Ciber resiliencia:
fortaleciendo el negocio

Con la colaboración de:

El término ciber resiliencia está en boca de todos por el incremento en el número de ciber riesgos; agentes sociales y económicos están incidiendo en este concepto que define la facultad de las empresas de responder ante incidentes de una manera ágil y garantizando una pronta recuperación de su ritmo de actividad.

Ciber resiliencia: fortaleciendo el negocio

La ciber resiliencia o resistencia cibernética es la capacidad de una organización para prepararse, responder y recuperarse ante cualquier amenaza; una habilidad que se ha vuelto imprescindible en los últimos tiempos para reponerse de situaciones como la pandemia y el incremento de ciberataques que se han producido

en los últimos meses aprovechando que las organizaciones estaban preocupadas por otras cuestiones. Pero ¿es la ciber resiliencia un concepto nuevo? Para hablar de 'ciber', primero hay que hablar del concepto 'analógico': la resiliencia o capacidad de un individuo, un sistema o una comunidad de atravesar eventos traumáticos, violentos o difíciles sin que ello signifique una transformación permanente en su estructura o su manera de ser. Y la ciber resiliencia adapta esas características al mundo digital.

CIBER RESILIENCIA NO ES LO MISMO QUE CIBERSEGURIDAD

La ciberseguridad es el resultado de proteger la información de un ataque identificando riesgos y estableciendo las defensas más apropiadas. La resistencia cibernética o ciber resiliencia acepta que existe una alta probabilidad de que un ataque tenga éxito por muy bien que estén preparadas las defensas de una empresa y enfatiza en la importancia de la gestión de incidentes y la planificación de la continuidad del negocio. Es, por tanto, un concepto mucho más amplio que abarca la seguridad informática y la resiliencia empresarial, y apunta no solo a defenderse de posibles ataques sino también a asegurar tu supervivencia después de cualquier incidente exitoso. Para ello, una empresa debe asegurarse de que su ciberseguridad sea lo más efectiva posible sin comprometer la usabilidad de sus sistemas, así como tener planes de continuidad de negocio sólidos e integrados, de modo que, si un ataque tiene éxito, puedan reanudarse las operaciones habituales de la empresa lo antes posible.

La pandemia ha tenido efectos catastróficos para muchas compañías: cambios en los modelos operativos y de trabajo, distintas opciones tecnológicas, utilización de herramientas externas a la organización, entorno de control de riesgos, capacidad de monitorización en tiempo real, etcétera. Las instituciones financieras, en particular, se

La ciber resiliencia acepta que existe una alta probabilidad de que un ataque tenga éxito y enfatiza en la importancia de la gestión de incidentes y la planificación de la continuidad del negocio

BUILDING REGIONAL CYBER-RESILIENCE (World Economic Forum)

CYBERARK BLUEPRINT

Guía normativa para el éxito de la Gestión de Acceso Privilegiado

Simple y normativa

Preparada para el futuro

Asesoramiento significativo basado en el riesgo

Para desarrollar de forma óptima los programas PAM, las organizaciones necesitan unas directrices estratégicas. El modelo de CyberArk ayuda a reducir el riesgo siguiendo tres reglas de oro que responden a las últimas iniciativas de transformación digital.

Obtenga más información y apúntese a una sesión sobre el modelo en https://www.cyberark.com/es/blueprint/

CYBERARK®

han visto afectadas de manera más significativas debido a la naturaleza presencial del negocio y la necesidad de mantener las operaciones durante esta crisis, pero en realidad, cualquier sector que no estaba preparado para una migración masiva al teletrabajo ha tenido que realizar cambios repentinos, de manera urgente y probablemente, poco seguros.

Un informe de The Business Continuity Institute (BCI), realizado en 76 países con más de 650 responsables de IT refleja que el 53% de los encuestados está "extremadamente preocupado" por los ataques cibernéticos. No es para menos. Las brechas de seguridad, que en un 84% se producen en la capa de las aplicaciones, de materializarse en un ataque cibercriminal pueden llegar a representar un coste medio anual, a nivel global, cercano a los 10.200 millones de euros. Los efectos a nivel mundial que han tenido los malware como WannaCry y NotPetya son un claro ejemplo de las pérdidas económicas que han sufrido las organizaciones poco ciber-resilientes.

Y es que, la amenaza cada vez mayor de la ciberdelincuencia con el aumento de la gravedad y la frecuencia de los ataques de ransomware, puede poner en peligro una infraestructura de TI y las operaciones del centro de datos si no se ponen los medios adecuados. Estos ataques cifran todos los datos de una empresa, lo que obliga a pagar un rescate a los atacantes o perder los datos. Siempre se deben tener copias de seguridad periódicas y exhaustivas de los datos en una red separada que pueda usarse para restaurar los datos borrados.

Continuando con el estudio antes mencionado, el 42% de los encuestados para el mismo se

10 consideraciones para ser más resilientes

La pandemia por COVID-19 ha hecho que coja aún más sentido el concepto de ciber resiliencia. ¿Qué lecciones se han aprendido y cómo articularlas para dar mayor fortaleza a las organizaciones? The Business Continuity Institute ha recogido los siguientes diez puntos:

1 Compile las lecciones aprendidas y las soluciones alternativas utilizadas por los directivos empresariales para mantener sus servicios priorizados.

2 Asegúrese de que los contactos realizados durante este tiempo se registren ahora en los planes de continuidad del negocio en lugar de esperar a un momento en que todo se estabilice. En realidad, este "asentamiento" rara vez ocurre.

3 Evalúe y registre los recursos utilizados para mantener el nivel de servicio durante la pandemia. Reflexione si esto fue más o menos de lo que estimó en su análisis de impacto comercial y observe las razones de esto.

4 Registre qué o quién le brindó ayuda (interna o externamente a la empresa) para mantener sus servicios priorizados.

5 Documente las lecciones identificadas con respecto a sus procesos de comunicación: cómo mantuvo actualizado a su equipo, qué funcionó y qué se podría mejorar. Sea lo más específico posible: se trata de aprender lecciones, no de un juego de culpas.

