FORO it Digital Security

Organiza

FORO it Digital Security

COMMVAULT · eset · Bitdefender BUILT FOR RESILIENCE · citrix · CyberRes A Micro Focus Line of Business · Cynet · proofpoint.

SONICWALL · SOPHOS · Secure&IT www.secureit.es · STORMSHIELD · WatchGuard · yubico

it Digital Security

Directora — **Rosalía Arroyo** rosalia.arroyo@itdmgroup.es
Colaboradores — Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez
Diseño revistas digitales — Contracorriente
Producción audiovisual — Miss Wallace, Alberto Varet
Fotografía — Ania Lewandowska

it Digital MEDIA GROUP

Director General Juan Ramón Melara juanramon.melara@itdmgroup.es
Director de Contenidos Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora División Web Bárbara Madariaga barbara.madariaga@itdmgroup.es

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

Protegiendo el nuevo perímetro

El perímetro de seguridad, tan cuidadosamente establecido hace décadas con la llegada de los firewalls, ha desaparecido. Los empleados están en todas partes, los datos dispersos y los recursos repartidos entre nubes.

Buscando dónde colocarle, hay quien apunta a la identidad mientras que otros que prefieren establecerlo en el dato, convertido por derecho en el principal activo de las empresas. Por otra parte, la misma desaparición del perímetro ha vuelto a dar protagonismo al endpoint, relegado durante años detrás del firewall.

De forma que la identidad, los datos y el endpoint se han convertido en elementos clave a proteger y en protagonistas de conceptos como la Cybersecurity Mesh, una estrategia de ciberdefensa que busca proteger de forma independiente cada dispositivo con su propio perímetro, lo que permite extender la seguridad allá donde se necesite.

Además de tecnología, es necesario aumentar la concienciación de los empleados y convertirlos en aliados en los procesos de ciberdefensa.

Cómo hacerlo de la mejor manera y con las tecnologías adecuadas es el foco de un nuevo Foro ITDS titulado “Protegiendo el nuevo perímetro” en el marco del cual se ha realizado ponencias, entrevistas y mesas redondas que os resumimos a continuación.

FORO it Digital Security

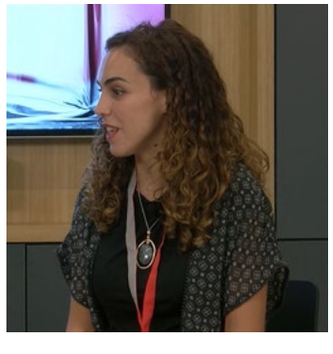
Sumario

Entrevistas

'Digitalización y ciberseguridad van de la mano'
Marina Rodríguez, DSN

'Que los datos sean auto gestionables da una confianza mucho mayor en el uso de los mismos'
Javier Fernández, Gobierno de Asturias

'El reto es asegurar una experiencia de usuario satisfactoria en un entorno de seguridad adecuado'
Elena García, Indra



'Hay que centrar los recursos en proteger y blindar los datos que de verdad son críticos'
Mabel González, SERMAS

Impulso tecnológico

"Somos muy buenos haciendo backup, y sobre todo haciendo restauración"
Sandra Espinoza, Commvault

"Hay que fortalecer el endpoint"
Sergio Martínez, SonicWall

"No es fácil que una organización por sí misma sea capaz de gestionar la ciberseguridad eficientemente"
Álvaro Fernandez, Sophos

"No queremos poner una barrera entre la concienciación y la tecnología"
Carlos Tortosa, ESET

El dato como perímetro de seguridad
Borja Pérez, Director General, Stormshield Iberia
Nuria Andrés, Estratega de ciberseguridad, Proofpoint

El endpoint recobra protagonismo
Carlos Castro, Strategic Account Manager, WatchGuard Cytomic
Javier Cazaña, Country Manager Iberia, Cynet

Identidad Digital, y cómo protegerla
Jacinto Grijalba, Cyber Security Sales Manager, CyberRes, una unidad de negocio de Micro Focus
Ricardo José Garrido Reichelt, Lead Sales Engineer AD& S, Citrix Iberia

La concienciación que no debe faltar
Francisco Valencia, CEO, Secure&IT
Fabio Cichero, Sales Manager Southern Europe, Yubico

Mesa redonda

Protección del dato más allá del backup

¿Quién es el responsable de la protección del dato?

MDR, la evolución natural para la protección del endpoint

La seguridad endpoint a debate

Identidad, el mayor tesoro que hay que defender

El reto de la gestión de la identidad

Formación para salvar la información

La concienciación como primera piedra de la estrategia de seguridad de la empresa

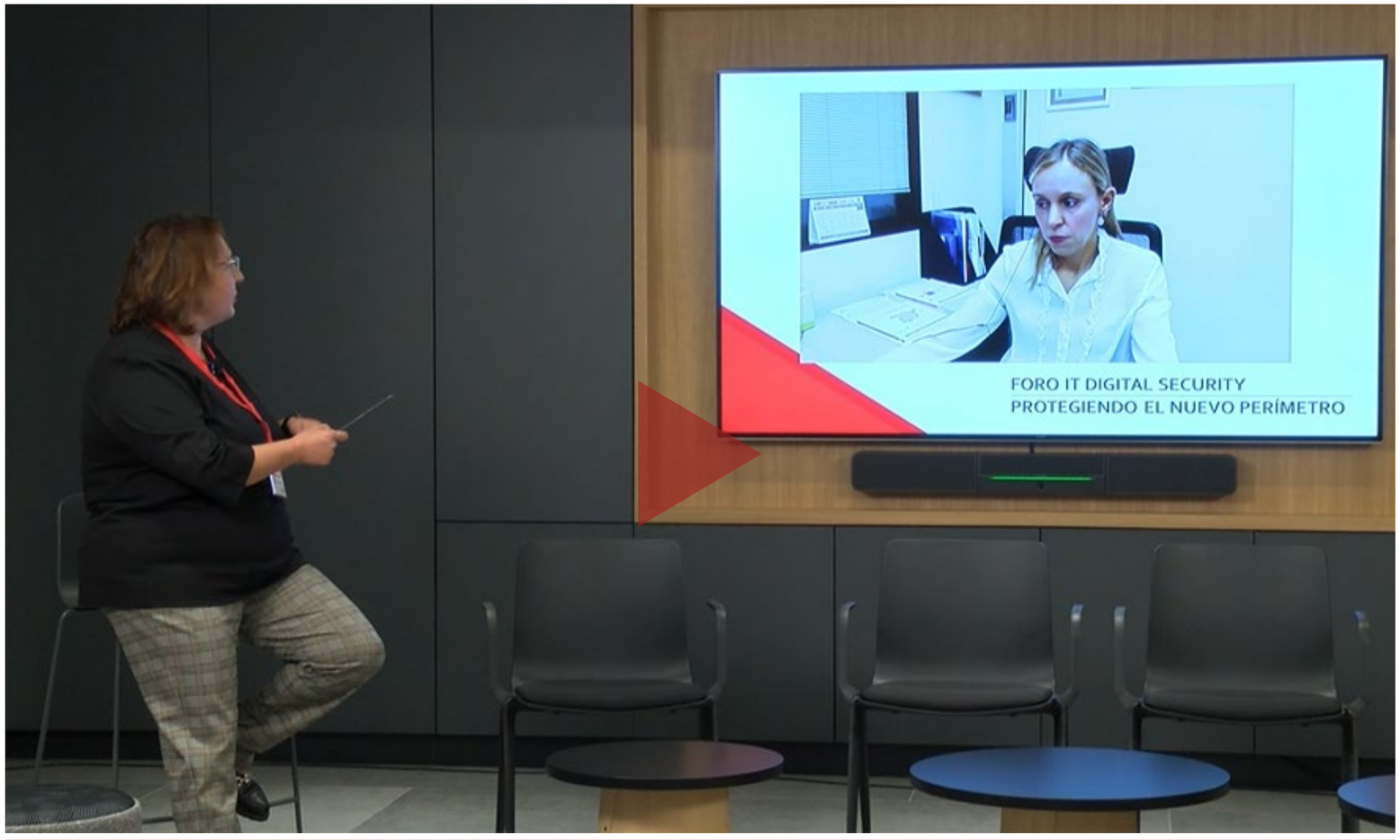
Marina Rodríguez Díaz, Jefa de Unidad de Ciberseguridad y lucha contra la Desinformación, Departamento de Seguridad Nacional (DSN)

‘Digitalización y ciberseguridad van de la mano’

“La cultura que todos debemos de tener en nuestra vida privada debería ser tan exigente como la que se nos pide en el ámbito laboral”, asegura Marina Rodríguez Díaz, Jefa de Unidad de Ciberseguridad y lucha contra la Desinformación, Departamento de Seguridad Nacional (DSN), durante una entrevista realizada en el marco del Foro ITDS ‘Protegiendo el nuevo perímetro’, en la que se le preguntaba si en España hay una cultura adecuada para hacer frente a la ciberseguridad, siendo la ciberseguridad un pilar estratégico de la innovación y la digitalización. “Un trabajador que en su vida diaria no es ciber seguro, probablemente tampoco lo va a ser en su gestión diaria de sus aplicaciones, de sus dispositivos, etcétera. Por eso la cultura de ciberseguridad es muy importante, muy extensiva y los mensajes tienen que ser muy variopintos”, añade la directiva.

Comenta también Marina Rodríguez Díaz que si bien las grandes empresas pueden estar formadas y dotadas la ciberseguridad porque son conscientes de las pérdidas que acarrean estos problemas, “cuando se relacionan con proveedores y con empresas de menor tamaño también se pueden ver resentidas porque se relacionan con ellas en unos términos muy asiduos en los que probablemente el nivel de seguridad o de alerta desciende”.

Nos cuenta la Jefa de Unidad de Ciberseguridad y lucha contra la Desinformación del DSN que, Desde el Departamento de Seguridad Nacional, la Estrategia Nacional de Ciberseguridad del año 2019 ya contempla el fomento de la cultura de ciberseguridad como una de las líneas básicas de actuación. Como iniciativas dentro del Departamento de Seguridad Nacional, se cuenta con el Foro Nacional de Ciberseguridad, donde en colaboración público privada hay dos grupos de trabajo, o dos subgrupos de trabajo dentro de uno, que trabajan por fomentar la cultura de ciberseguridad, por un lado, en el ámbito empresarial y, por otro lado, en el de la ciudadanía. “Finalmente quiero mencionar que los principales CERT de este país trabajan mucho en la concienciación y el fomento de la cultura y la formación en ciberseguridad”.



‘DIGITALIZACIÓN Y CIBERSEGURIDAD VAN DE LA MANO’ (MARINA RODRÍGUEZ, DSN)

CLICAR PARA VER EL VÍDEO

Asegurando que “España es un país ciberseguro”, comenta Marina Rodríguez que “los ciudadanos se enfrentan a retos diarios en su praxis diaria y contacto con procesos digitales. Somos un país que sufre mucho ciberataques porque somos un país muy digitalizado, y esto es un reto para la ciudadanía a la vez que una oportunidad”.

En cuanto a los retos a los que se enfrentan las empresas menciona la directiva que uno de ellos es “dotarse de un centro de operaciones de ciberseguridad adecuado”, algo que puede “no ser demasiado problemático en empresas grandes”; las

"Los procesos de digitalización cada vez son mayores y ello conlleva, para las empresas que se dedican a la ciberseguridad, mayores oportunidades de negocio"

"Un trabajador que en su vida diaria no es ciber seguro, probablemente tampoco lo va a ser en su gestión diaria de sus aplicaciones, de sus dispositivos, etcétera."

pymes, añade pueden tener mayores dificultades de acceso a estos servicios, aunque hay que tener en cuenta que, si en toda la cadena de relación hay un elemento ciber seguro, "esto nos afecta a todos".

¿Qué oportunidades ofrece la ciberseguridad en los procesos de digitalización? "Los procesos de digitalización cada vez son mayores y ello conlleva, para las empresas que se dedican a la ciberseguridad, mayores oportunidades de negocio, porque cada vez hay más superficie de exposición y, por tanto, cada vez hay más superficie que proteger", responde Marina Rodríguez. Añade que, en el entorno pyme, "la digitalización es una ventaja que, si son capaces de explotar pueden suponer un ahorro de costes considerable que, en el caso de una pyme, puede suponer la diferencia entre estar o no estar en el mercado".

Concluye la Jefa de la Unidad de Ciberseguridad y lucha contra la Desinformación del DSN que, "digitalización y ciberseguridad van de la mano".

Sandra Espinoza, Senior Sales Engineer, Commvault

‘Somos muy buenos haciendo backup, y sobre todo haciendo restauración’

“Es verdad que el perímetro no está tan definido como estaba antes”, comenzaba diciendo Sandra Espinoza, Senior Sales Engineer de Commvault, al comienzo de una ponencia realizada en el marco del Foro ITDS “Protegiendo el nuevo perímetro” y en la que asegura también que su compañía tiene mucho que aportar en esta era de transformación y movilidad gracias a una plataforma inteligente de gestión de datos.

Recuerda Sandra Espinoza en su intervención que la pandemia ha sido el gran detonante de la movilidad del dato, que está donde están los trabajadores o donde están los sensores recogiendo datos; esta situación ha provocado la existencia de un perímetro más amplio y que, “contar con una estrategia sólida de protección de datos”, se haya convertido en algo fundamental.

PONENCIA COMMVAULT
FORO ITDS “PROTEGIENDO EL NUEVO PERÍMETRO”

CLICAR PARA VER EL VÍDEO

La pandemia ha sido el gran detonante de la movilidad del dato

Haciendo referencia a un informe de Sophos según el cual el 71% de las empresas ha sufrido algún tipo de ataque, apuntaba Sandra Espinoza que la primera herramienta de recuperación ante cualquier tipo de ciberamenaza sigue siendo una herramienta de backup y de protección del dato, y que, si bien "somos muy buenos haciendo backup, sobre todo somos muy buenos haciendo restauración, que es una de nuestras grandes ventajas".

Continúa diciendo la Senior Sales Engineer de Commvault que es importante contar con un punto único de gestión donde podamos administrar tecnologías tanto de protección de datos basados en SaaS como herramientas de cyber deception que buscan engañar a los malos con objetivos totalmente falsos; "el futuro de la ciberseguridad está en tener tecnologías que se puedan hablar entre ellas; contar con una arquitectura, una estrategia de ciberseguridad en maya, donde todas las tecnologías puedan dar servicio y trabajar a la vez". Y Commvault, con su capacidad de integración vía APIS, técnicas de machine learning o incluso inteligencia artificial aplicada a la protección de datos, "es una pieza fundamental en este sentido".

Recordaba Sandra Espinoza que Commvault es capaz de proteger el dato allí donde se genere, ya sea en el centro de datos, en la nube o en el Edge, "ofreciendo garantías totales de recuperación". it

Contenido relacionado

- Commvault

Compartir en RRSS

FORO it Digital Security

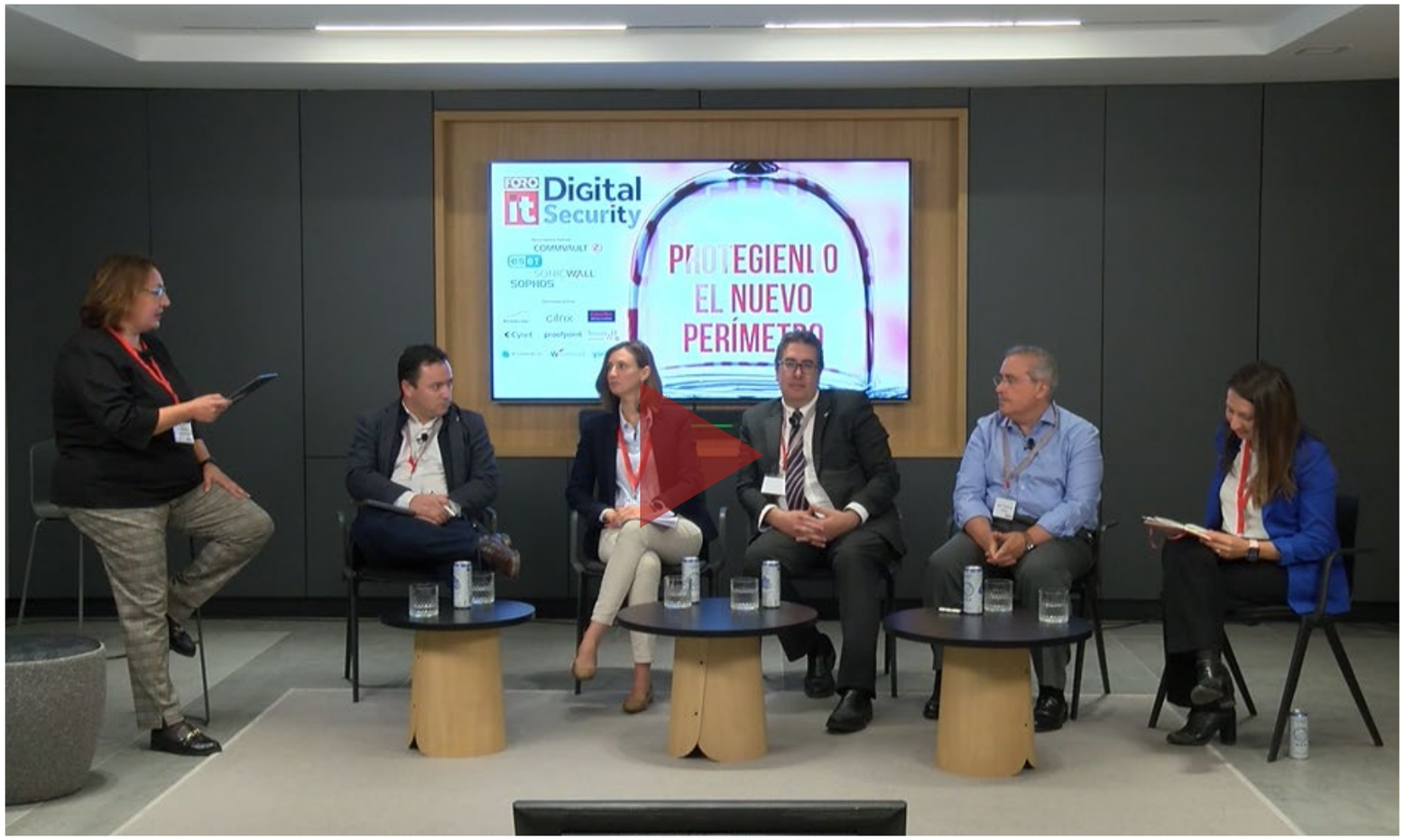
Mesa Redonda

Protección del dato más allá del backup

Los equipos de TI de las empresas se esfuerzan por mantenerse al día con un ecosistema de datos corporativos en rápida evolución. A pesar de haber hecho frente a numerosos retos, sigue habiendo importantes desafíos a la hora de mantener el control y seguridad de los datos en entornos cada vez más complejos.

En la búsqueda de un nuevo perímetro de seguridad, perdido con el avance de la nube, la movilidad y el trabajo remoto, hay quien mira a los datos como el elemento en torno al cual establecer un contorno de seguridad capaz de mantener la empresa a salvo del impacto de los ciberataques.

Ha sido en el marco del Foro ITDS “Protegiendo el nuevo perímetro” donde se ha celebrado una mesa redonda en la que hablar de los datos como nuevo perímetro de seguridad, de su gobernanza, disponibilidad o de continuidad de negocio. En esta mesa han participado Sandra Espinoza, Senior Sales Engineer de Commvault; Ángel Luis Sánchez García, CTO de SERMAS; María Luisa

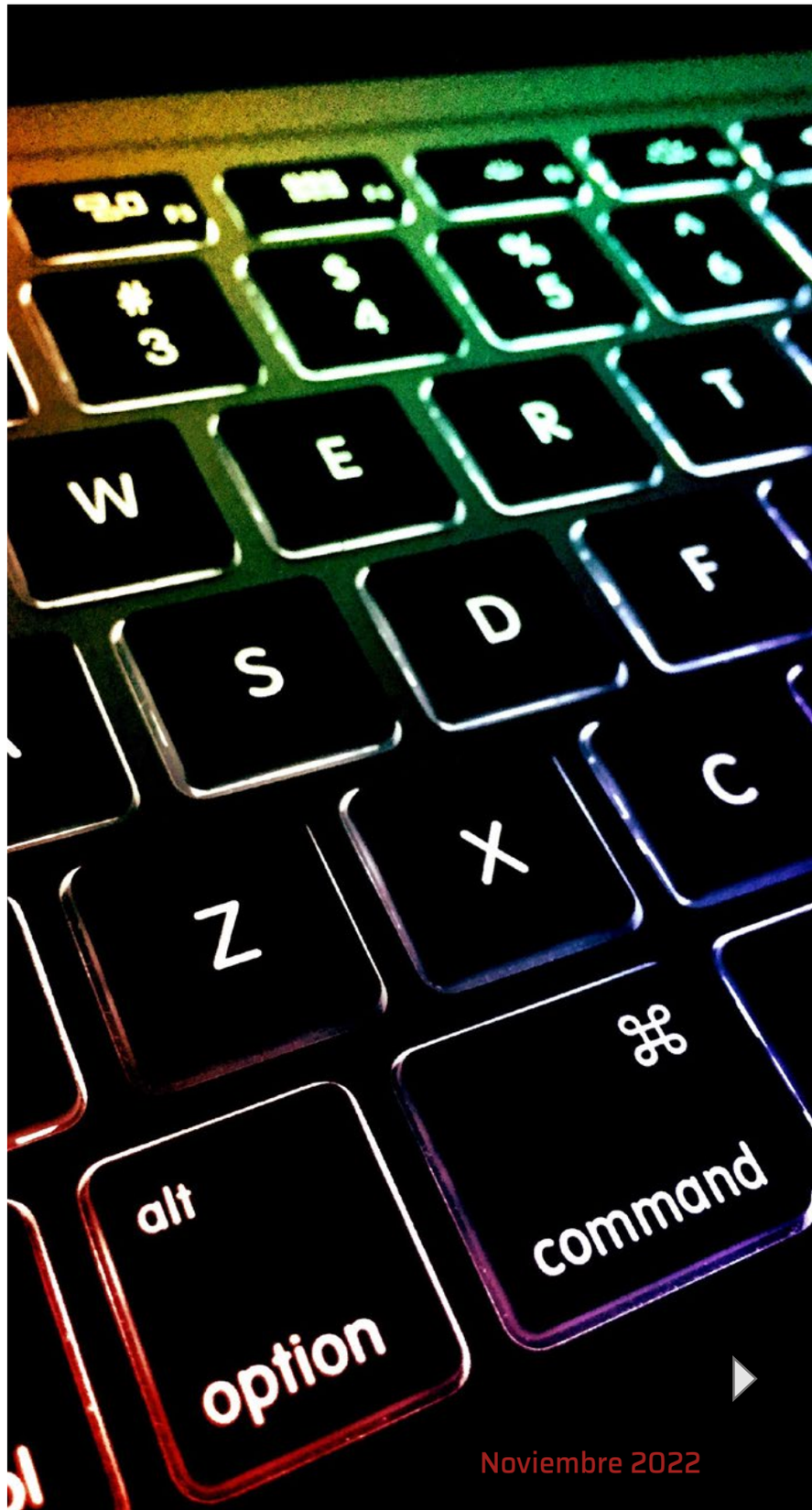


PROTECCIÓN DEL DATO MÁS ALLÁ DEL BACKUP

CLICAR PARA VER EL VÍDEO

Fernández, Jefa de y Protección de Datos de Mapfre; Rafael Pastor Vargas, Director de la Escuela Técnica Superior de Ingeniería Informática de la UNED y Director del Master en Ciberseguridad Aplicada; y Juan Manuel García Dujo, CIO y CISO de Cerealto Siro Foods.

