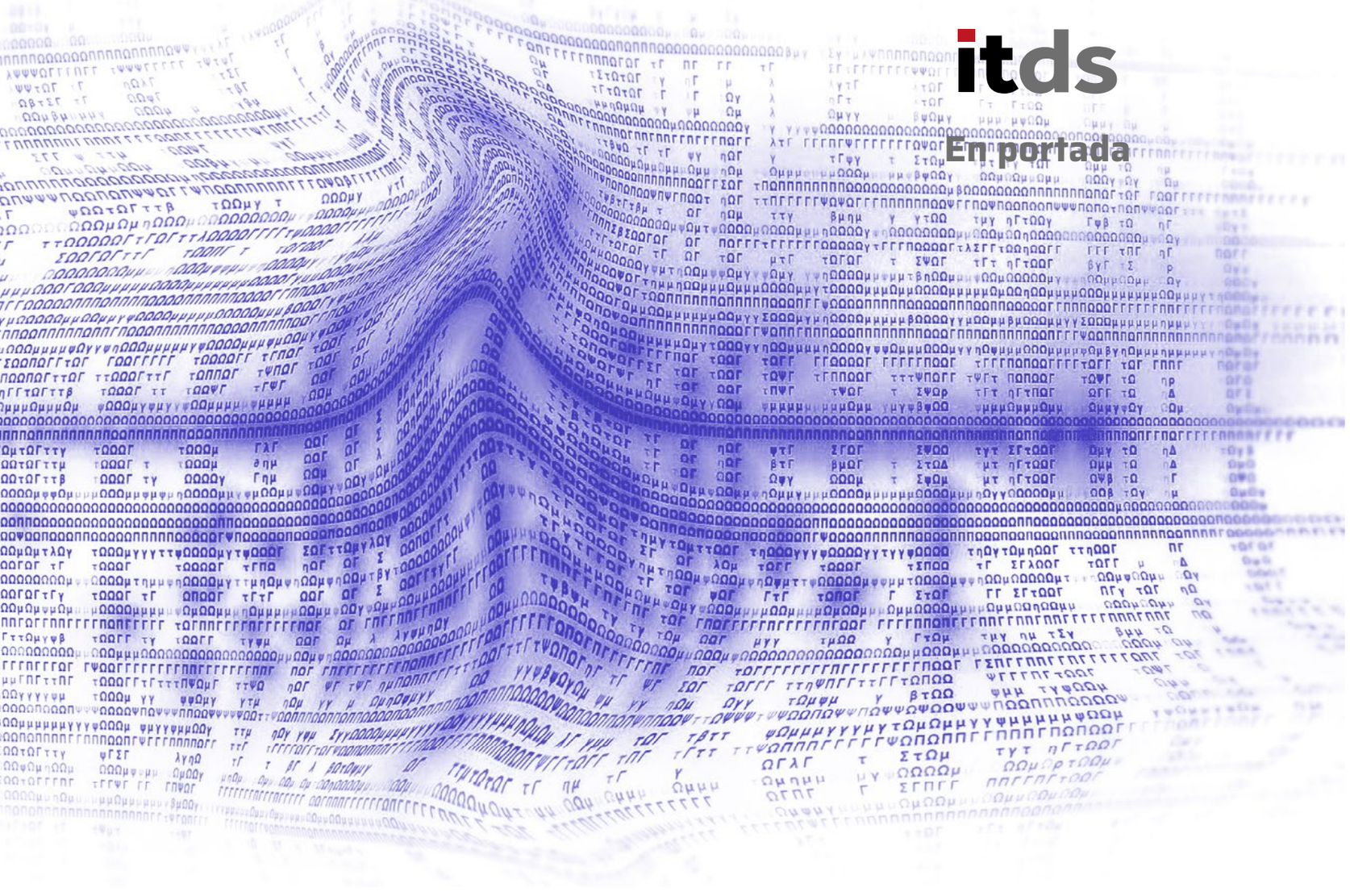
Agosto de 2022:

Plex

En agosto se produjo una filtración de datos en Plex, una aplicación de servidor multimedia utilizada por millones de personas, que puso en peligro los datos personales cifrados de sus clientes, incluyendo contraseñas, nombres de usuario y correos electrónicos. El acceso a la información personal de millones de personas puede dañar la confianza de una marca durante años.

Aunque la vulnerabilidad fue abordada, Plex sigue animando a sus clientes a restablecer sus contraseñas y activar la autenticación multifactor (MFA). De

En enero de 2020, Marriott fue hackeado de nuevo, afectando a 5,2 millones de registros de huéspedes



nuevo, esto debería ser una práctica ya habitual en 2022 -y a futuro- para protegerse contra las brechas de datos.

