CRÓNICA

X Encuentro de Cloud Security Alliance España

"Tuvimos que lidiar con la masificación de servicios en la Nube"

21 de octubre de 2020, Madrid. ISMS Forum, junto al Capítulo Español de Cloud Security Alliance, celebró el X Encuentro de Cloud Security Alliance España el pasado jueves 15 de octubre de 2020 donde más de 250 profesionales del sector, así como máximos expertos, representantes institucionales y empresas, se dieron cita en este evento online que se ha consolidado como uno de los congresos nacionales más importantes en materia Cloud.

Luis Buezo, presidente del Capítulo Español de Cloud Security Alliance y Miembro de la Junta Directiva de ISMS Forum fue el encargado de inaugurar el acto junto con **Mariano J. Benito**, CISO en GMV y Coordinador del Comité Técnico Operativo del Capítulo Español de Cloud Security Alliance. "Bienvenidos a esta décima edición de Cloud Security Alliance España, ya han pasado 10 años desde que empezamos este evento de carácter anual. Cuando comenzamos con la planificación de este año, nos planteábamos hacer algo especial conmemorando el aniversario, planeábamos invitar a distintos expertos que han pasado por el encuentro y hacerlo presencial, sin embargo, la situación no es la propicia. Aun así, quiero destacar y agradecer el esfuerzo de todos los miembros del Capítulo y de ISMS Forum para poner en marcha esta jornada, que contará con grandes expertos", comentó Luis Buezo al inicio de la jornada.

Jordi André i Vallverdú, CISO en CaixaBank, y **Alejandro Figueroa**, CISO en BBVA España, dieron comienzo al evento a través de una entrevista moderada por **Gianluca D'Antonio**, Academic Director, IE Master of Cybersecurity; Partner, Deloitte; y Chairman en ISMS Forum.

La entrevista perseguía el objetivo conocer la apuesta de Cloud Adoption & Security de las principales bancas españolas, el mantenimiento de su infraestructura *on premise* y sus preferencias en cuanto a modelo de Nube privada, pública o híbrida, y del modelo Security as a Service. "La pandemia ha significado una adopción clara y rápida de tecnologías Cloud, de un día para otro pasamos de cero smartphones con Teams en CaixaBank, a toda la plantilla. También contábamos con una VPN que no estaba dimensionada para absorber a toda la plantilla trabajando" comentaba Jordi André al comienzo de la entrevista. Por su lado, Alejandro Figueroa añadió "para nosotros la pandemia ha marcado una aceleración de todos los planes que teníamos sobre la mesa, es cierto que contábamos con todas las herramientas colaborativas (correo, agenda, etc.) trabajando en entornos Cloud, ya que en BBVA llevamos desde 2012 trabajando en la transformación digital, pero tuvimos que lidiar con la masificación de estos servicios en la Nube".

A la pregunta sobre los retos en seguridad que ha supuesto la aceleración del entorno Cloud Alejandro Figueroa contestó, "nuestro reto se basa en cómo podemos asegurar la adecuada utilización y tratamiento de la información, desde el punto de vista de la encriptación de la información, tanto en la transmisión como en el almacenamiento y en el consumo, así como la securización de los procesos que están detrás de estas operaciones, y desde el punto de vista

del proveedor, atendiendo a la geolocalización de los datos, dónde están ubicados los servidores del proveedor o la casa matriz del mismo, ya que en función de estas variables se establece una base regulatoria".

"Por nuestra parte, el mayor reto ha residido en transformar nuestra forma de ejecutar la seguridad. Venimos de una cultura de mucho control en todos los procesos y Cloud ofrece una flexibilidad que habilita mucho el negocio, pero que pone una gran presión en la forma tradicional de ejecutar el control", añadió Jordi André.

En cuanto a la estrategia de comunicación y concienciación que ambas entidades están adoptando los entrevistados apelaron a la formación de sus trabajadores y la creación de Guías de Buenas Prácticas con la intención de extender las capacidades de ciberseguridad a todos los proyectos.