Arrancábamos la mesa preguntando a los ponentes por lo retos a los que se enfrentan a la hora de gestionar y proteger los datos. Destacaba Ángel Luis Sánchez García la complejidad a la que se enfrenta SERMAS a la hora de proteger datos de todo tipo y especialmente sensibles de casi siete millones de personas; “nuestra preocupación es que el dato esté siempre disponible para el profesional que lo necesita y con la máxima seguridad”, aseguraba el directivo puntualizando que además de concienciación, que toda la organización entienda la importancia de la seguridad, hace falta tecnología,



"El dato está descentralizado, pero hay que tenerlo controlado"

Sandra Espinoza,
Senior Sales Engineer, Commvault

a lo que se suma el reto de tener que cumplir, como parte de la administración pública, el esquema nacional de seguridad.

Asegurando que la superficie de ataque ha aumentado, Rafael Pastor Vargas divide la seguridad en tres fases. La primera es la de prevención, donde se incluye la concienciación como elemento a destacar y que en UNED se trabaja a través del programa Cibercoorperantes desarrollado por INCIBE; la segunda es la proactividad, o supervisión de lo que está pasando a nivel de funcionamiento, algo que se ha complicado porque "cualquier móvil es una fuente de problemas"; la tercera fase, la reactiva, que es la que afecta al proceso de negocio. "Es importante tener estas fases muy bien delimitadas", concluía Rafael Pastor.

"Hay un lema que me encanta de mi compañía: 'En Mapfre cuidamos lo que importa'. Y no solo importa la persona, no solo importa el servicio, importa la confianza que nos depositan los clientes", aseguraba María Luisa Fernández, Jefa de Privacidad y Protección de Datos de Mapfre, para después añadir que existe un reto tanto en la gestión del dato, como en la disponibilidad del mismo. Hablando de la protección del dato planteaba la directiva que "si hemos perdido ese perímetro. Si lo que necesitamos es garantizar el control del dato, tenemos que irnos dentro del dato. Tenemos que securizarlo desde dentro". Mencionaba también que en el momento actual no basta con poner un firewall, o un control de acceso, sino proteger el dato desde el diseño a través de mecanismos en los

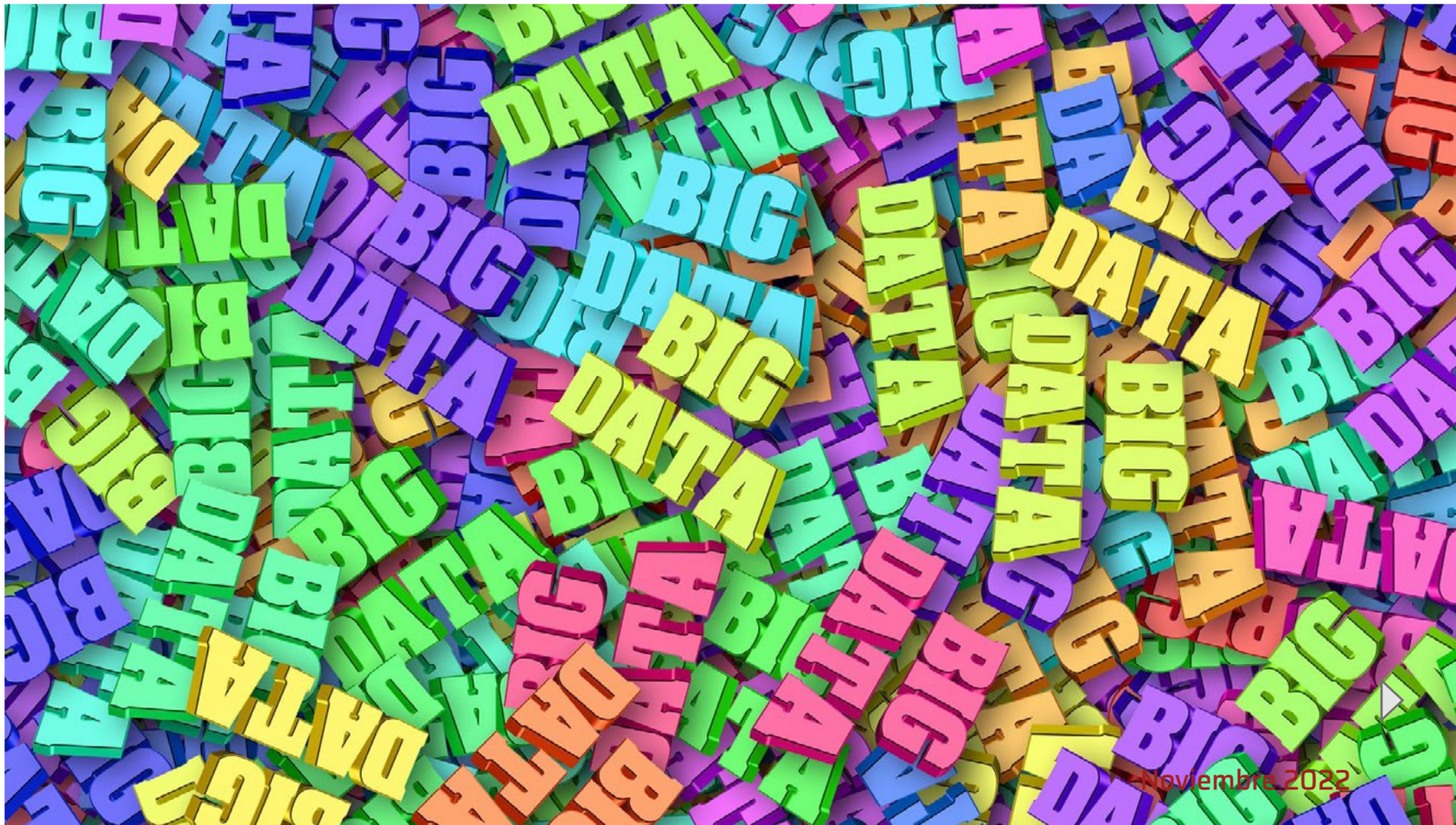
"Nuestra preocupación es que el dato esté siempre disponible para el profesional que lo necesita y con la máxima seguridad"

Ángel Luis Sánchez García, CTO, SERMAS

que, en caso de robo, el dato en sí mismo no tenga validez. Comentaba también María Luisa Fernández la importancia de las técnicas de anonimización del dato para explotarlo con garantías para concluir que la tarea es compleja y que el camino en el que estamos "es fascinante".

Destacaba Juan Manuel García Dujo la disponibilidad e integridad del dato como uno de los retos fundamentales a los que se enfrentan las compañías. Añadía en su intervención que hay que tener en cuenta dos factores de protección, por un lado "protegernos contra el atacante externo, que es algo histórico", y por otro del atacante interno, porque "la disponibilidad de la información hace que haya que protegerla también de nosotros mismos". Cumplir con GDPR es, en opinión del CISO de Cerealto Siro Foods, un tercer reto que el multicloud no ha hecho sino complicar. Desde la compañía estos retos se abordan con concienciación, tecnología y procedimientos porque "nos permiten sobrevivir a un ataque que sabemos que va a pasar".

Para Sandra Espinoza la dispersión de los datos es uno de los retos a los que se enfrentan las empresas; "el dato está descentralizado, pero hay que tenerlo controlado", aseguraba, añadiendo



que, para Commvault, ser innovadores y ofrecer a los clientes soluciones que den respuesta a los grandes cambios del mercado es otro gran reto. “Conseguimos que nuestras soluciones aporten valor”, decía, antes de enumerar un tercer reto: estar preparados, esperar la contingencia.

¿Cómo están evolucionando las necesidades de protección de datos en esta economía digital? Respondía Sandra Espinoza asegurando que la protección del dato se está moviendo a soluciones tipo SaaS, que los clientes piden que la solución sea agnóstica a la nube; que ya no piden únicamente una copia de seguridad sino “redundancia, disponibilidad de datos, soluciones de disaster recovery”, a lo que se añade una capa de prevención que ayude a evitar posibles ataques. Además, también se busca que sea una solución transversal capaz de garantizar las inversiones.

Durante el coloquio se preguntó a Ángel Luis Sánchez García por la estrategia adoptada por

"Si lo que necesitamos es garantizar el control del dato, tenemos que irnos dentro del dato. Tenemos que securizarlo desde dentro"

María Luisa Fernández,
Jefe Privacidad y Protección de Datos Mapfre

"Tenemos una estrategia muy completa en cuanto a los datos almacenados"

Rafael Pastor Vargas, Director de la Escuela Técnica Superior de Ingeniería Informática de la UNED y Director del Master en Ciberseguridad Aplicada

SERMAS para proteger y ofrecer alta disponibilidad a sus datos críticos. Explica el CTO del servicio de salud madrileño que, en su caso, los datos no estaban centralizados en un dataceter, sino repartidos en hospitales y centros de salud; "los datos estaban dispersos, nadie veía el dato de al lado, no había alta disponibilidad, las copias de seguridad se hacían en cinta…". Bajo el Plan Atenea se han ido modernizando las infraestructuras y se avanza en varios frentes, desde priorizar la recuperación, adoptar nuevas formas de archivado y, en general adoptar tecnologías que permiten a SERMAS funcionar internamente como un hiperescalar, permitiendo a los centros provisionar sus propios servicios. "Hemos simplificado toda la gestión y, al simplificarla, hemos mejorado la seguridad", asegura el CTO de SERMAS, añadiendo que "lo más importante para nosotros es, sin duda, la disponibilidad".

Con 50 años de historia, una red de centros nacionales y otros en el extranjero, la UNED adoptó los planes de trabajo con tecnología a partir del año 2000. Fue a partir de entonces cuando se empieza a recoger mucha información; "tenemos una estrategia muy completa en cuanto a los datos almacenados", asegura Rafael Pastor Vargas, explicando que ya se trabaja en modelos predictivos basados en Inteligencia Artificial y que se estudia la creación de data lakes específicos; mientras se determina "si es una buena solución agrupar tanta información o dejarla donde está ubicada ahora mismo", surge el debate acerca de cómo implementar "mecanismos de protección de la información en cuanto a su uso para poder ser utilizados en entrenamiento de algoritmos" explicaba el Director de la Escuela Técnica Superior de Ingeniería Informática de la UNED y Director del Master en Ciberseguridad Aplicada.

¿Hacia dónde va la regulación y normativa de los datos? Cuestión compleja que respondía María Luisa Fernández mencionando que además de la normativa sobre Inteligencia Artificial, en proceso de debate, se debe tener en cuenta la nueva Ley de Datos, Data Act, que para la directiva es una evolución del derecho de portabilidad, o eIDAS 2. En todo caso, aseguraba, el proceso de digitalización implica la recogida de grandes cantidades de información, algo que no es malo "siempre y cuando el usuario sea consciente de ello". El dato es control, es conocimiento, y su uso y disponibilidad se tendrá que ir regulando sectorialmente, por soluciones, y siendo conscientes de hacia dónde vamos, aseguraba la responsable de Privacidad y Protección de Datos de Mapfre.

"Somos custodios de la información de la compañía, no somos propietarios de ella", decía Juan Manuel García Dujo, añadiendo que, en el camino de asegurar la información deben estar involucrados tanto negocio como el propietario del proceso, y dejando claro a quién tengo de dar acceso a cada dato o qué aplicaciones tenemos que diseñar, con qué niveles de acceso y para quién de la compañía,

“porque si les haces formar parte del proceso, ellos van a ser mucho más proactivos a la hora de aportar información y ayudarnos a nosotros a proteger la información. Esa cultura es necesaria para que ellos sean parte de la solución final”, destaca el CIO/CISO de Cerealto Siro Foods.

Antes de poner fin al coloquio preguntamos a Sandra Espinoza sobe la madurez del mercado a la hora de proteger los datos de manera adecuada. “Es un mercado maduro, está claro, pero eso no nos exime de la innovación”, explicaba la ejecutiva de Commvault, añadiendo que las grandes preocupaciones están en torno a GDPR, la dispersión de los datos, el crecimiento incontrolado de los mismos, o las nuevas técnicas que se aplican a la información. Hay mucho por hacer y tecnologías de tipo scale out, cyber deception, inteligencia artificial aplicadas a la protección de datos “son los grandes dinamizadores del mercado y de los productos”, decía también Espinoza recordando que son muchos los clientes de la compañía que van más allá de la copia de seguridad.

"Somos custodios de la información de la compañía, no somos propietarios de ella"

Juan Manuel García Dujo,
CIO y CISO, Cerealto Siro Foods

Borja Pérez, Director General, Stormshield Iberia
Nuria Andrés, Estratega de ciberseguridad, Proofpoint

El dato como perímetro de seguridad

Borja Pérez, Director General de Stormshield Iberia, y Nuria Andrés, Estratega de ciberseguridad de Proofpoint, participaron en el Foro ITDS "Protegiendo el nuevo perímetro" para hablar sobre la identidad digital y cómo protegerla.

Ofreciendo la visión de su compañía sobre la protección del dato, aseguraba Borja Díaz que hoy dia hay una hiperactividad de los datos, que están repartidos en distintas localizaciones, y a los que accedemos y con los que trabajamos de manera muy distinta a como lo hacíamos en el pasado. Asegura Borja Pérez durante su intervención que "cuando hablamos de soluciones de seguridad en general y soluciones de cifrado en

"Los datos no se pierden por sí mismos. Son los usuarios quienes interactúan con la información"

Nuria Andrés,
Estratega de ciberseguridad, Proofpoint

PONENCIA STORMSHIELD - PROOFPOINT
FORO ITDS "PROTEGIENDO EL NUEVO PERÍMETRO"

CLICAR PARA VER EL VÍDEO

particular, no solo es importante la seguridad que ofrecemos a esos datos, es muy importante que la experiencia de usuario. Si las aplicaciones son pesadas, si las aplicaciones son complicadas, el usuario no las va a utilizar o va a hacer un mal uso de ellas". Además, las soluciones de seguridad y cifrado deben ser también soluciones sencillas de desplegar y de mantener, así como darle también más poder al usuario a la hora decidir con quién va a compartir esos datos, "cuál es su burbuja de confianza y no depender tanto del de los equipos de IT, que pueden dedicarse a la gestión de ciertas cosas, pero no a gestión de los datos, porque son los usuarios quienes son dueños de ellos".

Presumiendo de ser una empresa que tiene una estrategia de seguridad centrada en las personas, asegura Nuria Andrés, Estratega de ciberseguridad de Proofpoint, que la compañía crece hacia la protección de la información; "a mí me gusta hablar de la protección de la información y no de DLP, porque ni somos un DLP tradicional ni pretendemos serlo. Nuestra propuesta se sustenta en el concepto Insider Threat", explica la directiva, añadiendo que los datos no se pierden por sí mismos y que son los usuarios los que interactúan con la información.

Desde Proofpoint entienden la protección de la información con tres pilares: proteger el contenido de la información sabiendo qué datos hay que proteger; el contexto del usuario y las amenazas, porque si un usuario tiene una cuenta comprometida, se tiene que saber porque puede haber una posible fuga de información.

"No solo es importante la seguridad que ofrecemos a esos datos, es muy importante la experiencia de usuario en el uso de herramientas de cifrado"

Borja Pérez, Director General, Stormshield Iberia

Contenido relacionado

- Stormshield
- Proofpoint
- Ponencia Stormshield
- Ponencia CyberRes

Compartir en RRSS

FORO it Digital Security

Mesa Redonda

¿Quién es el responsable de la protección del dato?

Los datos son uno de los activos más importantes de las empresas de hoy en día. Es por ello que se han convertido en un gran objetivo de los ciberdelincuentes, por lo que la seguridad del dato es esencial en todo plan de seguridad empresarial.

La gestión y la protección del dato cada vez están teniendo más importancia, sobre todo en un contexto como el actual en el que el perímetro ha desaparecido. La descentralización del dato ha hecho que el número de posibles brechas a las que se enfrentan las empresas se multiplique. Para hablar de los retos en la protección del dato, cómo securizarlos correctamente, cuáles son sus principales amenazas y del impacto de normativas como el GDPR, nos acompañan en esta Mesa Redonda, celebrada en el marco del Foro ITDS "Protegiendo en nuevo perímetro", Borja Pérez, Director General de Stormshield Iberia; Nuria Andrés, estratega de ciberseguridad de Proofpoint; José Ramón Monleón, CISO

"Tenemos que definir los casos de uso y, sobre todo, a qué usuarios hay que controlar o vigilar"

Nuria Andrés, estratega de ciberseguridad, Proofpoint

de Orange; Alonso Hurtado, Socio IT, Risk & Compliance de Écija Abogados; Alberto López Rodríguez, CIO/CISO de Solaria Energía y Eva Cañete, CISO de Unicaja Banco.

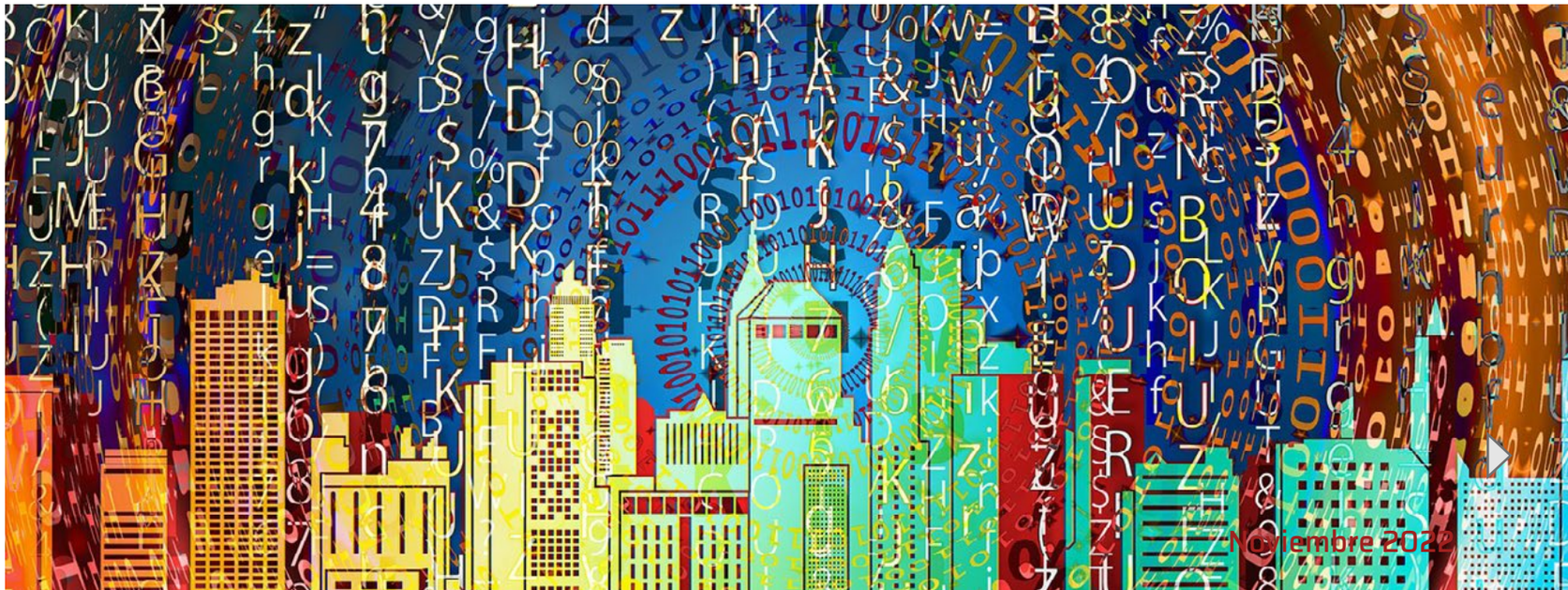
Los desafíos de la protección del dato

El primer tema a debatir en esta mesa redonda es el de los retos que rodean al dato. Para José Ramón Monleón, "A lo que nos enfrentamos es a la pérdida del perímetro, con equipos en un entorno virtualizado y con un cadena de suministro que cada vez es más importante. En ese contexto de pérdida de perímetro, uno de los retos principales es empoderar al usuario ya que es uno de los vectores de ataque más significativos".

Por el otro lado, también deben enfrentarse a retos del mundo de las comunicaciones, sobre todo a raíz de la llegada del 5G: "Cuando empezó se había tenido en cuenta ya la seguridad en su diseño y hoy los retos que debemos afrontar tienen que ver con desarrollar las medidas de seguridad, tenerlas en cuenta, aplicarlas e implementarlas para que esta nueva tecnología, que genera tantas expectativas, sea totalmente segura para nuestros clientes".

El primer tema a debatir en esta mesa redonda es el de los retos que rodean al dato. Para José Ramón Monleón, "A lo que nos enfrentamos es a la pérdida del perímetro, con equipos en un entorno virtualizado y con un cadena de suministro que cada vez es más importante. En ese contexto de pérdida de perímetro, uno de los retos principales es empoderar al usuario ya que es uno de los vectores de ataque más significativos".

Por el otro lado, también deben enfrentarse a retos del mundo de las comunicaciones, sobre todo a raíz de la llegada del 5G: "Cuando empezó se había tenido en cuenta ya la seguridad en su diseño y hoy los retos que debemos afrontar tienen que ver con desarrollar las medidas de seguridad, tenerlas en cuenta, aplicarlas e implementarlas para que esta nueva tecnología, que genera tantas expectativas, sea totalmente segura para nuestros clientes".



