FORO it Digital Security

ESTRATEGIAS DE CIBERSEGURIDAD INTELIGENTES:

HOJA DE RUTA Y MEJORES PRÁCTICAS

©freepik

PATROCINADOR PLATINO

making science

PATROCINADORES GOLD

BFY TU BIOMETRÍA SOLO CONTIGO

Barracuda. Your journey, secured.

Bitdefender

IKUSI velatia

cisco Partner

WatchGuard

SONICWALL

STORMSHIELD

V-Valley enhancing your business

WATCHGUARD FOR SOC

CON EL APOYO INSTITUCIONAL DE

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ESTRATEGIAS DE SEGURIDAD INTELIGENTES:

¿QUÉ HACER PARA MEJORAR LA PROTECCIÓN EN UN MOMENTO COMO EL QUE ESTAMOS VIVIENDO?

CADA VEZ MÁS, PROTEGER UNA EMPRESA SUPONE TENER EN CUENTA MULTITUD DE ASPECTOS. ASÍ LO ESTAMOS VIENDO EN EL SECTOR EN LOS ÚLTIMOS AÑOS EN LOS QUE TANTO LAS AMENAZAS COMO LOS VECTORES A TENER EN CUENTA SE HAN MULTIPLICADO EXPONENCIALMENTE. ¿QUÉ HACER PARA MEJORAR LA PROTECCIÓN EN UN MOMENTO COMO EL QUE ESTAMOS VIVIENDO?

El principal desafío en este momento es solucionar el problema antes de que los cibercriminales lo descubran y lo exploten. Prevenir antes de curar, como bien apunta el refranero español. Y precisamente con vistas a imponer esta visión, en IT Digital Security hemos celebrado un Foro en el que analizamos cómo está la ciberseguridad a día de hoy y cuáles son las claves y el camino a seguir para asegurar la empresa de forma inteligente.

Muchos problemas de ciberseguridad se centran en amenazas específicas como el ransomware, el robo de propiedad intelectual o vulnerabilidades de todo tipo a través de las cuales los ciberdelincuentes acceden a las redes de las organizaciones para causar daños catastróficos, pero la ciberseguridad va mucho más allá.

A día de hoy, cuando hablamos de seguridad ya no hacemos referencia únicamente a la necesidad de proteger la red, el perímetro o los dispositivos, hablamos de proteger todos los elementos que componen el entorno de trabajo y eso incluye aplicaciones críticas para el negocio, infraestructura de mensajería y colaboración, servicios en la nube, comercio electrónico y aplicaciones de fabricación, plantas de producción... y un largo etcétera que llega hasta los empleados y la necesidad inminente de formarlos en este ámbito.

LA TECNOLOGÍA HAY QUE CONFIGURARLA Y GESTIONARLA ADECUADAMENTE, SINO NO SE APROVECHARÁ SU VERDADERO POTENCIAL Y PODRÍAN DARSE PROBLEMAS DE SEGURIDAD A PESAR DE LA INVERSIÓN

Para poder desarrollar una estrategia de ciberseguridad sostenible y duradera, las empresas deben ser conscientes de su situación y hacer frente a numerosos retos de la forma más efectiva posible. El uso de la tecnología supone un nuevo paradigma digital, donde ya no importa la ubicación del usuario, el dispositivo desde el que se conecte o la idiosincrasia de la infraestructura a la que acceda. En este nuevo escenario ha de primar la planificación, adopción y gestión de medidas de ciberseguridad de forma proactiva, permitiendo al negocio avanzar y asegurar la continuidad pase lo que pase.

Pero ¿cómo equilibrar las necesidades de seguridad con una experiencia de usuario fluida y sin interrupciones? ¿Cómo se puede monitorear continuamente el estado de seguridad sin arriesgarse a obstaculizar la productividad y la motivación de los traba-

jadores? Trabajar de forma flexible, remota, respetando las necesidades individuales y con total seguridad es el mayor reto al que se ha enfrentado el tejido empresarial en mucho tiempo. Y precisamente este desafío fue el eje central de la IV edición del Foro IT Digital Security celebrado el pasado 25 de abril bajo el lema "Estrategias de ciberseguridad inteligente: hoja de ruta y buenas prácticas", en el que se abordaron los diferentes desafíos a los que se enfrentan las compañías actualmente y las mejores prácticas para hacerles frente.

Durante el evento quedó claro que conocerse bien es la mejor forma de consolidar la seguridad en los tiempos que corren, pero, ¿cómo puede conseguirse esto en ciberseguridad? Existen muchas formas, está claro, pero entre las más destacadas estaría utilizar servicios de pentesting que busquen los agujeros en el sistema o servicios de red team, lo importante es poder realizar una evaluación de riesgos de seguridad para identificar las posibles brechas, analizar la criticidad y aplicar controles de seguridad o soluciones que aseguren el control de los posibles vectores en caso de ciberataque.

Una vez que tengamos claro el statu quo, toca implementar soluciones capaces se asegurar la continuidad de negocio en caso de ciberataque. Toca prevenir.

Aquí es donde entran en juego las diferentes tecnologías de protección, detección y securización de redes, equipos, API... sin olvidar que las herramientas por sí solas y de forma automática no protegen. Hay que llevar a cabo una buena configuración y disponer del personal adecuado para su gestión.

Como hemos visto en varias ocasiones, en ciberseguridad la tecnología hace gran parte del trabajo, pero no lo hace todo sola. No vale solo con tener herramientas de seguridad para asegurar la buena protección de una compañía. Esa tecnología hay que configurarla y gestionarla adecuadamente, sino no se aprovechará su verdadero potencial y podrían darse problemas de seguridad a pesar de la inversión. De hecho, los errores de configuración relacionados con el acceso público a los buckets de almacenamiento, los permisos de las cuentas, el almacenamiento y la gestión de contraseñas... han provocado la exposición de miles de millones de registros.

Además de los errores de configuración y las vulnerabilidades, obtener acceso a cuentas privilegiadas en la nube puede permitir a los cibercriminales eludir la detección y lanzar toda una infinidad de ataques; sin embargo, muchas organizaciones siguen sin restringir adecuadamente los privilegios o el acceso de usuarios y cuentas con privilegios ni aplicar la verificación MFA.

VISIBILIDAD Y GESTIÓN: NO OLVIDEMOS LOS BÁSICOS

El seguimiento de intrusiones en la actualidad es, sin duda, una de las claves de la protección real. Las soluciones de seguridad de-

ben ser capaces de detectar activamente las amenazas. Para realizar esta tarea, se requiere una visibilidad completa de lo que ocurre en nuestro entorno. A día de hoy, las organizaciones pasan por alto más del 60% de las amenazas de seguridad sin siquiera saberlo. Contar con tecnologías como EDR, gestión automática de instalación de parches o MFA es vital para minimizar la superficie de ataque dependiendo de la empresa.

De nuevo, no vale solo con invertir en tecnología. Los ciberdelincuentes están en constante cambio y aprovechan de forma habitual cualquier tipo de vulnerabilidad o fallo por lo que es cada vez más necesario realizar un mantenimiento regular de parches y pruebas de penetración para comprobar que todo sigue funcionando correctamente a pesar de la cantidad de ataques que surgen cada día y las diferentes vulnerabilidades que se van encontrando paulatinamente.

A medida que el ciberespacio, la infraestructura de red y la cadena de suministro se han convertido en objetivos principales para los cibercriminales, tener en cuenta estos pasos puede ayudar a las empresas y organizaciones a garantizar, no una seguridad 100%, pero sí, que se ha hecho todo lo posible para proteger los activos, tangibles o intangibles, de la empresa, lo que a su vez puede evitar sanciones por parte de los organismos reguladores.

Si quieres conocer cómo implementar una estrategia de seguridad inteligente y cuáles son las claves para protegerse a día de hoy, no te pierdas el siguiente especial en el que analizamos todo lo ocurrido durante la IV edición del Foro IT Digital Security y cuáles han sido sus principales conclusiones. ■

EL SEGUIMIENTO DE INTRUSIONES EN LA ACTUALIDAD ES, SIN DUDA, UNA DE LAS CLAVES DE LA PROTECCIÓN REAL

CONTENIDO RELACIONADO

Errores de configuración y cuentas comprometidas ponen en riesgo los entornos cloud

Ciberresiliencia

Así es la propuesta de la nueva Ley de Ciberresiliencia de la Comisión Europea

Que la seguridad de tus activos digitales no te quite el sueño

Making Science te ayuda a implementar una estrategia de seguridad multi-norma, adecuada a las necesidades de tu negocio, escalable y sin silos.

CONTACTA CON NOSOTROS

making science

THE DIGITAL ACCELERATION COMPANY®

WWW.MAKINGSCIENCE.ES

SARA GARCÍA BÉCARES, RESPONSABLE DE RETECH CIBERSEGURIDAD EN INCIBE

"NO PODEMOS DIGITALIZAR A NUESTROS CIUDADANOS Y A NUESTRAS EMPRESAS Y DEJARLES ABANDONADOS EN UN SISTEMA QUE POR SÍ MISMO PUEDE SER PELIGROSO PARA ELLOS"

La ciberseguridad es un elemento cada día más importante en nuestra vida cotidiana, tanto en la vertiente personal como en la profesional, algo que se debe al incremento paralelo de la digitalización de nuestra sociedad. Sin embargo, pese a que los niveles de concienciación de empresas y ciudadanos deberían estar incrementándose, lo cierto es que desde INCIBE detectan una sensación de falsa seguridad que incrementa los niveles de indefensión.

Como punto de arranque de la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas, conversamos con Sara García Bécares, responsable de RETECH Ciberseguridad en INCIBE, sobre el estado de la ciberseguridad en nuestro país. Para esta responsable,

Repasamos el estado de la ciberseguridad en España de la mano de Sara García Bécares (INCIBE).

"la ciberseguridad en los últimos tiempos está mucho más presente, dejando de ser una cosa del sector de la tecnología para pasar a ser algo que afecta a toda la ciudadanía, lo que es bueno porque se tiene más conciencia de que según crece la digitalización, tiene que ir de la mano la ciberseguridad. No podemos digitalizar a nuestros ciudadanos y a nuestras empresas y dejarles abandonados en un sistema que por sí mismo puede ser peligroso para ellos".

UNA REALIDAD DIVERSA, PERO PREOCUPANTE

En esta realidad, no podemos hablar de unanimidad en el nivel de concienciación alrededor de la ciberseguridad, pero, tal y como reconocía Sara García, "tenemos que seguir trabajando mucho con los ciudadanos y con las empresas para seguir potenciando esa concienciación. Según las cifras que manejamos en INCIBE, hace diez años la gente era más consciente del riesgo. Ahora tienen un sentimiento de falsa seguridad, pero el número de incidentes ha crecido muchísimo, igual que los diferentes técnicas de ataque, cada vez más sofisticadas".

PRINCIPALES INCIDENTES DE SEGURIDAD

A la vista de los datos recabados por INCIBE, "el principal tipo de incidente es la filtración de datos. Hay una gran preocupación y se está viendo que hay muchas fugas, que se roban datos, que hay datos de carácter personal circulando... es una gran preocupación porque es un problema muy común. Pese a la concienciación, nos encontramos con sistemas vulnerables que no están parcheados correctamente, que no tienen los dispositivos o las herramientas necesarias. Otro tipo de incidente destacado es el fraude on-line en sus diferentes variantes. El phishing y el ransomware siguen encabezando la lista".

