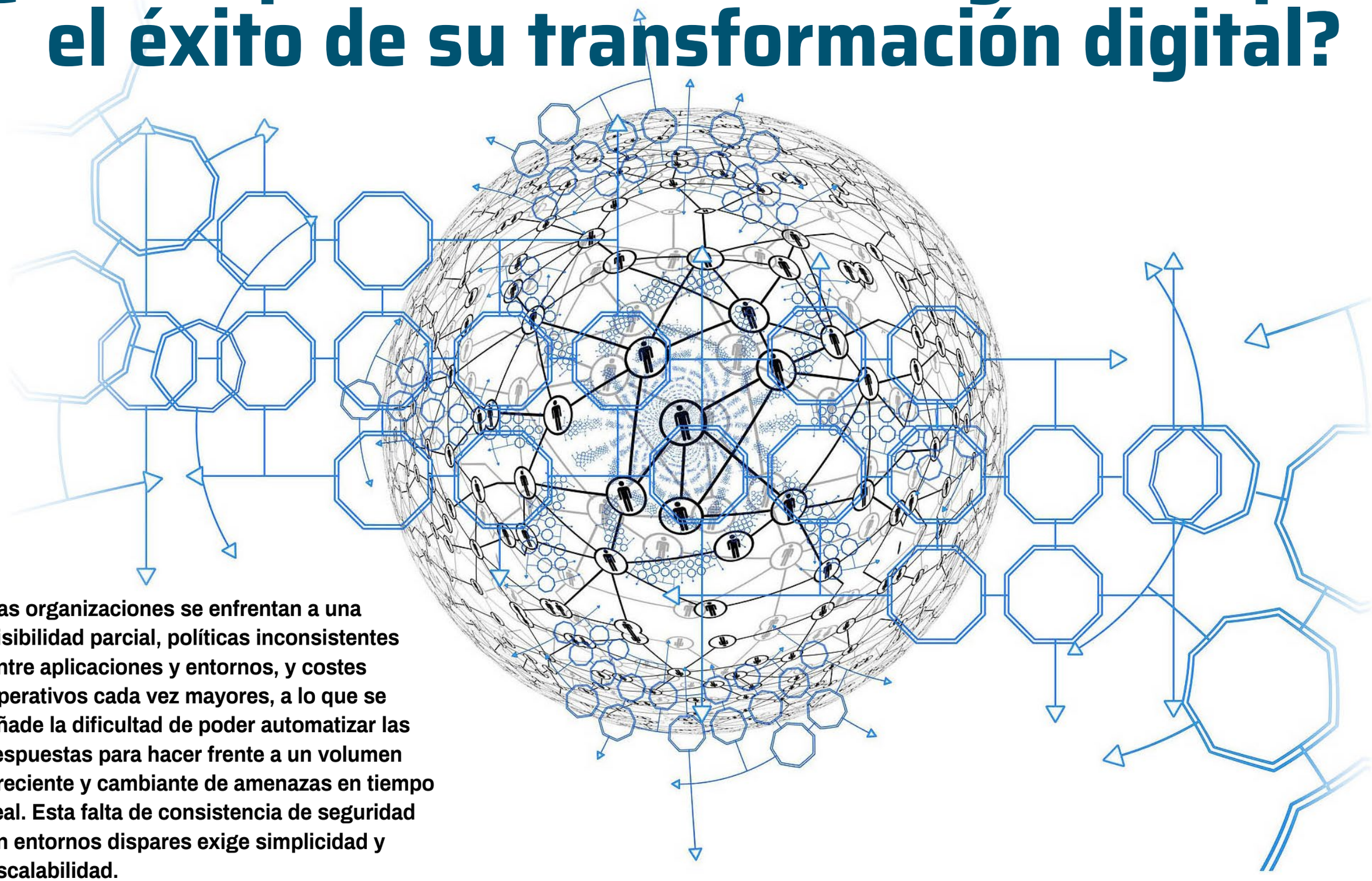
¿Qué importancia tiene la seguridad para el éxito de su transformación digital?

Organiza: it Digital Security

Patrocina: f5

¿Qué importancia tiene la seguridad para el éxito de su transformación digital?