6 Considere lo que va a hacer con las actividades no priorizadas que se han suspendido y documente las opciones para abordarlas.

7 Elabore un plan de recuperación para volver a la nueva normalidad. Por ejemplo, quién y en qué orden recupera los servicios durante la etapa de recuperación.

8 Planifique el trato con el personal que ha sufrido un duelo. Algunas organizaciones pueden haber tenido algunos empleados que han fallecido: esto afectará a la moral y debe gestionarse con sensibilidad y coherencia en toda la organización.

9 Coordínese con otros equipos y departamentos para que todas las iniciativas que esté planificando cuando vuelva a la normalidad se implementen de manera coherente y oportuna.

10 Recuerde que debe realizar todas las acciones anteriores porque puede haber otro incidente que perturbe su negocio en un futuro cercano. Por lo tanto, documentar ahora "lo que funciona" (quién hará qué, qué dejará de hacer y a quién debo decirle) es vital.

preocupa de la violación de datos y un 36% de las interrupciones no planificadas de las TIC. Sin embargo, uno de los puntos más interesantes del estudio es el modo en el que el cambio climático y sus inesperados fenómenos meteorológicos, los cambios regulatorios (como el RGPD) o las pandemias como la de la COVID-19, amenazan la continuidad de negocio. La implantación del teletrabajo por la pandemia de la COVID-19 requiere poner especial cuidado en el acceso remoto a los sistemas de las empresas desde redes domésticas, ya que no solo las usan los empleados de una organización, sino todo el núcleo familiar que puede estar menos acostumbrado a los intentos de ataques de phishing, por ejemplo.

Según los expertos, estos son los nuevos desafíos que hay que considerar cuando se aborda un proceso de transformación digital.

Todos los departamentos de una empresa deben coordinarse junto con el de TI y evaluar constantemente sus estrategias de resiliencia e integrar nuevas tecnologías en sus operaciones para garantizar la seguridad de las empresas

UNA INFRAESTRUCTURA DE TI ROBUSTA

Pero la ciber resiliencia no solo se basa en detener los ciberataques. A medida que experimentamos una mayor intensidad de huracanes, incendios forestales y otros desastres naturales, nos hemos dado cuenta de que la resistencia de la infraestructura tecnológica de una organización es primordial para la rápida recuperación. El nivel de resiliencia de las infraestructuras es directamente proporcional al impacto económico que producen este tipo de incidencias. Muchas organizaciones han cerrado sus ubicaciones físicas, cambiado la conectividad y las operaciones del centro de datos para mantener la actividad empresarial, lo que ha provocado un replanteamiento de las infraestructuras de TI para continuar la actividad del negocio. Estos cambios han sido tan importantes como la infraestructura tradicional.

Con los ataques informáticos hemos experimentado lo mismo. Tenemos que ser capaces de recuperarnos lo antes posible de cualquier ataque. Con la infraestructura crítica que depende de los sistemas de TI basados en datos, es necesario que las infraestructuras y los centros de datos críticos estén continuamente disponibles.

COORDINACIÓN EMPRESARIAL, LA CLAVE DE LA RESISTENCIA

Todos los departamentos de una empresa deben coordinarse junto con el de TI y evaluar constantemente sus estrategias de resiliencia e integrar

Ahora, cuando más grande es la contingencia,
más necesaria es la ciberseguridad.

En estos últimos meses,
los problemas de ciberseguridad
han crecido junto con las dificultades
de los negocios por mantener su actividad.

ISIT,

el nuevo modelo
de oferta de Sothis
para proyectos de Tecnología,
permite a las empresas
evitar la barrera de entrada
que supone el desembolso inicial
también en proyectos de Ciberseguridad.

Para que ninguna empresa tenga que elegir
entre protección o liquidez.

Porque la seguridad no puede depender
de la circunstancia.

Sothis

www.sothis.tech

nuevas tecnologías en sus operaciones para garantizar la seguridad de las empresas.

Una buena estrategia de ciber-resiliencia debería conjugar diferentes ámbitos, comenzando por llevar a cabo una gestión de los riesgos continua, ya que no hay lugar para la relajación. Esta gestión debe ir en paralelo con el negocio, disponer de todas las métricas necesarias y tener la habilidad de adaptarse y escalar ante diferentes escenarios.

Además, debe tener una infraestructura segura y resiliente, es decir, estructurada y consistente; capaz de desplegar una defensa en profundidad que ataje las amenazas rápidamente mientras mantiene controles de los riesgos identificados.

Solo así es posible alcanzar una defensa proactiva y predictiva; una defensa, además, que es mucho más efectiva si tiene una capa de inteligencia artificial tanto para la analítica de datos como para el soporte de operaciones tecnológicas, lo que aporta capacidades predictivas ante potenciales problemas. Y por encima de todos estos puntos, la dirección empresarial. Menos del 50% de las empresas reconoce que su junta participa activamente en la estrategia de seguridad general, y muchos lo consideran un problema de TI en lugar de la gestión de riesgos general.

La dirección del negocio debe tomar parte en la construcción de la ciber resiliencia corporativa estableciendo una estrategia de arriba hacia abajo, es decir, comunicarse con todos los departamentos, para gestionar los riesgos de ciberseguridad y privacidad en toda la empresa.

La falta de elaboración de un plan que recoja las disposiciones de ciberseguridad y resiliencia podría constituir un menoscabo en la perspectiva presente y, sobre todo, futura por parte de la dirección del negocio. Minimizar los efectos de una intrusión en el sistema empresarial aplicando principios de continuidad del negocio demuestra interés por las consecuencias a largo plazo para la organización y ayuda a mantener el nivel que esperan de ella los clientes.