"PESE A LA CONCIENCIACIÓN, NOS ENCONTRAMOS CON SISTEMAS VULNERABLES QUE NO ESTÁN PARCHEADOS CORRECTAMENTE, QUE NO TIENEN LOS DISPOSITIVOS O LAS HERRAMIENTAS NECESARIAS"

LA APORTACIÓN DE INCIBE

Según nos explicaba nuestra interlocutora, "desde INCIBE tenemos muchas líneas de actuación porque nuestro público objetivo es muy grande. Hablamos de ciudadanos, empresas, especialmente al sector PYME, pero también de los distintos sectores estratégicos y de la gran empresa. Por tanto, el foco y las iniciativas son diversas. Un ejemplo es la Oficina de Seguridad del Internauta, con la línea gratuita de ayuda 017, donde se está haciendo mucho hincapié en no esperar y tratar de solucionar los problemas de manera preventiva. Tenemos toda una línea dedicada a menores, educadores, padres, porque es un tema que preocupa y que nos tiene que ocupar bastante tiempo. Tenemos otra línea, Proteger tu Empresa, muy dedicada a pymes y autónomos, que normalmente se encuentran muy indefensos porque no tienen los conocimientos ni las capacidades necesarias. Y, por supuesto, damos servicios a todos los sectores críticos". ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

DESCÁRGUELO AHORA EN:
SONICWALL.COM/THREATREPORT

2023

INFORME DE CIBERAMENAZAS DE SONICWALL

EL CAMBIANTE PANORAMA DEL CIBERCRIMEN

SONICWALL®

sonicwall.com | @SonicwallSpain

CÓMO HACER QUE LA NUBE TAMBIÉN FORME PARTE DE LA SEGURIDAD DE TU EMPRESA

LA TRANSICIÓN CRECIENTE HACIA ENTORNOS BASADOS EN LA NUBE Y MODELOS IAAS, PAAS O SAAS OFRECE A LAS EMPRESAS LA CAPACIDAD DE ALIGERAR LA TI PROPIA Y SU GESTIÓN. PERO ESTO NO SIGNIFICA QUE HAYA QUE DESCUIDAR NI SU ADMINISTRACIÓN NI SU SEGURIDAD, PUES A ESTAS SOLUCIONES CLOUD SE CONFÍAN ACTIVOS IMPORTANTES PARA LA EMPRESA: DATOS, DISPOSITIVOS, APLICACIONES... LOS PROVEEDORES DE NUBE SIGUEN LAS MEJORES PRÁCTICAS DE SEGURIDAD Y CUENTAN CON MEDIDAS ACTIVAS PARA PROTEGER SUS SERVIDORES. SIN EMBARGO, LAS EMPRESAS DEBEN APLICAR SUS PROPIAS HERRAMIENTAS PARA PROTEGER TODO SU ECOSISTEMA.

Para hablar de ciberseguridad y nube, se celebró, con la colaboración de Making Science, en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas, un debate en el que participaron responsables de seguridad de Bit2Me, Cofares, Coren, Grupo Howden, JSV Logistic, Sanoma, y Wizink.

DESAFÍOS DE LA NUBE PARA LA CIBERSEGURIDAD

Evidentemente, la nube implica una serie de desafíos para la estrategia de ciberseguridad de la empresa. Tal y como indica-

Analizamos el papel de la nube en la estrategia de ciberseguridad de las organizaciones de la mano de Bit2Me, Cofares, Coren, Grupo Howden, JSV Logistic, Sanoma, y Wizink, con la colaboración de Making Science.

“La flexibilidad de la nube viene acompañada de un incremento de las vulnerabilidades”
Washington Gómez, CISO de **Bit2Me**

“La nube nos permite mejorar nuestra flexibilidad, pero tenemos que asegurar un servicio sostenible en caso de desastre”
Pedro Iván Montes,
Director de Ciberseguridad y Redes de **Cofares**

ba Óscar Rodrigo, Responsable de Infraestructuras Cloud y Ciberseguridad del Grupo Howden, “poder contar con la nube es una ventaja y, a la vez, un problema. Pero aprovechamos esa ventaja a nivel de seguridad, complementando las herramientas que ofrecen los proveedores de nube, y subiendo a cloud aquellos elementos que lo necesitan, y dejando en local los que no”.

Para Pedro Iván Montes, Director de Ciberseguridad y Redes (CISO) de Cofares, “cloud es un desafío para todas las empresas, sobre todo para aquellas que prestan servicios importantes para la sociedad. La nube nos permite mejorar nuestra flexibilidad, pero tenemos que asegurar un servicio sostenible en caso de desastre, por lo que es necesario definir qué llevamos a la nube y qué no”.

Desde la perspectiva de Washington Gómez, CISO de Bit2Me, “la flexibilidad de la nube viene acompañada de un incremento de las vulnerabilidades. El crecimiento en cloud debe ir acompañado siempre de una capa de ciberseguridad. Cualquier recurso que se vaya creando en cloud debe cumplir siempre con los requisitos establecidos de ciberseguridad. Y mantener esta elasticidad con los mismos niveles de seguridad es un desafío, igual que integrar la seguridad en el desarrollo”.

Se mostraba de acuerdo con él David González, CISO de Coren, que añadía que “también hay que vigilar los costes, para lo que hay que controlar la eficiencia del código, y, dependiendo del uso que se haga de la nube, establecer los elementos y niveles de seguridad, el acceso, el cifrado de los datos, las actualizaciones... hay que ser conscientes de las tareas de seguridad que dependen del proveedor y las que dependen de tu propia organización”.

En palabras de Luis Ballesteros, CISO de Wizink, “la seguridad está en nuestro ADN, porque somos una entidad hiper-regulada. Pero no podemos renunciar a cloud, por lo que el reto es hacer entender a la organización el modelo de seguridad compartida. Tener un servicio en cloud es un centro de datos más, para nosotros no hay diferencia. La seguridad es la misma, es estratégica para la compañía. Debe estar por diseño desde el inicio. La sensación de falsa seguridad puede ser un problema si no asumes tu parte de seguridad, y en la parametrización adecuada es donde está el reto”.

Señalaba Mario García, CTO de JSV Logistic, que “para nosotros es esencial la seguridad y la continuidad de las operaciones. Por ello nuestro modelo es híbrido. No podemos tener una caída porque las operaciones no pueden parar. La seguridad va a

“Hay que ser conscientes de las tareas de seguridad que dependen del proveedor cloud y las que dependen de tu propia organización”
David González, CISO de **Coren**

“Hay que aprovechar el conocimiento del proveedor y apoyarte en la capacidad de los partners”
Óscar Rodrigo, Responsable de Infraestructuras Cloud y Ciberseguridad de **Grupo Howden**

depender del modelo de nube que elijas”. Finalizaba esta primera ronda David de la Rosa, ISO de Sanoma, apuntando que “el mayor reto es proteger la información personal que gestionamos de nuestros clientes. Es necesario acompañar a cada una de nuestras empresas a la velocidad que cada una necesita, y hay que trasladar el modelo de gestión on-premise a cloud, porque no son los mismos recursos y, además, nos encontramos con el problema del talento”.

CRITERIOS RELEVANTES DE CIBERSEGURIDAD A TENER EN CUENTA

Continuaba David de la Rosa señalando que “desde el área de seguridad hemos de acompañar al negocio. Hemos de establecer nuestros estándares de seguridad, ya sean por regulación o por decisión de compañía, pero debemos acompañar la decisión y asegurarnos de que se implementan sea cual sea el proveedor de nube que elija negocio”.

“Hay que identificar qué llevamos a cloud y qué dejamos on-premise, porque la nube es la principal entrada de amenazas”
Mario García, CTO de **JSV Logistic**

“El mayor reto es proteger la información personal que gestionamos de nuestros clientes”
David de la Rosa, CISO de **Sanoma**

Mario García (JSV Logistic) compartía que “cuando piensas en una migración a cloud o diseñas un servicio específico en la nube, debes entender muy bien qué necesita el negocio. Depende de la industria en la que estés, de la regulación… pero hay que identificar qué llevamos a cloud y qué dejamos on-premise, porque la nube es la principal entrada de amenazas, y cuanto más concreto sea el espacio a proteger, será más sencillo. En un proveedor analizamos sus certificaciones, analizamos su política de protección de datos, establecemos una política de gestión en base a los mínimos privilegios posibles, hacemos hincapié en los planes de backup y recuperación, vigilamos los sistemas de cifrado…”.

En el caso de Luis Ballesteros (Wizink), “independientemente del proveedor, tenemos una política de selección donde intervienen muchas áreas del banco. Se mira de una forma multidisciplinar. En el caso de la seguridad, como se van a gestionar datos sensibles, hacemos una evaluación al proveedor, tanto previa a la contratación como de forma periódica. Se hace contra nuestras políticas y nuestros estándares, porque elegimos proveedores porque lo hacen de forma más eficiente que nosotros, pero los datos son nuestros y somos responsables de ellos. Las certificaciones que tengan ayudan, pero no nos limitamos a eso. Pero las opciones de seguridad del proveedor se tienen que contratar, y el departamento de seguridad debe participar desde el principio para asegurarse de que se incluyan desde el principio”.

Para David González (Coren), “es necesario ver las necesidades del negocio, repasar las certificaciones, y analizar dónde es más fuerte cada uno de ellos para cada proyecto concreto”.

Señalaba Washington Gómez (Bit2Me) que “es principal para una migración es un análisis de riesgos, para descubrir los que pueden aparecer en la nube que no existían en una realidad on-premise. Una correcta evaluación de riesgo nos ayudará a implantar nuevos controles para un modelo de nube. Además, un adecuado diseño de la plataforma nos ayudará a reducir los tiempos de respuesta de nuestro plan de recuperación, y eso nos va a dar la flexibilidad que necesitamos”.

Continuaba Pedro Iván Montes (Cofares) comentando que “distinguimos entre dos servicios en la nube. Aquellos en los que implementamos nuestra propia estructura, y aquellos que consumimos con responsabilidad compartida pero delegada. Hay que explicar muy bien a la organización que, además de los costes propios del servicio, hay otros relacionados con la seguridad. Hay que tener las partidas adecuadas para

“No podemos renunciar a cloud, por lo que el reto es hacer entender a la organización el modelo de seguridad compartida”

Luis Ballesteros, CISO de **Wizink**

el servicio concreto que quiere consumir la compañía. Nos preocupa que los proveedores cumplan la normativa en España, pero lo más importante es la criticidad que va a tener el propio servicio en la nube”.

Concluía Óscar Rodrigo (Grupo Howden), indicando que “seguramente todos nos apoyamos en un partner, además de en el proveedor, y es importante que sean especializados para que te aporte más valor. Cuanto más especializado sea, más fácilmente van a retener talento. Hay que aprovechar el conocimiento del proveedor y apoyarte en la capacidad de los partners”.

LA VISIÓN DEL PROVEEDOR

Miguel López, Architecture & Infrastructure Engineering Director de Making Science, aportaba al debate la visión de su compañía para ayudar a las empresas en un despliegue seguro en cloud. Tal y como explicaba, la apuesta de Making Science pasa por garantizar una serie de elementos, como son la identidad centralizada y la autenticación, la protección de usuarios y activos, evitar fugas de información, observabilidad y detección de amenazas, escalabilidad y confiabilidad, agilidad y facilidad de implantación, control de costes y cumplimiento normativo. Para ello, como Partner Premier en todos los verticales de Google, “hemos creado un ecosistema en torno a los productos de Google, solucionando todos los puntos básicos”.

A partir de ahí, “como nos hemos dado cuenta de que esto nos funciona para nosotros, hemos dado el paso y se lo hemos ofrecido a los clientes. Para ello, creamos para cada uno de ellos su propia estancia sobre plataforma Google y empezamos a ingestar sus propias fuentes, ofreciéndoles, sobre ello, un servicio de SOC y SOA para acercar la seguridad a empresas que, si no, no se lo plantean porque los costes eran muy elevados de primeras”. ■

“Acercamos la seguridad a empresas que, si no, no se plantean hacerlo por un problema de costes”

Miguel López, Architecture & Infrastructure Engineering Director de **Making Science**

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

MIGUEL LÓPEZ, ARCHITECTURE & INFRASTRUCTURE ENGINEERING DIRECTOR DE MAKING SCIENCE

“LA SEGURIDAD ES PARTE INTRÍNSECA DEL NEGOCIO”

La seguridad es un elemento esencial para las empresas, tanto cuando hablamos de infraestructuras on-premise como cuando se plantean la migración a la nube. Pero los beneficios que aporta cloud implican un incremento de la inseguridad, que las empresas no pueden obviar. Making Science ha aprovechado su propia experiencia como empresa para desarrollar un servicio que pone a disposición de sus clientes.