El ransomware mira a los MSP

En el Reino Unido, Advanced, un proveedor de servicios gestionados (MSP) del Servicio Nacional de Salud británico (NHS), sufrió un ataque de ransomware en agosto. El ataque provocó una importante interrupción de los servicios de emergencia del NHS en todo el Reino Unido. Advanced recurrió a Microsoft y a Mandiant para que le ayudaran con la clasificación y las investigaciones. En Estados Unidos, otro MSP, NetStandard, sufrió un ataque que le obligó a cerrar sus servicios en la nube “MyAppsAnywhere”.

Los MSP son objetivos tentadores para las bandas de ransomware porque tienen acceso a los datos de varias empresas y, por tanto, ofrecen múltiples fuentes potenciales de rescate. En el pasado, el conocido grupo REvil ya atacó a varios MSP.

Last Pass

El 25 de agosto, el proveedor de administración de contraseñas, Last Pass, utilizado por más de 30 millones de personas, anunció que un tercero había sido capaz de infiltrarse en su red accediendo a una cuenta de desarrollador comprometida. Según su CEO, Karim Toubba, un actor no autorizado habría robado “partes del código fuente y alguna información técnica patentada de Last Pass”. Esto significa que no se violaron los datos de los clientes y que las medidas de seguridad y cifrado de la compañía para las contraseñas de sus clientes cumplieron su cometido. Sin embargo, esta brecha de ciberseguridad llevó a Last Pass a contratar a un equipo externo y a trabajar para protegerse contra más brechas en el futuro.

Septiembre de 2022:

Uber

La compañía descubrió que había sido hackeada a mediados de septiembre por un adolescente después de que el hacker comprometiera la aplicación de mensajería Slack de un empleado y la utilizara para enviar un mensaje a los trabajadores de Uber anunciando que la empresa había sufrido una violación de datos diciendo: “Soy un hacker y Uber ha sufrido una brecha de datos” seguido de varios emojis. Esto hizo que la empresa cerrara su servicio de mensajería interna y sus sistemas de ingeniería para llegar al fondo del incidente.

Al parecer, recurrió a lo que se denomina un ataque de fatiga MFA, en el que una vez que se han obtenido las credenciales de un empleado, si la empresa emplea herramientas de autenticación multifactor (MFA), el atacante bombardea al empleado con solicitudes de autenticación, en su teléfono móvil. En un principio, el empleado las rechazaba, ya que no está iniciando sesión, pero en este caso el atacante acabó contactando con

Las empresas deben ser conscientes de los riesgos asociados al robo de criptomonedas

él a través de WhatsApp y haciéndose pasar por personal del ser del equipo técnico de Uber, le explicó que tenía que aceptar la solicitud de autenticación o seguirían llegando. Ante la insistencia de las peticiones el trabajador accedió. El hacker pudo entonces alterar la MFA añadiendo su propio dispositivo.

Tras esto, el atacante se conectó a través de la VPN corporativa y comenzó a buscar. Al poco tiempo encontró un script de Powershell que contenía las credenciales de administrador de la plataforma de gestión de accesos privilegiados (PAM) de la empresa, Thycotic. A partir de aquí, todas las credenciales importantes estaban disponibles.

El hacker detrás del ataque a Uber también afirmó que podía piratear varias bases de datos de la empresa, incluidos los datos de mensajería. Uber ya se había enfrentado a un ciberataque en el pasado y no lo denunció, lo que le llevó a una batalla legal y asumir importantes costes económicos. Esta vez tomaron se precauciones antes.

Octubre de 2022:

MediBank

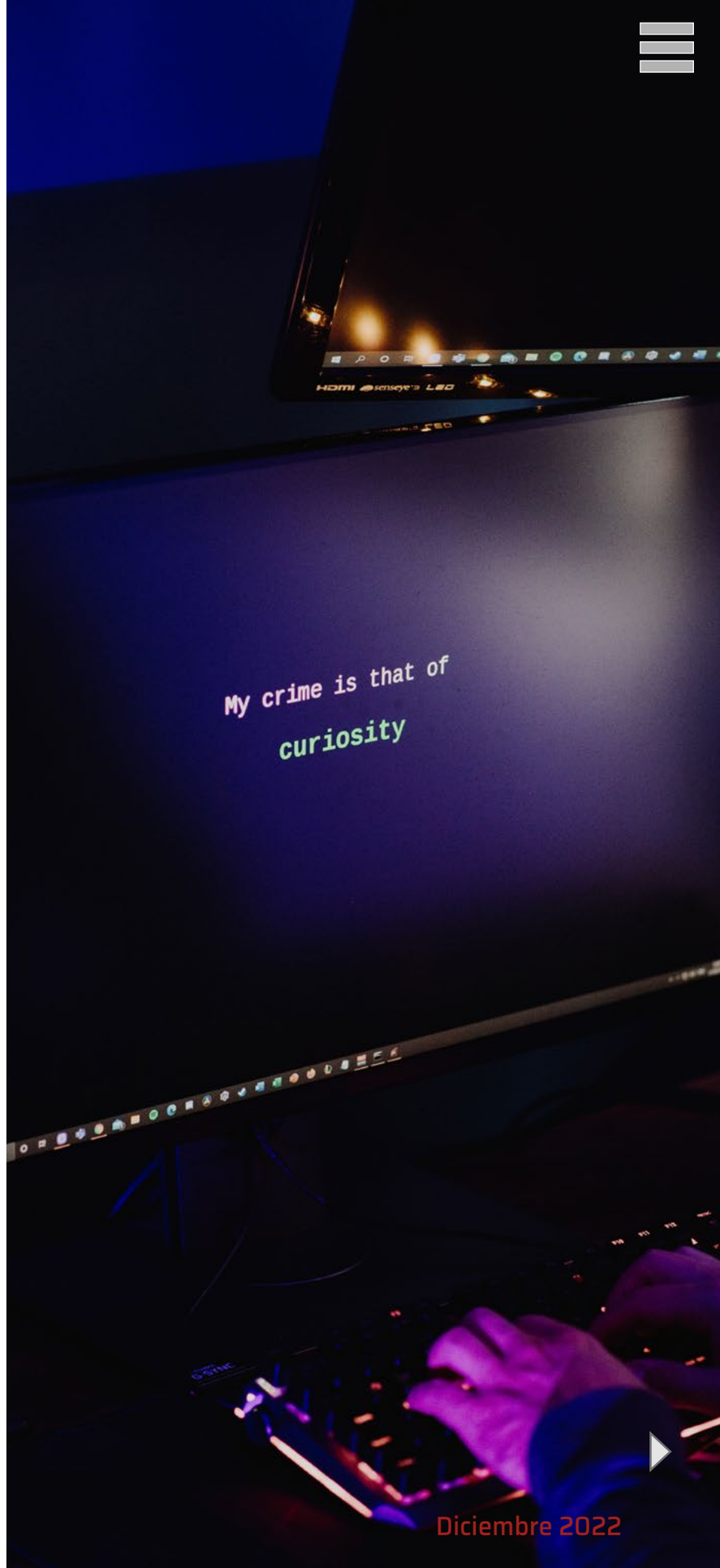
La aseguradora de salud MediBank reveló el pasado 25 de octubre que los datos de casi 4 millones de sus clientes habían sido expuestos a un hacker. La aseguradora australiana dijo que la información personal que pudo haber sido obtenida incluye el nombre, la dirección, la fecha de nacimiento e incluso los números de las tarjetas de seguro.

Para arreglar las cosas, MediBank afirma que ofrecerá una compensación a quienes se hayan aprovechado del acceso a su información privada. El coste estimado de este ciberataque para la empresa es de entre 25 y 35 millones de dólares. Desde entonces han llevado a cabo una investigación y han añadido más supervisión de la red y han determinado que el hacker ya no está presente.