Además, aplicar ciertos protocolos también es un deber legal. Como tal, el liderazgo en este respecto no es simplemente una buena práctica, sino una práctica fundamental. ■

Minimizar los efectos de una intrusión en el sistema empresarial aplicando principios de continuidad del negocio demuestra consideración de las consecuencias a largo plazo para la organización y ayuda a mantener el nivel que esperan de ella los clientes

MÁS INFORMACIÓN

- ¿Qué es la ciber resiliencia? (Banco Central Europeo)
- Ciberresiliencia, primeros pasos para proteger tu empresa ante posibles incidentes (INCIBE)
- 46 métricas para mejorar la ciberresiliencia en un servicio esencial (INCIBE)
- Cyber Resilience, COVID-19 Response and the 'New Normal' – Learnings and Predictions (Guy Carpenter – Oliver Wyman)
- Haciéndose más resiliente: la necesidad de identificar lecciones y actualizar los acuerdos de continuidad de negocio (Business Continuity Institute)

Las 5 prácticas de Cyberseguridad que toda organización debería tener.

Ir al artículo ›

F5 LABS

Ciber resiliencia:

cómo garantizar la continuidad del negocio ante contingencias globales

La pandemia por COVID-19 ha obligado a las empresas a dar una vuelta de tuerca a sus estrategias de continuidad de negocio, apostando por un concepto más amplio que abarca desde la ciberseguridad, a la continuidad del negocio, la comunicación y la gestión del riesgo: la ciber resiliencia. Banco Sabadell, Leroy Merlin, Redsys, Sareb, Secretaría General de Administración Digital, ElevenPaths (Telefónica), Universidad Rey Juan Carlos, Citrix, Cyberark, f5, Sothis e ICRAITAS, debatieron sobre este concepto en una mesa redonda virtual de IT Events.

Si algo han aprendido las empresas en los últimos meses, caracterizados especialmente por estar viviendo una pandemia, es que hay que estar preparados ante cualquier circunstancia para evitar incidencias en los negocios. Unos negocios que dependen altamente de su infraestructura tecnológica y que se enfrentan a ciberataques y brechas de seguridad que están aumentando su frecuencia y severidad hasta tal punto que debemos asumir que no seremos capaces de defendernos contra todo, que es inevitable sufrir un suceso como los anteriores. Además, la situación surgida por la pandemia ha añadido mayor tensión a las estructuras tecnológicas incorporando nuevas circunstancias como la necesidad de teletrabajo, diluyendo el perímetro, po-

CIBER RESILIENCIA: CÓMO GARANTIZAR LA CONTINUIDAD DEL NEGOCIO ANTE CONTINGENCIAS GLOBALES

niendo en duda muchos principios que se daban por sentados.

¿Cómo deben responder las organizaciones ante esta realidad? Entendiendo que la ciberseguridad por sí sola ya no es suficiente; que solo su combinación con la resiliencia empresarial (alineando personas, procesos y tecnología) les permitirá sobrevivir y garantizar la continuidad del negocio. Con este motivo, IT Digital Media Group, a través de su división IT Events, organizó una mesa redonda para conocer cómo habían vivido las empresas esta circunstancia y cuáles habían sido las lecciones aprendidas. El encuentro, celebrado en modo virtual, estuvo patrocinado por Citrix, Cyberark, f5, y Sothis, y en él participaron portavoces de Banco Sabadell, Leroy Merlin, Redsys, Sareb, Secretaría General de Administración Digital, ElevenPaths (Telefónica) y la Universidad Rey Juan Carlos. Además, contó con la colaboración de ICRAITAS.

El objetivo de este encuentro fue identificar cuál es la situación actual de las empresas tras una circunstancia como la pandemia por COVID-19, cómo ha afectado a la protección de las infraestructuras y datos corporativos, cuáles han sido los puntos fuertes, los retos planteados, y cómo se deben mejorar a futuro. Así pues, Javier Carvajal, experto en ciberseguridad y director general de ICRAITAS, señaló en su exposición previa al debate que "la pandemia por COVID-19 ha sido un test de estrés de muchas cualidades, comportamientos y actitudes. Lamentablemente, ha supuesto una prueba de rendimiento de las personas y las infraestructuras porque durante todos estos meses hemos atendido eventos de perspectiva económica, gestión de personas, etcétera, y la digitalización ha sido uno de los grandes cambios para todos". En este sentido, las organizaciones necesitan resiliencia, para adaptarse positivamente a las situaciones adversas, y ciber resiliencia, para hacer lo propio con las TI corporativas. Y todo ello, desde cuatro puntos de vista: infraestructura disponible y usable; recursos humanos disponibles a tiempo; una cadena de suministro alineada con la estrategia; y un plan de contingencia y continuidad de negocio.

En su análisis, Carvajal destacó que "hemos perdido la visibilidad en la superficie de ataque porque la vigilancia que teníamos bajo control se ha desplazado a cada casa. La consecuencia es que cada uno trabaja con una infraestructura condicionada a que otros que vivan en el mismo domicilio entren a Internet para conectarse por ejemplo a Netflix". Igualmente incidió en la importancia de la cadena de suministro. "Estamos extendiendo nuestro riesgo de una manera que no pensábamos nunca. Hay un 54% de empresas que no monitorizan su estado de ciberseguridad; el 62% no mantiene su empresa con los mismos estándares y el 63% no dispone de recursos suficientes".

Bajo este marco, "la COVID-19 nos ha trasladado un reto en dos áreas fundamentales: seguridad y departamento de riesgos. Es fundamental que los profesionales se incluyan en todos los procesos de negocio de la organización para disminuir los riesgos y tener una estrategia correcta. Hemos de reposicionar la seguridad como un motor de crecimiento; es fundamental para asegurar los resultados y es importante empoderar a las empresas para ser socios colaborativos", afirmó. "Además, el ciber riesgo no se ve, igual que no se ve la COVID. Sin embargo, hemos de ser prudentes porque no verlo no significa que no exista, sino que hay que tenerlo presente e implicar a toda la organización", concluyó Carvajal.