Tal y como explicaba en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas, Miguel López, Architecture & Infrastructure Engineering Director de Making Science, “la propia naturaleza de Making Science desde nuestra creación en 2019 nos ha llevado a poner unas bases para proteger nuestros datos y los datos de nuestros clientes para, a partir de ahí, poder seguir creciendo”.

Miguel López analizaba en su ponencia cómo aprovechar la propia experiencia de Making Science en beneficio del cliente en el área de seguridad.

Según recordaba este responsable, “al principio IT y desarrollo estaban por separado, luego pasamos a DevOps y ahora a SecDevOps, pero lo cierto es que la seguridad es parte de la conceptualización del proyecto donde está el partner y el despliegue de arquitectura para el servicio al cliente”.

REQUISITOS DE UN ENTORNO OPERATIVO SEGURO

La apuesta de Making Science pasa por garantizar una serie de elementos, como son la identidad centralizada y la autenticación, la protección de usuarios y activos, evitar fugas de información, observabilidad y detección de amenazas, escalabilidad y confiabilidad, agilidad y facilidad de implantación, control de costes y cumplimiento normativo. Para ello, como Partner Premier en todos los verticales de Google, “hemos creado un ecosistema en torno a los productos de Google, solucionando todos los puntos básicos”.

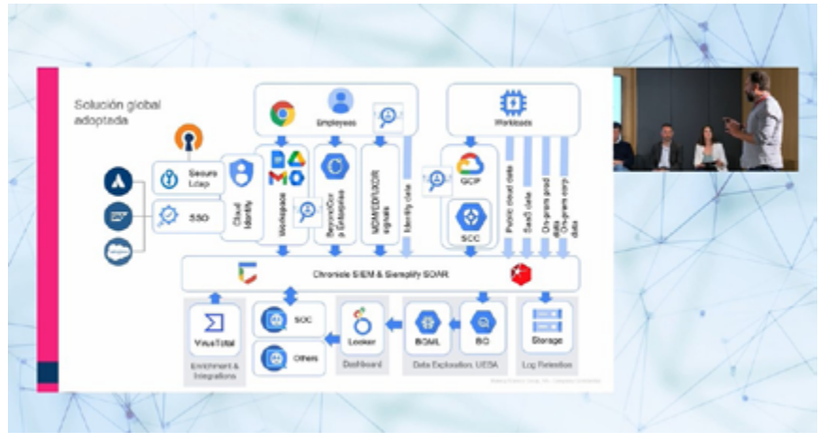
A partir de ahí, “como nos hemos dado cuenta de que esto nos funciona para nosotros, hemos dado el paso y se lo hemos ofrecido a los clientes. Para ello, creamos para cada uno de ellos su propia estancia sobre plataforma Google y empezamos a ingestar sus propias fuentes, ofreciéndoles, sobre ello, un servicio de SOC y SOA para acercar la seguridad a empresas que, si no, no se lo plan-

“LA SEGURIDAD ES PARTE DE LA CONCEPTUALIZACIÓN DEL PROYECTO DONDE ESTÁ EL PARTNER Y EL DESPLIEGUE DE ARQUITECTURA PARA EL SERVICIO AL CLIENTE”

tean porque los costes eran muy elevados de primeras”.

APROVECHAR LA PLATAFORMA EN BENEFICIO DEL CLIENTE

Con esta estrategia, “hemos conseguido el cumplimiento multinormativo, porque para nosotros era importante hacerlo tanto en Europa como en Estado Unidos; hemos reducido de forma significativa los costes, porque, a nivel de hardware, no hubiera tenido sentido montar una infraestructura on-premise, porque no tenemos una visión clara de cómo seremos en el futuro y no sabemos cuáles habrían sido los costes de aprovisionar y mantener lo que hubiéramos podido necesitar, a la vez que hemos reducido los costes operativos, porque con mucho menos personal estamos dando mucho más servicio; hemos reducido y mejorado los tiempos de análisis y de respuesta, porque estamos avanzando mucho en la automatización porque muchas de las



mismas plantillas propias nos sirven para los clientes; a nivel de usuario, hemos creado una experiencia unificada, porque todo está centralizado; por último, aprovechamos los datos tanto para seguridad como para negocio, y eso ayuda a conseguir más presupuesto para invertir en seguridad, porque esta es parte del negocio”. ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

La ciberdelincuencia en España representa el 15,6% de los hechos delictivos*.

No dejes que los ciberdelincuentes acaben con tu negocio.

b FY

TU BIOMETRÍA
SOLO CONTIGO

b-fy.com

b-fy.com

*** Informe sobre la Criminalidad en España 2021.**

PROTECCIÓN Y RECUPERACIÓN ANTE AMENAZAS: CLAVES PARA ASEGURAR EL FUTURO

TENER UNA ESTRATEGIA SÓLIDA DE PROTECCIÓN DE LOS ACTIVOS DE LA EMPRESA ES CADA VEZ MÁS VITAL. EN EL CONTEXTO ACTUAL, EN EL QUE LA PROLIFERACIÓN DE ATAQUES NO CESA, SE IMPONE UN ANÁLISIS DE RIESGO Y UNA PREVENCIÓN ADECUADA PERO TAMBIÉN, TENER UN PLAN DE RECUPERACIÓN ESTABLECIDO Y TESTADO QUE PERMITA LA CONTINUIDAD DEL NEGOCIO EN CASO DE ATAQUE.

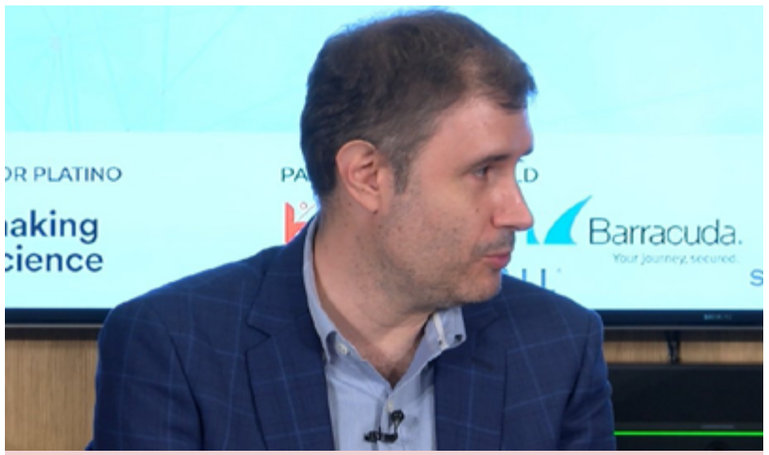
Para hablar de protección y recuperación ante amenazas, en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas, celebramos un debate que contó con la colaboración de SonicWall y Stormshield Iberia, y la participación de Banco Cooperativo Español, Coren, Hermanas Hospitalarias, Pitcher y Restaurant Brands Iberia.

PLANES DE PROTECCIÓN Y RECUPERACIÓN

Arrancaba el debate José Manuel Beltrán Sánchez, CISO de Hermanas Hospitalarias, indicando que, en realidad son dos

Hablamos de protección y recuperación ante amenazas con la colaboración de SonicWall y Stormshield Iberia, y la participación de Banco Cooperativo Español, Coren, Hermanas Hospitalarias, Pitcher y Restaurant Brands Iberia.

“Hay que definir los planes de respuesta, pero, sobre todo, actualizarlos y testearlos”
Miguel Ángel Hernández Santiago, Responsable de Riesgos Tecnológicos de **Banco Cooperativo Español**



“La concienciación es parte fundamental de la protección y la prevención” David González, CISO de **Coren**

aspectos diferentes “y hemos de tener en cuenta los puntos fuertes y débiles de cada uno, tanto a nivel técnico como presupuestario y humano. Nosotros llevamos años trabajando en diferentes elementos de la protección, y hemos visto que modelos muy instalados en la Sanidad necesitaban ser reemplazados y contar con la ayuda de especialistas en cada caso que, bajo tu dirección, puedan aportar la experiencia necesaria. Pero ¿cómo responder a un ataque? Nosotros identificamos los activos críticos para nuestra actividad, y todo lo que tiene que ver con datos o con la interrupción de un servicio hay que restaurarlo en tiempo real; y nos aseguramos de que las copias de seguridad del resto de activos están preparadas y son las adecuadas”.

Francisco Javier Farfán Contreras, CISO de Restaurant Brands Iberia, apuntaba que “trabajamos con un entorno muy cambiante al que la seguridad debe adaptarse. Por eso, hemos diseñado una respuesta ante incidentes de manera global, porque la confianza de los clientes es lo más importante. Queremos ofrecer una respuesta que no sea solo desde la seguridad, sino desde toda la organización. Contamos con herramientas de respaldo, concienciamos al usuario, pero la clave es dar una respuesta holística, que nos ayuda también a una detección temprana de la incidencia”.

Para Miguel Ángel Hernández Santiago, Responsable de Riesgos Tecnológicos de Banco Cooperativo Español, “por regulación, lo más importante para nosotros son los datos. Estamos sometidos a regulaciones nacionales e internacionales que tenemos que cumplir. Tenemos planes de recuperación que probamos cada seis meses, tanto nosotros como auditorías externas. No vale decir que estamos preparados, hay que demostrarlo. Cada día hay más intentos de fraude y robo digitales que físicos, y, además, son más productivos, y el mayor problema que detectamos es la concienciación de los usuarios, porque son el principal vector de riesgo. El cibercrimen es un negocio muy lucrativo, y la concienciación del usuario es esencial”.

Continuaba David González, CISO de Coren, señalando que “la concienciación es parte fundamental de la protección, y lo que hacemos, además, es centrarnos en proteger no una ubicación, sino al individuo sin confiar en nada. Verificamos que la conexión es de quién dice conectarse y que tiene los permisos y herramientas adecuadas. En cuanto a la respuesta ante incidentes, hemos creado un comité multidisciplinar y hemos definido planes de respuesta

“No solo hay que pensar en enemigos externos, sino que hay que controlar los posibles incidentes internos para proteger los datos de los pacientes”
José Manuel Beltrán Sánchez, CISO de **Hermanas Hospitalarias**

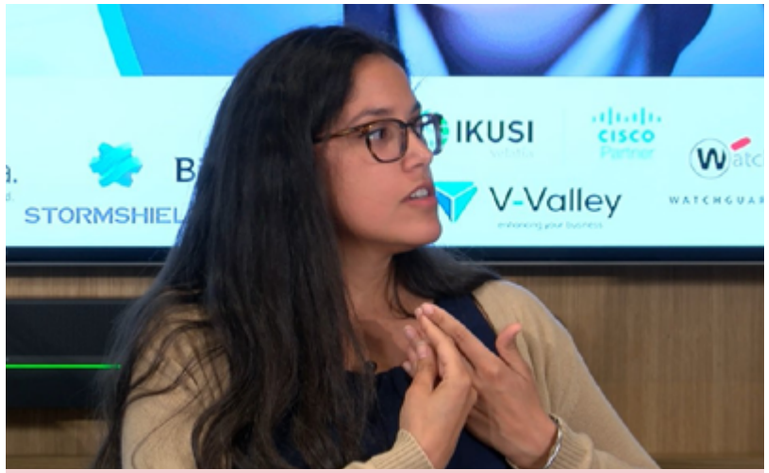
en caso de problema que vamos probando poco a poco, identificando los activos más críticos. Además, contamos con sistemas de recuperación en caliente con duplicación simultánea para recuperación inmediata en caso de desastre”.

Finalizaba esta ronda de opiniones Glenda Suárez, Director IT QRC & Security de Pitcher, que comentaba que “no tenemos que recoger más datos de los necesarios, y garantizamos una solución que permite al usuario conservar el control de los datos mientras nosotros les damos el servicio, lo que minimiza la superficie de ataque para los cibercriminales. No solo hay que analizar la posibilidad de ser atacados, sino también la de que lo sean nuestros clientes o nuestro entorno empresarial. Hay que incrementar la atención a la protección en todos los niveles”.

CÓMO HACER FRENTE A UN ATAQUE

Continuaba Glenda Suárez explicando que “en caso de ataque, es fundamental contar con un plan de respuesta ante incidentes que tenga en cuenta todas las necesidades. Hay que seguir las pautas marcadas e identificar los riesgos, así como tener en cuenta los requisitos que impone la regulación y los plazos necesarios, o los contratos que has firmado con tus clientes. En caso de ataque, es fundamental tomar las decisiones correctas ya previstas en el plan de respuesta”.