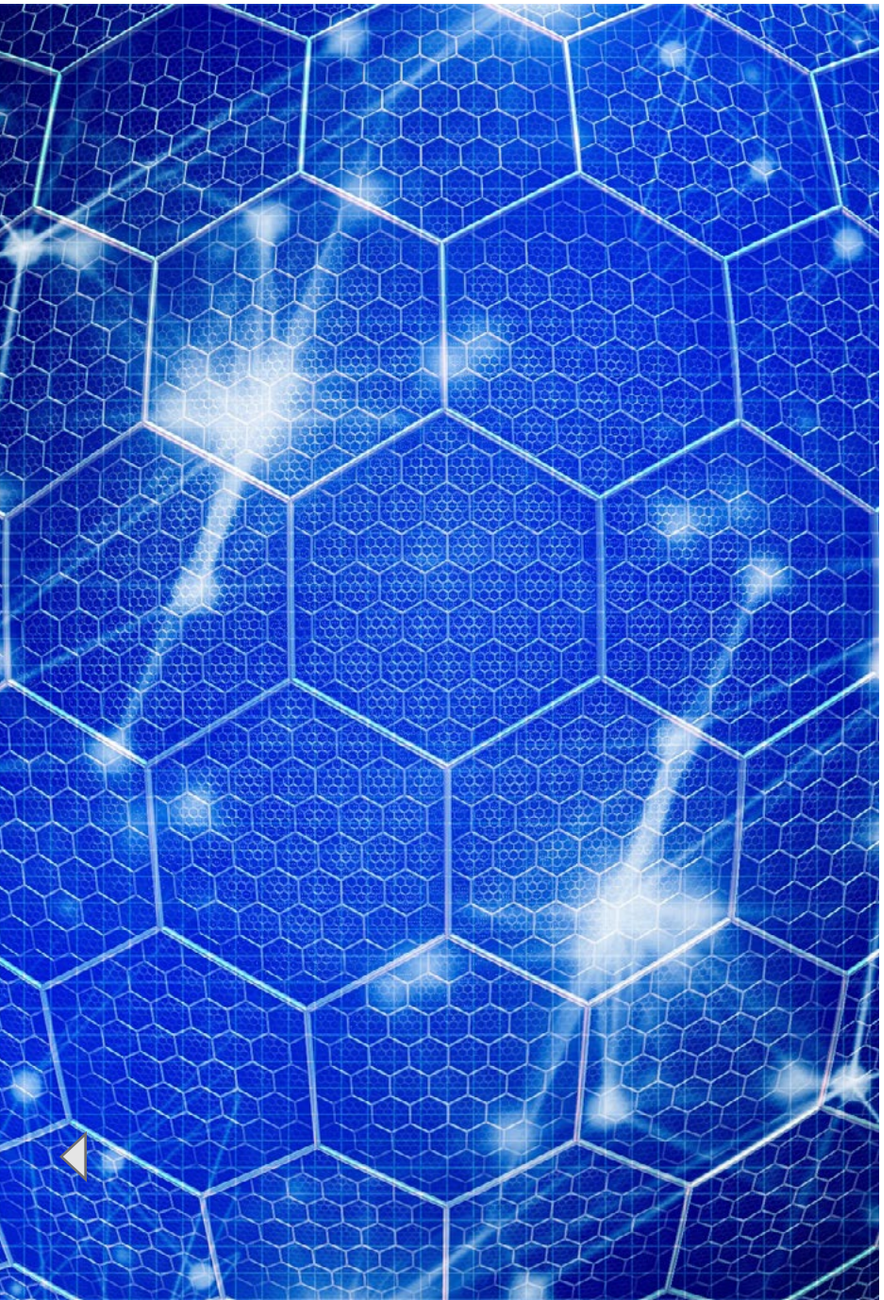
Noviembre de 2022:

CJPJ, Hacienda y la Policía Nacional

El Consejo General del Poder Judicial emitía un comunicado a principios de noviembre en el que informaba de que había detectado “un ciberataque a las redes de las Administraciones Públicas españolas en el que resultó afectado el Punto Neutro Judicial (PNJ)”. EL PNJ es cómo se denomina a red de telecomunicaciones que conecta a los juzgados y otros órganos judiciales con el resto de instituciones del Estado, pero cuya gestión depende del órgano de gobierno de los jueces. Este PNJ fue la vía utilizada, supuestamente, para saltar al resto de instituciones conectadas.



Una de ellas es la Dirección General de la Policía, de la que los hackers obtuvieron los datos de alrededor de 50.000 miembros del Cuerpo. Los hackers o sus clientes tienen ahora en su poder el nombre, la dirección y el resto de datos que aparecen en el DNI de esos policías nacionales, según informaba Eldiario.es. Otros organismos afectados, según informó el CGPJ, son la Agencia Tributaria, de donde los atacantes obtuvieron datos de cerca de medio millón de contribuyentes, el Servicio Público de Empleo o el Instituto Nacional de Seguridad Social



Diciembre de 2022:

Está por escribir, pero seguro que se presenta apasionante…

Conclusión

Si alguna lección aprendida nos llevamos de lo que va de año, es que la ciberseguridad no puede dejarse de lado. El ritmo al que las empresas, sin importar su tamaño, están experimentando violaciones de ciberseguridad resulta alarmante. Con los recientes ataques de alto perfil dirigidos a la sanidad, las finanzas, el retail, las administraciones públicas, el sector industrial y energético, está claro que el panorama de amenazas sigue evolucionando a un ritmo vertiginoso. Los ciberataques seguirán existiendo, pero hay que estar preparados.

Los principales vectores de ataque siguen siendo, como vemos en esta pequeña lista de ejemplos, el robo de credenciales y los correos electrónicos phishing, por lo que es crítico seguir concienciando a las organizaciones de la importancia de proteger sus sistemas. Por eso, las labores de formación y educación continuas siguen siendo vitales… como en la vida misma.