Las organizaciones se enfrentan a una visibilidad parcial, políticas inconsistentes entre aplicaciones y entornos, y costes operativos cada vez mayores, a lo que se añade la dificultad de poder automatizar las respuestas para hacer frente a un volumen creciente y cambiante de amenazas en tiempo real. Esta falta de consistencia de seguridad en entornos dispares exige simplicidad y escalabilidad.

Analizar la situación a la que se enfrentan los responsables de ciberseguridad de las empresas, cómo las organizaciones pueden perseguir y lograr su transformación digital con mayor rapidez y confianza sabiendo que la seguridad de sus aplicaciones, especialmente las nuevas que impulsan una transformación importante, no ralentizará el proceso de desarrollo e implementación de aplicaciones, es el objetivo de un Encuentro ITDS patrocinado por F5 en el que participaron Juan Maza, CIO Y CISO del Centro Farmacéutico Valencia; Rafael Hernández, CISO de Cepsa; David González González, CISO de Coren – Alimentos de Galicia; Jorge Tomé, responsable de ciberseguridad y continuidad de negocio del Grupo Prisa; Gabriel Moliné, CISO de Leroy Merlín y Juan Rodríguez, Country Manager de F5.

Arrancaba el debate Juan Rodríguez, country manager de F5, recordando los 25 años de historia de la compañía, que se inició ante la necesidad de balancear aplicaciones y servicios en entornos multicapa para ir evolucionando hacia otro tipo de servicios, como DDoS y, en los últimos años, “en función de lo que nos habéis ido pidiendo los clientes”, hacia servicios de fraude y servicios SaaS basados en cloud. “Nuestro principal foco de negocio ahora es dotar de servicios, securización y que se pueden desplegar las aplicaciones y servicios en cualquier entorno multi cloud”.

La transformación digital, acelerada durante los últimos años, permite optimizar procesos y mejorar la competitividad, pero no está exenta de retos.

"Cuanto más se acelere la transformación digital, más debe acelerarse la innovación"

Juan Maza, CIO Y CISO, Centro Farmacéutico Valencia

**ENCUENTROS ITDS.
SEGURIDAD Y TRANSFORMACIÓN DIGITAL**

CLICAR PARA VER EL VÍDEO

Para Juan Maza, CIO Y CISO del Centro Farmacéutico Valencia, uno de los principales retos a la hora de hacer frente a la transformación digital es "la resistencia al cambio", que ha llevado a apostar por una transformación digital gradual que no tenga un gran impacto en el usuario o cliente, así como a "incidir mucho en la formación y apoyo a todos los usuarios, porque venimos de un modelo de negocio heredado de mucho tiempo". Mencionaba también Juan Maza como gran reto el asegurar un entorno IT "que cada vez está más fragmentado, lo que crea una superficie de ataque mucho más grande".

Coincide David González, CISO de Coren, en que la resistencia al cambio es uno de los principales retos de una transformación digital que en su compañía se inició hace años "empezando por las principales industrias del grupo hasta llegar a las pequeñas explotaciones de los diferentes socios". Habla de retos tecnológicos que siguen afectando al mundo rural, donde una buena conectividad sigue siendo una asignatura pendiente.

> F5 es capaz de mejorar la experiencia usuario desde el punto de vista de aplicación, dato y de seguridad, y además en cualquier modalidad -onpremise o nube

Para Gabriel Moliné, CISO de Leroy Merlín, acompañar el proceso de transformación digital "sin ser un stopper para el negocio" es uno de los principales retos que genera esta digitalización. Menciona el directivo que, si bien los canales digitales no han sido la principal fuente de ingresos de su compañía, en los últimos años ha habido una transformación que convierte en objetivo principal el mundo digital, acompañado del mundo físico, que ha requerido, entre otras cosas, una gestión del dato de una manera diferente. Menciona también la ciberseguridad como un reto importante debido al aumento del área de exposición, así como "el cambio del modelo de gestión de la ciberseguridad para intentar garantizar una seguridad por diseño".