Para David González (Coren), “lo esencial es saber lo que tienes que recuperar. Si co-



“No solo hay que analizar la posibilidad de ser atacados, sino también la de que lo sean nuestros clientes o nuestro entorno empresarial”
Glenda Suárez,
Director IT QRC & Security de **Pitcher**

“Trabajamos con un entorno muy cambiante al que la seguridad debe adaptarse”
Francisco Javier Farfán Contreras,
CISO de **Restaurant Brands** Iberia

noces tus activos y procesos puedes decidir los que son críticos para la compañía en alineación con el negocio, no solo desde el punto de vista de IT. Tras esto, hay que conocer los problemas a los que te puedes enfrentar en cada caso. No se trata de tener solo una respuesta ciber, sino que hay que tener en cuenta todas las posibles incidencias para poder definir los plazos y las fórmulas de recuperación”.

Desde el punto de vista de Miguel Ángel Hernández (Banco Cooperativo Español), “hay que pasar por todos estos pasos que comentaba David, pero sobre todo hay que revisarlos, porque en ocasiones se establece un plan pero las circunstancias han cambiado en el momento del desastre. El plan debe estar muy alineado con las unidades de negocio, porque tienen una visión diferente a la de TI. Nosotros diferenciamos entre incidentes, como puede ser un borrado accidental de una carpeta, y ciber-incidentes, como un ataque, y determinamos el nivel de exposición y afectación para poner en marcha una respuesta, que implica al comité de respuesta, que implica a diferentes perfiles y responsables”.

En palabras de Francisco Javier Farfán (Restaurant Brands Iberia), “antes solo había que fijarse en la calidad del producto para mantener la reputación. A día de hoy, si la compañía no tiene la confianza del usuario, podría tener un efecto grave para el negocio. Hay que conocer la compañía desde todas las instancias para aplicarlo también en la seguridad. Es la única forma que tenemos para transmitir a la dirección la importancia de la protección y el plan de respuesta. Hay que tener clara la infraestructura, identificar los posibles puntos débiles, y estar preparados ante incidentes para que no afecten a la reputación”.

Finalizaba esta onda de valoraciones José Manuel Beltrán (Hermanas Hospitalarias), que recordaba “que las consecuencias de un incidente son graves. En nuestro sector deberíamos seguir los pasos de otros, como el bancario, para formar, concienciar y proteger a las organizaciones. Es importante saber reaccionar a un ataque de verdad, no a una leve incidencia, y hay que reconocer que es necesario contar con ayuda externa que aporte el conocimiento, la capacidad y los recursos pertinentes. Además, no solo hay que pensar en enemigos externos, sino que hay que controlar los posibles incidentes internos para proteger los datos de los pacientes”.

LA RESPUESTA DE LA INDUSTRIA

Los retos y problemas expuestos en el debate no son nuevos para la industria, porque,

como reconocía Borja Pérez, Country Manager de Stormshield Iberia, "estamos en contacto directo con los CISO de empresas de diferentes perfiles y sectores. Las grandes empresas pueden contar con un plan de respuesta y las herramientas adecuadas, y, sobre ellas, nosotros podemos aportar nuestra experiencia y nuestras soluciones. Pero no solo las herramientas de ciberseguridad deben formar parte de la respuesta, pero son esenciales en la arquitectura de protección. Pero, como no podemos abarcar todos los aspectos de la ciberseguridad, cada vez hay más cooperación entre los diferentes jugadores y se trabaja en la interoperabilidad para ayudar en esta línea".

Para Sergio Martínez, Iberia Regional Manager de SonicWall, "hablamos de una sofisticación y sutileza sin precedentes en el cibercrimen. En nuestra encuesta anual a CIO y CISO, más de la mitad creen que la situación es peor, pese a que siguen incrementándose los presupuestos de ciberseguridad. Hay mayor concienciación y recursos, pero también más amenazas. La transformación digital ha cambiado la realidad del negocio y la protección debe adecuarse a la nueva situación. El entorno es totalmente distinto, y hay que adaptarse. Por otra parte, lo que más ha crecido han sido los ataques IoT".

De hecho, recordaba Borja Pérez que en el entorno IT está más clara la estrategia de respuesta, "pero no así en el entorno OT". ■

CONTENIDO RELACIONADO

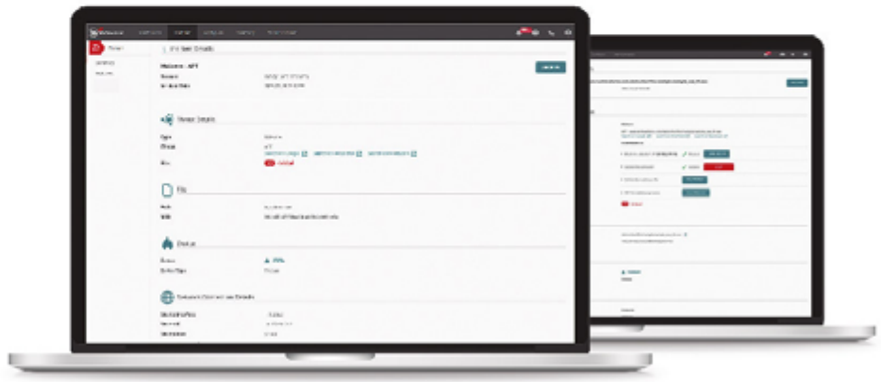
IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

"La transformación digital ha cambiado la realidad del negocio y la protección debe adecuarse a la nueva situación"
Sergio Martínez,
Iberia Regional Manager de **SonicWall**

"Nosotros podemos aportar soluciones y experiencia, pero es esencial diseñar un plan de respuesta"
Borja Pérez,
Country Manager de **Stormshield Iberia**

WATCHGUARD

THREATSYNC®



Agilice las operaciones de seguridad y reduzca el tiempo y los recursos necesarios para gestionar múltiples herramientas de seguridad con nuestro enfoque de seguridad unificado basado en XDR.

Amplíe la visibilidad, detecte antes y responda más rápido con WatchGuard ThreatSync.

Seguridad inteligente, de forma sencilla.

Ventas: +34 911 410 918
Soporte: +34 918 295 204
Email: spain@watchguard.com
www.watchguard.com/es

GESTIÓN DE IDENTIDADES Y ACCESOS: CLAVE EN UN MUNDO HÍBRIDO

La gestión de identidades y accesos como elemento clave en un mundo híbrido, fue el tema central de un debate en el que participaron Bit2Me, Broseta Abogados, Capital Energy, Fluidra e Indra, y que contó con la colaboración de B-FY, Ikusi y WatchGuard.

SEGÚN GARTNER, EN 2020, EL 50% DE LOS FALLOS EN LA NUBE SE DEBIERON A UNA GESTIÓN INADECUADA DE LAS IDENTIDADES, EL ACCESO Y LOS PRIVILEGIOS. EN 2023, ESE PORCENTAJE AUMENTARÁ AL 75%. A DÍA DE HOY, ES MÁS FÁCIL SER VÍCTIMA DE UN ROBO DE IDENTIDAD O DE UN SECUESTRO DE DATOS QUE SERLO DE UN ROBO A MANO ARMADA O ALLANAMIENTO DE MORADA. PHISHING, SUPLANTACIÓN DE IDENTIDAD, RANSOMWARE...

SON MÚLTIPLES LOS ATAQUES CUYO OBJETIVO ES HACERSE CON LOS DATOS DE EMPRESAS Y USUARIOS PARA ACCEDER A LOS RECURSOS CORPORATIVOS. LA IDENTIDAD SE HA CONVERTIDO EN UN NUEVO OBJETIVO DE LOS CIBERATACANTES Y LAS EMPRESAS DEBEN PRESTAR TAMBIÉN ATENCIÓN A SU PROTECCIÓN.

“La gestión de identidades es una pieza fundamental en la estrategia de ciberseguridad de la empresa”
Washington Gómez, CISO de **Bit2Me**

“Querríamos una identidad digital europea para que con un único certificado podamos identificarnos globalmente, tanto interna como externamente”
Manuel Asenjo, Director IT de **Broseta Abogados**

Para hablar de gestión de identidades y accesos como elemento clave en un mundo híbrido, en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas https://bit.ly/ForoITDSOD, celebramos un debate en el que participaron Bit2Me, Broseta Abogados, Capital Energy, Fluidra e Indra, y que contó con la colaboración de B-FY, Ikusi y WatchGuard.

GESTIÓN DE IDENTIDADES: PIEDRA ANGULAR DE LA SEGURIDAD

El encargado de abrir el debate fue Washington Gómez, CISO de Bit2Me, que explicaba que “la gestión de identidades es una pieza fundamental en la estrategia de ciberseguridad de la empresa. Para nosotros es esencial la gestión de identidades internas y también la de nuestros clientes, para que quien acceda a nuestro servicio es quien dice serlo, para evitar fraudes y robo de identidades”.

Para Ángel Uruñuela, CISO de Fluidra, “es un elemento clave, tanto en el apartado de empleados, como para el e-commerce B2B y los clientes finales. A todo esto sumamos seis redes IoT. La identidad es clave, y en los últimos años casi todas las empresas han puesto en marcha un proyecto de este tipo, y creemos que va a seguir siendo fundamental en los próximos años”.

En el caso de Manuel Asenjo, Director IT de Broseta Abogados, “como despacho de abogados, tenemos información relevante de nuestros clientes y eso nos hace tener un nivel de acceso protegido con múltiple factor para evitar la pérdida de datos que, en nuestro caso, tendría un grave efecto reputacional”.

Añadía Jorge Crespo, Responsable de Operaciones Globales IT de Capital Energy, que “el reto es securizar tanto la parte IT como OT e IoT, y por eso tenemos que cubrir todas las necesidades de los negocios. Hasta ahora, la protección de la identidad era sencilla en IT, pero en los últimos años se ha vuelto mucho más compleja”.

Y finalizaba esta primera ronda de opiniones Elena García Díez, CISO de Indra, indicando que “la identidad es el nuevo perímetro. Por eso la seguridad debe empezar por la gestión de las identidades, porque no podemos aferrarnos a otros elementos que nos den garantía de la protección que estamos ofreciendo. Nuestros profesionales están en movimiento constante e interactuando con tecnología en diferentes plataformas, por lo que tenemos que fortalecer la identidad que necesita cada profesional, sabiendo que el negocio es lo primero y la disponibilidad es el principio de la seguridad”.

“El reto es securizar tanto la parte IT como OT e IoT, y con eso cubrir todas las necesidades del negocio”
Jorge Crespo, Responsable de Operaciones Globales IT de **Capital Energy**

“La ciberseguridad no ha cambiado tanto, pero la realidad ha hecho que las empresas pongan foco en ella”
Ángel Uruñuela, CISO de **Fluidra**

¿CÓMO HA CAMBIADO LA GESTIÓN DE IDENTIDADES?

En los últimos años la realidad del mundo IT ha cambiado mucho y, con ello también la gestión de las identidades. Continuaba Elena García indicando que “en nuestro caso, en los últimos años se ha producido una consolidación de un modelo que llevaba implementándose mucho más. Pero hemos visto un incremento de la velocidad del ciberdelincuente para aprovechar las identidades que consigue, lo que supone un punto de vulnerabilidad. En estos tres años se han sentado las bases de la necesidad de una protección multifactor y de utilizar los mecanismos más robustos”.

Para Jorge Crespo (Capital Energy), “nosotros hemos tenido la suerte de nacer directamente digitales, no tenemos nada on-premise. Ahora el reto es seguir las necesidades de negocio, poder dar una solución rápida y segura al negocio”.

En palabras de Manuel Asenjo (Broseta Abogados), “el perímetro ha volado. Ya no tienes un castillo que proteger, y hay que proteger cada uno de los puntos de acceso, cada uno de los usuarios. Hay que buscar los puntos en común, los dispositivos, y, en nuestro caso, te hacen falta dos para poder iniciar una sesión, y, si puedes añadir algún elemento más, propio del usuario, mejor”.