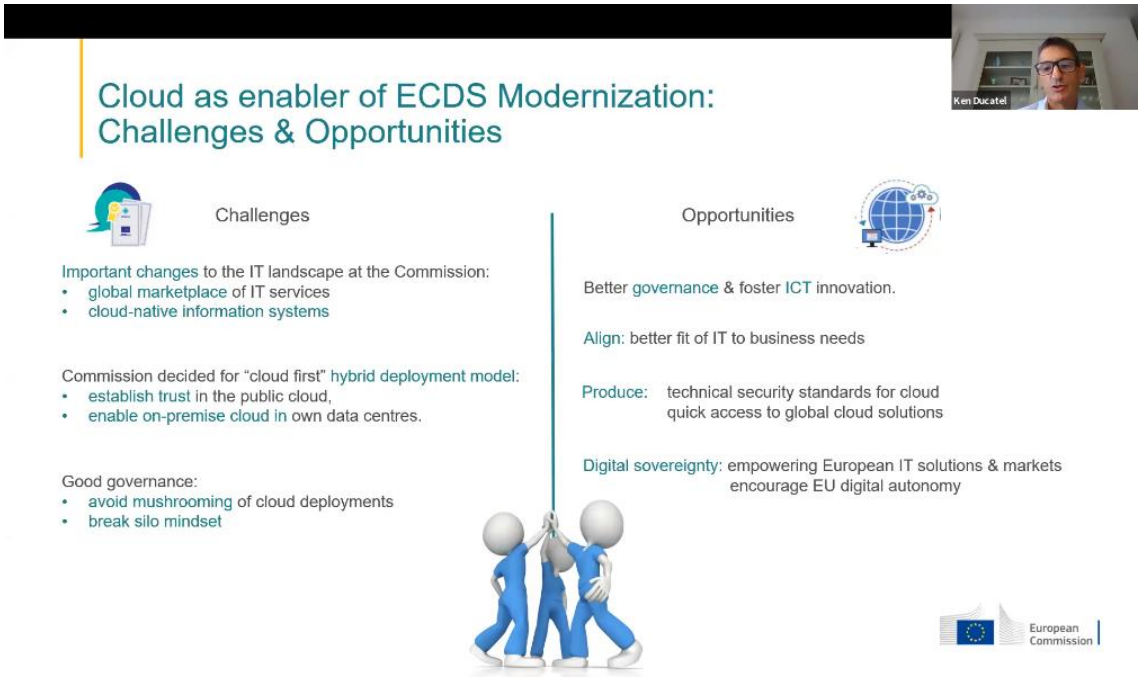
Por otro lado, se hizo mención al incremento del Shadow Cloud. "Una de las grandes premisas que planteamos en nuestros planes de seguridad es contar con una mayor claridad entre el Shadow IT y el Shadow Cloud, a través de la creación de proyectos que nos permitan trabajar con las unidades de negocio y soporte para que entiendan con qué estamos trabajando y cuáles son los riesgos que están detrás del uso de este tipo de modalidades en cuanto a lo que son las tecnologías hoy disponibles. A partir de ese entendimiento, nuestro objetivo es hacer un inventario y clasificación del estado IT y Cloud con el que contamos, y clasificarlo posteriormente para realizar un análisis de riesgos", comentó Alejandro Figueroa.

"En nuestro caso la adopción de tecnologías Cloud ha sido más tardía que en BBVA, y por tanto la aproximación ha sido diferente. Hemos establecido medidas tanto organizativas como técnicas para poder limitar el riesgo que confiere la adopción de Cloud. A nivel organizativo hay que destacar la implantación de un gobierno de externalización centrado en compras, en el cual participan áreas jurídicas o de seguridad de la información, entre otras, y lo que trata es de evaluar los riesgos que supone cada iniciativa, de manera que al estar centrado en compras, no puede salir ninguna iniciativa sin pasar por un análisis previo de ciberseguridad donde además se aplican los controles necesarios para mitigar el riesgo", declaró Jordi André.

Ken Ducatel, Director at Directorate for IT Security, DG DIGIT, European Commission, participó en este encuentro con una ponencia bajo el título de "Digital Transformation and Cloud Security at the European Commission".