"Nuestro mayor reto es sobrevivir", asegura Jorge Tomé, responsable Ciberseguridad y continuidad de negocio del Grupo Prisa. Comenta que en su

"La ciberseguridad es la parte diferencial de un proceso de transformación digital"

Rafael Hernández, CISO, Cepsa

compañía "seguimos teniendo gente que escribe noticias e información, y seguimos teniendo gente que escribe libros, pero ya no se imprimen en ningún sitio". El convertirse en 100% digital tiene un reto asociado: todavía hay mucha gente que piensa que una vez tiene internet las noticias es algo que tiene que estar ahí, que no debe tener un coste. "Nos hemos tenido que adaptar a un cambio totalmente de paradigma, de ser una empresa de logística, de compraventa de papel a una empresa que lo que genera son contenidos digitales y los distribuye a audiencias millonarias", explica. Respecto a la ciberseguridad "tenemos la desgracia de que nuestro negocio está en la exposición y somos objetivos prioritarios para cualquiera que quiera tener cierta notoriedad en el en el mundo de Internet", lo que ha llevado a la compañía a tener que aprender y desarrollar capacidades de respuesta a este entorno hostil.

"La transformación digital es un procedimiento que hemos lanzado internamente para mejorar nuestros procesos de producción", dice Rafael Hernández, CISO de Cepsa, añadiendo que la ciberseguridad es la parte diferencial de un proceso de transformación digital. El reto, asegura, es acompañar a los nuevos procesos a que sean más seguros y más útiles para nuestros usuarios y empleados". Explica también el directivo que antes de la pandemia Cepsa ya contaba con un programa muy agresivo de digitalización y migración a la nube que la pandemia aceleró, y que la función del CISO es "dar soluciones a los problemas que se nos presentan, que son distintos de los que teníamos hace 20 años".

Para el responsable de F5 en España y Portugal, durante los últimos años han cambiado los tipos

Aplicaciones Adaptativas

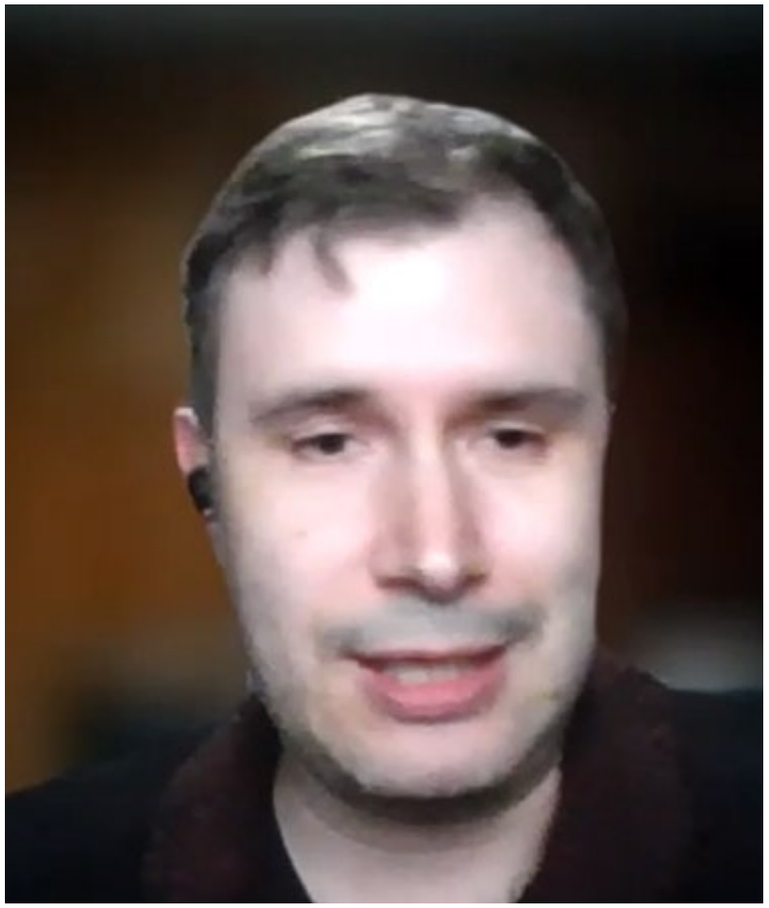
La forma en la cual tenemos montadas nuestras infraestructuras tiene que cambiar", decía en un momento de su intervención Juan Rodríguez. Aseguraba que Tecnologías como SD-WAN o SASE permiten optimizar el ancho, pero no que mi aplicación la entregue en el extremo, que cada vez cobra más importancia.