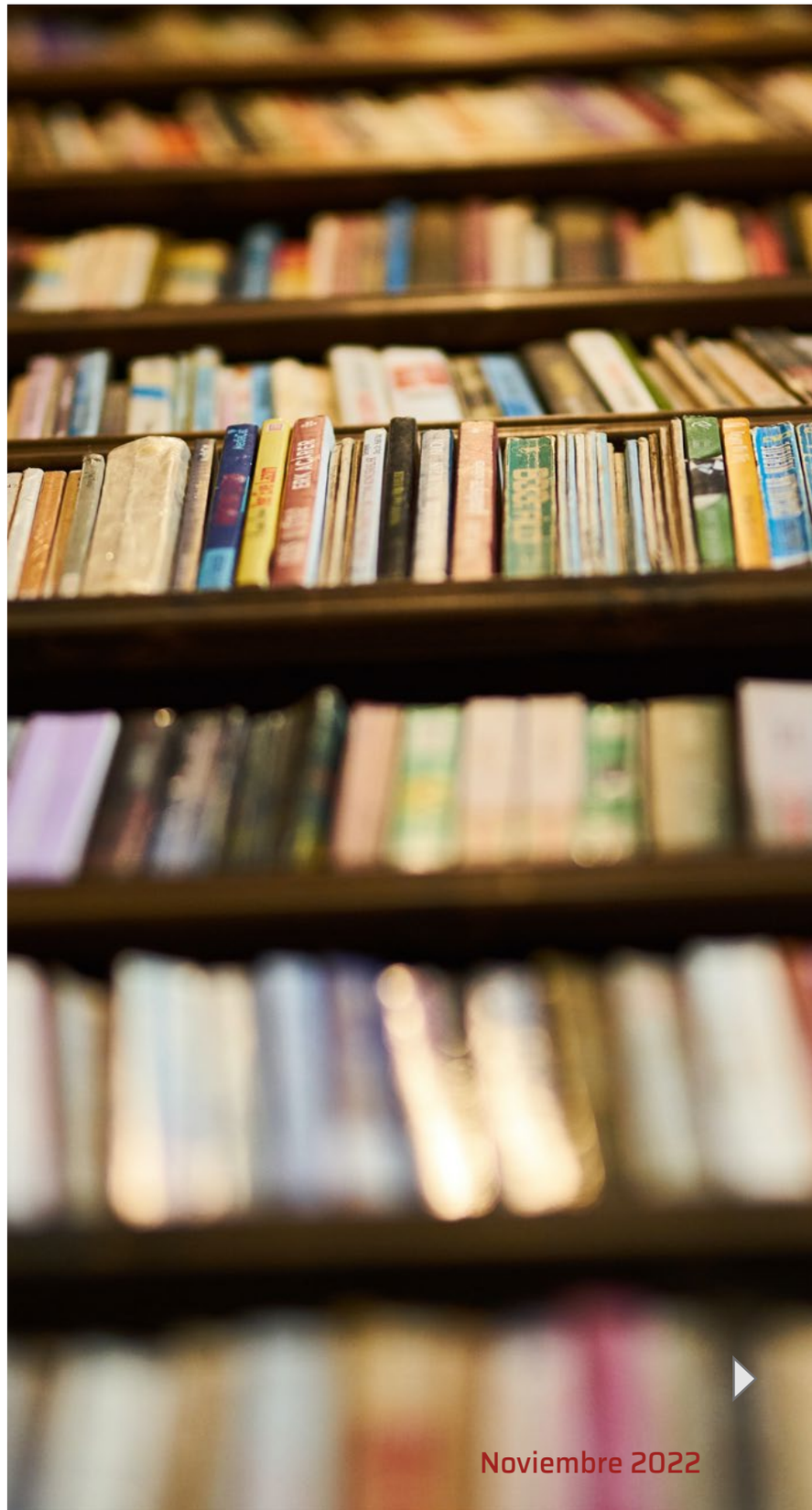
"El mercado de seguridad del dato está creciendo realmente"

José Ramón Monleón, CISO, Orange

Según Alonso Hurtado, "Cada vez vemos que hay más presión regulatoria, más normas que regulan, entre ellas una relativamente reciente con relación a las medidas de seguridad con el 5G. Cada vez vemos también mayor uniformidad de las normativas, al menos dentro del Espacio Económico Europeo, cosa que viene a facilitar en cierta medida y a romper ese tabú de la legislación local, que siempre está apegada a lo puramente local, porque parece que ya por fin se ha dado cuenta el regulador de que o ponemos soluciones globales al menos regulatoriamente, o no va a valer para mucho", y añade: "el usuario al final es eslabón débil. Entonces es el ataque que estamos viendo más típico es vía usuario, que acaba contaminando a toda la organización y acaba poniendo en jaque a toda la organización en cuestión de segundos".

En el caso de Alberto López Rodríguez, "dado el crecimiento que estamos experimentando desde hace tiempo aquí, sobre todo el reto es ir por delante de toda implantación de procesos. En base a los procesos nuevos que se están implantando para dar cobertura al crecimiento de la empresa, tenemos que ir por delante para implicar a la ciberseguridad por diseño en todo". "El perímetro, yo ya doy por hecho que está perdido en su amplio sentido, en tanto que tenemos un mix tanto de sistemas on premise, entornos e infraestructuras on premise, como en el cloud, para poder dar cobertura de manera ágil a todo el negocio a nivel internacional", añade.

"Para mí el mayor reto al que nos enfrentamos es el síndrome de Diógenes. Yo creo que ese síndrome de Diógenes existe y es flagrante, porque al final almacenamos una cantidad de información tremenda que es muy difícil proteger, porque tiene un ciclo de vida muy largo en el que además se mueve por múltiples lugares, lo compartes con auditores, con terceros de todo tipo y, por tanto, ese perímetro que antes tenías de protección ya no lo



¿QUIÉN ES EL RESPONSABLE DE LA PROTECCIÓN DEL DATO?

CLICAR PARA VER EL VÍDEO

"Por sí solo el DPO no va a poder hacer nada si no tiene al lado al CTO, si no tiene al lado al CISO"

Alonso Hurtado, Socio IT, Risk & Compliance, Écija Abogados

tienes, y tienes que ir a proteger el dato allá donde esté y donde se mueva" apunta Eva Cañete. Además, pone de relieve que "el problema que tenemos es que, al tener tal cantidad de información, si tratamos de proteger toda esa información como se tuviese la misma criticidad, tenemos un problema. Por lo tanto, es fundamental clasificarla y eso además ayuda a concienciar a nuestro propio usuario. Si nuestro usuario también tiene que participar en esa clasificación y es consciente de ese valor que tiene para la entidad, también nos va a ayudar a protegerlo".

En este sentido, Borja Pérez añade que, en su caso, "los proyectos que acometemos de cifrado de datos no vienen normalmente de IT, sino que vienen de alguna parte de negocio que necesita cifrar algunos datos en concreto, algunos datos críticos para el negocio. Y cada organización es un mundo,

"Sobre todo, GDPR ha sido precursora para darnos cuenta de la importancia de los datos"

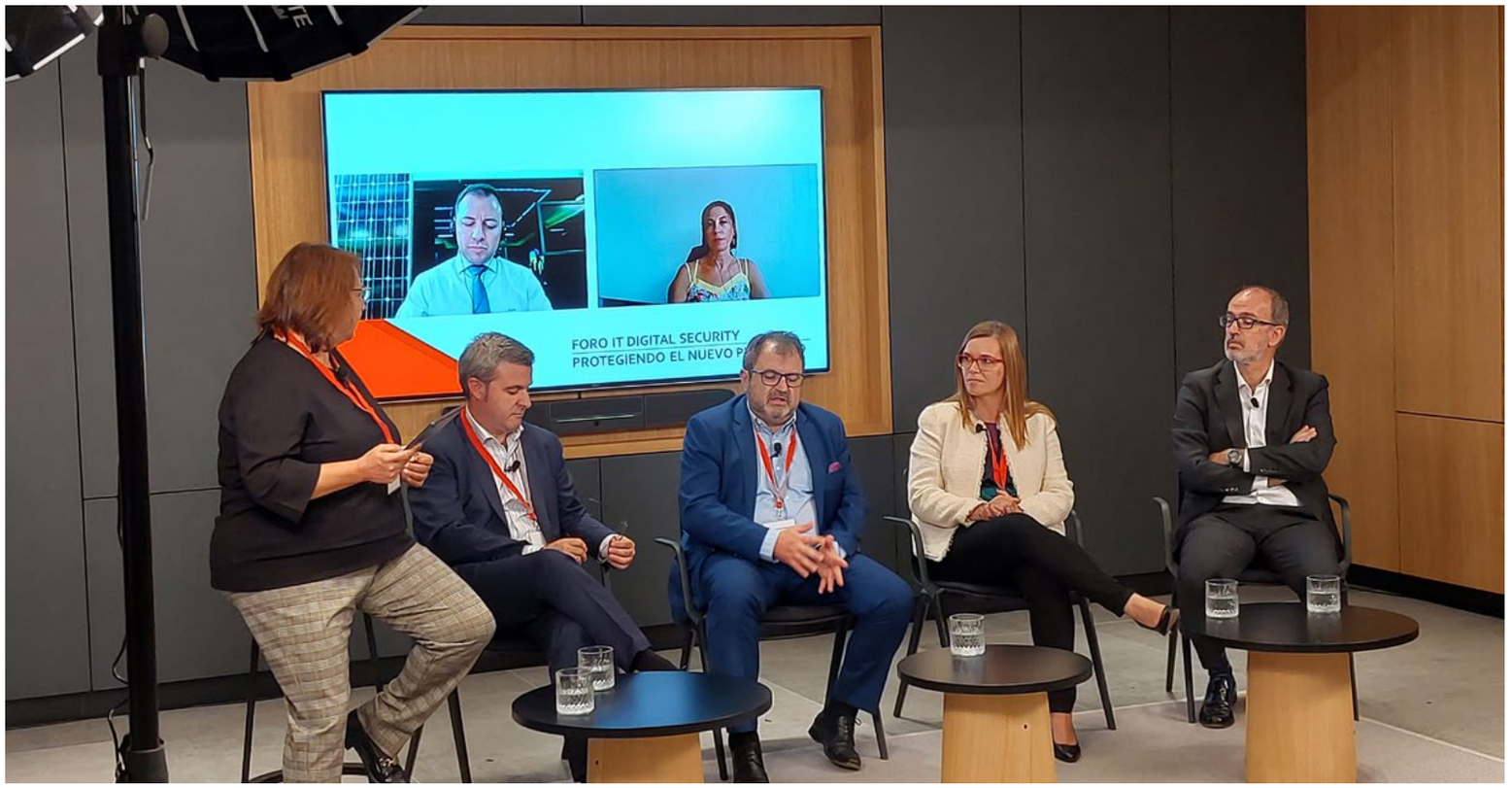
Alberto López Rodríguez, CIO/CISO, Solaria Energía

pueden ser datos de ingeniería, cuando estamos en industria, pueden ser datos de los pacientes, si estamos hablando con el SERMAS… Hay una labor previa de clasificación de la información y después ya entramos a poner las herramientas o los procedimientos que sean necesarios".

Por su parte Nuria Andrés va más allá, explicando que "siempre que hemos desplegado soluciones de protección de la información nos hemos centrado sólo en el dato, en clasificar la información. Pero hay que tener en cuenta al usuario, hay que tener en cuenta el contexto del usuario y sobre todo también ahora el compromiso de cuentas, las amenazas, porque al final un usuario puede tener una cuenta comprometida y no ser consciente de ello. Con lo cual yo destacaría que tenemos que proteger la información teniendo en cuenta al usuario, empoderando al usuario y educando al usuario, entrenando al usuario, haciendo que el usuario trabaje para nosotros y sobre todo, entendiendo su contexto".

Proteger la información en un mundo sin perímetro

Para Borja Pérez, "El uso que hacemos de los datos no tiene nada que ver con lo que hacíamos hace unos años. Tenemos datos distribuidos por todas partes, no sabemos dónde están físicamente muchas veces. Accedemos a ellos continuamente".



Es por esto que aboga por facilitarle la vida al máximo al usuario: “Las soluciones que le demos tienen que ser lo más fáciles, lo más transparentes para el usuario. Las primeras soluciones que había de cifrado de datos eran muchas veces engorrosas para el usuario y yo creo que es de lo más peligroso que hay, tener soluciones de seguridad o soluciones de cifrado que no usa el usuario adecuadamente porque son incómodas o porque le estorban en su trabajo. Creo que los desarrolladores o los fabricantes de soluciones tenemos que ir mucho en esa línea, de que las soluciones sean lo más amigables, lo más transparentes posible para el usuario”.

Nuria Andrés aprovecha para explicar por dónde empezar a la hora de mantener una buena securización del dato: “tenemos que definir los casos de uso, y definir los casos de uso es: qué información hay que proteger, porque toda la información no la podemos proteger, dónde está esa información, cuándo está en peligro esa información…”, añadiendo: “y, sobre todo, a qué usuarios hay que controlar o vigilar”.

El mercado de la seguridad del dato

En la actualidad, según José Ramón Monleón, “el mercado está creciendo. Existen cada vez más soluciones y las empresas tienen cada vez más necesidades, con lo cual ahora mismo es un mercado en auge. Las cifras que se manejaban antes de la crisis de Ucrania eran de doble dígito, con un 35% de crecimiento a diez años”. Además, destaca la importancia del Kit Digital “que ha hecho posible que se ofrezca a las empresas una serie de soluciones a un precio reducido gracias a los fondos europeos. Eso permite que las instalen, las prueben y que puedan empezar a protegerse, con lo cual es un punto muy a favor”.

Alonso Hurtado pone en valor la figura del DPO: “por sí solo el DPO no va a poder hacer nada si no tiene al lado al CTO, si no tiene al lado al CISO, y todos ellos trabajan de forma común para lograr categorizar adecuadamente y etiquetar adecuadamente la información y posteriormente podrá adoptar las medidas correspondientes”. Y añade que lo importante realmente es “correlar información, es decir, coger las características de qué es lo que está ocurriendo y ser capaces de forma no automática, pero sí de forma semiautomática, de identificar qué es lo que hay, qué es lo que está viajando por esas redes con la finalidad de poder adoptar medidas específicas, que en ocasiones muy probablemente tengan que ver con obligaciones legales directamente”.

"Para mí el mayor reto al que nos enfrentamos desde el punto de vista de los datos es el síndrome de Diógenes"

Eva Cañete, CISO, Unicaja Banco.

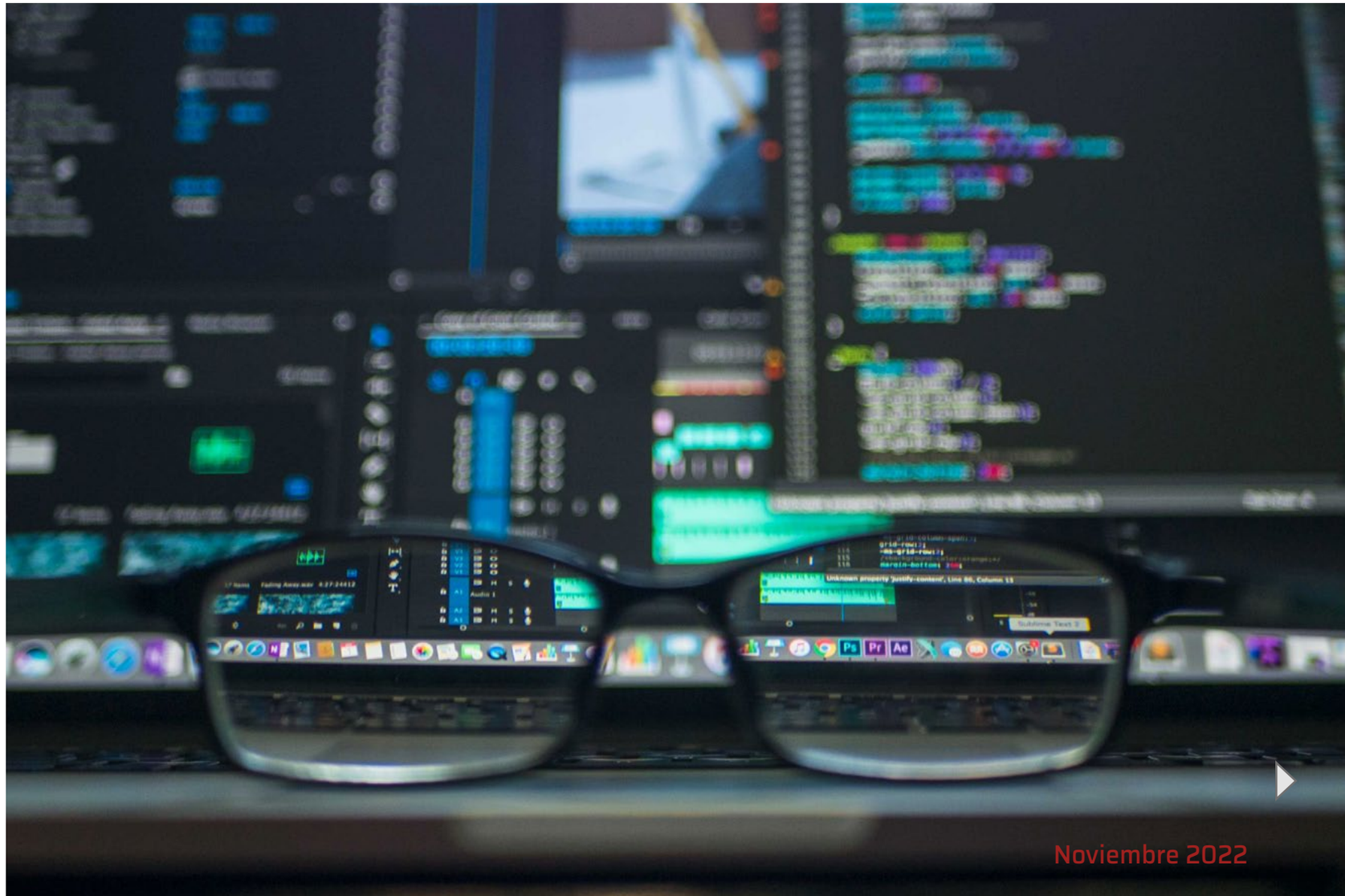
"El uso que hacemos de los datos no tiene nada que ver con lo que hacíamos hace unos años"

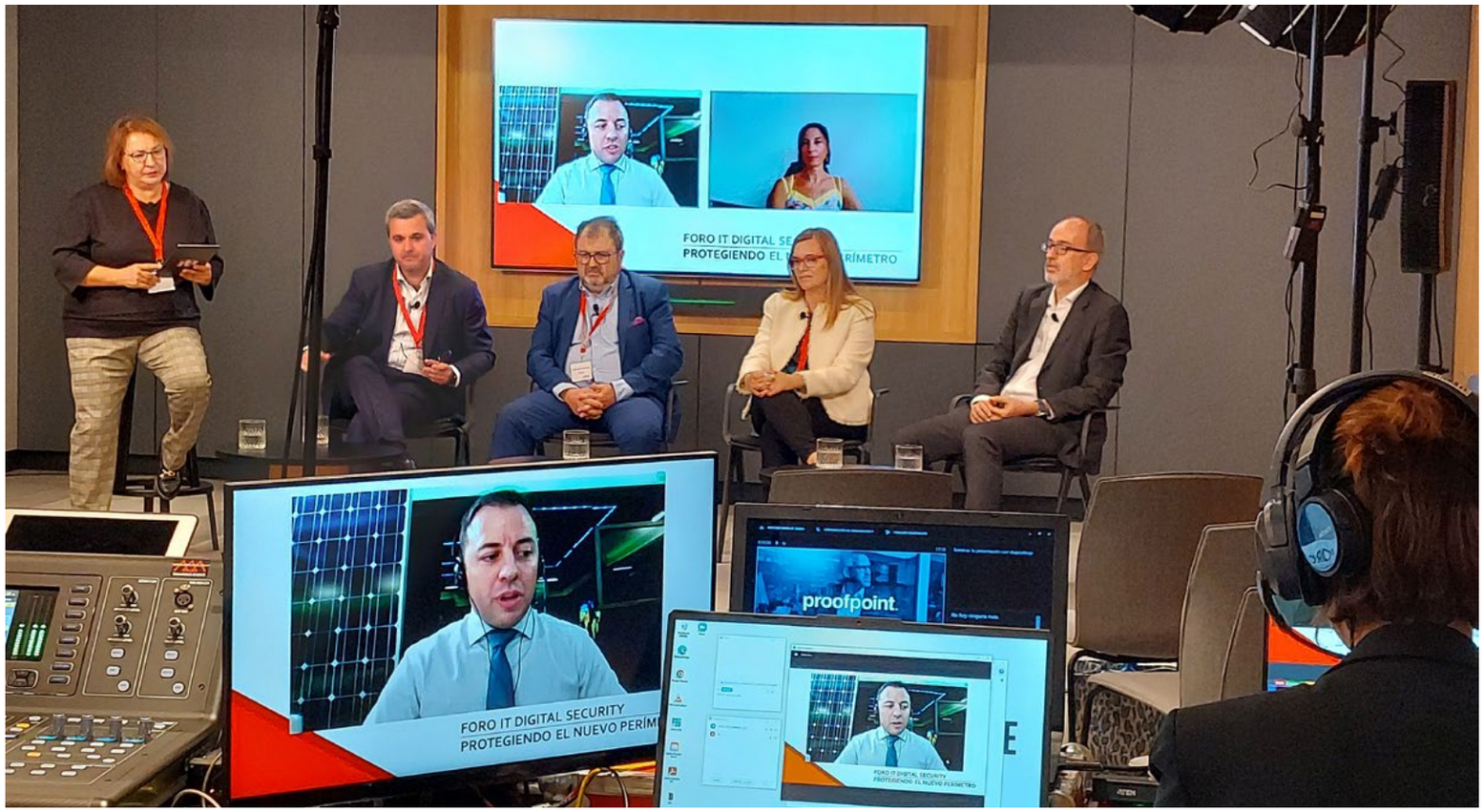
Borja Pérez, Director General, Stormshield Iberia

Legislación y otros factores como el backup

Normativas como el GDPR han tenido un gran impacto en la manera en que se afronta la protección de los datos. Como comenta Alberto López Rodríguez, esta normativa "sobre todo ha sido precursora para darnos cuenta de la importancia de los datos". "Muchos de nosotros hemos aprovechado para también implantar esa concienciación y ese diseño y arquitectura por defecto en todos los temas de seguridad. Desde mi punto de vista, ha sido precursora y lógicamente, porque era incondicional cumplir con normativa". Por otra parte, hace mención a la concienciación: "En tanto que el usuario que hace uso de esos datos y esa información no esté concienciado del mal uso que se le puede dar, y si se le da, lo que puede ocurrir, de nada sirven unos y otros servicios y tecnologías".

Otro de los puntos importantes a tener en cuenta al hablar del dato es el backup. Como señala Eva Cañete, "hay que tener en cuenta a la hora de





establecer la estrategia de backup que hay dos tipos de empresa. Por un lado tenemos las grandes empresas, que tienen más madurez en el proceso de respaldo de la información, donde además tienen todo un proceso de plan de continuidad de negocio, con su plan de recuperación y que además esos planes se prueban como mínimo un par de veces al año. Por tanto, el reto principal de este tipo de empresas estaría quizás en esa situación más tendente a nuevas amenazas, como son las amenazas de los ransomware". Por otro lado, la portavoz habla de las PYMEs, "donde los controles de seguridad que aplican son quizás todavía bastante insuficientes y donde muchas de ellas no tienen una política de backup adecuada. Entonces ahí estamos hablando de otro reto, ahí estamos hablando de que tienen que concienciarse, de que necesitan tener esas copias de seguridad, esos respaldos, necesitan tener esos planes de recuperación".

Borja Pérez también saca a colación el tema de las claves: "Algunas empresas prefieren que las claves no las gestione Google, prefieren gestionarlas ellas mismas y el propio Google es consciente de ese problema y abre sus APIs para que terceros como nosotros desarrollemos soluciones de gestión de claves. Pero lo que es fundamental para que funcione, es que el usuario siga usando Google for Workspace como lo utilizaba antes de implantarse esta solución de cifrado, que simplemente tenga que darle un clic a un botón para que se cifre el correo, se cifre el documento y lo envíe a quien desee". Por ello pone el foco en la usabilidad: "Creo que ese conflicto que ha habido tradicionalmente, cada vez que se ha intentado o se ha acometido un proyecto de este tipo, lo solucionamos desarrollando aplicaciones cada vez más sencillas de utilizar y menos invasivas".

Para finalizar, Nuria Andrés comenta que "en función de si la empresa es pequeña o la empresa es grande, el reto es distinto. Y es verdad que iniciativas como la del kit digital están ayudando a las pymes de este país a tener en cuenta la ciberseguridad, porque muchas veces piensas que eres una empresa pequeña y que a ti no te va a pasar nada. Yo creo que en la protección del dato hemos venido muy de las soluciones on premise. Lo teníamos todo dentro del perímetro y todo lo teníamos dentro de casa, dentro del castillo. Pero claro, la información ha salido fuera del castillo y tenemos que tener en cuenta la protección del mundo Cloud".