Enlaces de interés…

- Tres de cada cuatro aplicaciones de retail contienen fallos de seguridad
- Nueva herramienta gratuita de la AEPD de ayuda a la notificación de brechas
- Los ciberataques externos solo suponen un 23% del total
- Los consumidores pagan el precio de las brechas de datos

Compartir en RRSS

it Digital Security

Mejorando tu seguridad con Servicios Gestionados

WatchGuard

SOPHOS

Diciembre 2022

Mejorando tu seguridad con Servicios Gestionados

Los servicio gestionados en general, y los de ciberseguridad en particular, se han convertido en parte fundamental de la gestión empresarial. Los servicios gestionados surgen como una solución que permite seguir desarrollando el negocio sin las limitaciones habituales propias de asumir la planificación, gestión de proyectos y la contratación de perfiles profesionales.

Fotos: Ania Lewandowska

Para debatir sobre sus ventajas qué se espera de ellos, qué se echa en falta y cómo ayudan a los responsables de ciberseguridad de las empresas a hacer frente a los retos que se les plantean cada día, IT Digital Security ha organizado un Encuentro ITDS en el que han participado Elena García Mascaraque, Global Director Managed Security Service Providers en WatchGuard Technologies; Álvaro Fernández, Sales Manager Iberia de Sophos; Alfonso Delgado, Responsable de Infraestructura y Seguridad IT de la Asociación Española contra el Cáncer; Teniente Coronel Carlos Córdoba Fernández, Jefe del Área de Centros de Operaciones de Ciberseguridad del Centro Criptológico Nacional CCN-CERT; Luis Villafruela, Head of Cibersecurity de Iberdrola; David Cerrato de la Macorra, IT Director & CISO de KRUK España y Luis Ballesteros, CISO de WiZink.

"A un servicio gestionado le pediría saber adaptarse a las empresas al que van dirigido"

Alfonso Delgado, Responsable de Infraestructura y Seguridad IT, Asociación Española contra el Cáncer

Iniciamos la reunión preguntando a los asistentes por los retos de ciberseguridad a los que se están enfrentando. En los bancos siempre ha habido robos, atracos, pero mientras que antes los delincuentes tenían que hacerlo de manera presencial, "ahora lo intentan desde cualquier parte del mundo, en remoto y sin que se les vea la cara", comenta Luis Ballesteros, CISO de Wi-Zink, como uno de los retos a los que se enfrenta.

No olvida que, además, los ciberataques son más sofisticados, que las motivaciones ya no solo son económicas y que el perímetro de seguridad ha desaparecido.

En su doble función de director de TI y responsable de ciberseguridad de Kruk España, una empresa que se encarga de gestión de deuda, David Cerrato explica que entre sus retos está el cumplir con las normas de seguridad que exige cada

banco. Además, el ser una empresa polaca ha hecho que el riesgo se haya multiplicado durante la guerra Ucrania-Rusia. Añade que evolucionar al ritmo que se requiere para asegurar el negocio es también un reto importante.

Representante del CCN (Centro Criptológico Nacional), el Teniente Coronel Carlos Córdoba Fernández destacaba que los atacantes están ahora perfectamente organizados y que, si bien los pequeños organismos compran medidas de seguridad, el robo de credenciales se ha convertido en un reto porque con ellas te saltas todas esas medidas, por lo que hay que comprobar

comportamientos extraños. Sobre APTs, espionaje con móviles, etc., son temas con los que no hay que asustar a las pequeñas empresas.

A priori se puede pensar que una ONG no va a ser víctima de un ciberataque, pero según Alfonso Delgado, Responsable de Infraestructura y Seguridad IT de la Asociación Española contra el Cáncer (AEC), son víctimas de ataques automatizados e incluso dirigidos, como medio de llegar a otras empresas. Menciona la concienciación como un reto importante y que la externalización de servicios de seguridad es fundamental, sobre todo entre las pymes.

En su turno, Luis Villafruela, Head of Cibersecurity de Iberdrola, explica que si bien no tan avanzado como la banca, en Iberdrola se lleva tiempo invirtiendo y evolucionando en temas de ciberseguridad. Destaca como retos la pérdida de perímetro, así como la concienciación y el poder coordinar un plan de seguridad que tenga los mismos niveles en todos los eslabones de la cadena.

Destaca Elena García Mascaraque el papel que la filosofía Zero Trust tiene en la realidad a la que se enfrentan las empresas. Plantea que controlar el acceso a los sistemas, el comportamiento de los usuarios con medidas de control del endpoint, tecnologías de autenticación multifactor, y un servicio de monitorización de las amenazas de seguridad 24/7 son tres pilares sencillos que, desde diferentes grados de complejidad, cualquier empresa debería poder acceder.