"Los grandes retos de la Comisión Europea en el entorno Cloud podemos dividirlos en tres áreas que abarcan: cambios en el escenario de las IT, la apuesta por la implantación y desarrollo de un modelo híbrido de Nube, y una buena gobernanza y aplicación" comentó el ponente.

"Es necesario diseñar un nuevo camino que incluya la redistribución de competencias y poder contar con equipos multifuncionales que nos ayuden a realizar mejores evaluaciones y gestiones del riesgo. Debemos tener en cuenta que un nuevo entorno abarca nuevos riesgos", explicó Ken. "Nuestro propósito es convertirnos en un centro de excelencia que reúna una comunidad central de conocimientos técnicos, con una gobernanza más sólida, primando la seguridad, y con una mayor integración de las necesidades de las empresas", añadió el experto.



Zero Trust: Cómo garantizar el acceso seguro desde cualquier lugar

La siguiente ponencia "Zero Trust and Secure Access. Who, What, Where, When and Why" vino de la mano de **Alex Thurber**, Chief Revenue Officer en Pulse Secure.

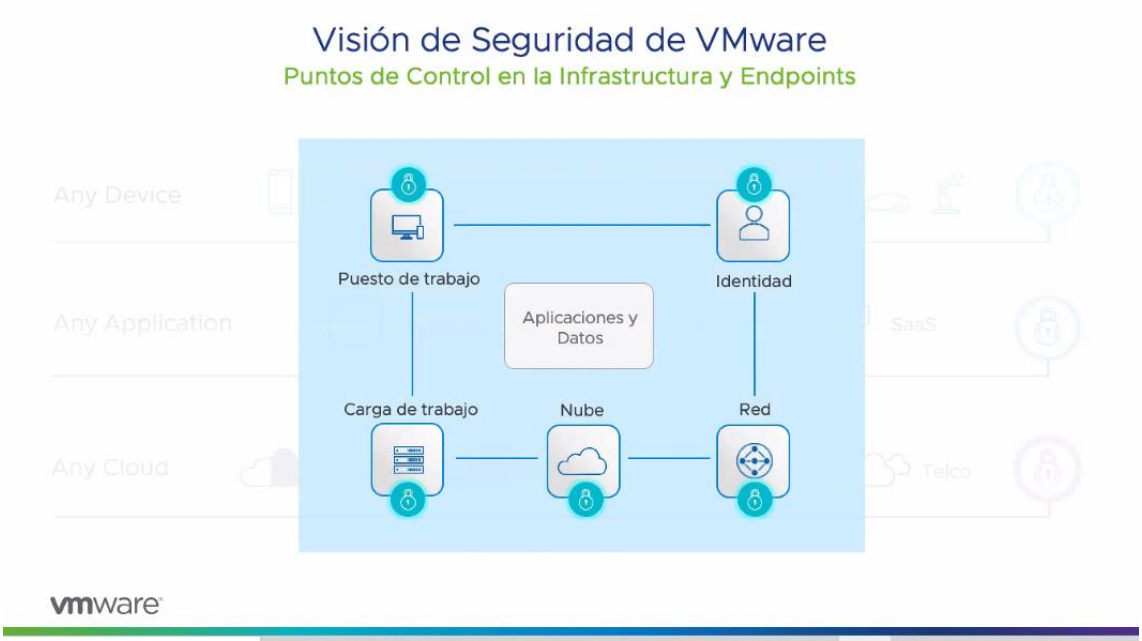
El experto se centró en una nueva investigación realizada por Pulse Secure que indica que el 84% de las empresas aumentarán probablemente la capacidad de trabajo desde casa más allá de la pandemia a pesar de las preocupaciones de seguridad. “A pesar de los problemas de seguridad y las preocupaciones derivadas del aumento masivo y repentino de las iniciativas de trabajo desde casa (Work From Home, WFH) causadas por la crisis sanitaria mundial de la COVID-19, un tercio (38%) de las empresas estadounidenses observaron aumentos de productividad durante el trabajo a distancia y un asombroso 84% prevé una adopción más amplia y permanente de la WFH más allá de la pandemia”, comentó Alex.