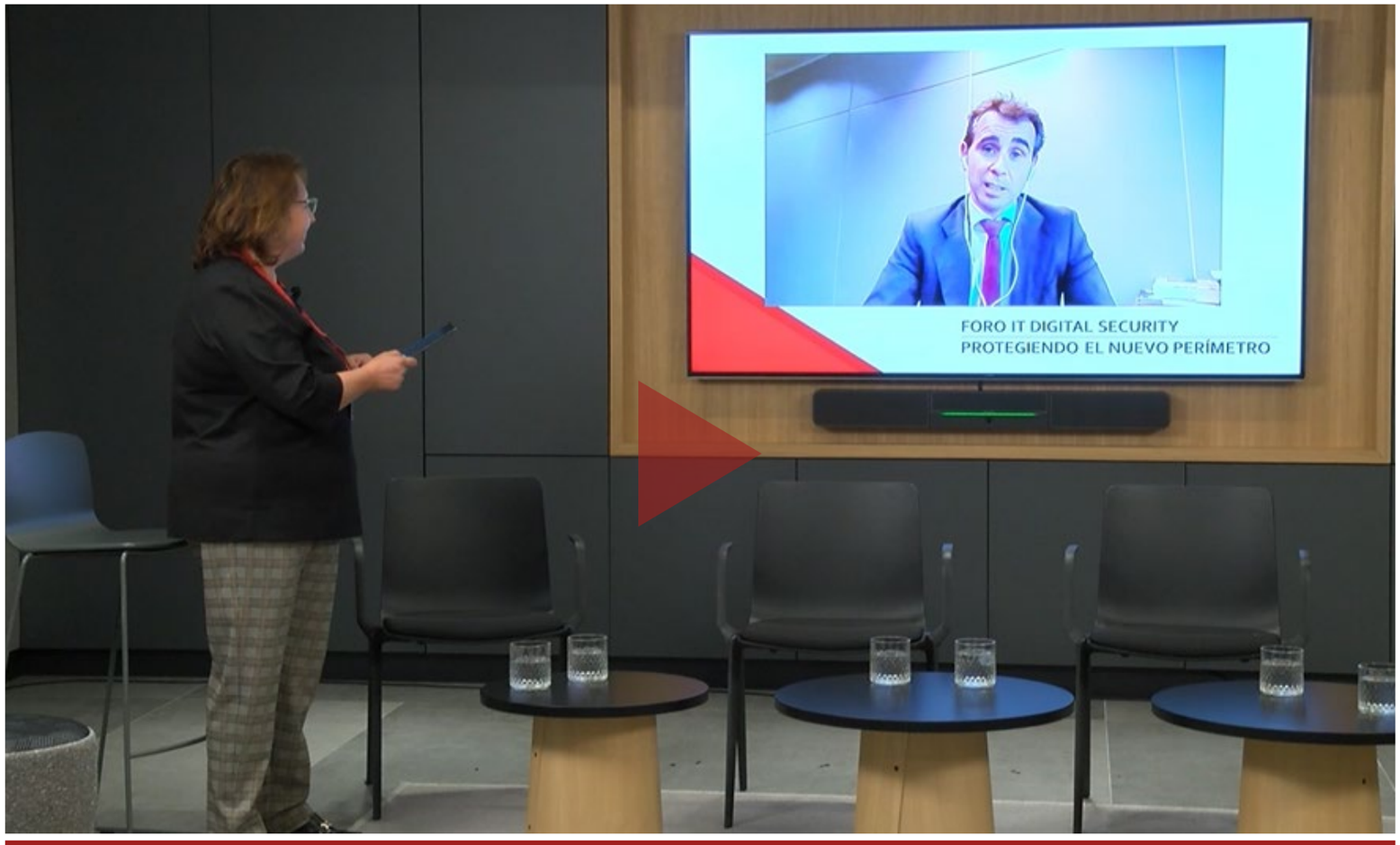
Javier Fernández Rodríguez, Director General de Seguridad y Estrategia Digital, Gobierno del Principado de Asturias

‘Que los datos sean auto gestionables da una confianza mucho mayor en el uso de los mismos’

Para Javier Fernández Rodríguez, Director General de Seguridad y Estrategia Digital del Gobierno del Principado de Asturias, hay una mayor concienciación en cuanto a la relevancia que le ha cobrado la ciberseguridad, que hay una mayor tendencia a la hora de tomar medidas, “pero tengo la sensación de que todavía necesitamos algo más de formación en esta materia y que algunas veces se nos olvida tener la consideración necesaria en todo el ámbito de seguridad”.

Añade el directivo, en una entrevista realizada en el marco del Foro ITDS ‘Protegiendo el nuevo perímetro’, que cualquier proyecto tecnológico debe contemplar un análisis muy pormenorizado de los requerimientos en materia de seguridad, “y tengo la sensación de que no siempre se recuerda esto con la debida importancia”.

Preguntado sobre los retos de ciberseguridad para las administraciones públicas, responde Javier Fernández que “se podría centralizar en el cumplimiento del esquema Nacional de Seguridad”. Explica que, aunque se puede cumplir el ENS sin las certificaciones, “creo que el hecho de certificarse te supone una obligación en el mantenimiento de las medidas que tienes en marcha” y que, aunque “no te garantizan ni mucho menos eliminar los riesgos en materia de ataques, sí te obliga a tener una política de seguridad que minimiza esos riesgos”, que es, por otra parte “a lo que podemos aspirar en cualquier organización”.



“ES EL MOMENTO DE EXPLICAR, Y QUE SE ENTIENDA, QUÉ ES LA IDENTIDAD DIGITAL SOBERANA”

CLICAR PARA VER EL VÍDEO

Hace unos meses presentaron la nueva identidad digital corporativa del Principado de Asturias. Nos cuenta Javier Fernández Rodríguez que con esta acción se persiguen dos objetivos. “Por un lado, mejorar la experiencia de nuestros usuarios, de la ciudadanía, de las empresas a la hora de relacionarse con nuestra administración por medios digitales”. Un segundo motivo ha sido modernizar la marca con un diseño de portales nuevo que tuvieran una visibilidad adecuada en los diferentes medios digitales que se utilizaban.

Desde el Gobierno de Asturias se está impulsando la identidad digital soberana. Reconoce el Director General de Seguridad y Estrategia Digital de esta comunidad que quizá el concepto no se entiende todavía muy bien, pero que “es en el momento en que se les explica y se sepa lo que es”. Añade que, teniendo en cuenta que el dato está en el centro

"Todavía necesitamos algo más de formación en materia de ciberseguridad"

de todo “el poder ser propietarios de los datos que estamos compartiendo, gestionar cómo los compartimos, a quién permitimos el acceso a esos datos individuales, tendría que tener una gran aceptación”.

Añade Javier Fernández Rodríguez que el hecho de que esos datos puedan ser auto gestionables “da una confianza mucho mayor, una transparencia mucho mayor en el uso de los mismos, y permitirá avanzar en nuevas aplicaciones que quizás hoy pueden generar dudas”.

El evento en el que se produce esta entrevista se centra en la seguridad más allá del perímetro tradicional que se estableció con los firewalls. Si tuviera que establecer un perímetro de seguridad, ¿dónde lo colocaría? “En los usuarios” responde el directivo.

Álvaro Fernández, Key Account manager, Sophos

‘No es fácil que una organización por sí misma sea capaz de gestionar la ciberseguridad eficientemente’

PONENCIA SOPHOS
FORO ITDS “PROTEGIENDO EL NUEVO PERÍMETRO”

CLICAR PARA VER EL VÍDEO

Cybersecurity-as-a-Service, o “hacernos responsables de la ciberseguridad de los clientes”, es hacia donde está evolucionando el mercado, asegura Alvaro Fernández, Key Account manager de Sophos, al comienzo de su ponencia. Añade el ejecutivo que las amenazas están creciendo, que los ciberataques se están sofisticando y que el tiempo que un atacante pasa dentro de una organización también ha aumentado, lo que lleva a las compañías “a ir estableciendo diferentes barreras que lleven a los ciberdelincuentes a invertir más tiempo en conseguir sus objetivos”.

No se olvida Álvaro Fernández del ransomware, una amenaza por la que se ven afectadas cada vez más empresas y cuyo impacto tiene un coste medio de recuperación de 1,4 millones de dólares. Esta mayor complejidad lleva

Contenido relacionado

- Sophos
- Ponencia Foro ITDS - Sophos

Con la ciberseguridad como servicio las organizaciones van a tener menos riesgos, más eficiencia y costes más bajos

al ejecutivo de Sophos a asegurar que “no es fácil que una organización por sí misma sea capaz de gestionar la ciberseguridad eficientemente”, lo que lleva directamente al concepto de ciberseguridad como servicio. ¿Qué es lo que busca esta propuesta? “Las organizaciones van a tener menos riesgos, más eficiencia y costes más bajos”, aseguraba el directivo al tiempo que señalaba que la seguridad como servicio es la conjunción de servicios, tecnologías, conocimientos y herramientas capaces de responder a los incidentes de seguridad y a los ataques.

Definía Álvaro Fernández el Cybesecurity-as-a-Service como un SOC instantáneo que puede operar el cliente, Sophos, o de forma conjunta por ambas partes; integra barreras de seguridad, que pueden ser de Sophos o de terceros; y cuenta con un equipo de expertos en ciberseguridad que pueden estar buscando esas amenazas dentro de la organización para responder en caso de que sea necesario, “y todo esto a través de una plataforma de operaciones de seguridad que puede hacer la gestión de los productos, las operaciones de seguridad y el control del servicio”.

La propuesta de Ciberseguridad como servicio permite optimizar la prevención, así como minimizar los tiempos de detección y de respuesta, algo que es clave “para hacer frente a cualquier incidente de seguridad”.

FORO it Digital Security

Mesa Redonda

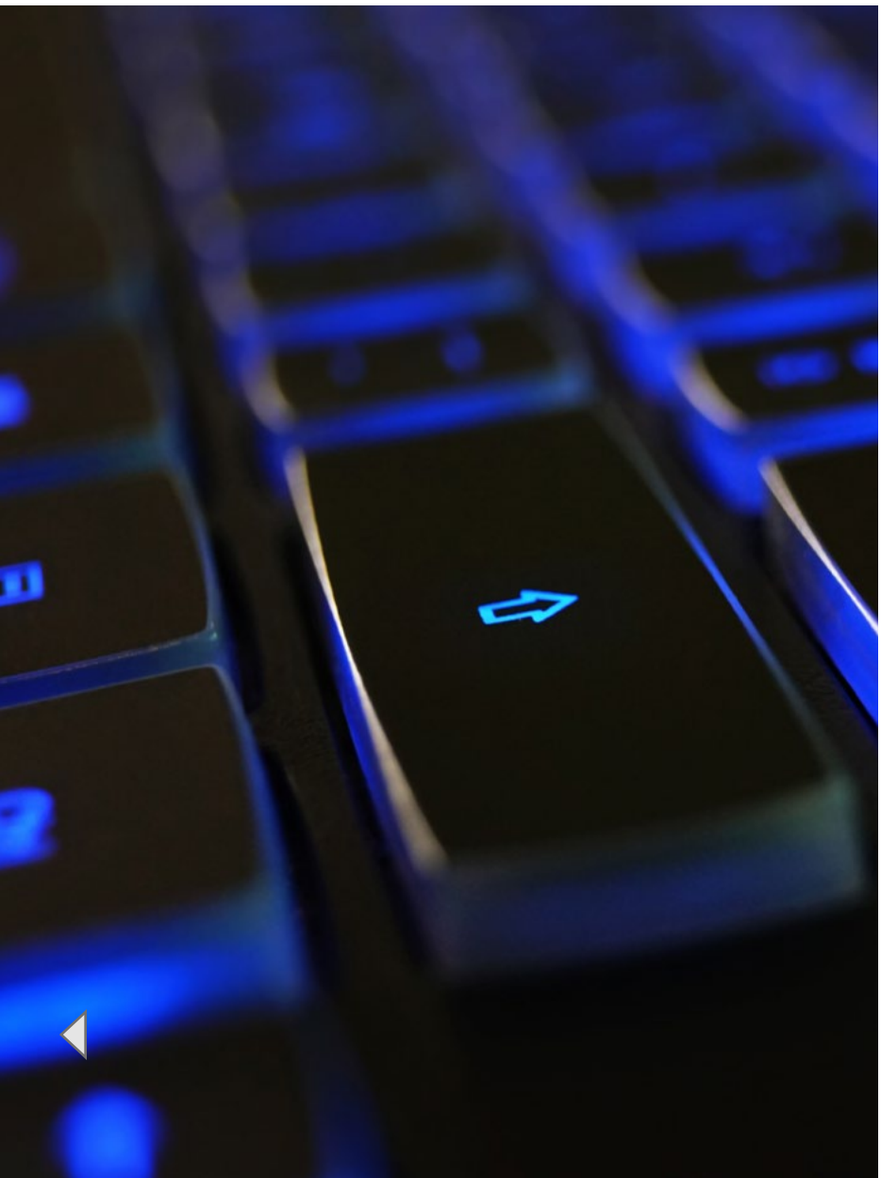
MDR, la evolución natural para la protección del endpoint

Si hay un elemento que ha recuperado protagonismo como consecuencia de la pérdida de perímetro, es el endpoint. Todo dispositivo, incluyendo ordenadores, portátiles, tablets, impresoras, sensores… que se conecte a la red y acceda a los recursos de la empresa, debe ser vigilado.

A lo largo de los años, el malware ha evolucionado y las soluciones de punto final se han nivelado para mantenerse al día con las amenazas constantes. Los proveedores de seguridad han adoptado la seguridad de punto final como un servicio para administrar mejor las nuevas amenazas. Sobre los retos que genera la seguridad endpoint, la llegada del EDR o el impacto del ransomware hemos hablado en una mesa redonda celebrada en el marco del Foro ITDS "Protegiendo en nuevo perímetro" y en la que participaron Álvaro Fernández Díaz de Güemes, Key Account manager de Sophos; Francisco Alonso Batuecas, Jefe Área CISO, Ministerio del Interior – Secretaría

de Estado; Manuel Barrios Paredes, Global CISO de SGS y Josep Bardallo, Director TI / CISO & DPO de Grupo Recoletas.

Para Manuel Barrios, el primer reto a la hora de proteger los endpoint adecuadamente es “saber lo que tenemos en las organizaciones”, teniendo en cuenta que el mundo del endpoint “no se queda en los puestos de trabajo y los servidores, como era tradicionalmente”, sino que tenemos que tener en



MDR, LA EVOLUCIÓN NATURAL PARA LA PROTECCIÓN DEL ENDPOINT

CLICAR PARA VER EL VÍDEO

cuenta todos los elementos conectados a nuestra red, esto es elementos IT, OT e IoT que va, desde las Smart TVs, CCTV o termostatos inteligentes que son puntos de entrada y ataque de los ciberdelincuentes y muchas veces no existen mecanismos de protección específicos para ellos”.

Identifica Francisco Alonso Batuecas un escenario muy parecido reconociendo al mismo tiempo que en el Ministerio del interior ha habido un antes y un después con la pandemia porque planteó un puesto de trabajo con movilidad; “no nos quedó más remedio que lanzarnos a este nuevo reto”, aseguraba el directivo añadiendo que dentro del Ministerio del Interior se está abordando un plan de transformación digital que lleva a la adopción de sistemas más modernos y seguros.

Asegurando que los entornos son cada vez más heterogéneos decía Josep Bardallo durante el

coloquio que la visibilidad es el gran reto a la hora de proteger el endpoint. Menciona también la “convivencia” porque “por mucho que yo quiera que tengamos proyectos de migración de los entornos legacy, yo sé que te va a venir una máquina de telemedicina y va a tener un sistema que va a estar obsoleto en un año y tú tienes que convivir con eso”, lo que supone tener soluciones de seguridad en los puntos finales “que sepan trabajar con eso”.

Como proveedor de seguridad planteamos a Álvaro Fernández si los dispositivos móviles y el Internet de las Cosas son los grandes olvidados de la seguridad endpoint. Responde diciendo que no cree que esto sea así, sino que los responsables de ciberseguridad de las compañías buscan establecer su línea de prioridades e ir trabajando sobre ellas. Plantea que las ofertas de ciberseguridad como servicio puede abrir opciones porque “muchas veces esos dispositivos ya están gestionados, les falta la capa de seguridad”.

Sobre el impacto que ha tenido el trabajo en remoto acelerado como consecuencia de la pandemia, dice Álvaro Fernández que “tecnológicamente se puede abordar de una forma sencilla y efectiva un trabajo híbrido de verdad. Es decir, que el trabajador pueda estar en cualquier parte y trabajar de la misma forma, esté fuera o dentro de la organización”.

> "Tecnológicamente se puede abordar de una forma sencilla y efectiva un trabajo híbrido de verdad"
>
> Álvaro Fernández Díaz de Güemes, Key Account manager, Sophos

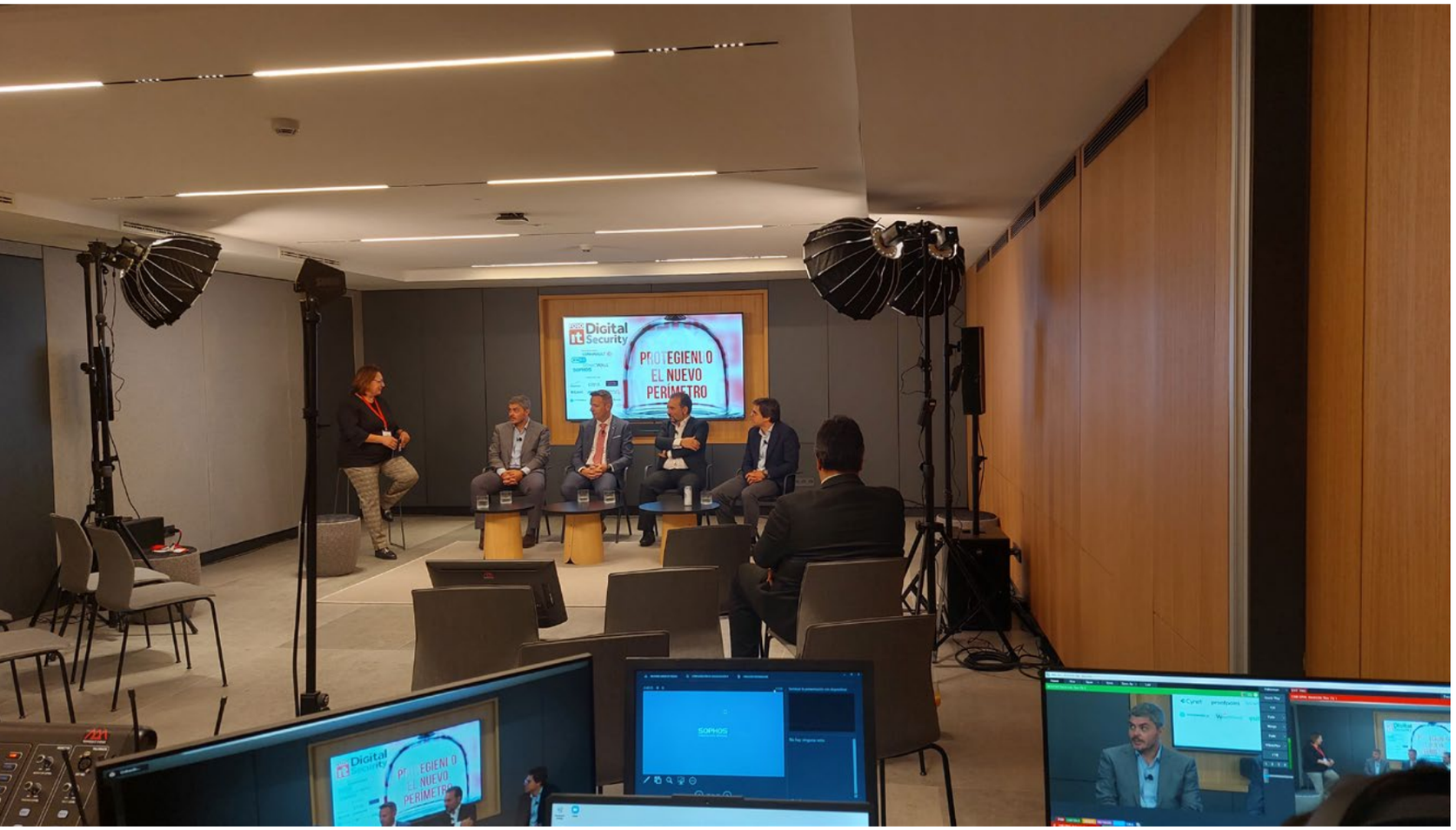
"El endpoint es lo que está definiendo el nuevo perímetro, pero la gestión de la identidad es muy importante"

Francisco Alonso Batuecas, Jefe Área CISO, Ministerio del Interior - Secretaría de Estado

Del antivirus se pasó al antimalware, después al EPP (Endpoint Protection) y se ha seguido avanzando hacia el famoso EDR/XDR/MDR… En entornos tan heterogéneos como el de SGS "tenemos que tener de todo", asegura Manuel Barrios, añadiendo que, frente a las amenazas actuales, un mecanismo basado en firmas ya no es suficiente y "hemos ido hacia mecanismos de EDR, que son casi fundamentales en cualquier organización". Es más, en opinión del CISO de SGS, en los actuales ataques de ransomware, "si los equipos hubieran estado parcheados y con soluciones de EDR", la mayoría no hubieran tenido éxito. En cualquier caso, concluye, "siguen existiendo puntos vulnerables en una organización, no existen tecnologías para poderlos proteger y para un atacante son puntos de entrada, y hay que bregar con esos riesgos".

Sobre si la empresa española está o no preparada para las soluciones la opinión de Manuel Barrios es que no se trata de que esté o no esté, sino de "tiene que estar preparada por obligación. Si no lo está, está asumiendo un riesgo inasumible", asegura.

"Nosotros tenemos EDR desde hace tiempo", dice Francisco Alonso Batuecas, añadiendo que no sólo vale con este tipo de herramientas, sino que tienes que implantar otras. Menciona en concreto las de



automatización “para poder interpretar toda la información de las diferentes herramientas que tenemos en seguridad” para que los tiempos de respuesta sean ágiles. Recuerda también el directivo el ambicioso proyecto de SOC para la AGE liderado por Ángel Amutio.

Sobre si Zero Trust está impulsando una mejorar de la ciberseguridad menciona el responsable de ciberseguridad del Ministerio del interior que es un concepto que no se queda en el endpoint; “el endpoint es lo que está definiendo el nuevo perímetro, pero la gestión de la identidad es muy importante, así como la gestión de accesos y todo esto se hace para proteger la información”, comenta el directivo.

Mencionamos el ransomware como una de las amenazas que quitan el sueño a los responsables de ciberseguridad. “Hoy en día ya está asumido que vamos a tener incidentes”, asegura Josep Bardallo, añadiendo que lo más importante es contar con cualquier elemento, producto o tecnología que ayude a detectar el incidente muy rápidamente. Por eso la detección y respuesta son imprescindibles”

"El primer reto a la hora de proteger los endpoint adecuadamente es saber lo que tenemos en las organizaciones"

Manuel Barrios Paredes,
Global CISO, SGS

"Lo más importante es contar con cualquier elemento, producto o tecnología que ayude a detectar el incidente muy rápidamente. Por eso la detección y respuesta son imprescindibles"

Josep Bardallo, Director TI / CISO + DPO, Grupo Recoletas

"Que tenga mucha capacidad de respuesta" es una de las características que el CISO de Grupo Recoletas le pediría a un EDR. Añade una segunda: "que sea cuanto más heterogéneo mejor" para que de servicios a los actuales entornos. Menciona también que "no podemos proteger a los usuarios porque se han dispersado, pero sí los datos", lo que les empuja a buscar tecnologías que funcionen sin nube y sean autónomas.