Durante su intervención, Álvaro Fernández, Sales Manager Iberia de Sophos, destaca que, aunque positiva, la normativa es un reto, así como la

"El mensaje hacia la administración pública es que la seguridad gestionada es obligatoria porque todo se ha vuelto mucho más complicado y ya no vale un antivirus"

Carlos Córdoba Fernández, Jefe del Área de Centros de Operaciones de Ciberseguridad del Centro Criptológico Nacional CCN-CERT

evolución de los ataques, que obliga a las empresas a vigilar y monitorizar lo que está ocurriendo, algo nada fácil porque se necesita contar con un equipo de gente especialista en ciberseguridad, "lo que demuestra la necesidad de contar con servicios de seguridad gestionados".

Proveedores de confianza

La atomización que existe en el mercado de seguridad a nivelo de fabricantes se refleja también en la cantidad de proveedores de servicios que existen en el mercado. Habla David Cerrato de los Golden Providers, o proveedores de confianza con los que poder establecer una relación y saber en todo momento quién y cómo se está dando el servicio "para protegerte no sólo de los ataques externos, sino de los internos". Con más de 300 están en el departamento de IT, "nos consideramos una empresa tecnológica", dice Cerrato explicando que se trabaja con proveedores porque "no puedes saberlo todo", y que la clave está en saber quién de todos esos proveedores es que el que sabes lo que necesitas que sepa. "El gran secreto es cómo escoger", asegura.

"Para nosotros externalizar los servicios es fundamental", asegura el responsable de Infraestructura y Seguridad IT de Asociación Española contra el Cáncer. Añade Alfonso Delgado que hay muchos básicos que en muchas empresas no están cubiertos porque no cuentan con especialistas y se mantiene de acuerdo con David Cerrado en lo que se refiere a saber escoger el proveedor de confianza que sepa lo que necesita el cliente; "la externalización es

"El reto es tener el partner de alto nivel con gente buena dentro de la empresa y que el conjunto de servicios y soluciones estén bien enlazadas"

Luis Villafruela, Head of Cibersecurity, Iberdrola

fundamental. Necesitamos contar no sólo con proveedores que tengan el conocimiento, sino que miren por el cliente, no solo por el por el negocio", comenta.

Los proveedores son totalmente necesarios. Lo hacen mejor y de manera más eficiente. Lo asegura durante este Encuentro ITDS Luis Ballesteros. Añade que no se puede ser experto en todo, que "no hay que olvidar que la responsabilidad no se delega" y que cada empresa debe saber dónde está, dónde quiere llegar, y establecer un marco de ciberseguridad que, en opinión del CISO de WiZink, debe tener cuatro dominios fundamentales: gobierno, protección, vigilancia y resiliencia. Respecto al contrato con proveedores, empieza con la parte de la selección de proveedores para lo que hay que hacer un procedimiento interno de validación que establezca "que se van a cumplir las expectativas que esperas a nivel de servicio, y además van a gestionar tu información confidencial tal como tú lo harías".

Para Carlos Córdoba Fernández hay una fase clave: La responsabilidad no se delega. En el caso de las entidades locales o diputaciones, que es lo que compete al Jefe del Área de Centros de Operaciones de Ciberseguridad del CCN, "el problema es que hay una persona o ninguna" y hay que concienciarles de que ellos tienen una responsabilidad. El mensaje hacia la administración pública es que la seguridad gestionada es obligatoria porque todo se ha vuelto mucho más complicado y ya no vale un antivirus, pero "no podéis olvidaros de que la responsabilidad es vuestra". Desde el CCN se impulsa

"El gran secreto es cómo escoger a tu proveedor de servicios de confianza"

David Cerrato de la Macorra,
IT Director & CISO, KRUK España

la compra de tecnología a través del Catálogo STIC, al tiempo que la Red Nacional de SOC está impulsando la compartición de información entre proveedores, porque “el que piense que haciendo la guerra por su lado va a triunfar, está totalmente equivocado”.

Explica Luis Villafruela que en Iberdrola existen distintos niveles de servicios gestionados. Si bien la parte de gobierno no se delega, sí que se cuenta con proveedores en otras cuestiones, como el mantenimiento de la postura de seguridad. Reconoce que existe un “proceso de selección de proveedores ya muy evolucionado y que

“el reto es tener el partner de alto nivel con gente buena dentro de la empresa y que el conjunto de servicios y soluciones estén bien enlazadas”.

Dice Álvaro Fernández que los servicios de seguridad gestionados aparecen por necesidad y que la seguridad se ha convertido en habilitadora del negocio. Asegura también que el talento es clave, no sólo conseguirlo, sino retenerlo, así como la escalabilidad del servicio que se está dando. Explica que desde Sophos se ha invertido mucho en tecnología, así como en Inteligencia Artificial para poder escalar que ha permitido, en tres años, pasar de cero a doce mil clientes en el servicio de detección y respuesta. Desde Sophos estamos siendo pioneros en ofrecer los servicios de detección y respuesta (MDR) no sólo sobre tecnología de Sophos, sino sobre tecnología de terceros para proteger al máximo nivel a las organizaciones.