LA VISIÓN DE LAS EMPRESAS

BANCO SABADELL. Javier Sánchez Ureta, Director de Control de Riesgos

Las entidades financieras, tradicionalmente bien preparadas a nivel tecnológico y de ciberseguridad, han sido objeto durante estos meses de un recrudecimiento de los ciberataques. “Con el gancho de la COVID-19 hemos visto a clientes sufrir phishing y proliferar herramientas para suplantar a todo tipo de entidades y, a partir de ahí, conseguir las credenciales de la banca a distancia o las tarjetas de los clientes de las entidades bancarias”, explicó Javier Sánchez-Ureta, Director de Control de Riesgos de Banco Sabadell, en la mesa redonda, quien también resaltó el cambio de ubicación del puesto de trabajo como otro de los grandes desafíos de la situación: “Teníamos una infraestructura muy bien dimensionada para el trabajo en remoto, aunque se tuvieron que hacer ajustes porque todo lo provocado por la pandemia eran cambios que no imaginábamos”.

Y es que, muchas veces, no se pueden contemplar todos los escenarios y hay que ir tomar decisiones según se van produciendo los acontecimientos. “Nuestra organización está involucrada en todas las áreas relevantes. Tenemos una estructura de comités de gestión de crisis jerarquizada: gold, silver y bronze, donde se involucra en cada caso a las áreas relevantes para la toma de decisiones. La peculiaridad con esta pandemia es que el comité silver que se activó, no se desactivó en ningún momento y ha estado durante meses activado permanentemente para hacer un seguimiento más pormenorizado de la evolución de los acontecimientos. A modo de ejemplo de situaciones que, paradójicamente, intentas prever y planificar pero luego tienes que adaptar a marchas forzadas, era la existencia de planes de continuidad que contemplaban llevar a los empleados a un edificio de respaldo en caso de incidencia, por si no se podía acceder a algunas instalaciones, pero resultó que no podía llevarse a cabo ya que la única instalación válida alternativa era la propia casa del empleado”, explicó.

Ha sido un proceso de adaptación permanente. “Nos hemos ajustado a cada inconveniente “real time” y hemos podido bajar muy a tierra todas estas necesidades, directrices y formas de hacer. Ha habido que identificar a los líderes porque son situaciones de estrés y complicadas para que sean capaces de reflexionar y transmitir”, señaló el director de Control de Riesgos de Banco Sabadell, quien apuntó como derivada de esta situación un giro hacia el insourcing “porque se compensan los riesgos de los proveedores que no han sabido adaptarse frente a las posibilidades económicas de escala y ahorros de costes del outsourcing”.

Asimismo, Sánchez-Ureta resaltó el papel del empleado. “Suele ser el eslabón más débil en la cadena cuando hablamos de proteger la información corporativa. Los empleados han hecho un gran esfuerzo de adaptación, y ahora viene una época en la cual la gente se puede relajar y bajar la guardia porque está cansada de esta nueva forma de trabajar y se pueden incrementar los riesgos asociados a la ingeniería social contra estos empleados. Así que hay que entender cómo se sienten las personas trabajando desde casa para determinar sobre qué y quién poner el foco para que esas posibles amenazas no se materialicen”.

LEROY MERLIN. Gabriel Moliné, CISO

Una de las mayores consecuencias del confinamiento para los negocios fue la pérdida de contacto con los clientes; una circunstancia que obligó a compañías como Leroy Merlin, cuya mayor parte de su actividad se produce de manera presencial, a redefinir su relación con el cliente y potenciar los canales digitales. "Nuestra empresa está destinada al contacto con el cliente. El acceso a la tienda es el principal canal de compra, por lo tanto, ha sido un reto monumental", aseguró Gabriel Moliné, CISO de Leroy Merlín durante el debate titulado "Ciber resiliencia, o cómo garantizar la continuidad de negocio ante contingencias globales".

"Tenemos una plataforma instalada de vendedores que vive del ámbito presencial, pero en poco tiempo incrementamos las conexiones remotas en un 130%, no solamente a nivel de equipos, sino de virtualización de escritorios", comentó. Sin embargo, al cambiar ciertas estructuras, hay que equiparlas para detener las posibles amenazas. "Hemos diseñado canales de comercialización que también han sido tentados por los cibercriminales, como la compra telefónica o la compra a través de WhatsApp. Cuando se incrementan nuevos canales, se incrementan nuevos vectores de ataque", explicó Moliné.

La empresa de bricolaje se encuentra en 16 países y la manera que ha impactado la COVID-19 en cada uno de ellos es diferente. "El modelo de relación en el conglomerado ha tenido que cambiar y nos ha afectado de una manera importante toda la gestión de los diferentes lugares", puntualizó.

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. Miguel Ángel Amutio, Director de la división de planificación y coordinación de ciberseguridad de la Secretaría General de Administración Digital

Cuando surge una situación como la que hemos vivido, una de las primeras obligaciones de los gobiernos es predicar con el ejemplo en su respuesta. Miguel Ángel Amutio, Director de la división de planificación y coordinación de ciberseguridad de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, aseguraba en la mesa redonda que si bien el viernes 13 de marzo se declaró el estado de alarma, a la semana siguiente, más del 70% de la plantilla estaba en condiciones de teletrabajo. Para este cometido, el Ministerio se enfrentó a dos grandes retos: "asegurar la continuidad de todos los servicios públicos digitales y facilitar que todo el personal pudiera teletrabajar. Hemos implementado todas las medidas del Esquema Nacional de Seguridad que nos viene dada por el marco común de mecanismos de conformidad, monitorización etc. Desplegamos recomendaciones de teletrabajo y protección para todo el personal, tanto de configuración segura de front office y back office, como recomendaciones para la configuración segura de herramientas de videoconferencia. Implementamos medidas contra el phishing y correos maliciosos fraudulentos y se reforzaron las medidas de vigilancia y movimiento a listas negras", explicó Amutio, quien destacó la colaboración del CCN para el despliegue de servicios de monitorización y respuesta para apoyar a las entidades del sector público.