Cuando hablamos de EDR hablamos de ser capaces de detectar algo, entendiendo qué está pasando realmente, que la protección automática o automatizada no ha sido capaz de detectar. El siguiente paso, la evolución natural, es hacerlo de una manera gestionada, y eso es el MDR (Managed Detection and Response), necesario porque la mayoría de las empresas no tienen la capacidad de analizar todos los datos y entenderlos.

"Tarde o temprano necesitas alguien de fuera que esté vigilando y actuando rápidamente", asegura Josep Bardallo, añadiendo que el MDR "va a pasar por delante de los SOCs". Explica que ahora mismo el SOC es alguien mirando un montón de alertas y lo que hace el MDR es automatizar todo eso "y que haya gente con capacidad de responder en tiempos muy cortos, que es lo que la empresa quiere".

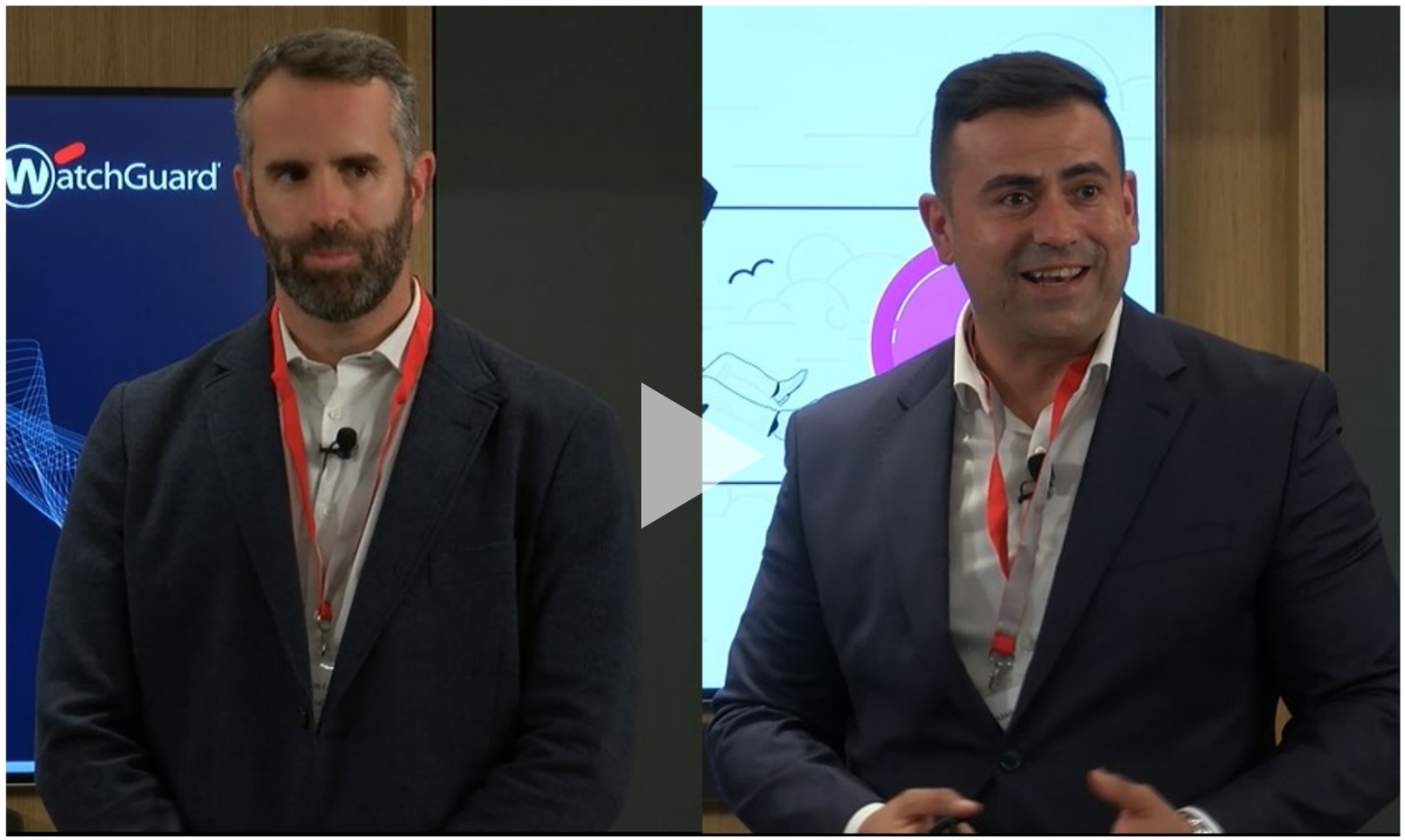
Para Francisco Alonso Batuecas contar con un MDR o un EDR capaz de automatizar tareas "es fundamental porque si no el SOC no va a ser suficiente".

Manuel Barrios destaca que un MDR sobre todo aporta la especialización. Dice que cuando una empresa se enfrenta a un evento de malware "una compañía que propone ese tipo de servicios y que está bregando con tu caso y con el de otras empresas, aporta un conocimiento y una especialización que es de un valor añadido bastante importante".

Carlos Castro, Strategic Account Manager, WatchGuard Cytomic
Javier Cazaña, Country Manager Iberia, Cynet

El endpoint recobra protagonismo

Carlos Castro, Strategic Account Manager de WatchGuard Cytomic, y Javier Cazaña, Country Manager Iberia de Cynet ofrecieron su visión de la protección del endpoint a través unas ponencias en el Foro ITDS "Protegiendo el nuevo perímetro".



PONENCIA WATCHGUARD - CYNET
FORO ITDS "PROTEGIENDO EL NUEVO PERÍMETRO"

CLICAR PARA VER EL VÍDEO

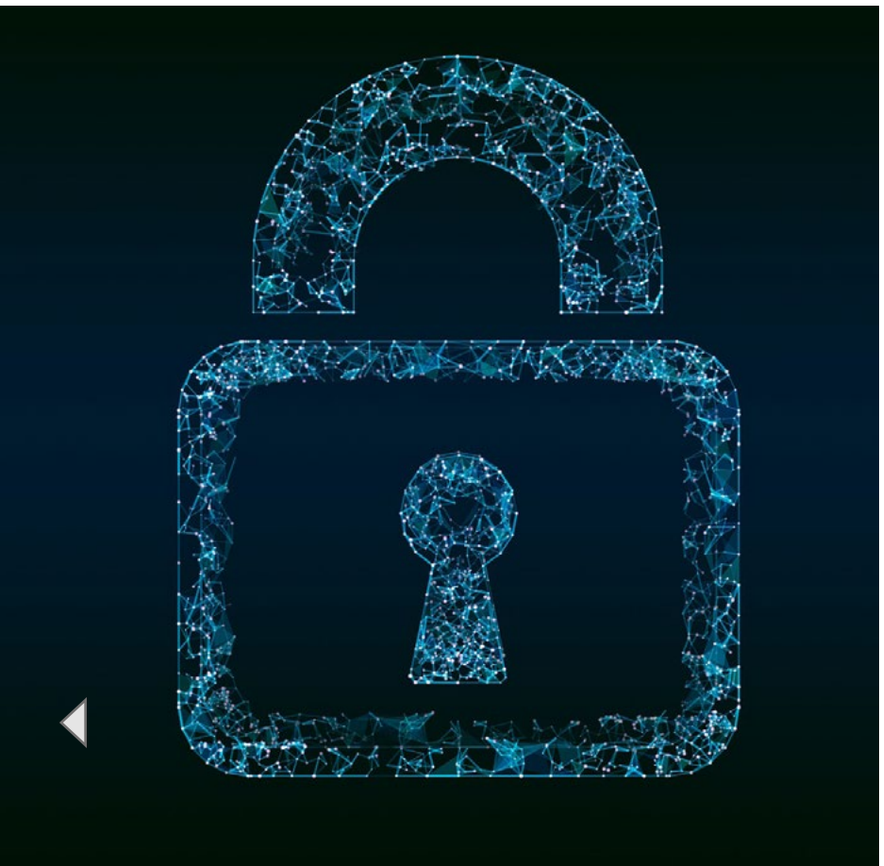
Quiso centrarse Carlos Castro en el Framework de defensa del endpoint de la compañía centrándose en dos o tres puntos clave que marcan la diferencia y dan valor a los clientes. La primera, asegura el directivo, es una "inteligencia colaborativa compartida", porque, en este complejo mundo de la ciberseguridad "es un requisito imprescindible unir fuerzas". El segundo punto a destacar tiene que ver con la filosofía Zero Trust que busca no permitir ningún tipo de acceso o de ejecución hasta que se haya analizado y donde se tiene en cuenta el contexto porque "hay cosas que son perfectamente válidas, pero dependiendo del contexto empiezan a ser sospechosas". Se añaden en este punto tecnologías antiexploit basadas en cloud, resolución de incidentes, etc. La tercera gran diferencia de WatchGuard Cytomic son los servicios de Threat Hunting que, para Carlos Castro, son "el complemento imprescindible y necesario para dar la última capa de protección a la que no llegamos de forma automatizada".

"Hay cosas que son perfectamente válidas, pero dependiendo del contexto empiezan a ser sospechosas"

Carlos Castro, Strategic Account Manager, WatchGuard Cytomic

Comienza su ponencia Javier Cazaña hablando de Cynet, una compañía que nace en 2015 para llevar tecnología de detección y respuesta más allá del mundo enterprise con la automatización como gran aliada. Cynet, asegura el directivo, "da respuesta a todas esas preguntas de los clientes con los que nos sentamos en el día a día", como es la falta de visibilidad, o lo complicado de encontrar recursos humanos. La propuesta de Cynet es un XDR capaz de analizar la información que proporcionan los diferentes sensores y herramientas de la empresa para analizarla "y decir automáticamente qué permito y qué no y cómo mejorar la postura de seguridad de una manera proactiva".

Destaca Cazaña que la compañía es capaz de acelerar el tiempo de respuesta y añadir técnicas de engaño, de Deception, como elemento diferencial a otras herramientas de detección y respuesta. "Nosotros no aparecemos en Gardner, pero somos los terceros en el MITRE", concluye Javier Cazaña.



"Cynet da respuesta a preguntas como la falta de visibilidad y de talento"

Javier Cazaña, Country Manager Iberia, Cynet

Contenido relacionado

- WatchtGuard Cytomic
- Cynet
- Bitdefender
- W Ponencia WatchGuard Cytomic
- W Ponencia CyberRes

Compartir en RRSS

FORO it Digital Security

Mesa Redonda

La seguridad endpoint a debate

Con la pérdida del perímetro y los nuevos formatos de trabajo multidispositivo y deslocalizado, la protección del endpoint ha cobrado una mayor importancia si cabe. Además, estas tecnologías deben ser sencillas y poco intrusivas en el día a día del trabajador.

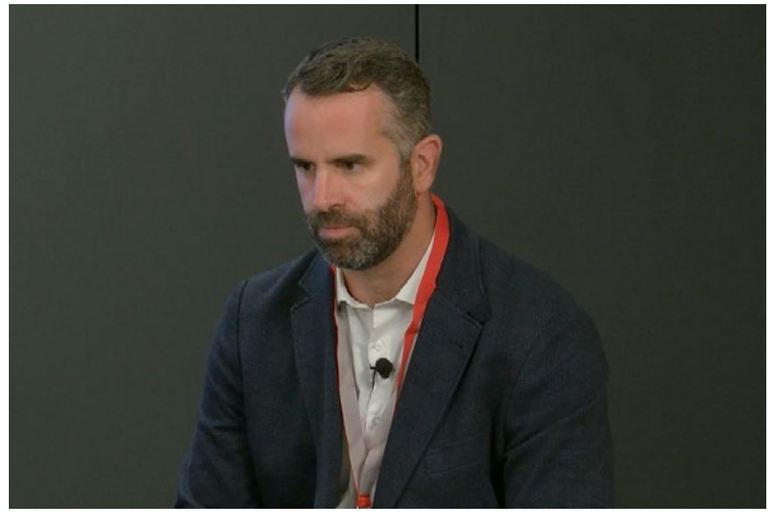
A día de hoy, los profesionales utilizan varios dispositivos para desempeñar su labor. Y no solo eso, sino que además ya trabajan desde cualquier lugar, lo que ha hecho que el perímetro prácticamente deje de existir. Además, tendencias como el bring your own device dificultan aún más si cabe la labor de los responsables de seguridad, que se enfrentan a un desafío mayor. Para hablar de los retos de la protección del endpoint, el papel del Zero Trust o tecnologías como el Threat Hunting, nos acompañan en esta mesa redonda Carlos Castro, Strategic Account Manager de WatchGuard Cytomic; Javier Cazaña, Director general de Cynet Iberia; Sergio Bravo, Iberia Sales Director de Bitdefender; Francisco Ramón García Otero, Responsable de Ciberseguridad de Naviera Armas Trasmediterránea; Pedro Navas Galán, CIO/CISO de Pons; Daniel Puente Pérez, Global CISO de Cirsa y Juan Carlos Castro Ortiz, CISO de Ayesa.

Los retos a la hora de proteger el endpoint

La securización del endpoint ha tomado un papel protagonista en todo plan de seguridad que se precie, sobre todo a causa de la gran cantidad de dispositivos diferentes que los trabajadores utilizan en su día a día. Como comenta Francisco Ramón García Otero, “nos enfrentaríamos a dos retos principales. El primero es una falta de estandarización en los endpoint”. Como indica el portavoz, en el mundo empresarial se utilizan diferentes marcas y

modelos de dispositivos, cada uno con estándares diferentes. “eso al final causa un problema, ya no a nivel corporativo con los dispositivos que se dan a los usuarios, que pueden ser más o menos estándar, sino con la incorporación del modelo de bring your own device, que estamos viviendo en muchas de nuestras compañías”. “Otro segundo punto es la pérdida de foco, porque nos centramos mucho en la empresa, en la gran empresa, en la pyme, pero nos estamos olvidando de un modelo de negocio que está generando mucho dinero, que son esos chavales que juegan a videojuegos en su casa y que estrimean, y que todos ellos tienen un PC en el que, con mucha suerte, tienen un antivirus y en el que ninguno de ellos tiene por detrás un departamento de ciberseguridad y ni mucho menos un CISO que les dé seguridad”.

Coincide Pedro Navas Galán, cuando señala que “el principal problema es que son muchos los dispositivos a proteger y variados”. “Hoy la tecnología sigue evolucionando, siguen apareciendo nuevos dispositivos y al final es complejo aplicar un esquema de seguridad para todos ellos. Sí que es cierto que el punto de partida tiene que ser una planificación estratégica, porque muchas veces el día a día nos impone de alguna forma tomar decisiones puntuales sobre ciertos casos, casuísticas y dispositivos, y nos focalizamos mucho en ciertos puntos y no hay una visión estratégica global a nivel de empresa. Entonces, es fundamental que al final



"Los dispositivos móviles simplemente forman parte ya del endpoint, son un endpoint más"

Carlos Castro,
Strategic Account Manager
de WatchGuard Cytomic.

"Se ha hecho una gran inversión durante los últimos años en tecnología"

Javier Cazaña,
Director general de Cynet Iberia

LA SEGURIDAD ENDPOINT RECOBRA PROTAGONISMOFOTO

CLICAR PARA VER EL VÍDEO

tengamos una idea muy clara de qué tenemos que proteger". Además, hace hincapié en la necesidad de una planificación: "una vez identificado mi plan estratégico, vamos a trabajar en esta línea. Luego ya, empezar a aplicar políticas, medidas de seguridad e ir trabajando en función de necesidades".

Daniel Puente Pérez va más allá, indicando que "todos nos hemos encontrado empresas en las que hay un sistema crítico para la empresa que está funcionando en un Windows completamente obsoleto, y eso también hay que protegerlo. Pero no por ser obsoleto no constituye un riesgo, sino justamente lo contrario. Suponen el mayor riesgo". Además, subraya la importancia del papel del usuario: "El endpoint casi siempre va asociado al usuario, y lo estamos empoderando cada vez. Antes tenía un ordenador muy cerradito, que hacía cositas muy encorsetadas y ahora les estamos dando mucha más

libertad y tenemos también que tutelarlos, tenemos que formarlos, tenemos que ayudarles. Así que los retos son incontables".

Para Juan Carlos Castro Ortiz, "estamos muy acostumbrados a trabajar con siglas tipo MDM, MTM, ahora UDM, de Unified Device Mangement... Nuestro plan de ciberseguridad pasa por ahí, por intentar recoger toda la telemetría que podamos de estos dispositivos finales", y añade: "en nuestro roadmap está integrarlo con una serie de outputs para intercambiar información entre las diferentes herramientas de seguridad que tenemos, que yo creo que es fundamental, y crear un poco esa red de malla SMA, que es un término que yo creo que se estará imponiendo durante el último año".

A la hora de hablar de tablets y smartphones, Carlos Castro apunta que "los dispositivos móviles simplemente forman parte ya del endpoint, son un endpoint más. Al final son los que nos definen el perímetro. Llevamos mucho tiempo hablando de

"El siguiente paso es intentar conseguir una visibilidad ampliada de lo que ocurre en los endpoints"

Sergio Bravo,
Iberia Sales Director de Bitdefender

"Para mí es crítico que un cliente que protege el endpoint sea capaz de trabajar de forma standalone, de forma autónoma"

Francisco Ramón García Otero, Responsable de Ciberseguridad de Naviera Armas Trasmediterránea

que el perímetro ya no existe, que el perímetro es muy difuso. Yo directamente empezaría a dejar de usar la palabra perímetro para definir esto, porque al final el perímetro lo están formando las personas que usan cada dispositivo y una persona además usa varios dispositivos al día para trabajar, en lo personal y para otras muchas cosas". Por otro lado, no se olvida de los dispositivos IoT: "En los dispositivos IoT sí que hay una variedad inmensa, imposible de controlar cada uno de los dispositivos, cada fabricante lo hace lo mejor que puede, otros lo hacen muy mal directamente, con unos agujeros de seguridad muy grandes. Al final, lo que tenemos que proteger no es sólo el dispositivo final, sino todo lo demás y todo lo que lo envuelve la comunicación y el endpoint con el que se va a conectar ese dispositivo…".

¿Qué es necesario para una buena solución de endpoint?

Javier Cazaña cree que "se ha hecho una gran inversión durante los últimos años en tecnología. Uno de los primeros retos es implementar realmente lo que se ha adquirido, pero claro, tiene que ser sencillo. Tiene que ser fácil el hecho de poder recibir esa información y poder automatizar al máximo para así tener esa eficiencia, de hecho muchos procesos deberían de ser automáticos. Tenemos la capacidad gracias a los análisis de comportamiento, de poder ir entendiendo y poder ir de una manera continua, mejorando nuestra postura de seguridad, de tal manera que en cualquier momento debemos de poder ir un paso más allá". Además, hace foco en la tecnología, en la usabilidad y en el precio, cuando indica que "toda esa estrategia

recae en tecnología. Tenemos que tener una tecnología sencilla que sea fácil de implementar, pero sobre todo que se ajuste a presupuesto".

Para Sergio Bravo, "las empresas en España están preparadas para este tipo de soluciones, pero por necesidad". Con la nueva realidad del trabajo, el formato híbrido, la eliminación del perímetro, el portavoz subraya que "han salido nuevos vectores, nuevas amenazas persistentes, que lo que hacen es que por fuerza las empresas hayan tenido que ir madurando para poder adaptarse y sobreponerse a estas nuevas amenazas que están surgiendo. Eso supone un reto importante". Es por ello que pone foco en un concepto que identifica como el siguiente paso en la protección del endpoint: la visibilidad. "Empezamos por antivirus, antimalware, protección de endpoint… ¿y ahora que hacemos? Todo eso está muy bien, pero nos quedamos en la parte de protección, vamos un pasito más allá. El siguiente paso es: vamos a intentar conseguir una visibilidad ampliada de lo que ocurre en los endpoints".

> "El principal problema es que son muchos los dispositivos a proteger y variados"
>
> Pedro Navas Galán, CIO/CISO de PONS

A la hora de enumerar las características que un responsable de seguridad le pide a una solución de endpoint, Francisco Ramón García Otero lleva el discurso a su terreno, apoyándose en las necesidades especiales de su compañía: "para mí es crítico que un cliente que protege el endpoint sea capaz de trabajar de forma standalone, de forma autónoma. Sé que no tenemos el ordenador de la NASA en cada barco, entonces hay un cierto nivel de cálculo y cierto nivel de criterio, pero sí que tenga una capacidad autónoma de proteger nuestros activos cuando no tienen una conexión abierta con el exterior.

Pedro Navas Galán lo pone más sencillo: "cuando analizas estas soluciones, te fijas en los estándares básicos, que tengas una consola única para gestionar todos los productos, algo que tengas en la nube, también que de alguna forma tengas capacidad de filtrado de web, que tengas filtrado de correo según la solución… Al final son medidas de seguridad que vas a aplicando". Para el portavoz, "el mercado es muy amplio, hay cantidad de soluciones de todo tipo, pero fundamentalmente lo que tengo que intentar es que esas soluciones vayan muy en línea con mi política de seguridad, porque puede ser la mejor solución del mundo, pero si no encaja en lo que yo tengo implementado…".

"El endpoint casi siempre va asociado al usuario, y lo estamos empoderando cada vez. Hay que ayudarle"

Daniel Puente Pérez, Global CISO de CIRSA

Zero Trust, Bring your own device y Threat Hunting

"Hemos pasado de una cultura en la que lo tenemos todo centralizado en los CPDs a una cultura en la que estamos queriendo, voluntaria o involuntariamente, llevarlo todo al endpoint. Ahí no debemos cometer el error de darle carta blanca al endpoint. El no confiar ciegamente tiene que ser siempre una premisa, pero no solo en esto, sino en casi todo", argumenta Daniel Puente Pérez, que añade: "estamos viendo cómo los malos siguen evolucionando, cómo hace cuatro días empezaron a impersonar el correo, luego las tarjetas SIM, ya nada queda fuera de su alcance. Por lo tanto, toda la política Zero Trust tenemos que seguir implementándola. Hace unos años ya se nos requerían los medios de identificación de algo que tengo, algo que soy y algo que sé, pues esto tenemos que llevarlo todavía a un punto más moderno".

Para Juan Carlos Castro Ortiz, el impacto del trabajo híbrido "ha sido alto. Nos enfrentamos a un aumento de la plataforma de exposición, eso es innegable. No es lo mismo estar bajo el paraguas de protección de la empresa que en un domicilio con salida directa a Internet. No obstante, gracias a los nuevos endpoints, podemos aunar varios elementos de detección y de tranquilidad, como por ejemplo la inteligencia artificial y el Big Data, que permiten mejorar de forma autónoma la detección y la prevención de amenazas complejas, así como su posterior eliminación o mitigación". Por otro lado, se muestra categórico cuando afirma que "no existe el endpoint perfecto, eso es imposible, sino el que mejor se ajusta a tu empresa u organización, en este caso a tu necesidad".