Destacaba el valor de las aplicaciones adaptativas, que reaccionan en función de las necesidades y los servicios que necesita el cliente, estén donde estén. Respecto a esto último comentaba el directivo de F5 que la compañía cuenta con soluciones que permiten a los clientes gestionar sus nubes de manera independiente y de una manera única que permite "desplegar servicios, aplicaciones y políticas de seguridad en cualquier entorno".

"Tener una aplicación legacy no significa que no la pueda llevar a la transformación digital", aseguraba también Juan Rodríguez, añadiendo que no hay que tirarla o empezar de cero, sino 'apificarla'. Si tiene buenos procesos de operación, "una aplicación Legacy apificada puede funcionar mejor que desarrollar una aplicación de cero en un entorno de nube", comentaba asegurando además que no porque una empresa esté desarrollando todo en un entorno de nube vaya más por delante en la transformación digital que aquel que tiene una aplicación legacy apificándose.

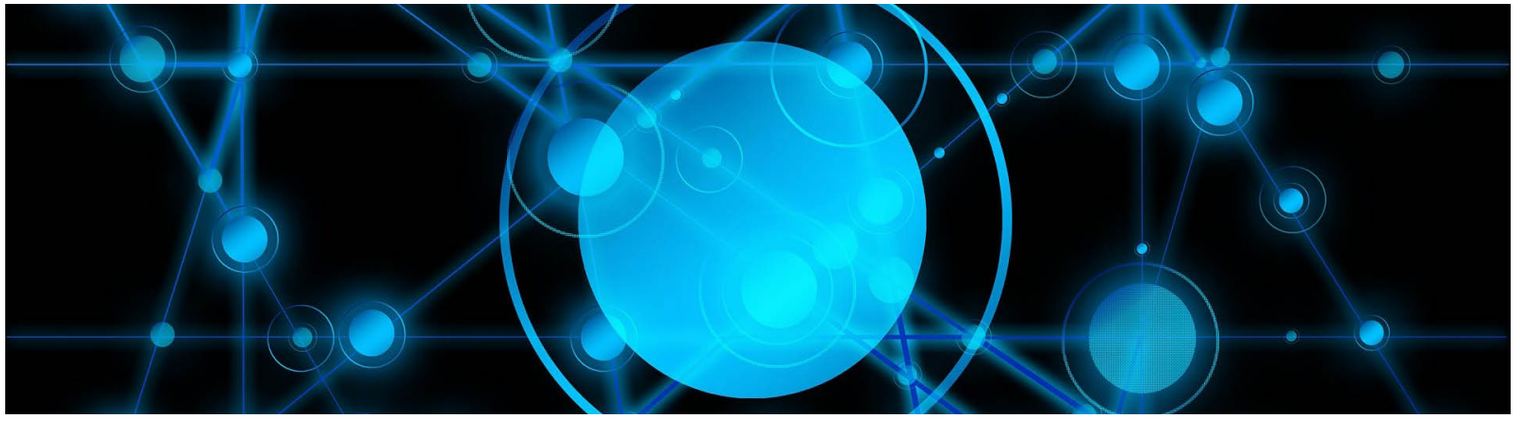
Sobre las aplicaciones adaptativas, destacar que utilizan un enfoque arquitectónico que facilita respuestas rápidas y totalmente automatizadas ante condiciones cambiantes, por ejemplo, los nuevos ciberataques, actualizaciones de la postura de seguridad, degradaciones del rendimiento de las aplicaciones o problemas en uno o varios entornos de infraestructura.

Y, a diferencia del estado actual de muchas aplicaciones, cuya seguridad, despliegue y gestión requieren mucho trabajo, las aplicaciones adaptativas se pueden llevar a cabo gracias a la recopilación y el análisis de la telemetría de seguridad y de las aplicaciones en directo, las políticas de gestión de servicios o las técnicas analíticas avanzadas.