"Hemos puesto en valor los servicios digitales que se prestaban y la necesidad de desplegar toda la ciberseguridad que acompaña a esos servicios. La formación y concienciación es una campaña permanente con mucho espacio de mejora. Durante el primer momento se ampliaron VPNs y cargas de trabajo en remoto y se terminaron de configurar puestos portátiles a gran escala para que la gente pudiera trabajar. Por eso las medidas eran las recomendaciones de protección del correo, los dispositivos móviles, aplicaciones etc. Todo el personal sabía las recomendaciones para poder distinguir situaciones de posibles incidentes, correos maliciosos...", afirmó Amutio. Y es que la concienciación es uno de los pilares de la ciber resiliencia. "Estamos promoviendo un escenario que implica de forma multidisciplinar a toda la organización, de ahí que tengamos el mandato de que nuestras entidades han de respetar una política de seguridad aprobadas al más alto nivel y la finalidad es implicar a los responsables, en definitiva, a los que tienen que liderar. Parte de las líneas de acción de la estrategia de ciberseguridad es que se promuevan en ciudadanos y empresas, concienciar y crear capacidades de retención de talento", destacó. "De todas formas, en nuestro Informe Nacional del Estado de la Seguridad siempre encontramos que la parte de la concienciación es un frente que requiere mucho trabajo. En mi departamento se están haciendo acciones de formación y ciberseguridad para el personal y campañas para detectar si se cae o no en los correos maliciosos con simulacros de phishing", incidió.

Ahora solo toca mejorar todo lo implementado. "Sacaremos conclusiones del teletrabajo, de los servicios en cloud, de la identidad electrónica que ha tenido que ver con la innovación de estos escenarios donde había transacciones de confianza en firma de documentos. Hay que repensar los mecanismos de identidad para que sea sencillo, donde todo funcione a gran escala de forma digitalizada", concluyó Amutio.

REDSYS. Miguel Ángel Fernández, Director de Fraude

"Tiempos de crisis, tiempos de imaginación", destacaba Miguel Ángel Fernández, director de fraude en Redsys, en la mesa redonda, para calificar el desarrollo de la actividad empresarial en estos meses de pandemia. "En tiempos de crisis buscamos soluciones que se adaptan al mercado. Por ejemplo, si no puedo hacer la compra, ha surgido que alguien la lleve a casa y para eso hay que estar preparado logísticamente. Aunque mucha gente no tenía ni un comercio en Internet; con un teléfono móvil y dándose de alta en Bizum, ha pedido a sus clientes que le pagaran por ese medio", detalló Fernández. "No tiene que pillarnos desprevenidos nunca más. Aunque hay que poner en valor que muchas cosas han funcionado muy bien en situaciones muy complicadas", añadió.

“Las personas han trabajado de manera magnífica pese a que la mayoría de las empresas no estaban preparadas para proporcionar teletrabajo ni los medios eran idóneos. Se han salvado los servicios esenciales porque teníamos la exigencia de hacerlo. Tenemos que dar las gracias a ciertas infraestructuras que ya estaban muy consolidadas”, comentó durante su intervención el portavoz de la entidad de procesamiento de pagos Redsys. Igualmente, reseñó “la buena calidad de las infraestructuras de comunicaciones, porque los móviles no se han caído, pero en las empresas, en general, la conectividad no ha funcionado tanto. Han hecho falta muchos equipos para conectarse y muchos empresarios no sabían si sus empleados tenían o no WiFi y, por lo tanto, conexión a Internet”.

Durante su intervención, Fernández abogó por hablar más de resiliencia en general, y no solo ciber resiliencia. “Las organizaciones cuyos negocios tengan una base tecnológica muy fuerte, están concienciados con la ciber resiliencia, pero el negocio tiene muchas facetas más que la ciberseguridad”. Así, por ejemplo, mencionó la concienciación: “es muy importante porque estamos en una dinámica de gestión de riesgos. A veces nos gastamos grandes cantidades en concienciar a nuestros empleados para no caer en campañas de phishing y, aun así, pican. Tengo que concienciarles para que hagan su trabajo con los mecanismos que le propon-

ga la empresa. Esta toma de decisión tiene que llevarse a cabo por parte del órgano que toma decisiones, que da los presupuestos, no solo los encargados de IT o ciberseguridad”, prosiguió.

Otro de los temas que Fernández puso sobre la mesa fue la gestión del personal. “Hace once años, con la Gripe A, hubo planes de contingencia para que los empleados no se contagiaran unos a otros. Sin embargo, en esta pandemia el problema ha sido no tener back up para los empleados que estaban enfermos. Ser ciber resiliente es tener un conjunto de medidas para todos -argumentó-. No obstante, hemos sabido gestionar muy bien en remoto y hemos visto que no nos ha hecho falta estar en una ubicación concreta para controlar todo”.

Desde Sareb, y por su naturaleza bajo la que aúna a entidades privadas y públicas, uno de los aspectos más destacados para la ciber resiliencia en tiempos complicados es “que los proveedores y administraciones públicas han de estar alineados con nosotros. Somos una inmobiliaria y si no hay notarios o juzgados abiertos, el negocio se queda parado”, comentó Pablo Blanco, gerente IT GRC, durante el debate. “Ha habido una gran dependencia tecnológica en el confinamiento y se ha visto que es necesario ser ciber resiliente. Todo el mundo está más a gusto en casa, con más confort, pero los riesgos son los mismos o más que en la oficina, aunque también depende de la operativa de la empresa”, afirmó Blanco.

SAREB. Pablo Blanco Iñigo, Gerente IT GRC

En Sareb tienen un dicho: se juega como se entrena. Por eso considera el responsable de IT GRC que estaban preparados. “Teníamos una buena dinámica de teletrabajo porque trabajamos en remoto los viernes. La verdad es que cuando en enero y febrero este virus estaba en China sabíamos que iba a llegar aquí en algún momento. Empezamos a realizar pruebas de las capacidades de red y a partir de ahí entramos en la dinámica de intentar lidiar con los ciberdelincuentes. No ha sido un camino de rosas, pero ha sido llevadero”, señaló. También realizaron muchas pruebas y simulacros de ciberseguridad “y se ha visto que eso que hicimos es inversión, se ha llevado a la práctica y ha funcionado. Aunque hay que seguir concienciando al proveedor y al empleado”, apuntó Blanco.