Apuntaba Ángel Uruñuela (Fluidra) que “la ciberseguridad no ha cambiado tanto, pero sí la transformación de las empresas, y, en nuestro caso, el 75% de nuestros sistemas han ido a la nube, además de la adopción del teletrabajo y el incremento del cibercrimen, que ha hecho que las empresas pongan foco en la seguridad. Hay muchos retos en la identidad, y uno de ellos es el multifactor, porque ahora no parece que ya sea suficiente y hay que seguir madurando en esta línea”.

Concluía Washington Gómez (Bit2Me) indicando que “el mayor desafío ha sido ir añadiendo capas de manera constante para incrementar la confianza en que la persona es quien dice ser. Hemos pasado de un usuario y una contraseña compleja a múltiples factores de autenticación y, en nuestro caso, evaluamos también el contexto del dispositivo y la conexión. Esto nos ha llevado a una gestión mucho más compleja que implica más tiempo y recursos. Y hay veces que cuando la seguridad es mayor, puede suponer una molestia para los usuarios. Es decir, hay que incrementar la seguridad de manera transparente para el usuario”.

MEJORAR LA GESTIÓN DE IDENTIDADES DE CARA A FUTURO

Según explica el CISO de Bit2Me, “a futuro la adopción de Web3, con tecnologías como

“La identidad es el nuevo perímetro”
Elena García Díez, CISO de **Indra**

Blockchain, nos va a permitir crear identidades seguras de forma fiable”, a lo que añadía el CISO de Fluidra que “tenemos programas ambiciosos para unificar la gestión de acceso a todas nuestras compañías, y esperamos poder completarlo en cuatro años, junto con otros de acceso privilegiado, así como todo el gobierno de la identidad. Por otra parte, estamos trabajando en temas de accesibilidad y deception, para tener esa alerta temprana en la gestión de la identidad. Empezamos a poner el foco en los dispositivos móviles, como en el resto de los end-points”.

Para el Director IT de Broseta Abogados, “tenemos dos peticiones internas. Primero, passwordless, trabajar sin contraseñas, y single sign on para todos nuestros activos digitales. A nivel externo, querríamos una identidad digital europea para que con un único certificado podamos identificarnos globalmente, tanto interno como externo”.

En palabras del Responsable de Operaciones Globales IT de Capital Energy, “hacemos mucho hincapié en reforzar la seguridad del usuario y sus dispositivos, porque las opciones son muy variadas. Internamente, es un reto facilitar la llegada de los usuarios al mundo OT, hacer esa transición de redes independientes a integradas de forma sencilla para el usuario, sin que eso afecte a la seguridad”.

Terminaba la onda de opiniones con la CISO de Indra, que apuntaba que “las estrategias y líneas de trabajo son similares, porque el enemigo es común. El riesgo es el mismo. El CISO tiene que tapar cientos de agujeros y al malo le basta con encontrar uno. La ventaja que tenemos es que sabemos hacia dónde vamos y tenemos clara la estrategia. Passwordless tiene que ser el futuro, igual que el trabajo en la formación y concienciación del empleado, porque cualquier estrategia fracasará si no somos capaces de integrar todos los elementos del ecosistema. Por último, estar cerca del negocio para poder dar una respuesta segura de disponibilidad permanente”.

“La entrada indeseada a nuestros sistemas viene por un problema en la gestión de la identidad, y ahí hay que poner el foco”
Miguel Abreu, CEO de **B-FY**

LA VISIÓN DE LA INDUSTRIA

A la vista de estos retos, señalaba Miguel Abreu, CEO de B-FY, que “la entrada indeseada a nuestros sistemas viene por un problema en la gestión de la identidad, y ahí hay que poner el foco. Nosotros ofrecemos una solución de identificación como servicio basada en biometría, lo que supone una solución real sin contraseña. Si atendemos a la definición de Identity-First Security de Gartner, deberíamos tener tres pilares en la gestión de identidades: coherencia, contexto y la continuidad. Nuestra solución es convergente en el uso del

móvil para acceder a activos físicos y on-line; hace un uso innovador del QR asociado al activo; y la continuidad, permitiéndonos preguntar todas las veces que haga falta sin que resulte engorroso para el usuario".

En palabras de Luis Enrique Laguna, Responsable de Ingeniería de Preventa de Ikusi, "un robo de identidad se produce a nivel mundial cada 80 segundos. Es vital tenerlo en cuenta. Nosotros vemos la ciberseguridad como un proyecto global y continuo. Las amenazas son crecientes y también continuas".

Por su parte, Ricardo de Ena, Area Sales Manager zona Norte de WatchGuard, explicaba que elementos como "single sign on o passwordless son fundamentales. Igual que no forzar de más a los usuarios. Por eso nosotros apostamos por políticas basadas en la ubicación del usuario. Evidentemente, las múltiples capas son necesarias y en nuestras soluciones se incluyen. Nosotros trabajamos con una pre-autenticación previa al multifactor de autenticación, y chequeamos el dispositivo, que está donde dice estar, que cuenta con permisos y todas las actualizaciones…".

LO QUE NOS DEPARA EL FUTURO

Indicaba Miguel Abreu (B-FY) que "nos enfrentamos a verdaderas organizaciones delictivas que seguirán aprovechándose de las empresas menos preparadas y obteniendo beneficios con ello. Los ataques aumentarán y su creatividad también, con lo que hay que estar preparados para ello".

Coincidía con él Luis Enrique Laguna (Ikusi), que afirmaba que "cuanta más protección tengamos, más posibilidades hay de estar seguros".

De un futuro sin contraseñas hablaba Ricardo de Ena (WatchGuard), pero "hasta llegar allí, los ciberdelincuentes seguirán muy activos y hay que poner las barreras necesarias". ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

"Vemos la ciberseguridad como un proyecto global y continuo"
Luis Enrique Laguna, Responsable de Ingeniería de Preventa de **Ikusi**

"Los ciberdelincuentes seguirán muy activos y hay que poner las barreras necesarias"
Ricardo de Ena, Area Sales Manager zona Norte de **WatchGuard**

NEGOCIO Y CIBERSEGURIDAD

HAGA QUE SU NEGOCIO ESTÉ CIBERTRANQUILO

En la era de la transformación digital y en un momento en el que la soberanía digital plantea interrogantes, **hacer que su negocio esté cibertranquilo es vital dado el impacto financiero de los ciberataques.**

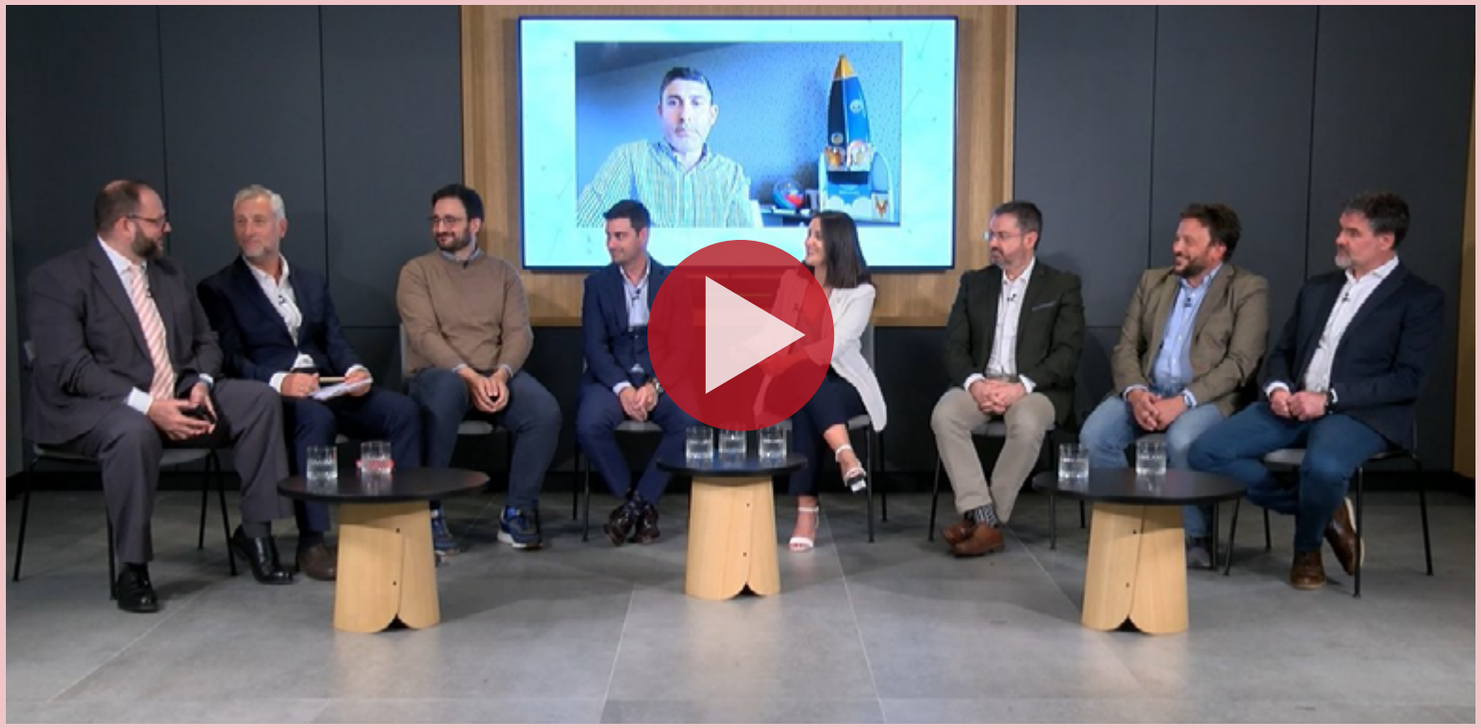
Para la protección de redes, datos, estaciones de trabajo y servidores: al elegir las soluciones Stormshield, recurre a un actor de la ciberseguridad en el que puede confiar.

STORMSHIELD

www.stormshield.com

CIBER-RESILIENCIA:

ASEGURAR LA CONTINUIDAD DEL NEGOCIO



Analizamos la ciber-resiliencia de las organizaciones, un factor clave para asegurar la continuidad del negocio, de la mano de Barracuda Networks, Bitdefender y V-Valley, con la participación de Clarke Modet, Editorial Edelvives, Enagás, Fintonic y Nationale Nederlanden.

A DÍA DE HOY CUALQUIER EMPRESA TIENE UNA GRAN DEPENDENCIA DE SU INFRAESTRUCTURA TECNOLÓGICA PARA DAR SOPORTE A LA MAYORÍA DE SUS ACTIVIDADES, LO QUE HA HECHO QUE EL CONCEPTO DE CIBER-RESILIENCIA HAYA ADQUIRIDO UNA IMPORTANCIA VITAL TANTO PARA GRANDES COMO PEQUEÑAS Y MEDIANAS CORPORACIONES. EN ESTE DEBATE TRATAMOS DE APORTAR UNA VISIÓN AMPLIADA Y HOLÍSTICA DEL CONCEPTO DE RESILIENCIA, QUE INCORPORE NUEVAS AMENAZAS EMERGENTES Y TRADICIONALES.

Para hablar de ciber-resiliencia, se celebró, con la colaboración de Barracuda Networks, Bitdefender y V-Valley, en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas, un debate en el que participaron responsables de seguridad de Clarke Modet, Editorial Edelvives, Enagás, Fintonic y Nationale Nederlanden.

“Es básico poder protegerte, pero, sobre todo, en caso de ataque, responder de manera rápida para poder mantener las operaciones”
Jesús Abascal Santamaría,
CISO de **Clarke Modet**

LA IMPORTANCIA DE LA CIBER-RESILIENCIA

Daba inicio al debate Jesús Abascal Santamaría, CISO de Clarke Modet, explicando que “la ciber-resiliencia es poder resistir cualquier tipo de ataque, de ahí la importancia para el negocio. Es básico poder protegerte, pero, sobre todo, en caso de ataque, responder de manera rápida para poder mantener las operaciones y el servicio a los clientes”.