"La experiencia de usuario tiene que ser uno de los objetivos a optimizar y mejorar"

David González González,
CISO, Coren - Alimentos de Galicia



y vectores de ataque, así como su frecuencia. “El ciberataque se está convirtiendo en un negocio y en un servicio” que se ha profesionalizado, recuerda el directivo, mencionando la experiencia del usuario como uno de los aspectos a tener en cuenta en los procesos de una Transformación Digital que llevan a la modernización de aplicaciones y migración de las mismas a la nube con el mismo nivel de seguridad. Durante su intervención comentaba también el directivo que el volumen de datos que estamos gestionando actualmente sobrepasa con mucho a lo que llevamos haciendo los últimos años, y que esto irá aumentando; “cuando más nos llevamos el dato y la aplicación al extremo, el volumen de datos que vamos a gestionar va a ser muchísimo mayor”.

Innovar en transformación digital

Planteamos a los diferentes ponentes si la aceleración de transformación significa que se necesita innovar más rápidamente. Para David González, de Coren, todos los negocios tienen que ir innovando, “pero no es lo mismo el sector alimentación en que podemos estar nosotros o ser el sector de retail”. Menciona la ciberseguridad como uno de los aspectos en los que se necesita innovar más rápidamente “porque si no estaríamos perdidos”.

Para Jorge Tomé cuando hablamos de entornos digitales “una las carencias que tienen es que son totalmente fluidos y que evolucionan muy

"Ya no te vale con mirar a un sistema de información, tienes que mirar al conjunto de todos los sistemas de información que estás operando y que se coordinan o se orquestan entre ellos para dar respuesta a los procesos de negocio"

Jorge Tomé, Ciberseguridad y continuidad de negocio, Grupo Prisa

rápidamente. Con lo cual si, si tienes que innovar en un entorno que de por sí es un entorno muy dinámico y muy rápido, la innovación efectivamente tiene que ser exageradamente más rápida todavía".

Dice Rafael Hernández que "todos tenemos que innovar, y en seguridad innovamos constantemente", pero que "una cosa es que innovemos nosotros y otra que ayudemos a innovar" para resaltar que cuando se ayuda a innovar se tiene que estar desde el principio, "y no en el diseño sino en el pensamiento, en la idea, para poder ajustar el camino al que queremos llegar". Añade que la ciberseguridad tiene cada vez más visibilidad "porque los comités de dirección necesitan información veraz. No necesitan saber quién se conecta o qué comunicaciones hay" y menciona que empresas como F5 "nos tienen que dar soluciones, posibilidad de visibilizar

"Acompañar el proceso de transformación digital sin ser un stopper para el negocio es uno de los principales retos que genera esta digitalización"

Gabriel Moliné,
CISO, Leroy Merlín

nuestras soluciones, visibilizar el contenido y la información que hay, porque nosotros somos los gestores de esa información y esas herramientas. Eso es innovar, usar bien la tecnología en cada momento".

En opinión de Juan Maza, "cuando más se acelere la transformación digital, más debe acelerarse la innovación". Añade que el problema es de adaptación a los cambios, una adaptación que es costosa.