A través de WatchGuard for SOC, WatchGuard provee de tecnología para proveedores de servicios a terceros, o MSSPs, o servicios internos de seguridad. “Nuestra filosofía es que la seguridad sea consumida como servicio y crear plataformas de seguridad”, explica Elena García Mascaraque, añadiendo que la Unified Security Platform de WatchGuard permite integrar no sólo soluciones de la compañía sino de terceros “permitiendo hacer sencillo lo complejo”, que no es otra cosa que la gestión de una ciberseguridad basada en decenas de herramientas.

La responsable de servicios MSSP de WatchGuard comentaba también que esa tendencia de seguridad a través de plataforma se convierte en fundamental el tema de las certificaciones y cumplimiento normativo porque se trabaja con datos muy sensibles “y vuestra tranquilidad también es la nuestra”; además de tener acceso a telemetría de 365 días que permiten a los SOCS hacer las investigaciones.

¿Qué le pedirías a un Servicio de Seguridad Gestionado?

Retención de talento es uno de los elementos que pediría el responsable de ciberseguridad de Iberdrola a un servicio gestionado. Explica Luis Villafruela que en ocasiones se encuentra con una

"Los proveedores son totalmente necesarios. Lo hacen mejor y de manera más eficiente. Pero no hay que olvidar que la responsabilidad no se delega"

Luis Ballesteros, CISO, WiZink

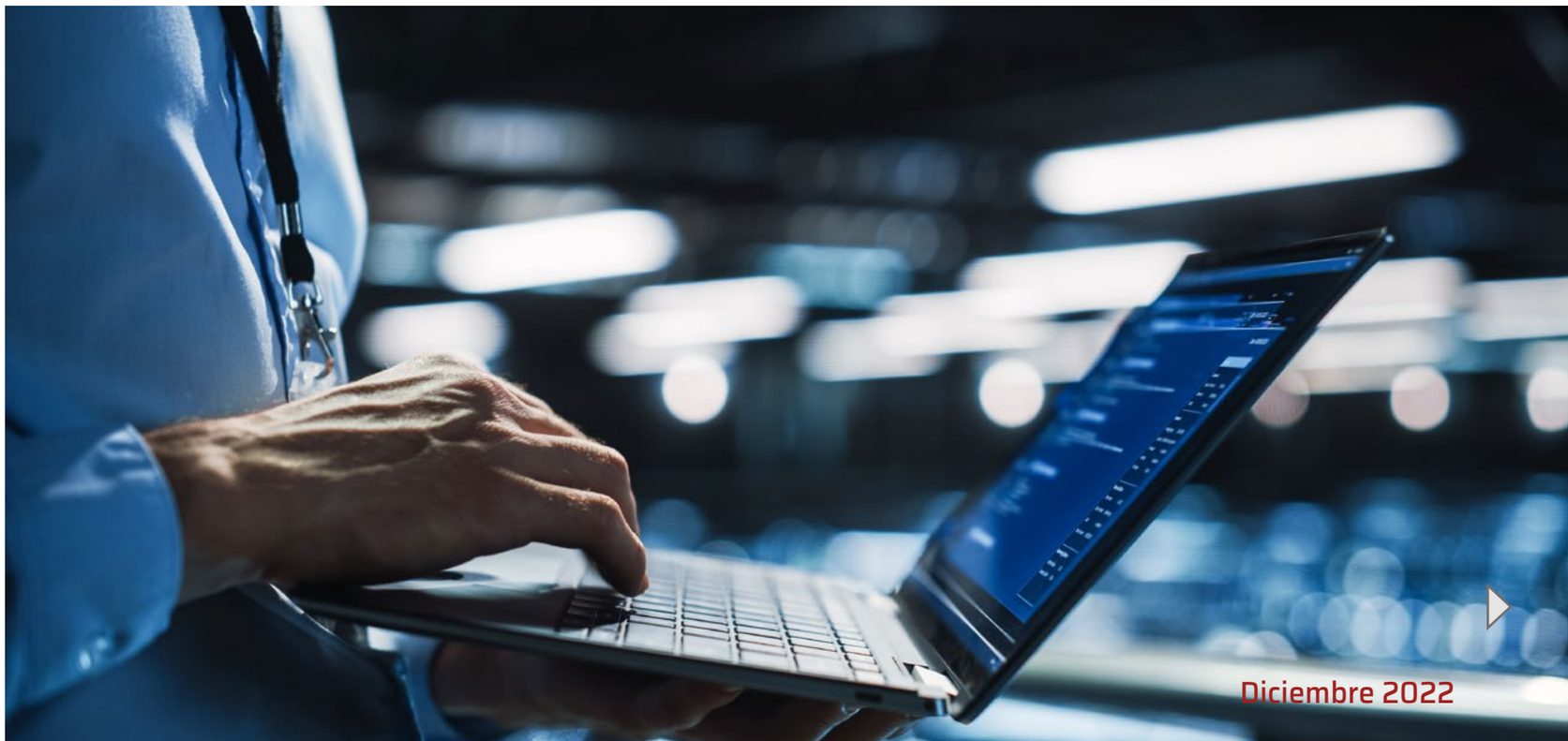
merma en la calidad del servicio prestado, “y eso es porque la rotación de personal es impresionante y los que llegan nuevos no tienen tanta experiencia”. Apunta también en su lista de deseos la convergencia de soluciones, sobre lo que asegura que se está haciendo un buen trabajo; y la compartición de inteligencia, “contar con plataformas comunes que permitan compartir IoCs, compartir ciberinteligencia”.