“En Sareb estamos sometidos a los mismos riesgos independientemente del lugar donde nos encontremos y tenemos un alto concepto de concienciación, aunque es diferente en cada empresa”, añadió. “La mujer del César no solo tiene que ser

honrada, sino parecerlo. Tenemos una parte táctica y otra estratégica. La táctica es la parte de gestión de personas, de seguridad física, de cumplimiento, de comunicación. Juntas toman decisiones para formular planes robustos de continuidad. Tenemos un comité estratégico donde está la alta dirección y los consejeros y algún accionista que apoya las decisiones de los demás", detalló Blanco. "Y la tecnología está ahí para ayudarnos. Es solo un cambio en la operativa. Igual que hay un departamento de marketing y otro financiero, tiene que haber uno de ciberseguridad. La guerra no solo es para militares, hay más gente involucrada. Igual que la ciberseguridad no es solo para técnicos. Todo el mundo tiene que ver con la seguridad".

ELEVENPATHS, TELEFÓNICA. Alejandro Ramos, Global Chief Security Operations Officer

Uno de los servicios esenciales que ha sido fundamental para el desarrollo de la actividad empresarial en los meses más críticos de la pandemia, ha sido el de las telecomunicaciones, que veía cómo se incrementaba exponencialmente el tráfico en las redes. Pero con la relativa calma posterior, ciertas técnicas y herramientas que se han implementado de manera rápida deberán reconsiderarse. Así lo reconocía Alejandro Ramos, Global Chief Security Operations Officer de ElevenPaths (Telefónica) durante la mesa redonda "Ciber-resiliencia, o cómo garantizar la continuidad de negocio ante contingencias globales": "nuestra percepción en general es que, cuando pase todo, debemos rehacer cosas que se han hecho con urgencia. Se han tomado decisiones asumiendo riesgos como levantar muchos accesos remotos o aplicaciones que antes no se podían gestionar desde el exterior de las oficinas. Hay que tener una reflexión para revisar todo con criterio y partir del diseño y seguridad desde el inicio".

Respecto a su análisis del estado de la ciberseguridad en estos meses, Ramos señala que Telefónica no ha aumentado sus incidencias durante la época más dura de la pandemia. "En el sector sanitario respondemos a 2 o 3 incidentes al mes, desde pequeñas y medianas empresas hasta grandes hospitales. Han sido los mismos incidentes que previamente a la COVID", comentó reseñando que las amenazas también han sido similares a las que había antes del confinamiento; "el mismo tipo de amenaza y características, las mismas solicitudes de rescate, la misma infraestructura y cifrado. Los ataques más avanzados han sido residuales", puntualizó.

Según Ramos, la resiliencia en una compañía de telecomunicaciones viene embebida. "No se entiende que se caiga una red, aunque a veces ocurre una caída masiva de las telecomunicaciones de manera excepcional, en algún país del mundo", destacó. "Desde Telefónica aportamos mucho valor, no solo con medidas

de seguridad sino con medidas adicionales. Es importante que haya una vía de mejora en la regulación. Lo mismo debería ocurrir con las medidas de seguridad para proteger al usuario igual que ocurre en el mundo de la privacidad. Hemos de llevar la seguridad de un juguete de un niño, de una lavadora o de un microondas a la ciberseguridad", razonó.

UNIVERSIDAD REY JUAN CARLOS.
José Antonio Rubio, Director de Seguridad de la Información

Educación ha sido otro de los sectores que han tenido un impacto más visible en estos meses de pandemia. "Esta situación ha supuesto una prueba de estrés importante. Hemos visto que el porcentaje de incidencias reportadas por los alumnos, el profesorado y el personal de administración y servicios se ha incrementado considerablemente", dijo José Antonio Rubio, Director de Seguridad de la Información en Universidad Rey Juan Carlos. Por su propia filosofía, las universidades intentan ser entornos abiertos, una cualidad que modela su postura ante la seguridad. "En la circunstancia actual ha sido complejo de adoptar. Contábamos con capacidades en materia de continuidad de negocio, pero hay algunos ámbitos en los que faltan cosas por hacer. Aunque la tecnología esté disponible, falta la normalización y choca con el entorno abierto que exige el negocio. Por ejemplo, hay investigadores que están en el otro lado del mundo y necesitan conectarse. Hay muchísima casuística", prosiguió, si bien reconoce que "en cuanto a capacidad de teletrabajo existía cierta normalización en cuanto a acceso peticiones etc., pero el número de usuarios se ha incrementado de forma notoria con muchas dudas en el uso y el centro de atención a usuarios ha sido vital para poner orden".

Respecto al volumen de ciberataques, la universidad experimentó un incremento notable contra el perímetro de su red, especialmente durante las primeras semanas de confinamiento, así como de ataques de phishing, si bien el entrenamiento previo de los usuarios hacía que muchos dudasen de su veracidad. "El CCN ha colaborado con nosotros haciendo simulacros de denegación de servicio, análisis de vulnerabilidades a aplicaciones web y, en cuanto a capacidad de seguridad a nivel de perímetro de red, hemos visto que estábamos bastante bien y hemos aguantado, aunque hemos optimizado un poco más los parámetros que teníamos en los dispositivos de red", continuó el CISO de la universidad.

Rubio, en línea con sus compañeros de mesa, señaló que la involucración de toda la organización es vital para lograr la ciber resiliencia. "En nuestro caso la alta dirección ha estado involucrada desde el primer momento, contando con el apoyo del comité de seguridad de la información. Cuando se vio que esta situación tenía mala pinta se activaron los mecanismos. Se ha observado la importancia de la tecnología con respecto a lo que es el negocio y la actividad diaria", dijo Rubio. Incluso, de forma previa a la pandemia se había lanzado un programa de Bug Bounty a los alumnos de carreras de corte tecnológico. "Hemos incorporado a los chavales para canalizar ese conocimiento y aportar un valor extra con apoyo controlado. Así, las cosas que han visto en la teoría de las clases relacionadas con seguridad informática las han podido llevar a la práctica", detalló.