Visibilidad

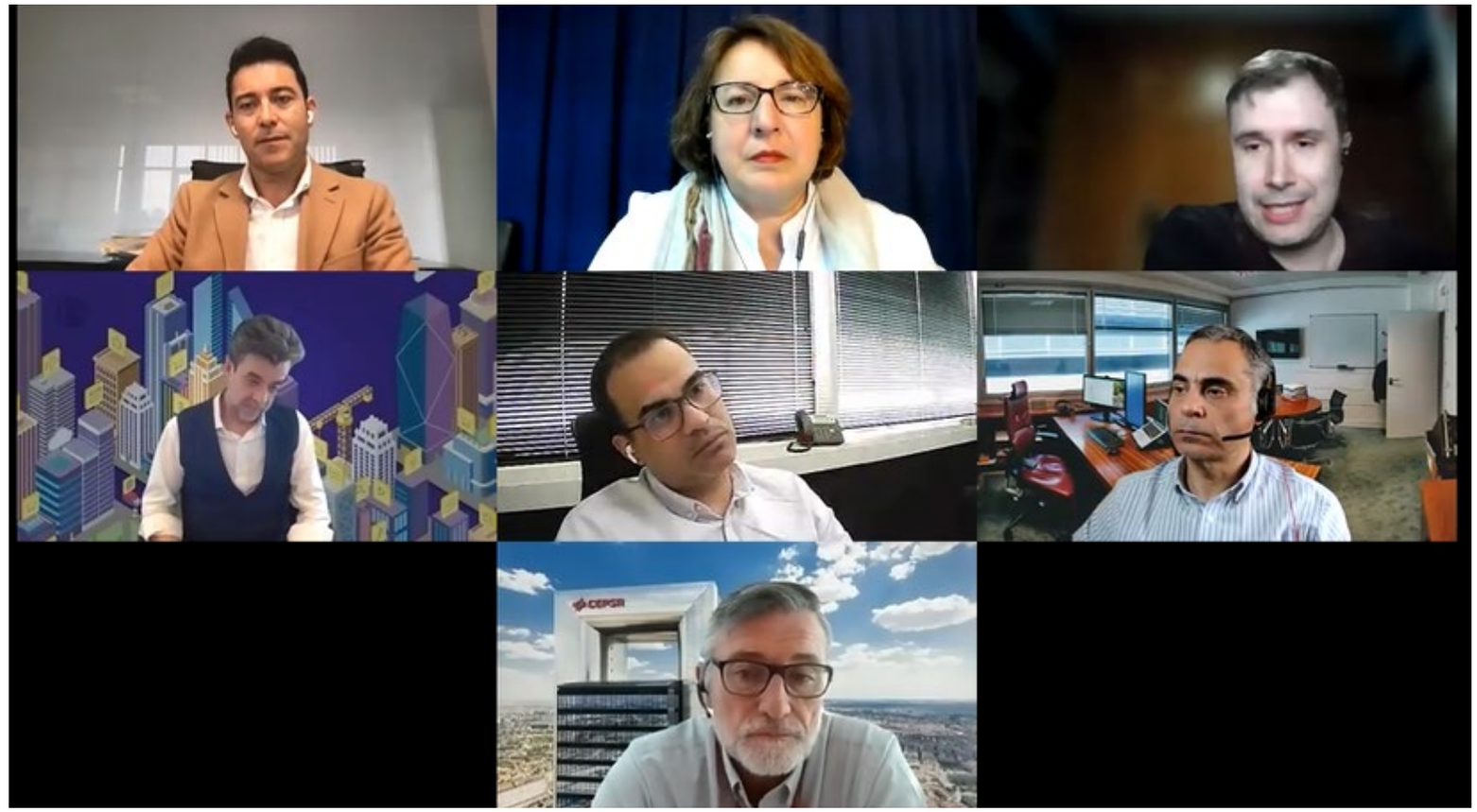
Planteamos en este encuentro cuán difícil es conseguir visibilidad para poder detectar problemas. Explica Gabriel Moliné que la transformación digital también conlleva un cambio de los instrumentos de trabajo y que no se trata de valerse únicamente de instrumentos técnicos para dar solución a la ciberseguridad, sino instrumentos legales o contractuales para poder tener cobertura y visibilidad de lo que acontece.

Si hace 20 años un proceso de negocio estaba contenido dentro de un sistema de información, hoy ese mismo proceso pasa por siete, ocho o diez sistemas de información distintos, que además no todos son tuyos, ni todos están en toda la interfaces. "Ya no te vale con mirar a un sistema de información, tienes que mirar al conjunto de todos los sistemas de información que estás

it whitepapers

EL ESTADO
DE LA ESTRATEGIA
DE APLICACIÓN EN 2022

El gran número de aplicaciones, integraciones y entornos está creando una complejidad que es casi inmanejable. Las organizaciones con visión de futuro reconocen la importancia de diseñar e implementar una estrategia de aplicación sólida para anticipar y responder mejor a los cambios en los intereses de los clientes y las condiciones del mercado. Lea el informe completo para saber cómo se compara su estrategia de aplicación.



operando y que se coordinan o se orquestan entre ellos para dar respuesta a los procesos de negocio", explica Jorge Tomé, añadiendo que el de la visibilidad es "uno de los retos más importantes que hoy tienen las organizaciones a la hora operar sus sistemas".

Todo es cuestión del riesgo, dice Rafael Hernández. Explica el directivo de Cepsa que, si se quiere que todo se conecte desde cualquier sitio, en cualquier momento y con cualquier dispositivo "habrá que asumir qué es lo que quieres en cada caso. Qué aplicación necesita una visibilidad del 100%" o en qué otras tienes que mirar para otro lado.