“A un servicio gestionado le pediría saber adaptarse a las empresas al que van dirigido”, asegura con rotundidad Alfonso Delgado, poniendo como ejemplo que no se puede querer vender un servicio de SOC a una empresa que no tenga el directorio activo en orden. Sobre que se delegue la responsabilidad en el servicio gestionado, apunta también el responsable de ciberseguridad de la AEC que en ocasiones “no hay conocimiento interno y te tienes que fiar de lo que te digan. Es muy importante la formación porque uno no puede ser CISO o responsable de ciberseguridad sin tener los conocimientos para, aunque sea, contratar una empresa y hacerle seguimiento de lo que tiene que hacer”.

“Profesionalidad” es lo que el Teniente Coronel Carlos Córdoba Fernández pediría a un servicio de seguridad gestionada. Menciona que rara es la empresa de seguridad que no venda SOAR, IA o machine learning, pero que, cuando hablamos de pymes, “lo que se necesita es algo muy sencillo, muy básico, que te proteja en el 95% de los casos y que cueste 100€ al mes”. Comenta también el Jefe del Área de Centros de Operaciones de Ciberseguridad, Centro Criptológico Nacional

"Nuestra filosofía es que la seguridad sea consumida como servicio y crear plataformas de seguridad"

Elena García Mascaraque, Global Director Managed Security Service Providers, WatchGuard Technologies



"Desde Sophos estamos siendo pioneros en ofrecer los servicios de MDR no sólo sobre tecnología de Sophos, sino sobre tecnología de terceros"

Álvaro Fernández,
Sales Manager Iberia, Sophos

CCN-CERT, que hay quienes se aprovechan de una falta de conocimiento para vender de más.

En el caso de David Cerrato de la Macorra, lo que pediría es conocimiento real, "una verdadera formación en ciberseguridad, que entienda lo que se está haciendo".

Retención de talento, flexibilidad y adaptación al entorno son los tres elementos que Luis Ballesteros pediría a un proveedor de servicios gestionados, porque "estamos contratando servicios gestionados porque lo hacen mejor y más eficiente. Y si de verdad queremos y que lo hagan mejor y más eficiente lo que no puede ser es 'café para todos' porque no es lo mismo proteger un comercio, una entidad financiera o una red eléctrica". Respecto a la opción de compartir conocimiento entre todo el ecosistema de seguridad, comenta Ballesteros que es algo que se lleva haciendo en el sector bancario, donde "tenemos muy claro que somos competencia en mercado, pero no en ciberseguridad, y esto se ha ido extendiendo".

Se plantea también durante el debate la necesidad de establecer, cuando se pueda, dos capas, una de consultoría de seguridad y otra del servicio en sí mismo. Si bien para las empresas grandes estas dos capas están diferenciadas, en entornos más pequeñas la línea es más difusa; en todo caso, para Alfonso Delgado "es fundamental recibir más consultoría de ciberseguridad que identifique los mínimos". Al respecto menciona David Cerrato que en Angeco, la Asociación Nacional de Entidades de Gestión de Cobro, se busca establecer unas guías de mejores prácticas, "unos básicos de lo que deberías implantar para poder trabajar con otras empresas. Tener una lista de 'to do' que me permita ir a un proveedor y decirle qué necesito tener". it

Enlaces de interés...

- EncuentrosITDS. Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?
- Encuentros ITDS. De la continuidad de negocio a la resiliencia segura
- Encuentros ITDS. Los servicios gestionados de seguridad a examen

Compartir en RRSS