El Threat Hunting es un elemento que poco a poco se ha ido incorporando a las consolas de manera natural. En palabras de Carlos Castro, "el

"Nos enfrentamos a un aumento de la plataforma de exposición, eso es innegable. No es lo mismo estar bajo el paraguas de protección de la empresa que en un domicilio con salida directa a Internet"

Juan Carlos Castro Ortiz, CISO de AYESA

Hunting es esa última capa de protección que va a permitir entender lo que ha pasado en un incidente, protegerte o parar un incidente que está cociéndose, que está preparándose. Tiene un problema, y es que para el Hunting, al final lo que necesitamos es personal con un conocimiento experto que es muy difícil de conseguir. Falta crecer, necesitamos muchas más personas con esa experiencia y con ese conocimiento". Y añade: "las empresas normalmente no serán capaces en general de aunar ese conocimiento en su propio personal. Es algo que los fabricantes como nosotros tenemos que ofrecer y estamos en capacidad de hacerlo".

Por su parte, Javier Cazaña pone de manifiesto que lo que debe haber "es una combinación tanto de tecnología como de educación, como de ese equipo humano que está alrededor. Cuando hablamos de Threat Hunting o cuando hablamos de tecnologías de nueva generación, no es lo mismo una compañía de 10.000 usuarios con un equipo de seguridad, que una compañía con 500 usuarios, que necesita también ese nivel de protección".

En esta última intervención, Sergio Bravo remarca que "nos encontramos con que, en general, las empresas evidentemente quieren tener toda esta potencia que tienen todas estas tecnologías, todos los fabricantes que ahora mismo estamos, pero muchas veces o no tienen personal en su departamento de ciberseguridad, o no tienen personal especializado, o no pueden tener un SOC en 24/7, no tienen los recursos, o son empresas más grandes que a lo mejor sí que tienen, sí que están dando pasitos en ese sentido, pero lo que quieren es complementar los servicios que ellos ya pueden estar dando con personal interno". Para el portavoz aquí es donde cobran importancia los servicios gestionados: "ahí es donde entran los servicios MDR gestionados, dados por un SOC con analistas expertos en 24/7, que están todo el día y que de verdad son ingenieros de inteligencia, que están perfectamente capacitados y acostumbrados a poder analizar y sacarle el jugo a todas estas herramientas".

Elena García Díez, CISO de Indra

‘El reto es asegurar una experiencia de usuario satisfactoria en un entorno de seguridad adecuado’

“Con naturalidad”, así ha afrontado el mercado la pérdida de perímetro según Elena García Díez, CISO de Indra, en una entrevista realizada en el marco del Foro ITDS ‘Protegiendo el nuevo perímetro’. Comenta también que, aunque se ha hablado mucho del impacto de la llegada masiva del trabajo remoto, “realmente los que nos dedicamos a esto ya veníamos viendo como nuestro perímetro se desdibujaba desde mucho antes”.

Mientras el perímetro se iba perdiendo, el mercado buscaba dónde colocarlo. Durante los últimos años se ha hablado de los datos, las identidades y el endpoint como los nuevos perímetros a proteger. No opina así Elena García, quien asegura que la visión sencilla, y la que en realidad ya se tenía cuando había perímetro, es que, “al fin y al cabo somos personas, y lo que

‘EL RETO ES ASEGURAR UNA EXPERIENCIA DE USUARIO SATISFACTORIA EN UN ENTORNO DE SEGURIDAD ADECUADO’ (ELENA GARCÍA, INDRA)

CLICAR PARA VER EL VÍDEO

tenemos que proteger es a las personas, que tienen una identidad y una manera de acceder a la información y a los sistemas, que es con sus dispositivos”.

Recuerda un cambio del entorno en el que se ha pasado de un único dispositivo a un entorno multi dispositivo cada vez más abierto “que nos ofrece un montón de oportunidades, tanto a nivel de gestión de la TI como de seguridad”. En este nuevo entorno, en el que una identidad es capaz de acceder a información y recursos distribuidos desde diferentes sitios y en cualquier momento, los retos son… “La clave de la identidad digital es tener claramente identificado tanto al usuario que accede como con qué va a acceder y a qué necesita acceder”, asegura la CISO de Indra añadiendo que “ahora, hacia lo que estamos trabajando en este perímetro desdibujado es entender el servicio, la

"La clave de la identidad digital es tener claramente identificado tanto al usuario que accede como con qué va a acceder y a qué necesita acceder"

aplicación, el dato al que efectivamente tiene que acceder”.

Recuerda también durante la entrevista Elena García que uno de los primeros objetivos de la seguridad es la disponibilidad y que se busca la disponibilidad de una identidad “que accede en diferentes momentos, desde diferentes dispositivos, a los mismos o diferentes datos y en el que el reto es asegurar una experiencia de usuario satisfactoria en un entorno de seguridad adecuado”.

Al preguntarle por la identidad de las máquinas tiene claro Elena García que “asumir que una máquina tiene una identidad quizás no es el camino”. A pesar de que estamos en el mundo de la inteligencia artificial “la clave para entender lo que sucede en cualquier entorno es entender quién provoca que suceda, y ahí de momento podemos tener procesos automáticos, podemos tener procesos de negocio, pero realmente el responsable de que un

"Zero Trust no deja de ser una oportunidad para dar paso al siguiente concepto, que es el del Zero Touch"

proceso se desencadene siempre termina en una identidad".

Sobre el impacto que ha tenido Zero Trust, dice que no viene a ser más que una evolución de los principios básicos de seguridad; "lo que pasa ahora es que podemos hacer realidad el ir poniendo controles en ese acceso que acompañen y que garanticen ese entorno de Zero Trust, entendido además como un Zero Trust dinámico y vivo. Que ayer pudieses acceder no quiere decir que hoy no vuelva a comprobar realmente cuáles son todas tus características de seguridad para proveer o no ese acceso", comenta la CISO de Indra, añadiendo que, además, Zero Trust no deja de ser "una oportunidad para dar paso al siguiente concepto, que es el del Zero Touch: no me tocas hasta que yo valido que las condiciones de seguridad con las que vienes son las que tienen que ser, y que además sigues teniendo el derecho o la necesidad de acceder a lo que estás intentando acceder".

Tiene claro Elena García que ninguna amenaza la quita el sueño. Explica que las amenazas van a estar siempre ahí, y "si eso nos está quitando el sueño es que realmente no estamos consiguiendo hacer nuestro trabajo como debiéramos. No estamos consiguiendo lanzar los mensajes". Añade que, en realidad, el contexto de amenaza es un contexto que no ha variado tanto; "no nos engañemos, las amenazas siguen siendo las que teníamos hace años. La amenaza está ahí. Lo que hay que hacer es trabajarla y asumir también que no puede ser que me quite el sueño a mí, porque esto de la seguridad es una responsabilidad compartida". it

Sergio Martínez, Country Manager Iberia, SonicWall

‘Hay que fortalecer el endpoint’

Hay una explosión de la superficie de ataque sin precedentes que nos ha llevado a una situación en la que cada vez hay un gap más grande entre lo que tienen las organizaciones respecto a lo que necesitan, explica al inicio de su ponencia Sergio Martínez, country manager para la región de Iberia de SonicWall.

“Los riesgos se han convertido en infinitos porque, además, estamos en un entorno de ciberguerra”, asegura el directivo en el marco del Foro ITDS “Protegiendo el nuevo perímetro”, destacando algunas de las últimas tendencias detectadas por el último Cyber Threat Report de la compañía: el ransomware ha decrecido, porque cada vez es más focalizado; y uno de los mayores retos a los que nos enfrentamos son las amenazas encriptadas, que crecieron un 132% respecto al mismo periodo del año anterior.

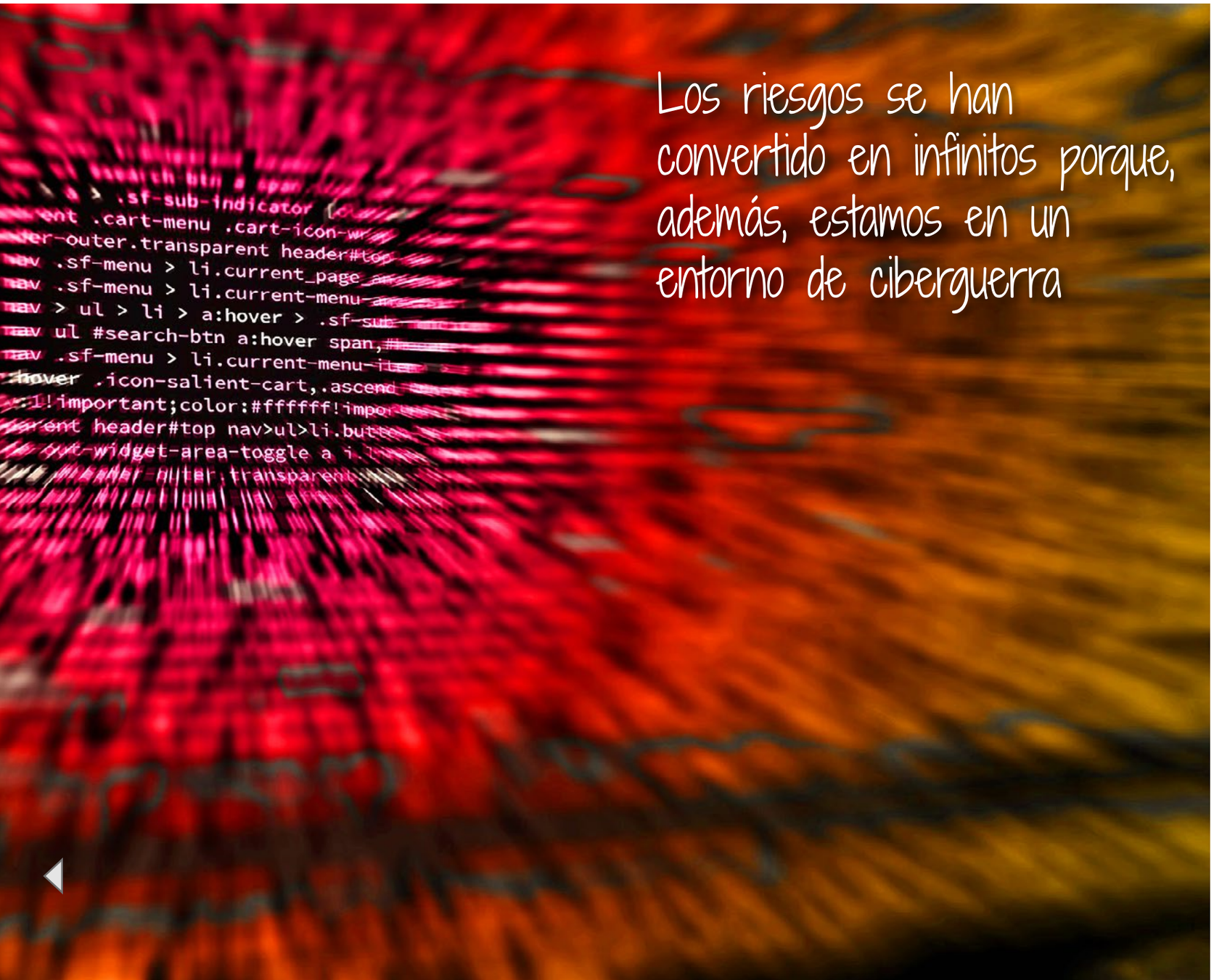
En este entorno, en el que además hay que proteger el robo de credenciales para evitar movimientos laterales, “el firewall solo ya no sirve. Hay que fortalecer el endpoint construyendo una defensa multicapa, desenmascarando las amenazas avanzadas, reduciendo los falsos negativos e identificando el robo de credenciales”. Y todo ello intentando automatizar lo más posible.

Propone Sergio Martínez durante su ponencia cinco ideas que pueden ayudar a cambiar la defensa tradicional y hacer frente a la desaparición del perímetro. La primera es una defensa por capas que hagan frente a ataques cada vez más sofisticados; lo segundo sería el contar con una visibilidad central para detectar y responder “porque una defensa por capas necesita una coordinación”; Capacidades para detectar lo desconocido con el uso de inteligencia artificial, o sandbox avanzado con múltiples

PONENCIA SONICWALL
FORO ITDS “PROTEGIENDO EL NUEVO PERÍMETRO”

CLICAR PARA VER EL VÍDEO

estrategias como elementos fundamentales para detectar comportamientos extraños; la cuarta idea tiene que ver con el acceso remoto seguro, acelerado en los últimos años y que requiere desplegar doble factor de autenticación, controlar el endpoint o desplegar estrategias de Zero Trust; y todo lo mencionado anteriormente con un TCO y unos costes disruptivos asumibles por cualquier pyme “porque al final esto no tiene por qué ser algo sólo de gran cuenta, ni mucho menos”.



Contenido relacionado

- SonicWall
- Ponencia Foro ITDS - SonicWall

Compartir en RRSS

FORO it Digital Security

Mesa Redonda

Identidad, el mayor tesoro que hay que defender

La identidad se ha posicionado en el centro de las estrategias de seguridad. La autenticación multifactor (MFA) y el inicio de sesión único (SSO) han logrado asegurar aún más el proceso de inicio de sesión, yendo más allá de la combinación tradicional de nombre de usuario y contraseña. Sin embargo, esto ya no es suficiente para protegerse contra atacantes sofisticados y hábiles que usan credenciales y derechos legítimos para obtener acceso a los recursos y datos que necesitan.

Para hablar de los retos de proteger las identidades adecuadamente, el impacto del trabajo remoto o el camino hacia el passwordless se celebró una mesa redonda en el marco del Foro ITDS "Protegiendo el nuevo perímetro" que reunió a Sergio Martínez, Iberia Regional Manager de SonicWall Iberia; David Villelga, CIO/CISO del Centro Universitario U-tad; Jose Luis Paramio, CISO de Userlytics; Mónica de la Huerga, CISO de Sopra Steria; y Carlos J. Fernández, CIO de la Universidad Europea.

"Saber que quien dice que está detrás de esa identidad es realmente quién está y, sobre todo, que esa identidad puede acceder a donde quiere acceder" es uno de los grandes retos a los que se enfrentan las empresas a la hora de proteger las identidades adecuadamente. Así lo aseguraba Mónica de la Huerga, añadiendo que no hay que olvidar que, aunque muchas amenazas vienen de fuera, "hay veces que desgraciadamente tenemos el enemigo en casa, con lo cual hay que también verificar esos accesos, aunque sean legítimos, para tratar de anticiparnos a los insiders".

IDENTIDAD, EL MAYOR TESORO QUE HAY QUE DEFENDER

CLICAR PARA VER EL VÍDEO

"Hay que pasar de la gestión mera del password a una estrategia multifactor"

Sergio Martínez, Iberia Regional Manager, SonicWall Iberia

Identifica José Luis Paramio al usuario como uno de los grandes retos a los que se enfrenta para proteger la empresa. Explica el directivo que en Userlytics existe una política de contraseñas de obligado cumplimiento que establece la longitud de las contraseñas, la longevidad de las mismas, etc., "pero también tenemos muchos servicios, y unos permiten establecer una política de seguridad seria, pero otros no tanto". Complica la situación el no poder saber si las contraseñas que se utilizan en la empresa se están reutilizando en la vida privada, "y luego está el onboarding y des-onboarning de los usuarios".

Tener empleados y miles de alumnos con necesidades de acceso complica la situación. Recuerda David Villelga que el teletrabajo exigió la apertura de todos los sistemas y cambió definitivamente el paradigma de la seguridad. "Ahora el mayor vector de

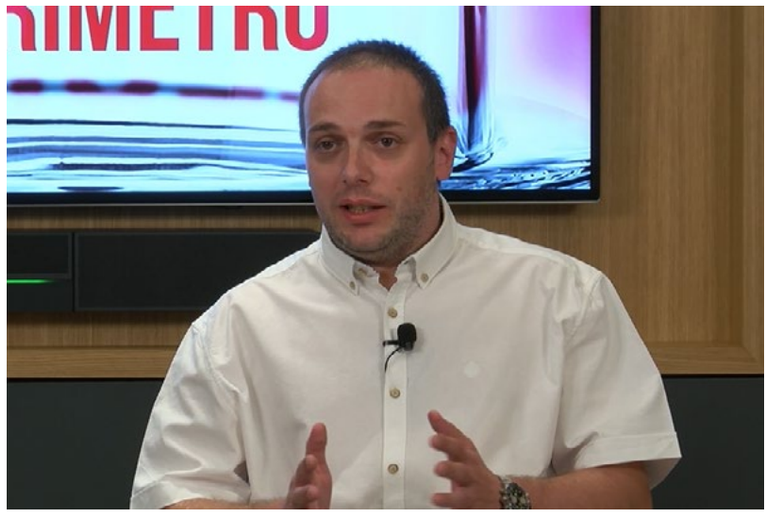
"Ahora el mayor vector de ataque que podemos tener es el usuario"

David Villelga, CIO/CISO, Centro Universitario U-tad

ataque que podemos tener es el usuario, y para poder identificarlo hay que irse a un modelo Zero Trust donde haya por detrás un doble factor de autenticación que identifique bien a la persona que está accediendo a los sistemas, e incluso que sus dispositivos son realmente los que son", explica el directivo de U-tad, añadiendo que se buscan sistemas de Single Sign-On (SSO) para que con una sola credencial se tenga acceso a todo lo que se necesita.

"Vencer la permisividad descontrolada post pandemia" es, en opinión de Carlos J. Fernández, uno de los principales retos a los que se enfrentan las empresas. El que más y el que menos, asegura, abrió puertas que, desde el punto de vista de la seguridad, no hubiera abierto. El tiempo ha generado un entorno de enseñanza híbrida en la que alumnos y profesores pueden estar en el campus o en casa, "y todo eso hubo que acomodarlo teniendo en cuenta que había que volver a poner las medidas de seguridad que habíamos levantado sin frenar esa evolución del negocio". Se añade que, a pesar de que la formación y concienciación ha mejorado muchos hábitos, la gente sigue cayendo en un phishing.

A la hora de afrontar los retos para gestionar las identidades adecuadamente menciona Sergio



"Se trabaja con muchos servicios, y unos permiten establecer una política de seguridad seria, pero otros no tanto"

Jose Luis Paramio, CISO, Userlytics

Martínez el tener la capacidad de compartimentar, de desplegar estrategias de Zero Trust, así como "intentar pasar de la gestión mera del password a una estrategia multifactor". Recuerda además el directivo de SonicWall que ya existen directivas que indican que hay que ir más hacia este tipo de gestión de la identidad, que hace más difícil el robo de credenciales, el robo de cuentas que luego permite movimientos laterales en cualquier ataque para buscar piezas de mayor tamaño dentro de la organización.

Se plantea durante el coloquio si los modelos de trabajo híbrido han reforzado la inversión en tecnologías de gestión de identidades, de autenticación,

control de acceso… En opinión de Sergio Martínez, aunque hace tiempo que se están utilizando estrategias multifactor, hay que educar más al usuario porque “cualquier ataque de phishing bien pensado tiene un impacto bastante grande en cualquier organización si se dirigen bien.

Para Mónica de la Huerga, es muy importante establecer cuantas más medidas de seguridad mejor, desde monitorizar la red para detectar cualquier acceso; analizando los accesos, aunque sean legítimos; aprendiendo de las nuevas maneras que tienen los empleados trabajando en remoto de interactuar con la compañía; o anticipándonos y descartando falsos positivos para detectar una suplantación de identidad. “Seguimos pensando en que tenemos que construir un castillo y defenderlo, y volver a la idea de la defensa por capas”, dice la CISO de Sopra Steria.

Modelos como Zero Trust, que promueve la desconfianza, ¿está ayudando a reforzarla seguridad de las identidades? “Yo separaría Zero Trust de identidades”, dice José Luis Paramio, explicando que es afortunado porque no tiene una identidad interna que proteger, “todo está en la nube”. Añade que sí tiene Zero Trust en su red de servidores, pero que no es algo que haya “modificado mi forma de establecer los accesos a los servidores” y que hay que tener muy presentes los roles IAM.

Mantener el equilibrio entre la seguridad y la experiencia de usuario es un debate al que se han tenido que enfrentar la mayoría, sino todos, los responsables de ciberseguridad de las empresas. Como CIO y CISO del Centro Universitario U-tad, David Villelga se enfrenta a empleados, profesores y miles de alumnos, cada uno de los cuales trae su propio dispositivo. El reto es complejo y la manera de abordarlo es “segmentar mucho la red

"Desgraciadamente a veces tenemos el enemigo en casa, con lo cual también hay que verificar esos accesos, aunque sean legítimos"

Mónica de la Huerga, CISO, Sopra Steria

y utilizar el doble factor de autenticación para controlar quién accede a los dispositivos", explica el directivo. Como curiosidad, el hecho de que U-tad cuente con titulaciones sobre ciberseguridad hace que el Centro Universitario se convierta en banco de pruebas de esos futuros responsables de ciberseguridad.

Las contraseñas no son suficientes. Es una máxima que se repite desde hace unos años y con la que está de acuerdo el CIO de la Universidad Europea. El uso del doble factor de autenticación es algo que resulta tedioso en ocasiones, pero respecto a lo cual hay que concienciar. Añade Carlos J. Fernández que también se debe facilitar su uso porque hay dobles factores de autenticación que son más fáciles que otros. Asegura también el directivo que sí que se acabará en un entorno passwordless "porque iremos avanzando hacia la parte biométrica en la que el password eres tú".

La adopción de tecnologías de doble factor de autenticación se está realizando desde entornos muy basados en contraseñas, asegura Sergio Martínez, quien añade que se está empezando a huir del "algo que tienes" basado en el móvil al "algo que eres" basado en alguna lectura biométrica. Concluye el directivo de SonicWall asegurando que "vamos directos a entornos passwordless" y que la identidad es el mayor tesoro que tenemos y que hay que defender.

"Acabaremos en un entorno passwordless porque iremos avanzando hacia la parte biométrica en la que el password eres tú"

Carlos J. Fernández,
CIO, Universidad Europea.

Jacinto Grijalba, Cyber Security Sales Manager, CyberRes, una unidad de negocio de Micro Focus
Ricardo José Garrido Reichelt, Lead Sales Engineer AD& S, Citrix Iberia

Identidad Digital, y cómo protegerla

Jacinto Grijalba, Cyber Security Sales Manager de CyberRes, una unidad de negocio de Micro Focus, y Ricardo José Garrido Reichelt, Lead Sales Engineer AD& S de Citrix Iberia, participaron en el Foro ITDS "Protegiendo el nuevo perímetro" para hablar sobre la identidad digital y cómo protegerla.

"La mayoría de los ataques se producen por una suplantación de identidad", aseguraba Jacinto Grijalba, Cyber Security Sales Manager de CyberRes, una unidad de negocio de Micro Focus, al comienzo de una ponencia en la que destacó el Zero Trust como la arquitectura de ciberseguridad más apropiada para gestionar la identidad digital, o la capacidad de gestionar quién puede acceder a qué, cuándo y cómo. NetIQ, la tecnología de CyberRess para la gestión de accesos, tiene la ventaja de poder cubrir todos los que la arquitectura Zero Trust pide, desde la gestión del acceso, cómo los usuarios van a autenticar y acceder a los sistemas; la gestión de la identidad, diciendo cómo debe interactuar un usuario, cuáles deben de ser sus permisos y revisando que estos permisos son los que deben de tener; y obviamente incluyendo a aquellos usuarios que tienen el mayor privilegio dentro de las organizaciones y que pueden acceder

PONENCIA CIBERRES CITRIX
FORO ITDS "PROTEGIENDO EL NUEVO PERÍMETRO"

CLICAR PARA VER EL VÍDEO

"NetIQ, la tecnología de CyberRess para la gestión de accesos, tiene la ventaja de poder cubrir todos los aspectos que propone la arquitectura Zero Trust"

Jacinto Grijalba,

Cyber Security Sales Manager, CyberRes, una unidad de negocio de Micro Focus

a información muy sensible, que son los que a los que más debemos de controlar.