Recordando que el 60% del malware llega a las empresas a través de tráfico SSL, plantea que sean las empresas encargadas de mover el tráfico las que aseguren que ese tráfico está limpio, al igual que el Canal de Isabel II tiene que garantizar que el agua que llega a los hogares está limpia. Añadía también que la visibilidad es muy importante y que "tenemos que ir aprendiendo a que la Inteligencia Artificial y el machine learning nos ayuden a tener una visibilidad clara".

Comentaba Juan Maza que, en la misma medida que la transformación digital aporta muchas ventajas, también dificulta el seguimiento y visibilidad de

infraestructuras cada vez más complejas y que es complicado “rastrear bien y tener información clara y precisa de todo lo que necesitamos”.

Para David González, de Coren, los responsables de ciberseguridad se han convertido en gestores de riesgos; “tenemos que definir todos los riesgos y ver con los diferentes responsables el apetito de riesgo que tiene cada empresa o cada departamento”. Asegura que, aunque es posible conseguir visibilidad de todo, ésta requiere mucho tiempo y mucho esfuerzo.

Según datos de un estudio de F5, más del 90% de los responsables de TI y ciberseguridad de las empresas no tenían claro cuántas aplicaciones tienen o en qué estado están. La complejidad, no sólo en cuanto a los entornos tecnológicos de las empresas, sino de desarrollos ágiles que levantan aplicaciones nuevas, o versiones de las existes; modelos as-a-service contratados a golpe de tarjeta y en ocasiones sin conocimiento de los responsables, hace que “la forma en la que tenemos montada nuestras infraestructuras tiene que cambiar”, decía Juan Rodríguez, de F5, quien apuntaba además que las operadoras también están en un proceso de cambio, no sólo de servicios sino de nuevas tecnologías que permitirán, con la llegada de 5G “que yo pueda llevarme el dato y la aplicación al extremo”. Sobre el extremo asegura el directivo que “es lo que va a mandar todos vuestros negocios de aquí a futuro”.

En opinión de Rafael Hernández “necesitamos canales y entornos seguros para poder desarrollar las ideas de nuestra gente, que son muchas y muy variadas”.

"Nuestro principal foco de negocio ahora es dotar de servicios, securización y que se puedan desplegar las aplicaciones y servicios en cualquier entorno multi cloud"

Juan Rodríguez, Country Manager, F5

Microservicios

“Si tenemos en cuenta que los microservicios son sistemas que están distribuidos, con reglas de acceso complejas, y que suponen más tráfico que hay que monitorizar y una mayor superficie de ataque”, implementar y gestionar controles de seguridad de las aplicaciones en un entorno de microservicios para hacer frente a las amenazas es uno de los retos a los que se enfrentan los responsables de ciberseguridad, explica Juan Maza. Añade que la seguridad de la red, estrechamente relacionada con el tema de los microservicios, también es un reto y que ante los diferentes retos lo que se aplica es un mecanismo de defensa en profundidad.

El tener un producto digital que se basa en el desarrollo y puesta en producción continua de nuevos sistemas, nuevas aplicaciones y nuevas versiones, junto con la realidad de que el 90% de los sistemas de Grupo Prisa estén expuestos al exterior hace que “para nosotros sea extremadamente crítico la seguridad desde el momento cero y que está en el día a día de nuestros equipos de desarrollo”, decía Jorge Tomé.

Experiencia de usuario

“La experiencia de usuario tiene que ser uno de los objetivos a optimizar y mejorar”, dice David González cuando planteamos dónde se coloca esta experiencia en un proceso de transformación digital,

entrega de aplicaciones, multitud de herramientas y amenazas cada vez más avanzadas. Mencionaba el CISO de Coren que el desarrollo tiene que ser seguro por diseño y ya no sólo a nivel de software, sino de hardware "que es un problema muy serio y sobre todo en el mundo industrial".

¿Dónde colocamos la experiencia de usuario en este mundo cada vez más complejo de tecnología y de seguridad? "En el centro", responde Jorge Tomé. Explicaba el responsable de ciberseguridad del Grupo Prisa que lo que venden son experiencias a través de canales digitales, "y en estos canales la experiencia que tiene el usuario del consumo es clave. La web de El País está a un click de la web de la competencia. Al usuario no le cuesta nada irse".