Asimismo, el ponente presentó Pulse Zero Trust Access (PZTA), “ofrece a los usuarios un acceso sencillo a las aplicaciones y recursos de la organización, permitiendo establecer un control granular sobre cada solicitud de acceso, verificando automáticamente la identidad, el dispositivo y la postura de seguridad antes de autorizar una conexión directa y cifrada entre el dispositivo de ese usuario y las aplicaciones que puedan residir tanto en Nubes públicas, privadas o datacenters”.

Por otro lado, **Joaquín Gómez**, Enterprise VCN Sales Executive en VMware, presentó su perspectiva sobre “la Seguridad Intrínseca "Anywhere", un pasito más hacia el Zero Trust”.

“Cuando hablamos de ciberseguridad las capacidades que deberíamos abordar en una primera instancia es la prevención y la gestión de amenazas. Se trata de prevenir mediante políticas el ataque a nuestras infraestructuras a través de la detección y rápida respuesta, protegiendo así nuestras aplicaciones y datos. Este es el proceso que debería realizarse continuamente”, comentó Joaquín. “El paradigma está cambiando y hay tres puntos en los que deberíamos

focalizarnos para adaptar nuestra seguridad a esta transición: los usuarios, la Nube pública y privada y las analíticas. La adaptación a la nueva normalidad pasa por adaptar nuestra seguridad a las nuevas circunstancias. Nuestro enfoque se basa en una seguridad integrada en todas nuestras aplicaciones, en una plataforma unificada que nos ofrezca análisis continuos, y sobre todo centrada en el contexto, ya que no tenemos que proteger todo de la misma forma si las aplicaciones se encuentran en entornos de riesgo diferentes", declaró el ponente. El experto se centró en la explicación de su solución VMware SD-WAN Secure Access (ZTNA), el acceso seguro que ofrece VMware, a través de su red global de puntos de presencia (PoPs) VMware SASE desplegados en más de 100 ubicaciones globales, "nuestra visión reside en que podemos tener cualquier tipo de aplicación en cualquier entorno (Cloud, híbrido o privado) y accesibles desde cualquier dispositivo de manera segura y conectada a la red".



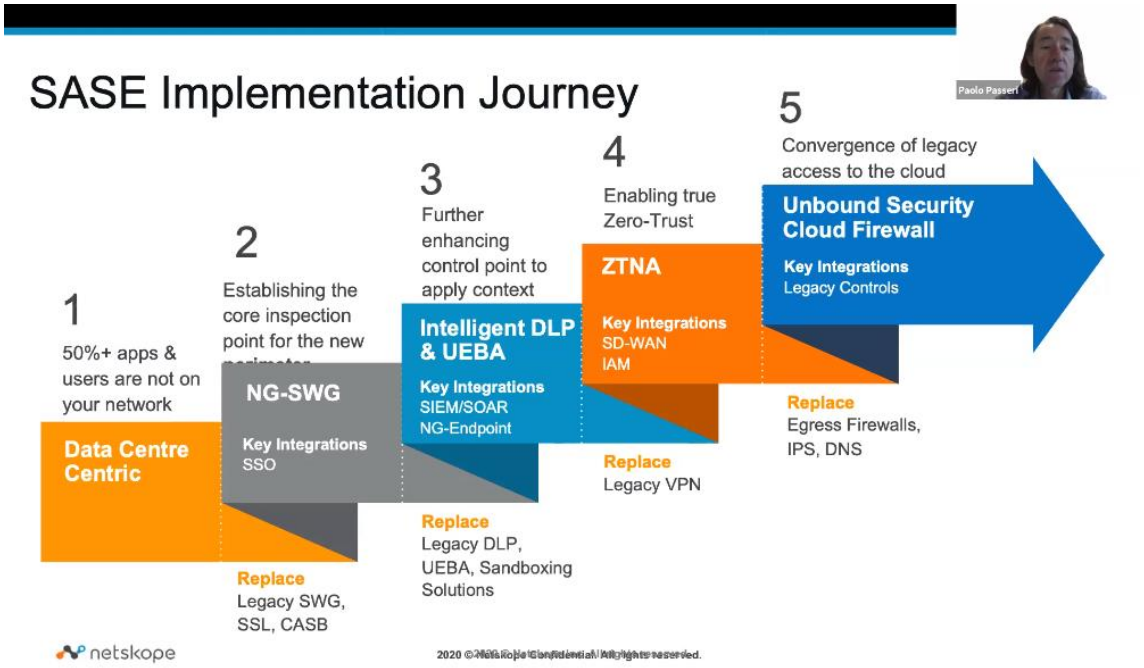
Potenciando la ciberseguridad a través del SASE