A Citrix se la reconoce por la virtualización, pero también juega un papel importante en el control de accesos a los recursos corporativos de una forma securizada "porque hoy la identidad es el nuevo perímetro, y dependiendo de esa identidad, tenemos que darle al usuario los recursos correspondientes". Y todo ello teniendo en cuenta el contexto, de forma que, dependiendo del mismo, de un nivel de riesgo que puede ser variable, se permite un tipo de acceso u otro. "En el momento en que mi contexto ha cambiado y hay un riesgo mayor, podemos iniciar acciones automatizadas para securizar el acceso y tener una traza si ha habido un ataque basado en esa identidad".

"Cuando el contexto cambia, la seguridad dentro de la organización cambia"

Ricardo José Garrido Reichelt, Lead Sales Engineer AD+ S, Citrix Iberia

Contenido relacionado

- CyberRes
- Citrix
- Ponencia CyberRes
- Ponencia Citrix

Compartir en RRSS

El reto de la gestión de la identidad

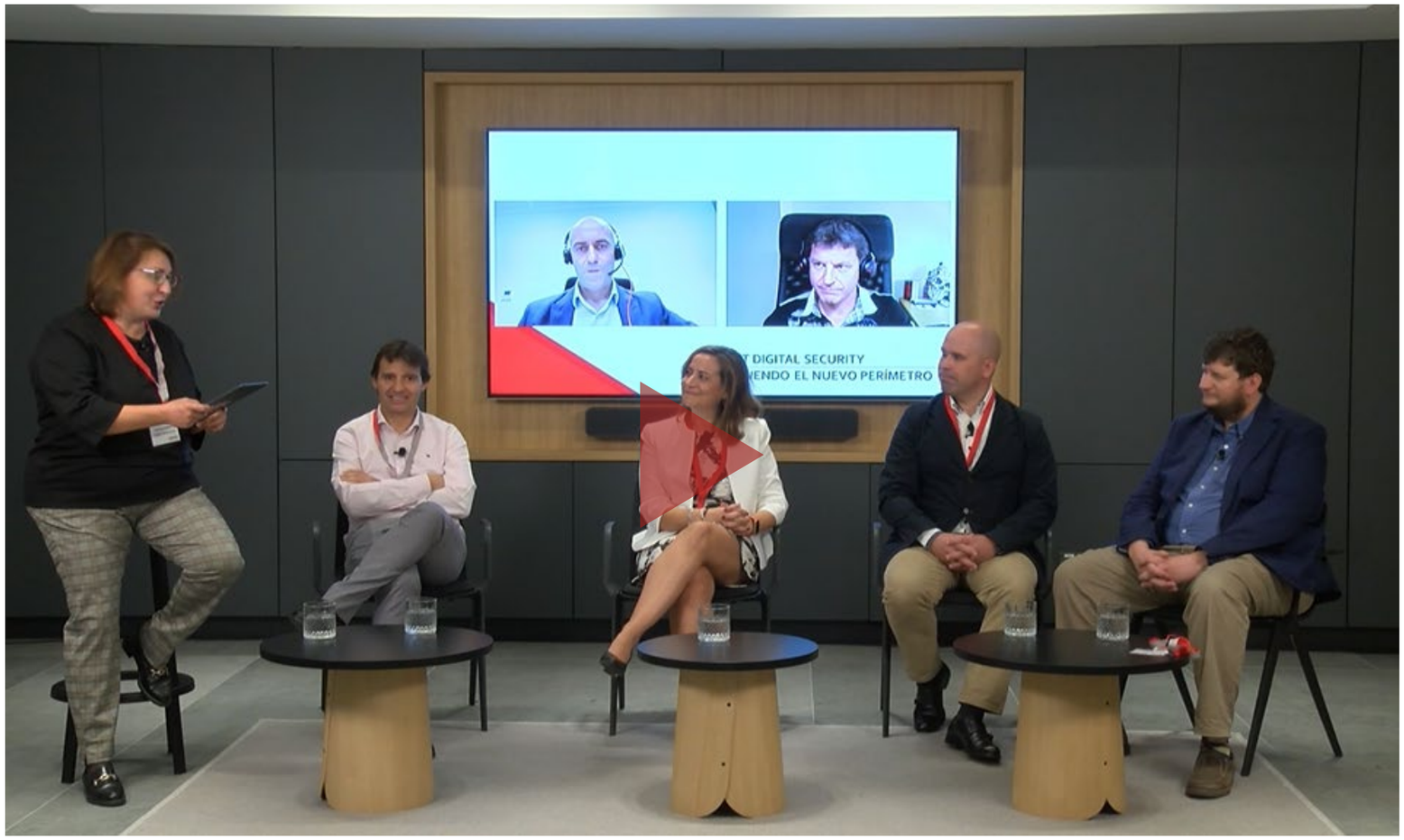
La protección de la identidad es clave en toda estrategia de seguridad que se precie. La ruptura del perímetro que ha provocado la implantación a gran escala del teletrabajo hace necesarias medidas de seguridad que protejan las identidades de los usuarios.

En los tiempos que corren, los usuarios necesitan conectarse desde cualquier lugar y en cualquier momento a la red corporativa, así como desde cualquier dispositivo que necesiten. Esto ha hecho que la protección de la identidad tome una relevancia de primer nivel, para hablar sobre cómo han impactado los modelos de trabajo híbrido en la seguridad de las identidades, los principios de Zero Trust y los retos que se plantean, hemos contado en esta Mesa Redonda IT con la participación de Jacinto Grijalba, Cyber Security Sales Manager de CyberRes; Ricardo José Garrido Reichelt, Lead Sales Engineer de Citrix Iberia; Maica Aguilar, Gerente de Seguridad de Ferrovial; Israel Devesa Cuevas, CIO de Capital Energy; Ángel Uruñuela, CISO de Fluidra y Toni García Estopa, CISO de LETI Pharm.

Retos de la gestión de identidades

En los últimos veinte años se ha observado poco a poco la caída del perímetro tradicional. Como señala Maica Aguilar, “hemos pasado a que la identidad se ha posicionado en el centro del ecosistema de protección, porque la información y necesidad de acceso a la misma se ubica dónde está la persona: en cualquier momento, desde cualquier dispositivo y en cualquier lugar. Con esta premisa, ha evolucionado la forma de monitorizar, de detectar y de proteger. Nosotros tenemos que ver en qué situación estamos y hacia donde tenemos que ir”.

Israel Devesa Cuevas remarca que, en el sector industrial, la ciberseguridad en el entorno OT lleva



EL RETO DE LA GESTIÓN DE LA IDENTIDAD

CLICAR PARA VER EL VÍDEO

cinco o diez años de retraso en comparación con el despliegue de soluciones de ciberseguridad en el mundo IT. “El reto principal es intentar poner en marcha todas las medidas, políticas y procedimientos que se han puesto dentro del ecosistema IT e incorporarlo dentro del ecosistema OT para garantizar la máxima seguridad de las infraestructuras. Es cierto que el entorno OT tiene peculiaridades que impiden una convergencia directa IT/OT en el ámbito de la seguridad y en concreto en el ámbito de la gestión de identidades. Por tanto, la industria deberá de buscar como afrontar esa convergencia de la que a día de hoy estamos algo alejados”.

“Por nuestra parte, creemos que una estrategia global de Access Management es vital. Hoy en día es uno de los temas que más han venido trabajando como reto interesante”, observa Ángel Uruñuela.

"Es muy positivo darle al usuario la opción de elegir la manera en la que se quiere autenticar"

Jacinto Grijalba,
Cyber Security Sales Manager,
CyberRes

> "La identidad, y su contexto, definen a qué voy a poder acceder"
>
> Ricardo José Garrido Reichelt, Lead Sales Engineer, Citrix Iberia

"No solo tenemos que hacer una estrategia segura en las empresas, sino que continuamente tenemos que estar evaluando los nuevos vectores de ataque. Y este es un vector de ataque que nadie o casi nadie vio venir".

Para Toni García Estopa, "El problema principal o el mayor reto que tenemos nosotros ahora mismo es tener clara la identidad y quién es y cómo lo identificamos". "En estos entornos en los que tienes una parte OT, no está de la misma manera alineado, hay diez o quince añitos de retraso, te encuentras a lo mejor con aplicaciones legacy que no vas a poder cambiar en veinte años. Para mí el principal reto es el cómo lo hacemos".

Según señala Jacinto Grijalba, las razones para implantar una solución de gestión de identidades son muchas: "Hay razones de ciberseguridad, obviamente, porque vamos a poder gestionar mucho mejor y reducir el riesgo de los accesos que estamos teniendo. Pero es que también hay razones de eficiencia. Uno de los problemas fundamentales para poner esto en marcha es poder gestionar los miles de usuarios que las organizaciones tienen, usuarios que pueden ser clientes también, que son usuarios que acceden a activos digitales que ponemos a su disposición. Eso no es fácil. No es una cuestión de tener un grupo de personas, es cuestión de tener automatismos que te ayuden a hacerlo de manera segura". El portavoz también comenta que hay razones relacionadas con el gobierno, con la privacidad y con el cumplimiento normativo.

El modelo de teletrabajo híbrido y la identidad

Los modelos de trabajo ya no son remotos, han girado hacia el modelo híbrido. Para Ricardo José Garrido Reichelt, "tenemos que pensar que nuestra herramienta la usan los usuarios, no su identidad. Luego, cuando van a querer acceder a los recursos, qué es lo que podemos hacer nosotros: facilitar ese

"Hemos pasado a que la identidad se ha posicionado en el centro del ecosistema de protección"

Maica Aguilar,
Gerente de Seguridad, Ferrovial

acceso. Ellos van a querer usar diferentes tipos de dispositivos donde esa experiencia de usuario es muy importante". De todas formas, no olvida la parte de la securización: "La parte de seguridad, evidentemente en nuestro caso es muy importante, en el sentido de que la identidad define a qué voy a poder acceder, el contexto de esa identidad".

Cuando hablamos de gestión de identidades, entran en acción conceptos como la autenticación, la autorización, la federación de identidades, las cuentas privilegiadas… Maica Aguilar comenta que "tradicionalmente se comenzaba con la centralización de la gestión de identidades, para permitir hacer una gestión de los usuarios y de los recursos de una forma automática. La identidad es una pieza que en muchos casos no se ve, pero está ahí y nos permite ese control, esa seguridad necesaria. En el ecosistema de la identidad hay múltiples necesidades como por ejemplo, gestionar identidades privilegiadas o gestionar robots y procesos automáticos. En estos casos hay que analizar estas necesidades de acceso y

"La tecnología de gestión de identidades está muy pensada y dirigida para el ecosistema IT y el ecosistema OT no se ha puesto al día"

Israel Devesa Cuevas, CIO, Capital Energy

gestionarlos adecuadamente , igual que con las identidades nominales, aunque no haya una persona detrás. Por ello que cada vez tenemos más soluciones específicas vinculadas a la gestión de la identidad".

Israel Devesa Cuevas vuelve a hablar sobre el mundo industrial señalando que "muchas de las infraestructuras que teníamos en España estaban desconectadas. Entonces, todas estas problemáticas no existían". Y añade: "En el momento que empezamos a querer aprovechar las nuevas tecnologías y la innovación en el mundo industrial, empezamos a tener los mismos problemas de ciberseguridad que ya habíamos resuelto, o que estamos en vías de resolverlos en el ecosistema de IT". "El problema nuevamente es que nos encontramos que la tecnología está muy pensada, muy dirigida para el ecosistema IT y el ecosistema OT necesita de tiempo para incorporar las soluciones sin poner en riesgo la seguridad de las infraestructuras".

Zero Trust y la gestión de identidades

"Los principios de Zero Trust están estrechamente ligados con la gestión de identidades. Zero Trust tiene diferentes definiciones dependiendo de los proveedores o de las agencias que hacen esta definición, se entiende de una manera o de otra. A mí personalmente me gusta mucho la definición que hace la Agencia de Ciberseguridad Americana, que define cinco pilares y el primero de los pilares es la identidad", apunta Ángel Uruñuela, que añade: "es muy importante en toda esta estrategia de acceso tener un enfoque adaptativo".

A la hora de implementar una solución de gestión de identidades, Toni García Estopa opina que "una de las primeras cosas que se tienen que tener en cuenta es la parte del gobierno. Si eso no lo tienes

"Es muy importante en toda esta estrategia de acceso tener un enfoque adaptativo"

Ángel Uruñuela, CISO, Fluidra

claro desde el principio, va a ser muy difícil poder desarrollar una solución real". "El problema es que suele hacerse al revés: queremos gestionar identidades, buscamos una solución y a partir de ahí nos aparecen una serie de necesidades de gobierno". Pero, ¿en ese gobierno de identidades se tienen en cuenta también las identidades de las máquinas?

"Para mí un robot tiene identidad. Al final hace una acción, que hay un código por detrás que la ejecuta, pero si se cambia el código, se cambia el comportamiento, con lo cual es una identidad más".

Autenticación multifactor y legislación

Jacinto Grijalba señala que desde hace tres años se ha observado un boom en el uso de tecnologías de autenticación multifactor: "La base instalada que tenemos actualmente puesta con esta tecnología, al menos en el territorio de España y Portugal, es diría que un 200% más que hace tres años". Para el portavoz ha sido muy positivo darle al usuario la opción de elegir la manera en la que se quiere autenticar: "una de las cosas que ha funcionado muy bien es pasarle el testigo al usuario para que él elija que método usar".

Para Ricardo José Garrido Reichelt, hay variedad a la hora de ver cómo están implantando las empresas españolas la seguridad de las identidades. "Depende de la empresa, si es grande. Las empresas grandes, evidentemente, suelen ir un poco más avanzadas en ese sentido". "En comparación con antes hemos avanzado bastante. Hay como siempre mucho trabajo que hacer y yo creo que una cosa que ha ayudado porque nos fuerza, es la legislación que viene por detrás". Para finalizar, señala que "hoy en día pasa algo y sí hay consecuencias, entonces creo que también, tanto a nivel de empresa grande como a nivel de empresa pequeña, ha ayudado que nos pongamos un poco las pilas en ese sentido".

"Si no tienes en cuenta la parte de gobierno desde el principio va a ser muy difícil desarrollar una solución real"

Toni García Estopa,
CISO, LETI Pharm

Mabel Gonzalez Centenera, Jefa de Servicio de Seguridad de los Sistemas de Información (CISO), SERMAS

‘Hay que centrar los recursos en proteger y blindar los datos que de verdad son críticos’

“Conocer al adversario. Ver quién te está atacando, qué es lo que quiere y qué es lo que pretende conseguir para poder protegerte mejor” es una de las principales funciones de los responsables de seguridad. Lo asegura Mabel Gonzalez Centenera, Jefa de Servicio de Seguridad de los Sistemas de Información (CISO) de SERMAS, en una entrevista realizada en el marco del Foro ITDS ‘Protegiendo el nuevo perímetro’.

Dice también la directiva que lo que más preocupa al colectivo son los grandes ataques de las grandes empresas del cibercrimen, “que son las que más daño están haciendo porque están totalmente profesionalizadas”. Esta profesionalización implica que estas organizaciones tienen departamentos de

'HAY QUE CENTRAR LOS RECURSOS EN PROTEGER Y BLINDAR LOS DATOS QUE DE VERDAD SON CRÍTICOS' (MABEL GONZÁLEZ, SERMAS)

CLICAR PARA VER EL VÍDEO

"La profesionalización de la ciberdelincuencia está generando ataques muy sofisticados y nos tenemos que poner a su altura en medidas de seguridad"

recursos humanos, incluso psicólogos en los departamentos de ingeniería social para crear ataques muy dirigidos. Una situación que lleva a que "el nivel de alerta en el que estamos sea grande, y más en el sistema sanitario".

La profesionalización de la ciberdelincuencia está generando ataques muy sofisticados "y nos tenemos que poner a su altura en medidas de seguridad". Asegura Mabel González SERMAS cuenta con medidas de seguridad muy avanzadas, pero "nos están exigiendo mucho más para poder competir y hacerles frente".

Respecto a la pérdida de perímetro, no tiene claro la CISO de SERMAS que pueda colocarse en las identidades, los datos o el endpoint. Comenta que la información viaja continuamente, que la mayoría de los ataques se producen por robo de credenciales y que hay que apostar por la concienciación y una buena política de contraseñas.

Sobre Zero Trust, que busca validar quién accede, desde dónde, con qué dispositivo y a qué información, dice Mabel González que está impulsando nuevas políticas de seguridad y la adopción de nuevas tecnologías.

Otro de los retos a los que se enfrentan las empresas es la protección de los datos, dispersos en

entornos híbridos. ¿Cómo se está abordando desde SERMAS esa protección del dato? “La seguridad es infinita, pero los recursos no”, comenta Mabel González, añadiendo que lo primero que hay que plantearse es saber cuáles son los críticos, porque hay datos sanitarios que son muy críticos y otros que no lo son tanto. “Hay que centrar los recursos en proteger y blindar esos datos que de verdad tienen que ser blindados”, asegura.

¿Qué hemos aprendido de la pandemia y de esa digitalización acelerada que generó? “Hemos dado un gran paso en ciberseguridad”, comenta la CISO de SERMAS. Recuerda que el sector sanitario se ha visto muy afectado y ha estado en el objetivo de los cibercriminales, lo que ha llevado a aprender a ser resilientes; “hemos aprendido que hay que tener una casuística muy variada de escenarios en los que debemos seguir dando un servicio. Y hemos aprendido, sobre todo, cuáles son los servicios esenciales donde tenemos que centrar todos los esfuerzos”.

"La seguridad es infinita, pero los recursos no"

Carlos Tortosa, director de grandes cuentas, ESET España

‘No queremos poner una barrera entre la concienciación y la tecnología’

ESET siempre ha estado muy preocupado en facilitar ciberseguridad a sus clientes, pero al mismo tiempo le ha dado mucha importancia a la concienciación, formación y educación. Así lo asegura Carlos Tortosa, responsable de grandes cuentas de ESET, al inicio de una ponencia realizada en el marco del Foro ITDS “Protegiendo el nuevo perímetro”.

Comenta el directivo que la mayor parte de las empresas tienen muy claro qué necesitan para proteger sus activos, y se utiliza una cantidad importante de tecnología para proteger a las organizaciones, “pero después nos damos cuenta de que estamos fallando, que tenemos una lista de actividades que realizar para mejorar esa tecnología”, y que el factor humano es importante.

¿Dónde nos damos cuenta de que el factor humano es importante? En vectores de ataque como el phishing, explica Carlos Tortosa, sumando a la lista la navegación web, compromiso de credenciales o uso de contraseñas débiles. Continúa su ponencia el directivo identificando cinco factores en los que el usuario se convierte en vulnerabilidad, como son la ingeniería social, la descarga de malware, la mala gestión del dispositivo (BYOD), incumplimiento de políticas internas y pérdida de

PONENCIA ESET ESPAÑA
FORO ITDS “PROTEGIENDO EL NUEVO PERÍMETRO”

CLICAR PARA VER EL VÍDEO

dispositivo. La mayor parte de estos factores “son evitables”, decía Carlos Tortosa.

Fundada en 1990 en Bratislava, Eslovaquia, ESET es una empresa 100% política de capital europeo. Desde sus comienzos la filial española ha dedicado tiempo a la concienciación en cualquier ámbito, bien sea en colegios, universidades o, evidentemente, en empresas, donde se han explicado los vectores de ataque y qué tecnología se pueden utilizar para mitigarlos.

Menciona en su ponencia un proyecto, un Portal de Educación, que se gestiona desde la plataforma de la compañía, y que busca no sólo formar a los empleados, sino concienciación y formación a técnicos de cualquier compañía o de nuestros partners. “Tenemos muy claro cómo tiene que ser esta plataforma”, asegura Carlos Tortosa, explicando que tiene que estar segmentado dependiendo de la persona que acceda; tiene que ser lo más intuitivo posible “porque no queremos poner una barrera entre la concienciación y la tecnología”; tiene que ser auto evaluable; contar con nuestra asistencia; y desarrollo de contenido exclusivo.

Se espera que la plataforma esté disponible en el primer trimestre de 2023.

Contenido relacionado

- ESET España
- Ponencia Foro ITDS - ESET

Compartir en RRSS

Noviembre 2022

FORO it Digital Security

Mesa Redonda

Formación para salvar la información

La necesidad de conciencia de seguridad nunca ha sido mayor. Los ciberataques son más, y más sofisticados y las empresas miran hacia la conciencia en ciberseguridad para mitigar el riesgo humano. La idea es que la capacitación en concientización sobre la seguridad resulte en una mejor toma de decisiones de los empleados y una mejor higiene de la seguridad. En última instancia, esto reduce el riesgo para el negocio.

Hoy en día, son muchas las empresas buscan capacitar a sus empleados para comprender cómo pueden seguir los procedimientos de seguridad para evitar ciberataques y reducir el riesgo para el negocio. Para hablar de todo ello, y en el marco del Foro ITDS "Protegiendo en nuevo perímetro", se organizó una mesa redonda en la que participaron Carlos Tortosa, Responsable de Grandes Cuentas de ESET España; David Moreno del Cerro, CISO de Tendam; Jesús Valverde, CIO y CISO de Isemaren; Consuelo Fernández de Miguel, CISO de Tecnatom; y Mónica de la Huerga, CISO de Sopra Steria.

"Somos firmes defensores de la concienciación, tanto en materia de seguridad como de privacidad", aseguraba David Moreno. Son muchos los años que llevan en Tendam utilizando programas

enfocados a formar a los empleados en la identificación de vulnerabilidades, vectores de ataque y diferentes elementos de riesgo desde diferentes ámbitos. Destaca la necesidad de ajustar estos programas en función del perfil del empleado porque, habiendo factores comunes, “hay ciertos matices que hacen que la formación tenga que ir dirigida”. “Si tengo que elegir entre invertir un euro en formación y un euro en tecnología, prefiero invertirlo en formación”, asegura el directivo de Tendam, añadiendo que los usuarios tienen que dejar de ser el eslabón más débil y convertirse en nuestro primer nivel de defensa; “con el suficiente trabajo y la suficiente dedicación pueden realmente ser parte de este departamento de seguridad”.

La formación y concienciación del empleado también tiene un peso importante en Sopra Steria, donde además hay una preocupación por hacerles

FORMACIÓN PARA SALVAR LA INFORMACIÓN

CLICAR PARA VER EL VÍDEO

"Las empresas más pequeñas tienen conciencia de lo que puede ocurrir cuando un empleado realiza una acción que puede generar una brecha de seguridad"

Carlos Tortosa,
Responsable de Grandes Cuentas,
ESET España

entender las políticas de seguridad; "que entiendan cuáles son los riesgos y por qué estan esas normas", algo que también repercutirá en su vida personal. "Todos los años tratamos de renovar esos programas de formación, de hacerlos distintos, sea un e-learning, sea algo más presencial, un tipo test… Incluso hacemos campañas de falso phishing para ver si lo que les estamos enseñando lo aprenden y lo interiorizan o no", comenta Mónica de la Huerga, concluyendo que "la formación tiene que existir porque si no la información estaría vacía".