Para Enrique Cervantes Mora, CISO de Fintonic, “la ciber-resiliencia es la capacidad que tiene la empresa para asegurar la continuidad de negocio ante cualquier contingencia, porque una interrupción de nuestro negocio afecta tanto a la actividad comercial como a la confianza que tienen en ti los clientes, y en el entorno financiero, parte de lo que vendemos es esa confianza”.

En la misma línea se posicionaba César Corachán, CIO y CDO de Enagás, que añadía que “la ciber-resiliencia está en nuestro ADN, porque Enagás es infraestructura crítica y tener la capacidad de mantener el negocio ante un ataque es algo integrado en nuestra compañía. Pero nosotros damos un paso más hacia cómo se gestiona esta ciber-resiliencia, concienciando a todos los elementos en esta línea, porque no todo es tecnología”.

En palabras de Daniel Damas Díaz, Head of IT Security, de Nationale-Nederlanden, “para nosotros la seguridad es esencial. La ciber-resiliencia es esencial porque volver al estado inicial tras una perturbación es el objetivo, y eso hay que prepararlo y practicarlo, y tener los mecanismos para resistir, mitigar y recuperarse”.

Finalizaba esta primera ronda de opiniones Miguel Martínez Ordóñez, CISO Editorial Edelvives, comentando que “ciber-resiliencia es la capacidad de mantener el negocio en funcionamiento. Para nosotros es muy importante mantener el servicio a profesores y alumno, además de la venta on-line. El problema reputacional sería desastroso”.

“Es muy importante simular para saber hasta dónde podemos llegar”
Miguel Martínez Ordóñez, CISO de **Editorial Edelvives**

HERRAMIENTAS PARA SER RESILIENTE

Continuaba Miguel Martínez indicando que para ser ciber-resiliente “intentamos utilizar la seguridad, porque, si no estás securizado, da lo mismo que tengas un plan de recuperación. Forma parte de nuestra protección una infraestructura de firewalls, end-points, SIEM... y todas las herramientas de protección, pero, además, concienciamos a los usuarios y tenemos establecidos controles y monitorizaciones. Además, tenemos planes de contingencia para poder recuperar todo en caso de caída”.

Daniel Damas (Nationale-Nederlanden) explicaba que “hay varios aspectos importantes. Empezamos por un análisis de riesgos e implementamos medidas de seguridad especiales donde hacen falta. La monitorización es muy importante para una detección temprana, lo

“Damos un paso más hacia cómo se gestiona la ciber-resiliencia concienciando a todos los usuarios, porque no todo es tecnología”
César Corachán, CIO y CDO de **Enagás**

“Elaboramos unos planes de recuperación que probamos para estar seguros de que todo es correcto en caso de que sea necesario”
Enrique Cervantes Mora, CISO de **Fintonic**

mismo que la concienciación de los usuarios, para que puedan ayudarnos a detectar riesgos. Por último, la gestión de vulnerabilidades es algo esencial en la organización”.

De una opinión similar era César Corachán (Enagás), que apuntaba que “nuestra estrategia pasa por tratar la ciberseguridad como algo integral. Intentamos dar respuesta proactiva a los problemas. Además, es muy importante medir para poder mejorar y se necesitan las inversiones necesarias. Esa visión nos ayuda a tener un plan de mejora continua. Pero quizá el eslabón más débil es el usuario, y es necesaria mucha concienciación para mitigar las amenazas antes de que ocurran”.

En el caso de Enrique Cervantes Mora (Fintonic), “al ser una empresa nativa cloud, tenemos unas serie de medidas de seguridad y tecnologías muy acordes, pero eso no sirve de nada si no has hecho una adecuada gestión del inventario, porque no puedes proteger algo que no sabes que tienes, ni puedes recuperarlo en caso de problemas. A partir de ahí, pasando por la capacitación de los empleados, elaboramos unos planes de recuperación que probamos para estar seguros de que todo es correcto en caso de que sea necesario. La innovación y la tecnologías son esenciales, pero hay aspectos que tienen que ver con los procesos que son la base para todo lo demás”.

Concluía Jesús Abascal (Clarke Modet) señalando que “hay que hacer valoración de riesgo y tener claro cuáles con tus activos críticos a la hora de dar continuidad de negocio. Además, hay que hacer análisis de recuperación y mejoras para poder ver tus debilidades. Quizá el 90% de los ataques de ransomware se pueden evitar con doble factor de autenticación. También están creciendo los Zero Days, sobre todo en la cadena de suministro. A partir de estas amenazas puedes conocer los riesgos, pero es esencial tener tus activos replicados para, en caso de problema, poder apagar lo viejo y conectar lo nuevo. Hace un par de años sufrimos un ataque de ransomware y pudimos recuperar el 90% del servicio, y, a partir de ahí, todo son mejoras aprendidas y mejoras”.

En palabras de Daniel Damas (Nationale-Nederlanden), “es esencial que la ciber-resiliencia entre en la cultura de la empresa. Para testear el sistema pusimos en marcha un ataque simulado de ransomware y las reacciones fueron inesperadas. Lo hicimos un viernes, en período de cierre mensual, y ahora los usuarios ya son conscientes de que si algo así ocurre, es un grave problema. Estos ejercicios valen la pena para involucrar a las personas, porque no puede ser solo un tema de seguridad”.

En su caso, recordaba Jesús Abascal, “la única ventaja es que la experiencia nos permitió crecer en seguridad de forma muy importante”.

“Es esencial que la ciber-resiliencia entre en la cultura de la empresa”
Daniel Damas Díaz, Head of IT Security de **Nationale-Nederlanden**

EL ELEMENTO ESENCIAL EN LA CIBER-RESILIENCIA...

Señalaba el CISO de Fintonic que “en nuestro caso, lo más importante son los datos de los clientes, que es el core de nuestro negocio, y, como tal, lo protegemos, y nuestros planes de recuperación pasa por ahí. Después, todo lo demás, pero los datos de los clientes son esenciales”.

Para el CIO y CDO de Enagás, “el mapa tiene que ser integral. Hasta no hace mucho, la seguridad era algo solo de tecnología, pero ahora es algo de compañía. Son esenciales la visibilidad, la concienciación y el entrenamiento de todos los elementos de la empresa, así como los métodos de respuesta. Lo más importante en seguridad es no improvisar”.

En palabras del CISO de Clarke Modet, “cuando toca negocio las compañías se dan cuenta de que la seguridad es una inversión, no un gasto”.

En opinión del CISO Editorial Edelvives, “intentamos involucrar a toda la empresa. Hacemos simulaciones y campañas para concienciar a los empleados. Es muy importante simular para saber hasta dónde podemos llegar.

...Y LO MÁS COMPLICADO DE HACER

Por otra parte, continúa, “lo más complicado fue involucrar a la dirección. Sin la dirección no puedes hacer nada, pero nos dedicamos a vender libros, y no somos una empresa de tecnología. Con datos e información hemos conseguido implementar las herramientas necesarias, pero nos queda mucho camino por recorrer, porque esto no es algo estático, sino dinámico. Por otra parte, es complejo recopilar toda la información necesaria para responder a la pregunta de qué pasaría si... Hay que determinar los activos críticos y tener todo localizado para poder recuperar en caso de desastre”.

Añadía el Head of IT Security de Nationale-Nederlanden, que “todos los años aprendemos lecciones por el propio dinamismo del negocio y la evolución de los riesgos. Por tanto, con más práctica más preparados vamos a estar”.

“Hay que planear, estructurar y tratar de evitar que las amenazas entren en el sistema”
Miguel López,
Director General de **Barracuda** Networks

Por su parte, César Corachán (Enagás), comentaba que “para bien o para mal, la tecnología está en continua evolución. Si tienes la capacidad de tener un sistema integral, esto es algo más que hay que integrar”.

Para Enrique Cervantes, “lo más importante es seguir el ritmo de la evolución del negocio con los planes de recuperación y protección. Tienes que adaptarte al negocio y a los clientes”.

Finalizaba Jesús Abascal (Clarke Modet) apuntando que “hay que superar la resistencia al cambio de los usuarios, porque, al ritmo que vamos, el cambio es constante y la ciberseguridad tiene que adaptarse. Sin olvidar los presupuestos, que es algo esencial”.

LA VISIÓN DE LA INDUSTRIA

Ante estos retos, Miguel López, Director General de Barracuda Networks, indicaba que "tenemos que orientarnos a estas necesidades. Hay que planear, estructurar, planificar y tratar de evitar que las amenazas entren en el sistema. Pero el error de partida es que a veces se piensa que eso es suficiente, pero, sin embargo, hay que ir más allá. Hay que planear qué puede suceder si entran en el sistema. Hay que tener medidas y herramientas como la IA para poder analizar y responder ante incidentes. Pero, además, hay que concienciar a los usuarios. No sirven de nada lo planes y las herramientas si los usuarios no están preparados.

Para David Gasca, Sales & Marketing Manager Cybersecurity de V-Valley, "nosotros podemos mostrarles las herramientas que necesitan, y creo que es esencial tener la capacidad para poder levantarte en caso de incidente. La ciber-resiliencia, en mi opinión, es la capacidad de poder estar preparado en caso de problemas. Hay que ser capaces de entrenar la capacidad de respuesta para que luego no sea una improvisación. Hay que conseguir que las empresas sean conscientes de la necesidad para poder dar ese paso. Por eso trabajamos con herramientas de deception para poder probar la capacidad de respuesta de una organización, y con otras para incrementar la visibilidad del CISO.

Concluía Sergio Bravo Gordillo, Iberia Sales Director de Bitdefender, añadiendo que "es importante saber las necesidades de las empresas para poder responder a ellas. Tratamos de aportar las herramientas para ayudarlas. Las nuevas amenazas se escapan de la seguridad tradicional, y hay que estar preparados para responder. Asimismo, es esencial tener una capa de detección y prevención, y ahí es clave la visibilidad de la organización. A esto hay que añadir la capa de respuesta al incidente, con capacidad para poder hacer un análisis forense para ver lo que ha ocurrido y poder parchearlos. Sin olvidar los protocolos de seguridad y su extensión a los usuarios. ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

"Es importante saber las necesidades de las empresas para poder responder a ellas"
Sergio Bravo Gordillo,
Iberia Sales Director de **Bitdefender**