La mesa redonda del día "Implicaciones de teletrabajo basado en servicios de Nube segura" contó con la participación de **Jorge Hurtado**, Vice President EMEA en Cipher, **José de la Cruz**, Technical Director Iberia en Trend Micro, **Enric Manez**, Enterprise Security Sales Executive en Akamai Technologies, **Joan Ruiz**, Systems Engineer en Fortinet, **Elena Cerrada**, Country Manager en Forcepoint, y como moderador, **Lucas Varela**, Digital Security en CaixaBank.

La temática giró en torno a cómo ha modificado el teletrabajo las prioridades en Seguridad (IoT inseguro, WIFIs abiertas, ordenadores de gaming con plugins "dudosos", etc.) y cómo se han adaptado los actores maliciosos a esta realidad. Asimismo, se abordó la perspectiva del Cloud, y en particular los conceptos relativos de Zero Trust que lleva embebido una solución a estos problemas, así como las ventajas que puede otorgar el SASE (escalabilidad, agilidad, elasticidad, globalidad…) y sus posibles fallos. Por último, se debatió sobre los riesgos asumidos por las empresas antes y después de la COVID-19, una comparación que ha revelado diversas cibervulnerabilidades en las empresas, pero que también ha sido muestra de la resiliencia y agilidad de las mismas.

En su ponencia “Transformation of the workplace. Towards a SASE architecture” **Paolo Passeri**, Principal Sales Engineer and Cyber Intelligence Specialist en Netskope, y **Samuel Bonete**, Regional Sales and Technical Director Iberia en Netskope, debatieron sobre la importancia de “inspeccionar todo el tráfico a cualquier aplicación Cloud para ver qué es lo que está haciendo el usuario y protegerlos cuando interaccionan en la Nube. Asimismo, tenemos que comprender a qué instancia está conectando el usuario, ya que no es lo mismo que un usuario haga *login* en una instancia corporativa del Office 365 o un Teams corporativo, a que lo haga en una instancia no corporativa. Tampoco se trata de bloquear todo lo que no sea corporativo, pero sí tenemos que entender qué hace el usuario dentro de esas otras instancias para poder aplicar controles”, declaró Samuel Bonete, a lo que Paolo Passeri añadió “con la COVID-19, muchas empresas han tenido que trasladarse al entorno Cloud rápidamente, sin embargo, no están concienciados ni educados en los riesgos que conlleva y cómo prevenirlos. Para entender el entorno al que nos enfrentamos hay que saber de dónde venimos”.

Los expertos expusieron su perspectiva sobre la transformación digital orientada a SASE. “Netskope cuenta con una plataforma de seguridad en la Nube que fue diseñada desde el principio para ser nativa en la Nube, unificada, y construida sobre microservicios. También se centra en los datos y la inteligencia en la Nube con posibilidad de actuar rápidamente frente a los cambios, y se alinea con la funcionalidad central de SASE”, comentó Paolo.



"Protección de servicios Cloud SaaS, PaaS, IaaS" fue el título de la ponencia de **Carlos Muñoz**, Security Advisor en McAfee, que comenzó con un análisis de cómo las empresas se han adaptado a los servicios Cloud en sus procesos de digitalización y de qué manera están protegiendo su información. “Dentro de este proceso de digitalización, la mayor parte del volumen de la empresa se encontrará en la aplicaciones SaaS, pero hay un 10% de la información que se acumula en Shadow IT/Cloud, alguien está utilizando Evernote para coger notas sobre una

reunión en lugar de One Note, y eso es algo que la organización tiene que analizar y aplicar políticas educativas o de restricción para evitar que ocurra".