Otra de las lecciones aprendidas en este tiempo, es la desigualdad social. "Nos hemos dado cuenta de que muchos estudiantes no tenían capacidad de asistir de forma telemática a las clases. A veces pensamos que, en 2020, los chavales tienen buena conexión en casa y un ordenador y hemos descubierto que no podemos dar nada por supuesto. Desplegar o entregar una cantidad significativa de portátiles a alumnos repartidos por toda España ha sido una tarea desafiante donde se ha comprobado que la tecnología es fundamental para que el negocio siga adelante", remató Rubio.

LA VISIÓN DE LA INDUSTRIA TI

Desde **CITRIX, Nuno Silveiro, responsable del área de networking**, explicó cómo han contribuido desde su compañía a la migración masiva al teletrabajo en este tiempo de pandemia y, con ello, a la ciber resiliencia de las organizaciones. “Hemos provisto soluciones de teletrabajo a los clientes que han tenido que hacer ajustes a su infraestructura para que los empleados pudieran acceder al sistema desde el exterior de las oficinas. En alguna ocasión, hemos desplegado la infraestructura desde el principio con soluciones de SaaS, de la nube, etc. Otros clientes no tenían capacidad para poder trabajar con este tipo de herramientas, y se han implementado soluciones sencillas por VPN que son paliativas para un punto inmediato, pero después habrá que repensarlas”, destacó Silveiro.

En este tiempo, el directivo observó que “una minoría de empresas tenía planes de continuidad desarrollados, pero la gran mayoría tenía planes de recuperación de desastres”. Con todo, la ciber resiliencia debe abarcar más allá de la ciberseguridad, pues es importante cuidar también la capa de aplicaciones y los datos. “Solo tener ciberseguridad sin tener esta capa de ciber resiliencia no sirve de mucho. Si la gente no consigue conectarse tenemos un problema de productividad, y si la gente consigue conectarse, pero de manera insegura, tenemos un problema aún más grande. En Citrix ayudamos a que todos los usuarios tengan cuidado y aportar un extra a la infraestructura de ciberseguridad y ciber resiliencia para garantizar que el enemigo oculto, es decir, el propio empleado, pueda filtrar información de la compañía”.

Asimismo, Silveiro apoyó la idea de involucrar a los diferentes departamentos de la organización para compartir ideas y ponerlas en común: “desde los directivos hasta los responsables directos de cada una de las áreas como seguridad, comunicación, acceso y contenido; el departamento de aplicaciones tiene que compartir sus datos, de qué tipo son y a cuáles

¿Cómo contribuye CITRIX a la ciber resiliencia de las empresas?
Nuno Silveiro, Responsable del área de Networking

han de tener acceso los empleados. Las redes tienen que estar controladas, porque al entrar desde el hogar, accede más gente. La experiencia de usuario es similar, pero con menos control", relató el participante de la mesa. Para ello, es fundamental "proteger el proceso de visibilidad, monitorización etc. Y desplegar mecanismos como factores múltiples de autenticación que incrementan la seguridad el dato. Si no se hace, serán vulnerables".

¿Cómo contribuye CYBERARK a la ciber resiliencia de las empresas?
Roberto Llop, Director regional para Sur y Este de Europa

Durante la pandemia y los momentos más duros de la COVID-19, la industria tecnológica ha vivido dos tipos de situaciones. "Hemos percibido que muchos proyectos estratégicos que las empresas iban a lanzar a principios de año se han aplazado. Pero ha habido que implementar los temas urgentes debido a las necesidades del momento y las organizaciones se han volcado mayoritariamente con los proveedores estratégicos para asegurar la cadena de suministro", comentó **Roberto Llop, director regional para Sur y Este de Europa de CYBERARK** durante la mesa redonda sobre ciber resiliencia de IT Events.

"En cuanto a la problemática en sí sobre que el perímetro ha desaparecido, nosotros, como proveedores de seguridad de la identidad y más concretamente de accesos e identidades privilegiadas, pensamos que las identidades se han convertido en el nuevo perímetro", apuntó Llop, quien destacó que la actividad, en este sentido, ha sido abrumadora. "Durante este confinamiento se han creado nuevas cuentas, accesos, credenciales privilegiados... Cuanto más acceso se necesita, más comunicación tiene que haber entre los distintos aplicativos. Además, los departamentos críticos como legal o finanzas requieren nuevos accesos y, por ende, se introducen nuevas vulnerabilidades que hay que abordar".

Asimismo, "la implementación de VPN o de VDI con sus correspondientes vulnerabilidades ha provocado que también se instalen tecnologías de acceso más modernas", dijo este participante de la mesa, quien destacó el incremento de vulnerabilidades en el puesto de trabajo detectado por su compañía. "Muchos empleados que no tenían conocimientos técnicos en ciberseguridad han podido ser atacados y ha quedado en evidencia que hay que pensar todo y no correr antes que andar", explicó Llop.

"Las organizaciones más ciber resilientes son las que han identificado cuáles son sus datos, sus activos más valiosos, sus amenazas, el im-

pacto que pueden tener en sus negocios y que han evaluado sus riesgos, pero la única manera de priorizar cómo se pueden tomar medidas para aumentar tu ciber resiliencia es adecuándose a una perimetración basada en ataques", continuó. Y es que, en opinión de Roberto Llop, las organizaciones no miden suficientemente bien cuál es su capacitación de ciber resiliencia. "En nuestras encuestas hemos observado que más del 53% de las organizaciones no realiza ningún tipo de test de estrés, aunque son muy valiosos para evaluar la posición de la empresa", dijo.

Para contrarrestar esto, desde Cyberark creen que una forma efectiva de gestionar los riesgos asociados a la resiliencia es gestionar la seguridad de la identidad. "Se ha hablado del tipo de ataques, pero nosotros tenemos muy claro que en la cadena de ataques no hay que impedir su infiltración inicial, porque la eficacia de estos ataques cada vez es mejor, sino contenerlos cuando entran para que no accedan a áreas de información de la empresa cada vez más críticas. Trabajando en seguridad de identidades, las organizaciones pueden tener su ciber resiliencia manteniendo sus activos".