Apunta Jorge Tomé que debe tenerse en cuenta que los usuarios empiezan a tener una cultura de ciberseguridad y que la clave es "proporcionarles una experiencia suave, un consumo sin esfuerzo de los contenidos, combinándolo con una sensación de seguridad, que puede confiar y que los datos que comparte con nosotros están protegidos y no acabarán en manos de quien no tienen que acabar".

Para Juan Maza "la transformación digital debe implementar tecnologías que sean fáciles de usar" y debe buscarse una buena experiencia de cliente tanto a nivel transaccional como e eficiencia o proceso. Comentaba también que se tienen que diseñar los servicios digitales con el usuario en mente, entendiendo por usuario tanto al cliente como al empleado.

Sobre la experiencia de usuario apunta Juan Rodríguez que durante la pandemia más del 70% de clientes online tuvieron que hacer algún tipo de transacción en eCommerce y que, por ejemplo, el tiempo de respuesta impacta drásticamente en la experiencia de usuario. Según datos de un estudio de F5, "la generación Z no pasa más de tres segundos en una página web que no le da un buen servicio. No les cuesta cambiarse", decía el directivo de la compañía apuntando también a que el 98% de la Generación Z hace sus transacciones comerciales en un móvil, "lo que quiere decir que no visitan ningún banco ni van a la tienda, lo hacen todo online. O tienes buena experiencia en este tipo de servicios, aplicaciones y seguridad, o estás perdiendo clientes". A lo que hay que añadir que tus competidores no están solo en España.

Añadía Juan Rodríguez que, entre otras cosas, F5 está ayudando a los clientes mejorando los accesos, de forma que, independientemente de cómo se conecte un usuario (móvil, Tablet u ordenador), la experiencia sea la misma, o reduciendo los mecanismos de control de acceso al poder detectar si un usuario es bueno o malo, "con lo cual F5 es capaz de mejorar la experiencia usuario desde el punto de vista de aplicación, dato y de seguridad, y además en cualquier modalidad –onpremise o nube".

A pesar de...

A pesar de que las empresas han invertido tanto en seguridad, ¿por qué todavía las vemos sufrir ciberataques y ataques de ransomware? ¿Cómo puede ayudar la industria a los responsables de ciberseguridad? ¿Cómo prevenimos ataques como Log4J o Solarwinds? A esta pregunta, planteada por Juan Rodríguez, responde Juan Maza asegurando que los sistemas de seguridad evolucionan al tiempo que evolucionan los ciberataques, que es importante monitorizar bien los sistemas para detectar amenazas, tener control sobre los usuarios, copias de seguridad distribuidas… "lo que se debe exigir es que las herramientas tengan cada vez más inteligencia artificial y que estén actualizadas al día".

En opinión de Jorge Tomé no se pueden prevenir ni impedir los ataques, sino que hay que centrarse en impedir que los ataques tengan éxito. Afirmaba que una solución que pretenda ser global y no de nicho para un problema muy concreto, "tiene que ser una solución capaz de consolidar, correlar y dar a la organización una visión completa de sus sistemas de información estén donde estén y de forma transparente", y que lo que cada vez valora más de los proveedores de seguridad con los que trabajan es "la ciberinteligencia" que permite saber con antelación qué APTs o grupos de ciberdelincuentes están haciendo cosas, "esto me aporta muchísimo valor".

La heterogeneidad de los sistemas, además de la existencia de los estados nación que se dedican a financiar a los ciberdelincuentes son dos razones para asegurar que evitar todos los ataques es imposible. Lo decía David González, añadiendo que a nivel legislativo sí que se podrían aunar esfuerzos para ir en contra de los ciberdelincuentes. En cuanto a los fabricantes, más que pelear por ser la empresa que antes detecta una amenaza o que tiene más información o más inteligencia sobre los ataques, "deberían compartir esa inteligencia y sus conocimientos para poder atajar o detectar cualquier tipo de ataque lo antes posible". Apuesta también el CISO de Coren por una visibilidad más sencilla, por contar con algún sistema "que me pudiera dar visibilidad y aviso de todo lo que pasa en mi empresa sin tener que pasar a través de cuatro o cinco consolas diferentes".

Enlaces de interés...

- F5 Labs
- F5 Blog
- F5 Aplicaciones Adaptativas

Compartir en RRSS