Carlos Muñoz definió la perspectiva de McAfee en cuanto a la securización de las aplicaciones nativas en la Nube a través de 5 casos de uso. "El primero está relacionado con la configuración de auditoría de los entornos IaaS, se trata de prevenir las vulnerabilidades debidas a las malas configuraciones en los entornos IaaS. El segundo, se basa en el control de datos confidenciales y escaneo de malware para evitar que los datos regulados y el malware se almacenen en el AWS 53 o Azure Storage. El tercero, alude al descubrimiento y gestión del Shadow IaaS con el objetivo de bloquear el acceso a instancias de IaaS no autorizadas. El cuarto, reside en llevar a cabo una protección avanzada frente a las amenazas, detectando a tiempo cuentas comprometidas, amenazas de usuarios privilegiados o internos, malware, etc. Por último, realizar un monitoreo de actividades y análisis continuo categorizando cualquier rastro de actividad".

La siguiente ponencia "La realidad del problema de irse por las Nubes" fue impartida por **Elías Grande**, Security Architect Discipline Leader en BBVA, que orientó su intervención hacia los antecedentes que llevan a "irse por las Nubes", los nuevos retos de seguridad planteados por el Cloud y un decálogo de buenas prácticas de seguridad para el Cloud.

"Desde el punto de vista del CISO, en Cloud seguimos teniendo los mismos objetivos y motivaciones, el cambio o impulso a mejorar proviene de la parte interna de la organización, pues tiene intereses en el Time to Market, la adopción de metodologías más ágiles, etc. para posicionarse delante de sus competidores. Por su parte, también identificamos un impulsor en el lado de la ingeniería, por todos los beneficios de automatismo, escalabilidad y oportunidades que ofrece el Cloud", explicó Elías.

El experto expuso su punto de vista sobre cuáles son los nuevos retos de seguridad TIC y retos regulatorios planteados por el Cloud que podemos ver en la siguiente imagen:

Mariano J. Benito, CISO en GMV y Coordinador del Comité Técnico Operativo del Capítulo Español de Cloud Security Alliance, fue el encargado de poner fin al evento con la presentación del **VIII Estudio del Estado de la Seguridad en la Nube**. Este documento ha abordado ámbitos clásicos del mismo, además de cómo ha influido la COVID-19 en la adopción de los servicios en la Nube. En este aspecto, el estudio arroja que la mitad de las empresas han podido responder a la COVID-19 con los servicios TI (locales o en la Nube) que tenían previamente disponibles. La otra mitad de las empresas han añadido servicios de videollamadas, VPN y escritorios virtuales, y para las más grandes, servicios de ciberseguridad adicionales.

"El estudio ha detectado por primera vez entre sus participantes a un perfil de usuarios específico: usuarios no técnicos de los servicios en la Nube", comentó Mariano. "También hemos podido ver por primera vez desde que realizamos este estudio, cómo el nivel de satisfacción de los usuarios con los servicios en la Nube es más alto que el nivel de exigencia de los requisitos que se les solicita a los Proveedores de Servicio", añadió.

Un año más, el **X Encuentro de Cloud Security Alliance España** se ha consolidado como uno de los mayores congresos nacionales en el que más de 250 asistentes disfrutaron en modalidad online de debates de alto rango en materia Cloud.

Desde ISMS Forum y el Capítulo Español de Cloud Security Alliance queremos agradecer especialmente a nuestros patrocinadores McAfee, Netskope, Pulse Secure, VMware, Akamai Technologies, Cipher, Fortinet, Forcepoint y Trend Micro su apoyo para que este encuentro digital pueda realizarse.

Sobre ISMS Forum

ISMS Forum -International Information Security Community- es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. ISMS Forum cuenta con más de 250 empresas asociadas y más de 1.250 profesionales asociados. La Asociación es ya, por tanto, la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España.

Contacto

Raquel García – Responsable de Comunicación Externa y Relaciones Públicas

rgarcia@ismsforum.es

Twitter: @ISMSForum

LinkedIn: ISMS Forum

Teléfono: +34 600 87 19 69