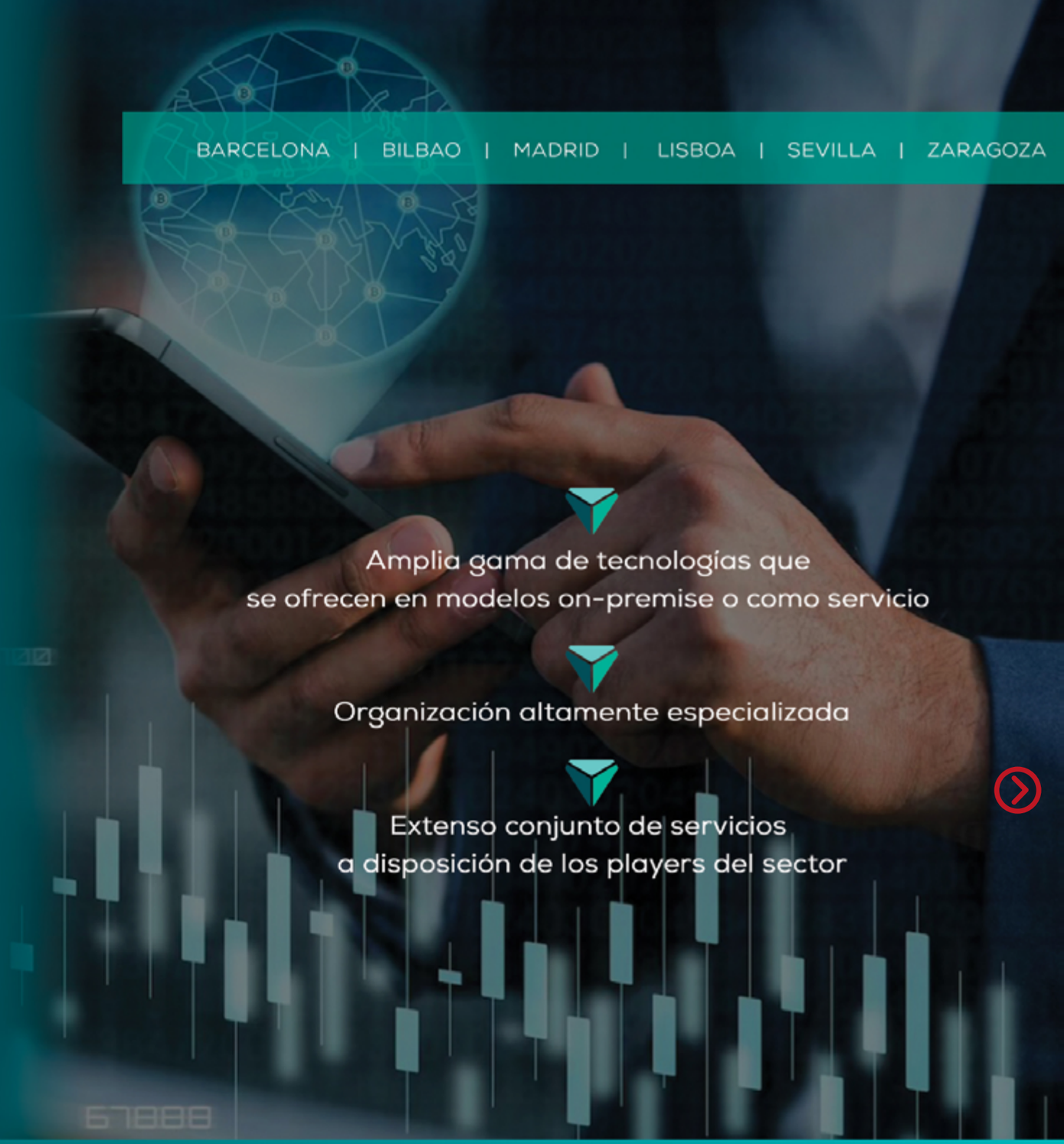
"Hay que ser capaces de entrenar la capacidad de respuesta para que luego no sea una improvisación"
David Gasca, Sales & Marketing Manager
Cybersecurity de **V-Valley**

V-Valley
enhancing your business

ESPECIALISTAS EN ADVANCED SOLUTIONS

Mayor rentabilidad y valor en tus proyectos de Ciberseguridad Corporativa

Acompañamos a los clientes a potenciar, aún más, sus proyectos de transformación digital dirigidos a clientes finales y Administraciones Públicas.



Network | Cloud | Workplace | Aplicación | Dato | Gestión

A10 · BACKBOX · VU · BROADCOM · CHECK POINT · CLOUDFLARE · CounterCraft · CyberRes · ENTRUST
ravenloop · kaspersky · McAfee · SONICWALL · MICRO FOCUS · Trellix · Skyhigh Security · TREND MICRO · WatchGuard

www.v-valley.es

seguridad@v-valley.com

JUAN MIGUEL PULPILLO, DPO DEL CENTRO DE CIBERSEGURIDAD INDUSTRIAL

"CUALQUIER VIOLACIÓN EN EL ÁMBITO IT U OT PODRÍA PROVOCAR INTERRUPCIONES DE SERVICIO E IMPACTAR EN LA INTEGRIDAD DE LA INFORMACIÓN"

Con el incremento de la digitalización de las organizaciones, especialmente las del sector industrial, se ha incrementado la superficie de exposición, y es más necesario que nunca contar con una estrategia de ciberseguridad OT e IT bien definida e integrada para poder soportar las operaciones y el negocio con el nivel de protección necesario.

La integración de la ciberseguridad de las operaciones (OT) y de la información (IT) es cada día más necesaria y de ello nos habló en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas Juan Miguel Pulpillo, DPO del Centro de Ciberseguridad Industrial, que nos explicaba que, "tenemos que partir de la premisa de que cualquier violación en el ámbito IT o OT podría provocar interrupciones de servicio e impactar en la integridad de la información".

Juan Miguel Pulpillo nos mostraba los elementos principales para contar con una adecuada estrategia que integre la ciberseguridad OT e IT.

DESAFÍOS EN LOS PROYECTOS DE DIGITALIZACIÓN

Explicaba este responsable que los desafíos a superar en los proyectos de digitalización pasan por "la propia digitalización de los procesos productivos, de la información, los productos y los servicios; la integración de IT y OT; la analítica de datos; el gobierno de la digitalización; y el ecosistema de la cadena de suministro".

Partiendo de la necesidad de seguridad y resiliencia de los entornos empresariales, en general, e industriales, en particular, los responsables, desde la perspectiva que nos ofrecía, Juan Miguel Pulpillo, deben atender una serie de desafíos en función de las tecnologías de digitalización. El primero sería "alrededor de IIoT, con dispositivos que nos proporcionan información de manera automatizada. Es muy difícil implementar a nivel de dispositivo medidas de seguridad adecuadas y, hoy por hoy, es uno de los puntos más débiles del ecosistema. Otro desafío es el que supone Big Data/Analytics y la inteligencia artificial, y todo el conocimiento y los datos que se están volcando sobre ella, así como la cloud o la información residual que puede quedar en los robots. En todo caso, las tecnologías habilitadoras de la digitalización industrial o empresarial debemos entenderlas en conjunto, porque no son independientes o únicas. Asimismo, no podemos olvidar la realidad aumentada, virtual y mixta, las tecnologías de la simulación, Blockchain, las comunicaciones…".

"ES MUY DIFÍCIL IMPLEMENTAR A NIVEL DE DISPOSITIVO MEDIDAS DE SEGURIDAD ADECUADAS Y, HOY POR HOY, ES UNO DE LOS PUNTOS MÁS DÉBILES DEL ECOSISTEMA"

RIESGOS DE LOS PROYECTOS INDUSTRIALES

En este tipo de proyectos, existen una serie de riesgos comunes que hay que resolver, como pueden ser: "la pérdida de visión y control del proceso o la información; la infección por malware; la explotación de vulnerabilidades, el robo de datos, identidades o propiedad intelectual; los errores humanos; o los fallos inherentes a la cadena de suministro".

ESTRATEGIA DE CIBERSEGURIDAD

Según nos explicaba el DPO del Centro de Ciberseguridad Industrial, "es imprescindible definir una línea base sobre la que desarrollar la estrategia de ciberseguridad, tanto a nivel de la entidad como de la cadena de suministro, que incluya identificar, clasificar y priorizar el valor de activos y procesos; un modelo de amenazas; un análisis de riesgo a todos los niveles y para todos los activos; segregación física de las redes; controles de acceso; gestión de identidades; protección adaptada a las necesidades de cada puesto; formación y concienciación; una adecuada configuración; aplicación de diodos de datos con cortafuegos para que no se comuniquen entre ellos; supervisión del tráfico; planes de prueba; medición de protección física; y mecanismos de respuesta ante incidentes estableciendo planes de recuperación y comunicación". ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

Implemente un Acceso Zero Trust a cualquier recurso.

Descubra una alternativa más segura y rápida a las VPNs.

barracuda.com

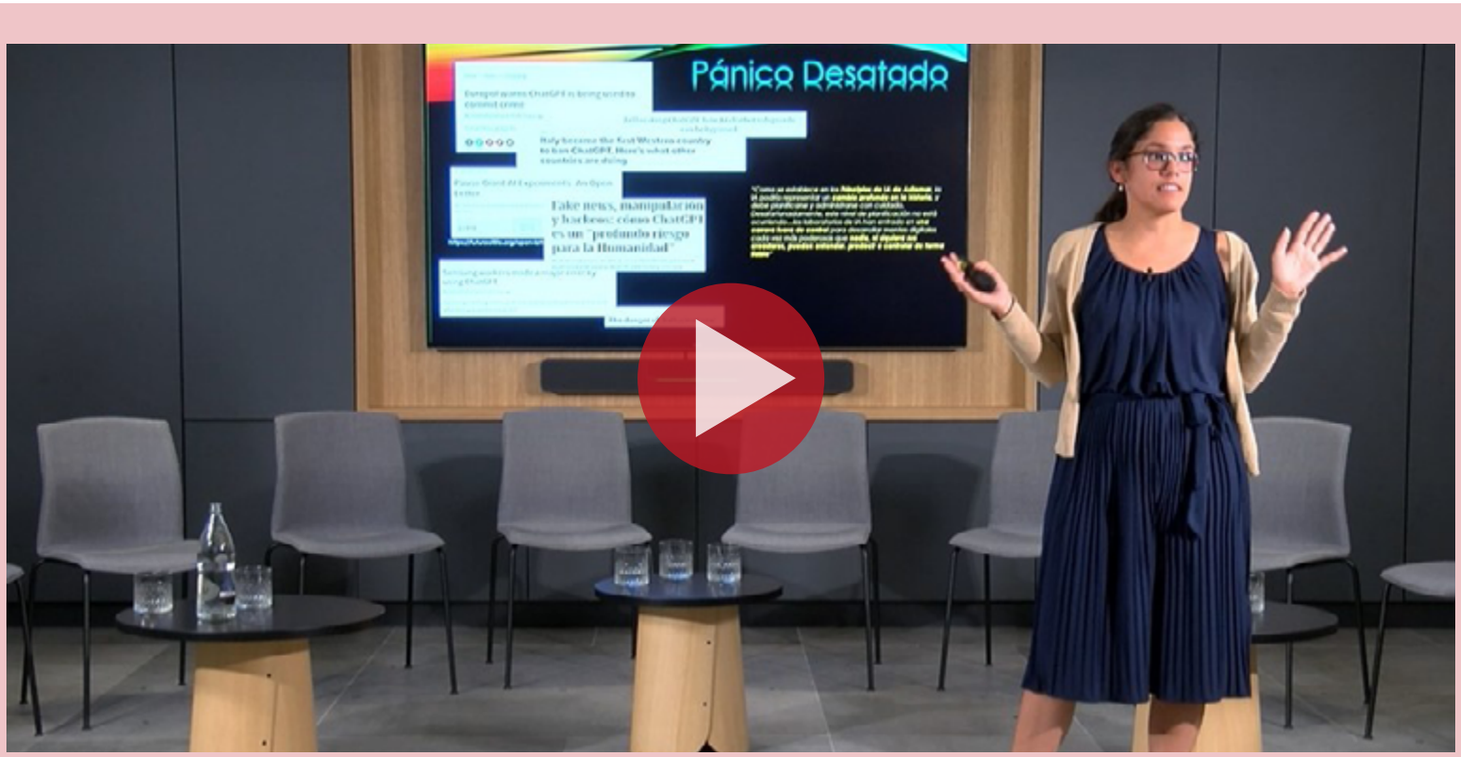
Barracuda®
Your journey, secured.

GLENDA SUÁREZ, DIRECTOR IT QUALITY, RISK & COMPLIANCE (QRC) & SECURITY DE PITCHER AG, Y MIEMBRO DEL GRUPO DE TRABAJO DE TENDENCIAS EMERGENTES DE ISACA

"CON LA IA NECESITAMOS UN MARCO DE ACTUACIÓN Y APOYAR AL NEGOCIO EN SU DESARROLLO"

La inteligencia artificial es una de las grandes protagonistas de la actualidad tecnológica, y su rol en el mundo de la ciberseguridad es cada día más demandado por las empresas. Pero, dadas las diferentes iniciativas para ralentizar su desarrollo ante las dudas que se han generado, ¿qué podemos esperar realmente? ¿Cómo podemos obtener valor de ella para la protección del negocio?

Para arrojar luz sobre este tema, en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas contamos con la intervención de Glenda Suárez, director IT Quality, Risk & Compliance (QRC) & Security de Pitcher AG, y miembro del Grupo de Trabajo de Tendencias Emergentes de ISACA, que apuntaba que los profesionales de la seguridad "nos estamos



La aplicación de la inteligencia artificial en la protección de datos, fue el tema central de la ponencia de Glenda Suárez (ISACA).

preguntando cómo podemos aportar valor en un momento como el actual".

IA Y ¿CIBERSEGURIDAD O CIBERDELINCUENCIA?