Si hay un efecto tecnológico que ha generado la crisis por COVID, es que el cibercrimen ha aumentado. "Se produce el caldo de cultivo perfecto. Las compañías reducen su vigilancia y hay una mayor incertidumbre que los atacantes aprovechan", comentó **Luis Miguel Cañete, Channel Manager Spain & Portugal de F5 NETWORKS** durante la mesa redonda; "la mayor parte de fraudes han sido basados en bots utilizando credenciales legítimas para fines ilegítimos. Son ataques bastante sofisticados porque tienen tanto el mismo hardware como el mismo usuario que nosotros para acceder a nuestras aplicaciones".

La reacción natural, pero no adecuada, es tratar de poner una especie de pista americana entre el usuario y la aplicación para que la validación sea correcta. "Esto genera muchísima fricción en el usuario. Es verdad que reduce los intentos de acceso no autorizado, pero no rebaja significativamente el fraude porque los ataques que generan la mayor parte son muy sofisticados. En la era pre-covid teletrabajábamos el 5% de la población y ahora somos el 35%. En las primeras semanas, vimos un fuerte incremento de la demanda de acceso seguro a las aplicaciones. La mayor parte eran clientes que ya lo tenían implementado,

¿Cómo contribuye F5 NETWORKS a la ciber resiliencia de las empresas? Luis Miguel Cañete, Channel Manager Spain & Portugal

pero no estaba sobredimensionado a toda la plantilla. No obstante, hemos visto también un aumento en las soluciones de protección de la propia aplicación", continuó.

Desde el punto de vista de las ciber resiliencia de las organizaciones, Cañete señaló que las compañías con una estrategia cloud o multicloud son intrínsecamente más resilientes: "han adaptado un desarrollo de aplicaciones basadas en micro servicios y en contenedores, y esto hace que tengan un alto grado de automatización que les permite una mayor elasticidad, respuesta de reacción, portabilidad, recuperación, etc., comparadas con las compañías tradicionales basadas en aplicaciones monolíticas alojadas en un CPD". Asimismo, destacó "la falsa sensación de seguridad que generan los centros de datos cloud porque su infraestructura está disponible y es resiliente, pero la seguridad de las aplicaciones y los datos son responsabilidad de cada cliente y son necesarias soluciones consistentes en distintos escenarios de nube pública y privada".

Asimismo, durante la sesión, Cañete puso el acento en la educación. "La formación es vital y no basta con que haya un plan. Es necesario que los empleados lo conozcan a la perfección. En un crucero, lo primero que se hace es darles una actualización del plan a los empleados, y si ocurre algo todos conocen el procedimiento para que todos los pasajeros tengan su chaleco y su bote; en las empresas debe ocurrir lo mismo", matizó.

¿Cómo contribuye SOTHIS a la ciber resiliencia de las empresas?
Raúl Prieto, Responsable del dpto. Gobierno de Seguridad de Información

Para su análisis del nivel de ciber resiliencia de las organizaciones y de respuesta ante la situación vivida, **Raúl Prieto, responsable del departamento de gobierno de seguridad de la información de SOTHIS**, nos remite a su propia experiencia. "Contamos con clientes que disponen de un plan de continuidad de negocio y que han tenido que hacer ajustes leves porque tenían tecnologías y aplicaciones ya preparadas, aunque hasta que no ocurre algo así no sabes si las pruebas que has hecho son o no efectivas en un entorno real", señaló. "Las decisiones que se tomaron en las primeras semanas fueron más acertadas porque hubo un comité de crisis, un responsable de plan de negocio, una involucración del área de seguridad física, legal, de marca, y de comunicación interna. Hemos visto que las empresas que contaban con este tipo de planes han tenido una adaptación más ágil, pero los clientes que no contaban con un plan de continuidad de negocio o tenían poco alcance o más acotado, han improvisado. Nos han llamado y ha sido un caos, además de que hemos entregado portátiles, habilitado VPNs,

conexiones en remoto de forma segura, analizado riesgos en la parte de seguridad, etc. de una manera desbordada".

"La vuelta a la normalidad está siendo más costosa –reconoce–. El teletrabajo ha aumentado notablemente, así como las amenazas hacia los empleados y a la cadena de suministro. También nos hemos encontrado que los clientes desconocían los SLA de los proveedores críticos, ni los datos del CISO, ni qué usuarios pueden o no acceder a sus sistemas", continuó. Igualmente se detectaron problemas a nivel organizativo y legal. "Desde elaborar normativas de teletrabajo, códigos disciplinarios, etc... Esta situación ha servido para poner en valor la importancia de contar con un plan de continuidad", destacó Prieto.

"Para que los planes salgan bien, tienen que intervenir un responsable de continuidad de negocio que no tiene por qué tener un perfil tecnológico, y tiene que haber una comunicación entre todas las áreas: seguridad física, la parte de instalaciones, jurídica, DPO, comunicación interna y externa. La continuidad no solo es responsabilidad del CTO o el CISO, sino que tiene que intervenir toda la empresa y ser supervisado por el comité de dirección", concluyó. ■

CONCLUSIONES

Javier Carvajal, experto en ciberseguridad y director general de ICRAITAS, colaboró en este evento aportando su visión sobre cómo habían vivido las empresas estos tiempos convulsos de pandemia, de qué manera habían afectado a sus operaciones y cómo se habían comportado las organizaciones para tratar de minimizar el impacto en los negocios y recuperar la actividad en el menor tiempo posible. A continuación, puedes ver los principales puntos de esta situación y algunas recomendaciones para ser más ciber resilientes.

ICRAITAS
Javier Carvajal, experto en ciberseguridad

MÁS INFORMACIÓN

Ciber resiliencia: cómo garantizar la continuidad del negocio ante contingencias globales