Con muy poco tiempo como CISO de Isemaren, Jesús Valverde asegura que hay una gran inquietud por la formación y concienciación en la compañía. Añade que "siempre es mejor invertir un euro en prevención y en formación porque si tengo 100, 200 o mil empleados, cada uno tiene dos ojos que me puede ayudar a detectar si hay algo extraño" e introduce el concepto de reconocimiento y compensación por la ayuda prestada. "Los de seguridad no somos los malos y los empleados no son el eslabón más débil", comenta también Jesús Valverde durante el coloquio.

"El problema es captar la atención del empleado", comenta la CISO de Tecnatom, donde cada año se realizan planes de formación y concienciación. La aproximación es "hacer contenidos cortitos que hablen de temas de actualidad, animando

"Si tengo que elegir entre invertir un euro en formación y un euro en tecnología, prefiero invertirlo en formación"

David Moreno del Cerro, CISO, Tendam

a que la gente participe por lo que usan para ello la red social corporativa", además dichos contenidos pueden servir también en su vida personal "porque la gente está preocupada porque sus hijos no tengan problemas con la ciberseguridad". Reconociendo que Tecnatom es una compañía con personal de alto nivel técnico, asegura que el mejor día es aquel en que recibe un mensaje de un empleado alertando de una actividad sospechosa porque "eso nos está ayudando a que construyamos una empresa concienciada en temas de ciberseguridad".

"Es un privilegio tener cuatro empresas aquí en las que su planes de formación son claros y evidentes", dice Carlos Tortosa, añadiendo que, desgraciadamente, no es lo habitual. Menciona que en empresas más pequeñas no se tiene conciencia de lo que puede ocurrir cuando un empleado realiza

"Los de seguridad no somos los malos que bloqueamos cosas, y el empleado no tiene por qué ser el eslabón más débil si le capacitamos adecuadamente"

Jesús Valverde, CISO, Isemaren

una acción que puede generar una brecha de seguridad. "Creo que queda muchísimo camino por recorrer", comenta el directivo de ESET, para quien los premios son importantes para despertar el interés de los empleados.

Cuando planteamos si es más peligroso un empleado despistado que uno malicioso, entra en juego la tecnología como el gran diferenciador. Explica Carlos Tortosa que hay una serie de herramientas que permiten a la empresa, cumpliendo normativas legales, monitorizar el uso de la información a la que acceden los empleados, un DLP.

A la hora de gestionar un programa de formación el principal reto es, también para David Moreno, "captar la atención del usuario. Que no lo perciba como una imposición. Que comprenda que es algo que le va a ayudar en su trabajo", asegura el directivo. Más allá de hacer vídeos cortos de tres minutos, muy dirigidos y muy segmentados en función del público, que la formación no sea pesada y que no sea demasiado recurrente, para Tendam otro reto importante es "gestionar todo esto a nivel internacional porque hay que tener en cuenta el lenguaje, la cultura, la oportunidad". Coincide también David Moreno con Carlos Tortosa en que el mayor problema está en la pymes; "nosotros trabajamos con muchísimos proveedores y un 80% no tienen un plan de formación".

Uno de los principales problemas que afectan a los empleados es el phishing, los correos maliciosos. Ponemos sobre la mesa de debate si debiera exigírseles a los proveedores de correo que el email llegara un poco más limpio.

Dice Mónica de la Huerga que no podemos quedarnos en decir que el usuario es el eslabón más débil y echarle la culpa de todo, y que cuanto más robusta sea toda la cadena en sí, mejor nos irá a todos y, por tanto; "cuanto más limpio llegue el correo, mejor para todos" y cuanto más tiempo dediquen los partners a fomentar la seguridad por diseño y a reforzar su seguridad, también impactará positivamente en el resto de la cadena.

En realidad, ¿se les puede exigir tanto a los empleados? ¿es lícito pensar en convertirles, como se ha dicho en algunas ocasiones, en firewalls humanos? Responde Jesús Valverde que

"El reto está en captar la atención del empleado"

Consuelo Fernández de Miguel, CISO, Tecnatom

en la medida en que se les den las herramientas, tecnológicas y formativas, y se les ayude en la identificación de amenazas son de gran ayuda; “les podemos exigir en la medida en la que nosotros respondamos a esa exigencia que le estamos dando”.

“Todos nuestros clientes industriales están pidiendo que nuestros empleados estén concienciados y formados. Eso es una petición clara, incluso haciéndote auditorías con tema de seguridad”, asegura la CISO de Tecnatom, explicando que desde hace tres o cuatro años la higiene de ciberseguridad de la cadena de suministro en los entornos industriales se ha reforzado. Supone un reto, porque “cada cliente tiene su política de seguridad, tiene sus normas. Y cuando tú vas a trabajar con un cliente, no solamente tienes que conocer y formarte en lo que tú en tu empresa te están exigiendo, sino lo que te está exigiendo el cliente para ese trabajo específico”.

> "No podemos quedarnos en decir que el usuario es el eslabón más débil y echarle la culpa de todo"
>
> Mónica de la Huerga, CISO, Sopra Steria

Compartir en RRSS

Francisco Valencia, CEO, Secure&IT
Fabio Cichero, Sales Manager Southern Europe, Yubico

La concienciación que no debe faltar

Francisco Valencia, CEO de Secure&IT, y Fabio Cichero, Sales Manager Southern Europe de Yubico, hablaron de la necesidad de formar y concienciar al empleado durante el Foro ITDS "Protegiendo el nuevo perímetro".

Iniciaba su ponencia Francisco Valencia asegurando que "la ciberseguridad, que suene muy técnico, no le importa a casi nadie. Lo que importa es que nuestro sistema siga funcionando", y esto tiene poco que ver con la tecnología y mucho con la capa de gestión. Explicaba el directivo que bajo una serie de servicios que su compañía ofrece bajo el paraguas de Gold Security ayudan a las compañía a elaborar sus estrategias de ciberseguridad en base a cinco grandes pilares: cumplimiento normativo; establecimiento de políticas, procesos y procedimientos internos de la organización; la tercera línea es la que conlleva la implantación de aquella tecnología que realmente sea eficaz "para poder aplicar los controles que necesitamos y que nos permitan disminuir los riesgos de nuestra organización"; la cuarta línea es la de Ciberseguridad Industrial; el quinto punto son los servicios de vigilancia de seguridad

PONENCIA SECURE&IT, YUBICO
FORO ITDS "PROTEGIENDO EL NUEVO PERÍMETRO"

CLICAR PARA VER EL VÍDEO

"Siempre pregunto a la alta dirección qué información tienes, dónde está y cuánto vale. Y no siempre me saben responder"

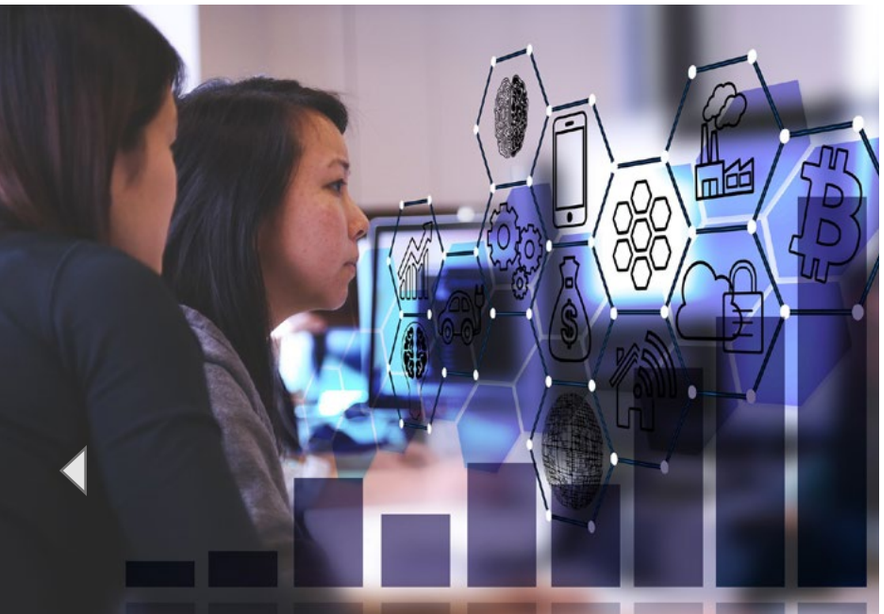
Francisco Valencia, CEO, Secure&IT

Contenido relacionado

- Secure&IT
- Yubico
- W Ponencia Yubico

que reciben unos 15 TB de datos todos los días que son analizados y procesados para responder a casi 10.000 ataques diarios. “Esta es la potencia que tiene Secure&IT y que ponga disposición del oyente”, concluye el directivo.

En su turno Fabio Cichero, Sales Manager Southern Europe de Yubico, destacó que su compañía es uno de los tres miembros fundadores de la Alianza FIDO, que busca desarrollar y promover estándares de autenticación que ayuden a reducir la excesiva dependencia mundial de las contraseñas. La YubiKey de Yubico es una llave diseñada para securizar el principal vector de ataque: el robo de credenciales, que es donde “los ciberdelincuentes comienzan su viaje dentro de un ciberataque”. Además de por su facilidad de uso, la Yubikey destaca porque es la única capaz de soportar los protocolos legacy (TOTP/HOTP), Smart Card, además de FIDO 2, FIDO U2F, OpenPGP… Por último, la gran ventaja de la llave de Yubico es que con un solo dispositivo se pueden hacer varias cosas, como entrar en nuestro dispositivo de Windows, hacer el login en la VPN y a continuación entrar en el IAM… “y todo esto con un solo token porque soporta todos los protocolos de identificación y autenticación”.



"Es importante entender la diferencia entre un pin y una contraseña. Una contraseña se comparte, un pin no"

Fabio Cichero, Sales Manager Southern Europe, Yubico

Compartir en RRSS

FORO Digital it Security

Mesa Redonda

La concienciación como primera piedra de la estrategia de seguridad de la empresa

Octubre es el mes de la concienciación en ciberseguridad. Una concienciación que se ha convertido en un elemento fundamental para proteger a las empresas, ya que el usuario sigue siendo el eslabón más débil de la cadena.

La formación y la concienciación de los usuarios en ciberseguridad se ha convertido en una de las tareas más importantes que tienen que llevar a cabo las empresas si quieren estar realmente protegidas. Para hablar sobre concienciación y programas de formación en las empresas sobre ciberseguridad, hemos contado en esta Mesa Redonda IT con la participación de Fabio Cichero, Sales Manager Southern Europe de Yubico; Francisco Valencia, CEO de Secure&IT; Andrés Sanz Mollejo, Ciberseguridad de CEPSA; Álvaro Ramos Suárez, Director NNTT y DPO de Clarkemodet; Gustavo Lozano García, CISO de ING; Ramón Ortiz, Responsable de Ciberseguridad de Mediaset y David Matesanz Ureña, Global CISO de Santander ASSET Management.

Concienciando al usuario

La concienciación cada vez tiene mayor peso en las empresas. Como indica Andrés Sanz Mollejo, “el usuario es la primera línea de defensa, y su educación y concienciación son un elemento clave sobre el que se está invirtiendo un significativo esfuerzo a todos los niveles de la organización, con especial foco en la medición y reporting a la Dirección de indicadores claros acerca del nivel de madurez de nuestra cultura en Ciberseguridad”.

De la misma forma se expresa Álvaro Ramos Suárez, cuando comenta que “para nosotros es absolutamente necesaria la concienciación”, y añade “lo que hacemos precisamente es concienciar a que las empresas conciencien a sus empleados de todo esto. Creemos que es algo básico”. Además, señala que esta concienciación es más importante ahora si cabe con el teletrabajo y pone el acento en las brechas de seguridad: “generan muchos problemas jurídicos a los abogados que nos dedicamos a esto y un secuestro de una base de datos es complejo”.

Para ING la concienciación también es una prioridad absoluta y está integrada en nuestros

"El secreto de un buen plan de formación es llevarlo al terreno personal"

Francisco Valencia, CEO, Secure&IT

LA CONCIENCIACIÓN COMO PRIMERA PIEDRA DE LA ESTRATEGIA DE SEGURIDAD DE LA EMPRESA

CLICAR PARA VER EL VÍDEO

"Me parece complejo el phishing, sobre todo en grandes compañías"

Álvaro Ramos Suárez, Director NNTT y DPO, Clarkemodet

procesos internos. “Yo creo que la concienciación en seguridad es algo que debe ser constante, no es algo que se tenga que hacer como un proyecto. La generación de contenidos debe ser innovadora, atractiva adaptada a las amenazas y a los riesgos que observamos, apunta Gustavo Lozano García, que añade: “Aprovechamos eventos significativos para reforzar mensajes y diseñamos ejercicios para poner a prueba los conocimientos con vistas a prevenir y dejar claro desde la perspectiva de protección de datos, lo que se puede y lo que no se puede hacer”.

Ramón Ortiz comenta que en Mediaset la formación está orientada en función de los diferentes colectivos y de los diferentes grados de exposición que los empleados y los directivos tienen con respecto a cuestiones de privacidad y específicos de ciberseguridad. Para él, el objetivo es “obtener de los empleados de Mediaset, una vez concienciados y una vez formados, que estén comprometidos con los aspectos de privacidad y seguridad de la información que manejan de la compañía, y extender también ese compromiso a su vida personal”. “El perímetro está roto, el teletrabajo ha extendido el ámbito de la ciberseguridad a la vida familiar y personal de los empleados, y ahí tenemos alguna iniciativa encaminada también a que los empleados

"La concienciación en seguridad es algo que debe ser constante, no es algo que se tenga que hacer como un proyecto"

Gustavo Lozano García, CISO, ING

de Mediaset en su vida personal tengan también ese ese factor de concienciación.

Para David Matesanz Ureña "la ciberseguridad es una de las mayores prioridades y obviamente, la concienciación en seguridad es entrar dentro de estas prioridades". Además, pone de relieve la calidad de la formación que están ofreciendo en Santander Asset Management, comentando: "fíjate si la concienciación de los empleados es importante, que la misma concienciación que estamos dando a nivel interno, la estamos poniendo a disposición de nuestros clientes".

Fabio Cichero hace hincapié en la idea de aprovechar esa formación no solo a nivel profesional, sino también en la vida privada. A pesar de ello, señala que "la concienciación y formación es importante, pero no podemos depender de los usuarios de cada uno", dejando clara también la importancia de las herramientas de seguridad. "En nuestro caso trabajamos mucho con nuestros clientes en formar a aquellos colectivos que realmente son más responsables de la gestión, alta dirección, consejos de administración, mando medio, etcétera, no solamente al usuario como individuo".

"Cuando hacemos planes de concienciación al usuario como individuo, lo que intentamos hacer es protegerle en su vida privada. Es parte de la premisa que me parece un poco paradójica de que en este sector, que gastamos miles de millones de euros y muchos están haciendo muy ricos, sigamos

"El phishing es el vector número uno y hay que ir hacia una tecnología que sea resistente a esto"

Fabio Cichero, Sales Manager Southern Europe de Yubico

echando la culpa al pobre Perico que ha recibido un correo y le ha dado al clic", apunta Francisco Valencia, que va más allá al señalar que "a quien realmente hay que concienciar y hay que subir su compromiso es a la alta dirección en todas las aristas, desde recursos humanos, hasta tecnología, logística, compras…".

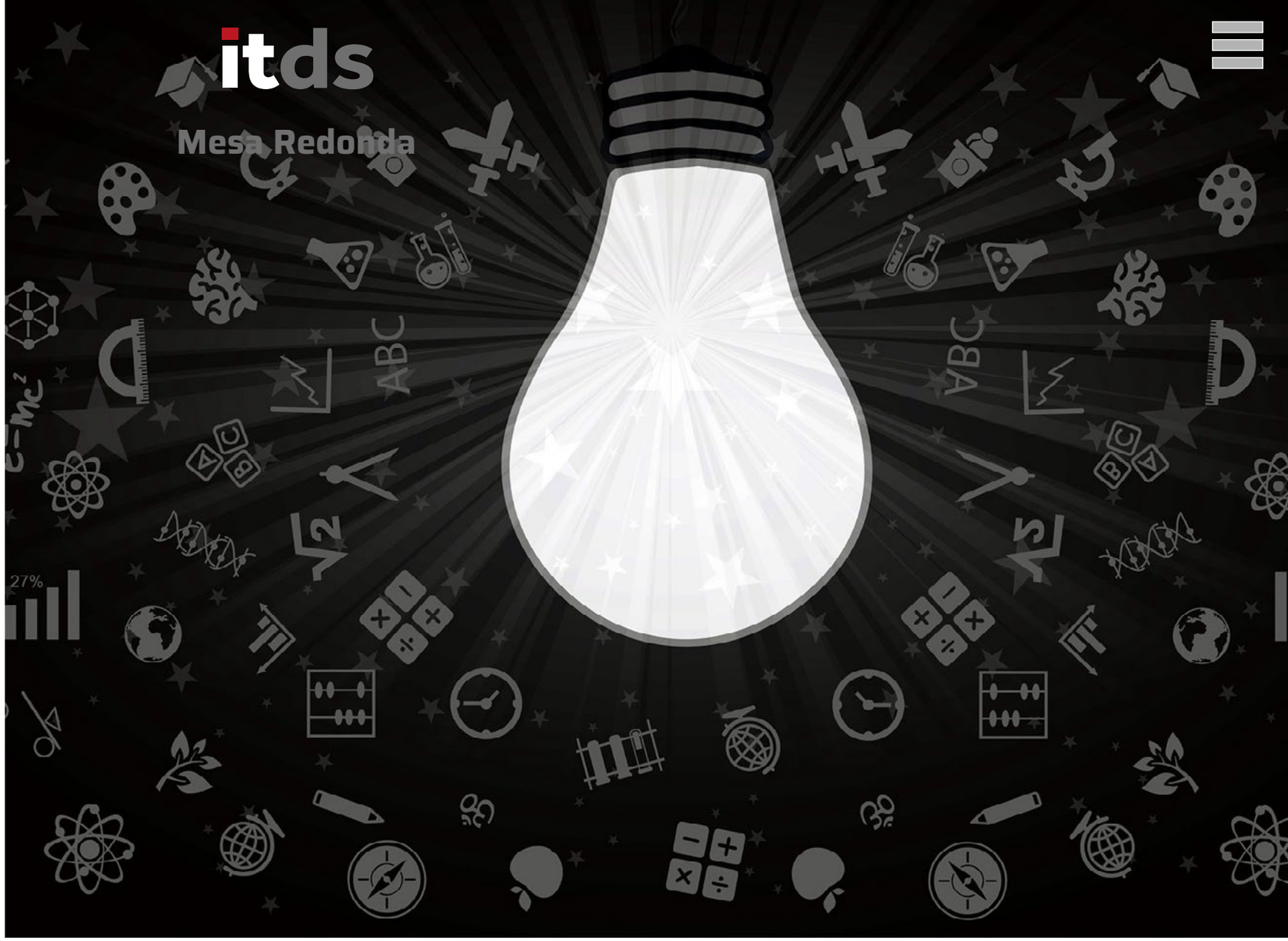
Los peligros del phishing

Una de las cuestiones que más se plantea es quién es más peligroso, un agente malicioso o un empleado despistado. Como comenta Francisco Valencia, "casi todos los ataques que se producen desde dentro se han hecho por usuarios que tenían privilegios para hacer lo que hicieron. Y por eso creo que hay que concienciar".

El phishing es desde hace muchos años uno de los principales vectores de ataque y es donde además muchos empleados caen. Así lo remarca Fabio Cichero: "es el vector de ataque número uno". Para el portavoz es necesario dar herramientas a los usuarios que, como apuntaba anteriormente,

"En un programa de formación lo primero que tenemos que saber es dónde estamos y a dónde queremos llegar"

David Matesanz Ureña, Global CISO de Santander ASSET Management.



puedan utilizar tanto en el ámbito profesional como en el privado.

Para Álvaro Ramos Suárez, el phishing es una de las cuestiones más complejas porque juega con la falta de formación del usuario y con las herramientas técnicas que deben pararlo. “Me parece complejo el phishing, sobre todo en grandes compañías”.

Invirtiendo en concienciación

Pero, ¿cómo se convence a los comités de dirección para que inviertan en estos programas de concienciación? “A los comités se les convence con datos, se les convence con sanciones y se les convence con pérdidas económicas que puedan tener”, señala Álvaro Ramos Suárez, que añade: “Hay que concienciar a las altas direcciones de la relevancia que tiene”.

Por otra parte, no todos los empleados tienen acceso a las mismas cosas, por lo que como indica Andrés Sanz Mollejo, “es fundamental que cada colectivo tenga su formación específica. En este sentido nuestra aproximación es proporcionar un

"La formación es un reto en sí misma porque no puedes utilizar la misma película todos los años"

Ramón Ortiz, Responsable de Ciberseguridad, Mediaset

baseline mínimo común para todos los usuarios, orientado a su entorno personal y profesional, para sobre éste aportar las capacidades específicas necesarias de cada puesto".

"Hay que considerar al empleado como un aliado. Y para que alguien sea un aliado en tu empresa y en cuestiones de seguridad de la información y de protección de datos, que para mí van totalmente de la mano, es fundamental enseñar", resalta Gustavo Lozano García, que añade: enseñar de una manera simple, fácil y divertida también es algo que debemos tener interiorizado".

Primeros pasos para formar en ciberseguridad

¿Por dónde debe empezarse un programa de formación y concienciación? David Matesanz Ureña lo tiene claro: “lo primero que tenemos que saber es dónde estamos y a dónde queremos llegar, y lo que queremos hacer para llegar a donde queremos llegar”. Para él, es importante entender cuáles son las amenazas y la madurez de la empresa antes de dar ningún paso.

Para Ramón Ortiz, la formación “es un reto en sí misma porque no puedes utilizar la misma película todos los años o cada seis meses a las mismas personas”. “Siempre nos encontramos con que hay que ir modificando o estableciendo novedades en el formato, porque aunque sea un formato muy atractivo o muy estimulante de gamificación o de un juego de rol, si te lo ponen dos veces en un año haciendo lo mismo pierde todo el interés y todo el impacto o novedad que pueda llevar”. Además, a la hora de hablar sobre los planes de formación, señala que “no pueden quedarse únicamente en esos aspectos genéricos o generales de los riesgos de seguridad a los que se ve expuesto, o a los errores más habituales que en los que puede incurrir los empleados o los directivos”.

A la hora de diseñar un buen plan de formación, Francisco Valencia cree que el secreto es llevarlo al plano personal: “Nosotros siempre intentamos en nuestros planes de concienciación a los clientes, a los empleados de nuestros clientes, llevarlo al plano más personal”. “Al final creo que estamos hablando siempre de empleados y de usuarios, pero lo que estamos haciendo es dar respuesta a una responsabilidad que como sector tenemos, que es concienciar a la población, sean o no empleados nuestros”.

Por último, Fabio Cichero aborda el tema del password, señalando que lo que hace es “quitar un poco esta responsabilidad o esta culpabilidad al usuario”. Además, el portavoz vuelve a hablar sobre los peligros del phishing: “necesitamos ir hacia un futuro de tecnología resistente al phishing” y añade: “el phishing es el vector número uno y hay que ir hacia una tecnología que sea resistente a esto”.

"El usuario es la primera línea de defensa, y su educación y concienciación son un elemento clave"

Andrés Sanz Mollejo, Ciberseguridad, CEPSA

Compartir en RRSS