En esta aportación de valor, la inteligencia artificial es esencial porque nos permite "crear nuestras propias aplicaciones, nuestro propio negocio desde el inicio. No necesitamos conocimiento previo. Tenemos una herramienta que nos da respuesta a todo, básicamente", pero, al mismo tiempo se ha creado un pánico colectivo que ha llevado a las instituciones y a las empresas a valorar que hay que tener cuidado con ella.

"ChatGPT ha reducido la barrera de entrada a los cibercriminales. Ahora hay más cibercriminales con mejor acceso a información y pueden llegar a crear mejores tipos de crímenes", explicaba Glenda Suárez que, por otra parte, recordaba que "se han creado nuevas barreras y restricciones2, si bien, por desgracia, ya hay muchos ejemplos de que han sido superadas.

Otro riesgo es la proliferación de las denominadas fake news, y el escaso control de la información, porque, como explicaba Glenda Suárez, "al usar ChatGPT y subir información tanto personal como información confidencial del negocio, estamos más expuestos", y por eso hay países, como Italia, que han decidido dar un paso al lado y analizar la situación antes de seguir adelante con el desarrollo de la IA.

UN DESARROLLO IMPARABLE

El desarrollo de la IA parece imparable, y "hablamos de miles de herramientas y agentes que se han creado a partir de ChatGPT. Facilita que las empresas puedan crear sus propias herramientas, sus propias aplicaciones, porque queremos ofrecer un producto mejor a nuestros clientes".

La clave no está en las herramientas, sino en el uso que se hace de ellas, y, apuntaba Glenda Suárez, "vamos rezagados en las tareas de cumplimiento con RGPD, además de que hay una falta de personal muy grande en el mercado. Mucho personal en funciones de privacidad no tiene conocimiento técnico y no se atreve a desafiar al equipo ejecutivo o a los dueños de producto".

La solución no puede ser tratar de frenar la innovación. Para Glenda Suárez, "estamos donde estamos hoy gracias a la innovación. Y esta innovación ha venido para quedarse. No podemos dar marcha atrás. Inteligencia artificial se va a quedar y va a cambiar la forma en que hacemos las cosas, la forma en que vivimos, cómo nos comunicamos, cómo producimos, o cómo trabajamos... Es necesario entender la IA y saber qué quiere nuestra empresa. Tenemos que trabajar con los ingenieros, los desarrolladores, los responsables de producto, con TI... para ver cómo encaja en nuestro negocio y conocer los requisitos de uso y los riesgos".

"ES NECESARIO ENTENDER LA IA Y SABER QUÉ QUIERE NUESTRA EMPRESA. VER CÓMO ENCAJA EN NUESTRO NEGOCIO Y CONOCER LOS REQUISITOS DE USO Y LOS RIESGOS"

"Lo importante" finalizaba, "es tener un marco de evaluación y apoyar al negocio, no bloquearlo. Porque al final la digitalización es inmensa y no podemos ir contra la corriente. Tenemos que adaptarnos y colaborar". ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

Bitdefender®

Generando confianza mediante la investigación y el desarrollo

Trusted. Always.

bitdefender.es

RUBÉN FRIEIRO, SOCIO DE RISK ADVISORY-CYBER DE DELOITTE

“LA CIBERSEGURIDAD ES UN RETO PARA LA ESTRATEGIA DEL NEGOCIO”

La ciberseguridad es un elemento esencial para el negocio, y, como tal, presenta una serie de retos y oportunidades que es necesario afrontar de la manera adecuada.

Para verlos con más detalle, Rubén Frieiro, Socio de Risk Advisory-Cyber de Deloitte, intervino IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas, y aseguró que hay que entender la ciberseguridad como un reto para la estrategia de negocio, más que como una estrategia en sí misma dentro de las labores que los CISO de las compañías hacen y realizan todos los días”.

Recientemente, Deloitte ha preguntado a los CISO por sus preocupaciones para este año, incluyendo entre estas cuestiones dos de las que nos habló Rubén Frieiro, si disponen o no de una estrategia de ciberseguridad y si esta está alineada con el negocio de la compañía, y a ambas preguntas respondieron de forma afirmativa.

Sobre la ciberseguridad como reto de la estrategia de negocio habló en la IV edición del Foro IT Digital Security Rubén Frieiro (Deloitte).

"Aunque más del 85% de las empresas dicen tener una estrategia de seguridad", indicaba, "lo que nos encontramos es que esa estrategia de seguridad está muy condicionada por algunos factores. El primero de ellos es que en más del 50% de las organizaciones españolas el CISO sigue siendo parte de la estructura de tecnología de las organizaciones. Las prioridades que se establecen atienden más a cuestiones puras de los servicios tecnológicos y de la protección de estos que a cuestiones relacionadas con el negocio en sí mismo. También vemos que los CISO, a día de hoy, dedican la mayor parte de su tiempo a actividades relacionadas con el gobierno de la ciberseguridad. Frente a otros años se ha incrementado el número de CISO que dependen del CEO, pero todavía el porcentaje es pequeño, lo que limita su capacidad para influir en el negocio. El tercer factor es en qué medida los CISO participan en los proyectos de transformación de la compañía, entendiendo estos como aquellas capacidades que las compañías tienen que poner en marcha para implantar su estrategia de negocio".

EL ROL DEL CISO DEBE EVOLUCIONAR

Para Rubén Frieiro, "el rol del CISO tiene que mudar a favorecer recursos que posibiliten adoptar con seguridad estos proyectos de transformación", y desde Deloitte han establecido una clasificación para determinar el nivel de madurez de las organizaciones en función de tres cuestiones, "la capacidad que tienen las organizaciones para tomar decisiones basadas en las amenazas que operan en su entorno, si hacen una gestión eficaz de la ciberseguridad, y la influencia real tiene el CISO en la agenda del comité de dirección".

En base a esta clasificación, "casi un 40% de las compañías tienen un nivel de madurez bajo porque hacen una o ninguna de estas actividades, un nivel de madurez medio otro 40% y un nivel de madurez alto un 20%. En las organizaciones maduras casi se dobla la percepción que tienen de la importancia de seguridad para cometer estos proyectos, con lo cual una compañía que ha desarrollado una función de ciberseguridad madura basada en la capacidad de planificación, en la gestión eficaz y en la capacidad de influencia en el comité de dirección, va a tener unos directivos, desde el punto de vista de negocio, que van a entender el valor que la ciberseguridad aporta en sus proyectos de transformación y, por lo tanto, los recursos a los que va a poder acceder el CISO de la organización van a ir más allá de los de gestionar. Por tanto, la ciberseguridad más que una estrategia en sí misma, al final, es un reto para la estrategia de negocio".

CONCLUSIONES

Este responsable extrae una serie de conclusiones de esta visión, "la estrategia de ciberseguridad si verdaderamente está alineada con el negocio, tiene que aportar valor a ese negocio y, evidentemente, ayudar a cumplir los objetivos; las organizaciones, desde el punto de vista de la ciberseguridad, tienen que impulsar su desarrollo externo, estar abiertas a captar talento que puedan necesitar para cubrir aquellas áreas a las que no llegan y pensar en alianzas que permitan reducir el tiempo de respuesta entre este tipo de proyectos; y, tercero, tenemos que tomar decisiones organizativas respecto a dónde ubicar la posición del CISO dentro de la organización". ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas

Ikusi, servicios gestionados de ciberseguridad para proteger a las empresas.

IKUSI velatia

cisco Partner

Trabajamos en la continuidad de tu negocio, para que tú te encargues de conquistar el mercado.

SARA GARCÍA BÉCARES, RESPONSABLE DE RETECH CIBERSEGURIDAD EN INCIBE

"SIN INVESTIGACIÓN NO HAY CIBERSEGURIDAD, Y SIN ESTA NO HAY TRANSFORMACIÓN DIGITAL"

La iniciativa RETECH, Redes Territoriales de Especialización Tecnológica, articula diversos proyectos regionales orientados a la transformación y especialización digital, asegurando la coordinación, la colaboración y la complementariedad.

RETECH se enmarca en la Agenda España Digital 2026 y constituye una Política Pública de Inversión Territorial en materia de digitalización, que cuenta con las comunidades autónomas para impulsar proyectos de carácter transregional orientados a la especialización y con claros efectos multiplicadores en los impactos esperados. Para conocer con más detalle esta iniciativa, participó en la IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas Sara García Bécares, Responsable de RETECH Ciberseguridad para INCIBE.

Según explican desde el propio organismo, "las Redes Territoriales de Especialización Tec-

La ciberseguridad es esencial en la transformación digital y, por ello, Sara García (INCIBE) mostró todos los detalles de la iniciativa RETECH Ciberseguridad.

nológica son una herramienta para que la transformación digital sea una realidad en todo el territorio, impulsando todas las potencialidades de cada región y su objetivo es la puesta en marcha de proyectos territoriales de transformación digital impulsados de manera conjunta. Para esta iniciativa, el Gobierno movilizará más de 500 millones de euros del Plan de Recuperación y fomentará el liderazgo y la cooperación regional en el impulso de proyectos tractores de alto impacto territorial y económico".

UNA APUESTA POR LA CIBERSEGURIDAD

RETECH nace de la co-gobernanza y "da respuesta a las propuestas de proyecto realizadas por las comunidades autónomas en los últimos meses, para impulsar nueve líneas de actuación: inteligencia artificial y otras tecnologías digitales habilitadoras aplicadas a las industrias; gemelos digitales; salud digital; tecnología de la moda; tecnología verde; ciberseguridad; redes de emprendimiento digital; tecnología con impacto social; y tecnología rural".

RETECH Ciberseguridad "será un modelo de colaboración entre INCIBE y las comunidades autónomas para el desarrollo de la ciberseguridad en sectores productivos estratégicos relevantes. Se trata de una iniciativa estratégica de país para el desarrollo del ecosistema de ciberseguridad, capacidades, industria, I+D+i, y talento, que, con la coordinación de INCIBE, aglutinará a 15 comunidades autónomas con un presupuesto inicial de 149 millones de euros. RETECH se articula a través de tres nodos, liderados por Cataluña, Navarra y Castilla y León, consolidando el liderazgo de España en el sector de la ciberseguridad".

I+D+I ALREDEDOR DE LA CIBERSEGURIDAD

Esta iniciativa y su estructura "formará parte de la Comunidad Nacional Española en torno al Centro Europeo de Competencia en Ciberseguridad, donde INCIBE actúa como Centro de Coordinación Nacional, NFCES. En todo este contexto, las universidades y el mundo de la investigación, entre otras, deberán jugar un papel destacado. El reforzamiento de la investigación y el desarrollo en ciberseguridad, es imprescindible para hacer frente a las crecientes ciberamenazas, porque sin I+D+i no hay ciberseguridad, y sin esta hay transformación digital".

En palabras de su responsable, "la iniciativa RETECH abre una oportunidad para el impulso de redes territoriales de especialización tecnológica de la mano de las comunidades autónomas, el gran impulso del ecosistema de la ciberseguridad en España.

Cada uno de los nodos mencionados "pone el foco en uno o varios sectores económicos, potenciando el que cada una de las comunidades autónomas pueda poner en valor, como puede ser el caso de la ciberseguridad aplicada al Turismo desde Baleares".

SITUACIÓN ACTUAL

Tal y como explicaba Sara García, "RETECH se presentó el pasado mes de marzo con la firma de este acuerdo de entendimiento entre 15 comunidades que va a dar forma a esta primera fase. En una segunda fase, se trabajará para que el resto de comunidades y ciudades autónomas que todavía no han participado se puedan unir a esta iniciativa". ■

CONTENIDO RELACIONADO

IV edición del Foro IT Digital Security: Estrategias de ciberseguridad inteligentes: hoja de ruta y mejores prácticas




ESTRATEGIAS DE CIBERSEGURIDAD INTELIGENTES:

hoja de ruta y mejores prácticas

¡Ver todos los contenidos!

FORO it Digital Security

PATROCINADOR PLATINO

making science

PATROCINADORES GOLD

BFY · Barracuda. Your journey, secured. · Bitdefender · IKUSI velatia · cisco Partner · WatchGuard · SONICWALL · STORMSHIELD · V-Valley enhancing your business · WATCHGUARD FOR SOC

CON EL APOYO INSTITUCIONAL DE

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD