isms forum | INTERNATIONAL INFORMATION SECURITY COMMUNITY

CSC CYBER SECURITY CENTRE

CYBER SECURITY STRATEGY

LA CIBERSEGURIDAD, UN ELEMENTO CLAVE FRENTE AL CAMBIO

IX FORO DE LA CIBERSEGURIDAD

ORGANIZADO POR EL CYBER SECURITY CENTRE (CSC) DE ISMS FORUM

SEPTIEMBRE 2020

PROTAGONISTA
Carles Solé (Banco Santander)
El CISO en tiempos de pandemia

FIRMA INVITADA
Roberto Baratta (ABANCA)
Resiliencia digital

ENTREVISTA
Eduardo Di Monte (OYLO)
Ciberseguridad y continuidad de negocio

www.ismsforum.es

Los pilares de la nueva sociedad de la información

BUSCAR EL ESPACIO COMÚN DE CONSENSO

Las nuevas tecnologías han irrumpido con fuerza en nuestra sociedad. Esto es un hecho que va mucho más allá de la adopción de los *smartphones,* o cualquier otro *smartdevice,* que vamos realizando a nivel individual. En la actualidad, la sociedad del bienestar se sustenta en una economía que tiene sus cimientos en las TIC (tecnologías de información y comunicaciones). De hecho, me costaría identificar empresas que, con independencia del tamaño, no hagan uso intensivo de las nuevas tecnologías en su modelo operacional. Esta dependencia, nos guste o no, incide directamente en nuestro modelo de vida, sea cual sea el grado de aceptación que cada uno tenga de estas nuevas tecnologías. Por poner un ejemplo muy simple, las empresas que prestan los servicios necesarios para que podamos encender la luz o llenar un vaso de agua dependen en gran medida de las TIC.

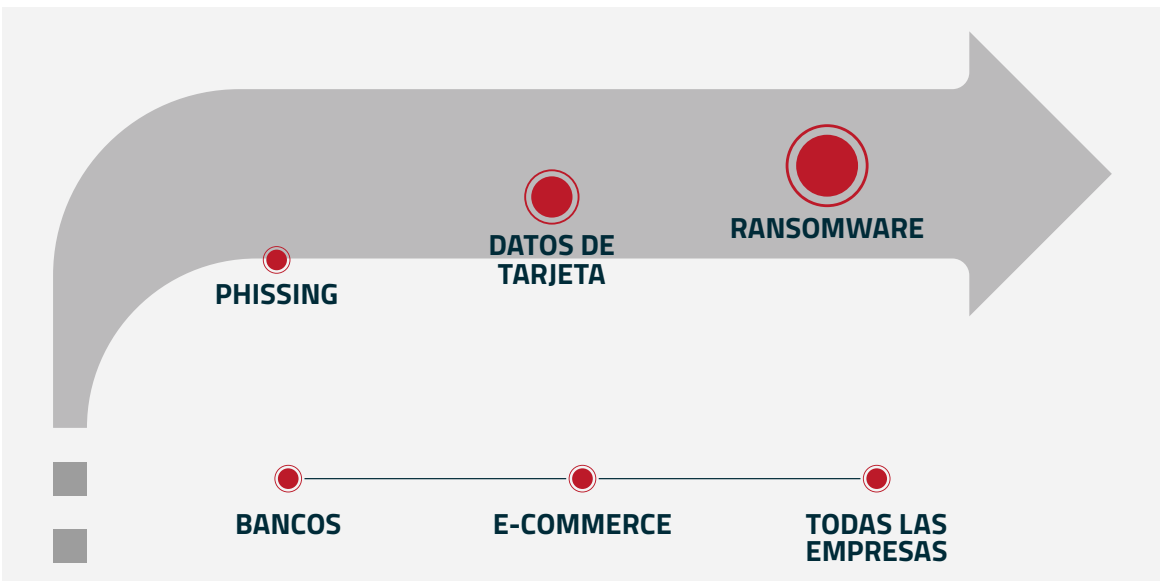
Este escenario, que ha cambiado mucho durante los últimos años, nos sitúa en un entorno muy complejo, no tanto por la adopción de las TIC (que ha sido relativamente gradual), sino porque ahora existe una mayor influencia de las TIC en todo tipo de contextos y esto abre un escenario de riesgo mucho mayor. Es evidente el importante impulso, y la creciente influencia, que ha venido desarrollando la industria del cibercrimen, que ha encontrado en el ámbito empresarial un ecosistema de crecimiento muy favorable.

> **En la actualidad, la sociedad del bienestar se sustenta en una economía que tiene sus cimientos en las TIC**

LA MAGNITUD DEL CIBERCRIMEN

Esta es una realidad que, como sociedad, nos está costando asumir, aunque los datos muestran una dura realidad. Si nos fijamos en los informes reportados por la unidad del FBI especializada en cibercrimen (IC3, Internet Crime Compliant Center),se puede observar un crecimiento considerable en las pérdidas derivadas de este tipo de acciones: desde los 1.100 millones de dólares en 2015 hasta los más de 3.500 millones de dólares en 2019, con un incremento especialmente importante en los dos últimos años (2018 y 2019).

Además, todo esto teniendo en cuenta que encontrar información sobre el cibercrimen es una tarea complicada, ya que normalmente debemos basarnos en datos parciales e incompletos que escoden aún más la magnitud real del problema. Es más, el propio FBI informa que solo se incluyen importes de pérdidas directas, sin tener en cuenta datos relacionados con lucro cesante,



interrupción de negocio, servicios profesionales de seguridad, etc.

Aunque el primero de los sectores que se vio amenazado directamente por la ciberdelincuencia fue el bancario, estas amenazas se han trasladado también a otros ámbitos como es el del eCommerce, buscando aprovechar la facilidad de monetización de los datos de tarjetas de crédito. A día hoy, el auge del *ransomware* o de las criptomonedas se ha traducido en un movimiento que se conoce como la "democratización del cibercrimen", y que expone a todas las empresas —con independencia del sector— al cibercrimen. De hecho, el crecimiento estimado de este tipo de prácticas es de dos dígitos altos. Esta situación está suponiendo un auténtico baño de realidad para las empresas, y pone sobre la mesa el riesgo al que están expuestas las TIC, que trasciende a la sociedad del bienestar.

UN NUEVO MUNDO

Como me recordaba un buen compañero de profesión, esta situación, salvando algunos aspectos temporales, es parecida a la que se vivió en el ámbito del transporte marítimo tras el descubrimiento del "nuevo mundo" (siglo XVI). Se trataba de un nuevo dominio que ha necesitado de cierto tiempo, y de un consenso común entre todos los países, para poder asentarse, desarrollarse y establecerse como uno de los pilares del comercio de los últimos siglos.

Algo similar ocurre con el ciberespacio. Se trata de un dominio emergente, que ofrece muchas posibilidades a la hora de mejorar el bienestar de la humanidad, pero también encara un conjunto de retos a los debe enfrentarse, y que ponen en riesgo el auge de estas TIC y, por tanto, el mundo tal y como lo conocemos hoy en día. El reto principal es algo simple pero muy necesario, y de carácter sistémico: se fundamenta en la necesidad de un acuerdo entre todos los países sobre lo que se debe, o no, permitir en un ciberespacio común que dé sustento a la sociedad global que podamos construir.

EL CONVENIO DE BUDAPEST

En el pasado se realizó un pequeño intento, aunque esto es algo que ha quedado desfasado, muy limitado y, en la práctica, con escaso efecto. En este Convenio de Budapest, presentado en noviembre de 2001, unos pocos países (principalmente de la UE) acordaron un consenso mínimo sobre colaboración ante la ciberdelincuencia, principalmente orientado a ámbitos como la propiedad intelectual o la pornografía infantil. Su objetivo era conseguir una estabilización del ciberespacio, que permitiera el desarrollo de una economía digital de verdad. A día de hoy, el Convenio de Budapest es difícilmente reutilizable para la economía digital que está vigente en la actualidad. Hay que tener en cuenta que el ecosistema digital que existía en 2001 difiere prácticamente completamente de la realidad que vivimos hoy en día. En cualquier caso, muestra cómo los países pueden establecer un espacio de consenso común, aunque sea pequeño, sobre lo que puede construirse en el futuro, aun teniendo que dejar algunos intereses empresariales para avanzar en ese bien común.

DANIEL LARGACHA

Director del Centro de Estudios de Ciberseguridad

ISMS FORUM

ismsforum.es

> **Es necesario un acuerdo entre todos los países sobre lo que se debe, o no, permitir en un ciberespacio común**

ENTREVISTA
EDUARDO DI MONTE,
CEO de Oylo

DEMOCRATIZAR EL *THREAT INTELLIGENCE*
Prevenir o mitigar los ciberataques

01 **EDITORIAL**
Los pilares de la nueva sociedad de la información

05 **ACTUALIDAD**
Noticias de ISMS Forum

06 **FIRMA INVITADA**
El CISO en tiempos de pandemia
Por Carles Solé (Banco Santander España)

07 **ENTREVISTA**
Eduardo Di Monte,
CEO de Oylo

"En materia de ciberseguridad, la clave está en el cómo, más que el qué"

11 **LA CERTIFICACIÓN DE SEGURIDAD DE LOS SISTEMAS OT**
Por Alberto Francoso (Ministerio del Interior)

13 **RESILIENCIA DIGITAL EN LA NUEVA NORMALIDAD**
Por Roberto Baratta (Abanca)

15 **LA SEGURIDAD EN IOT**
Visibilidad, supervisión y segmentación

17 **DEMOCRATIZAR EL *THREAT INTELLIGENCE***
Prevenir o mitigar los ciberataques

19 **NUNCA CONFIAR, SIEMPRE COMPROBAR...**
Tres medidas sencillas para mantener tu empresa segura

20 **EL CIBERDELITO COMO DESAFÍO EMPRESARIAL**
detectar, comprender, contener y eliminar

21 **ANALIZAR Y PERFILAR LOS COMPORTAMIENTOS**
IOC y librerías *threat hunting*

22 **MODELO DE SEGURIDAD *ZERO TRUST***
Forcepoint Private Access

23 **RETOS DE SEGURIDAD PARA EL *ENTERPRISE OF THINGS***
Visibilidad y contexto de los dispositivos

24 **APROVECHAR EL POTENCIAL DE SASE**
Componentes de seguridad en todos los entornos

25 **PROTECCIÓN DE ENTORNOS COLABORATIVOS**
Rendimiento y seguridad a partes iguales

26 **DEFENSA CONTRA AMENAZAS INTERNAS**
Un tercio de ataques son causados por empleados

27 **LA MIGRACIÓN A LA NUBE**
¿Qué va mal y por qué?

7 OCT

REGIONAL CYBER SECURITY FORUM DE BARCELONA

isms BARCELONA

csc CYBER SECURITY CENTRE

isms GALICIA

csc CYBER SECURITY CENTRE

5 NOV

REGIONAL CYBER SECURITY FORUM DE LA CORUÑA

Ciberejercicios Multisectoriales

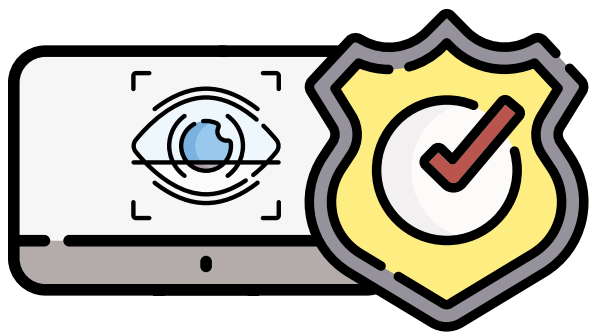
ISMS Forum pone en marcha una nueva edición de los Ciberejercicios Multisectoriales (CiberMS 2020). Su objetivo es el de generar concienciación sobre los riesgos en ciberseguridad y fomentar las buenas prácticas entre grandes organizaciones participantes. Básicamente, estos ejercicios se fundamentan en la evaluación de la resiliencia, la medición del estado de madurez y la mejora de las capacidades de detección y respuesta de las organizaciones en materia de ciberseguridad.

Este es un proyecto del Cyber Security Center (CSC) de ISMS Forum, uno de los grupos de trabajo de la Asociación, que fomenta el intercambio de conocimientos entre los principales actores y expertos implicados en el sector para impulsar y contribuir a la mejora de la ciberseguridad en España. La iniciativa se desarrolla a través de un conjunto de pruebas de seguridad y simulacros de ataque a los sistemas de las compañías españolas participantes. Se trata exclusivamente de poner a prueba los mecanismos de seguridad lógica de la entidad, así como la cultura de seguridad de los empleados y su capacidad para detectar y comunicar de forma correcta estos incidentes a los equipos de respuesta.

Dichas pruebas permitirán contrastar la relación entre los ataques lanzados y el impacto originado en la entidad participante, al tiempo que se comparan resultados con otras empresas en una representación anonimizada. La información obtenida durante la ejecución del proyecto será estrictamente confidencial.

La finalidad de los Ciberejercicios Multisectoriales es generar concienciación sobre los riesgos existentes a todos los niveles, reforzar la comunicación y la coordinación, entrenar a las empresas en la gestión de incidentes de ciberseguridad y, en definitiva, generar buenas prácticas sobre ciberseguridad en las organizaciones. Un año más, CiberMS pone de manifiesto el importante papel que tiene el sector privado en la ciberseguridad nacional y el bienestar de los ciudadanos, así como los beneficios de la colaboración público-privada. «

Observatorio de Ciberseguridad Nacional



ISMS Forum, junto con el board del Capítulo Barcelona, ha creado el Observatorio de Ciberseguridad Nacional, una plataforma para el desarrollo de indicadores que permite la puesta en común y el análisis de aquellas áreas que generan mayor preocupación, así como de los riesgos y retos más relevantes.

Desde 2011, el Cyber Security Centre, junto con ISMS Forum, se ha centrado en reunir a la mayor comunidad de expertos y organizaciones con interés y responsabilidades en materia de seguridad de la información, promoviendo la formación y excelencia de sus asociados. Por este motivo, pretende crear un estado de conciencia sobre la necesidad de la ciberseguridad para controlar y gestionar los riesgos derivados de la dependencia actual de la sociedad respecto a las TIC, un aspecto clave para asegurar el desarrollo socioeconómico del país. A través de estudios e investigaciones, reuniones mensuales, foros de debate, seminarios, y la estrecha colaboración con la Administración, el Observatorio Nacional de Ciberseguridad pretende servir de plataforma para el análisis del nivel de madurez, evolución y nuevos fenómenos en el ámbito de la seguridad de la información; la generación de indicadores nacionales sobre el estado de la ciberseguridad en empresas y entidades privadas y públicas; la promoción de conocimiento e investigación; la generación de métricas y referencias nacionales; o la argumentación para la interlocución con instituciones y reguladores.

El Observatorio Nacional de Ciberseguridad está dirigido a aquellas entidades públicas y privadas, socios corporativos e individuales, profesionales certificados (CCSP, CISA, CISM, CISP, etc.), consultoras, despachos y similares, que tienen por objetivo conocer el estado actual de la ciberseguridad en España. «

El CISO en tiempos de pandemia

CARLES SOLÉ
CISO
Banco Santander España
& Board Member
ISMS FORUM
ismsforum.es

MADUREZ Y COMPROMISO CON LA CIBERSEGURIDAD

La irrupción de la COVID-19 tomó al mundo por sorpresa. La rápida sucesión de acontecimientos provocó que gobiernos y compañías de toda índole se enfrentasen a decisiones vitales para su supervivencia ante una situación de crisis inesperada. Y a una velocidad sin precedentes. Un escenario de continuidad de negocio a escala mundial que, además, planteaba la adopción de medidas no convencionales o, al menos, no del todo contempladas hasta ese momento.

El teletrabajo masivo se convirtió en la principal estrategia. Primero por el cierre de las escuelas, que llevó a muchas familias a quedarse en casa con los niños. A los pocos días, el estado de alarma, que supuso el confinamiento general de la población. De la noche a la mañana plantillas completas de empleados que nunca habían trabajado desde casa iniciaron su andadura en un modelo que tanto debate ha suscitado durante años.

ACELERAR LA DIGITALIZACIÓN

Los equipos de tecnología fueron auténticos héroes habilitando en tiempo récord las infraestructuras necesarias: VPN, VDI, compra y plataformado de equipos, ampliación de comunicaciones, etc. Además, dando soporte en 24x7 al negocio. Pero, con tanta premura, cabía preguntarse si se contemplaban todos los riesgos, y las miradas se posaron en los CISO. Aquí la anticipación, la madurez y el compromiso con la ciberseguridad es lo que marcó la diferencia. Con los controles adecuados, el puesto de trabajo puede resultar igual de seguro en la oficina que en casa. Donde ya estaba el modelo implantado, la respuesta del CISO fue sencilla. Pero en otros casos, y sin opción de oponerse al teletrabajo, no quedó otra que asumir riesgos y acelerar, en la medida de lo posible, la implantación de nuevos controles.

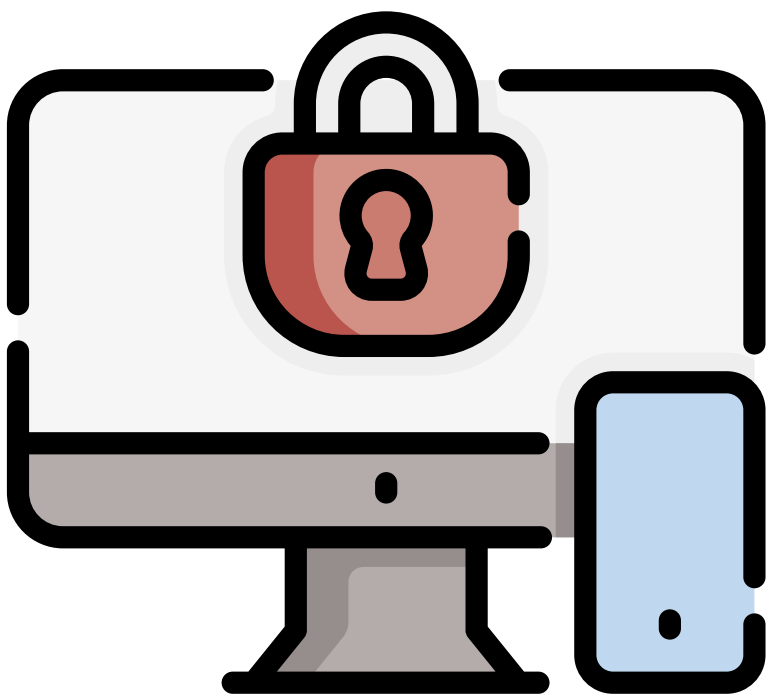
El rol de ciberseguridad durante los primeros meses de la pandemia también permitió acelerar la digitalización de muchos procesos en un momento en el que no era posible, en muchos casos, salir de casa. Los cambios en la Administración fueron muy significativos, de pronto podías realizar gestiones que antes eran presenciales y tediosas. Además, cabe esperar que la experiencia nos sirva a todos para quedarse, como en la ejemplar Estonia. Detrás de esta transformación, los CISO deben acompañar y apoyar los cambios, analizando los riesgos y buscando la mejor forma de mitigarlos.

ANTICIPACIÓN, REACCIÓN Y COLABORACIÓN

Por desgracia, y como viene ocurriendo en cualquier crisis, también los criminales acaban encontrando formas ingeniosas de sacar provecho. Se incrementan los engaños y las estafas por internet, a una población que vive momentos de incertidumbre y está ávida de información. El rol de los CISO es fundamental, ya no sólo dentro de sus empresas, protegiendo a sus clientes y empleados, sino en su dimensión colaborativa aunando fuerzas y experiencias para combatir lo que hace tiempo se ha convertido en una amenaza global.

La pandemia pasará, pero muchos de los cambios que ha conllevado van a quedarse, y aquí es donde los CISO ponen en valor su capacidad de anticipación, de reacción y de colaboración, convirtiendo esta crisis en oportunidades de mejora para los negocios y para la sociedad.

> **Con los controles adecuados, el puesto de trabajo puede resultar igual de seguro en la oficina que en casa**



En materia de ciberseguridad, la clave está en el cómo, más que el qué

Ingeniero en telecomunicaciones, y con una amplia formación en el ámbito empresarial y tecnológico, ha desarrollado su carrera profesional en el ámbito de la ciberseguridad industrial y de continuidad de negocio. Sus responsabilidades han incluido desde proyectos de consultoría e implementación en firmas como HP o KPMG, hasta el desempeño de roles directivos de seguridad y coordinador de crisis en Grupo Agbar (ahora Suez) para LATAM, y después, CISO a nivel global para esta multinacional. Hace cuatro años fundó Oylo Trust Engineering.

EDUARDO DI MONTE,
CEO de Oylo

¿Hoy en día se es consciente de la importancia de la ciberseguridad?

Durante los últimos años la ciberseguridad ha evolucionado mucho y se ha convertido en algo muy importante en todo tipo de ámbitos, aunque es cierto que la velocidad de este cambio ha sido diferente en función del entorno de aplicación, del sector, del tamaño de las organizaciones, de la geografía... Por ejemplo, la relacionada con IT tiene un nivel de madurez adecuado en cuanto a inversión, porque lleva muchos años desarrollándose, pero la que tiene que ver con OT (sistemas de operación) está todavía un tanto descuidada.

En cuanto a sectores, hay algunos que se han puesto a trabajar claramente en ello, pero hay otros cuya evolución está siendo más lenta y necesitan imprimir mucha más agilidad a este tipo de inversiones para poder reducir el periodo de riesgo. Me estoy refiriendo, sobre todo, a aquellos sectores que tienen una alta dependencia de la automatización en sus procesos de negocio, tales como los relacionados con minería, industria, fabricación, alimentación, energía eléctrica, etc.

Es importante resaltar que para que esta evolución sea posible es necesaria una interlocución a tres bandas, en la que se involucre a la alta dirección (que es quien toma

la decisión), el CISO (que es el responsable de llevarla adelante) y también al dueño del negocio. Estos tres pilares deberían ir de la mano, hablar un mismo idioma y estar alineados en este camino. De hecho, la velocidad de este avance suele estar limitada por la coordinación de estos tres elementos: alta dirección, CISO y negocio.

¿Hoy es más difícil mantener los sistemas protegidos que hace unos años?

No. No hay un *gap* tecnológico muy importante entre las tecnologías de protección y las amenazas existentes, aunque es verdad que todo lo relacionado con las ciberamenazas siempre va un paso por delante por su modus operandi. El *gap* está en el modo en el que llevamos adelante estas medidas de protección.

La clave para responder de forma adecuada antes los problemas de seguridad está en el modo en el que se implementan esas protecciones. Si se despliega una estrategia correcta, y se implementa una tecnología adecuada en tiempo y forma, su grado de protección es bastante elevado y el riesgo disminuye de forma considerable.

La respuesta no llega tanto a través de las tecnologías, sino más bien en la forma y el modelo de despliegue, y en la estrategia que se sigue. Esto es lo que marca la diferencia. La clave está en el cómo, más que el qué. Nosotros nos encontramos muchas empresas que han desplegado tecnologías en entornos OT que no están bien implementadas, y que no aportan nada.

¿Los entornos OT son los que más deben mejorar?

Es evidente que, en el ámbito de la OT, el grado de madurez en ciberseguridad es muy inferior al de IT. La razón es evidente: hablamos de plataformas que tienen un ciclo de vida muy largo —diez, quince o veinte años— y, lógicamente, esos sistemas no están preparados para las amenazas que están surgiendo ahora. Se diseñaron sin pensar que podían existir este tipo de desafíos. Por el contrario, en el ámbito de los sistemas de información tradicionales, el ciclo de vida es mucho más corto: entre tres y cinco años.

Pero, además, un sistema de control industrial no se puede actualizar de un día para otro porque, dependiendo del entorno, la inversión puede ser muy alta. De hecho, la solución adecuada no pasa por cambiarlos, sino por agregarles componentes específicos multimarca que soporten y disminuyan este riesgo.

Por otra parte, en ocasiones se tiende a tratar del mismo modo un sistema IT y OT. Se suele utilizar la misma metodología y proveedores para implementar algo que no tiene nada que ver. Estamos hablando de otro tipo de protocolos y lenguajes, de problemas diferentes o, incluso, de distintos responsables del proceso: en un lado tienes un CIO y en el otro el dueño de la planta. Además, el impacto no es comparable, dejar sin ordenadores a un número de empleados es radicalmente diferente a lo que ocurre cuando se para una planta de fabricación o, por ejemplo, cuando dejan de funcionar servicios que son esenciales para la población.

Utilizar la misma metodología y estrategia en IT y en OT es erróneo. Aunque en ambos casos hablemos de tecnología, son dos contextos diferentes y requieren de un grado de especialización, de una estrategia y de una forma de trabajo específica.

Garantizar esta continuidad de negocio es clave

La ciberseguridad y la continuidad de negocio son dos aspectos esenciales, que deberían ir siempre unidos, trabajar de forma conjunta. La ciberseguridad busca contrarrestar una amenaza que puede poner en jaque a la compañía y, justamente, la continuidad de negocio actúa cuando esa amenaza se materializa y pone en riesgo el funcionamiento del negocio. De hecho, su objetivo es garantizar que la recuperación ante un incidente sea lo más rápida posible y con el menor impacto.

En mi experiencia, hay todavía muchas organizaciones en las que estos dos ámbitos trabajan de forma separada y, en algunos casos, ni siquiera existe un área específica dedicada a la continuidad negocio. Para corregir esto es necesario contar con un modelo de gobernanza

> **El nivel de madurez de la ciberseguridad en IT no tiene nada que ver con la que existe en OT**

CONTAR CON UNA BASE SÓLIDA

Cada vez más, la ciberseguridad se está apoyando en todo tipo de tecnologías (automatización, inteligencia artificial y *big data,* biometría...) para garantizar la protección de los activos. ¿Cuáles son las más importantes y cómo se utilizan?

En cualquier caso, para poder incorporarlas a las políticas de ciberseguridad con garantías es esencial tener hechos "los deberes" con anterioridad. *"Automatizar, orquestar o aplicar tecnologías —como inteligencia artificial, big data o identificación por biometría, aportan un valor muy importante al modelo, pero requieren contar previamente con unos cimientos sólidos en materia de ciberseguridad".*

"Adoptar este tipo de tecnologías sobre una base de arena no tiene mucho sentido".

apropiado, que garantice que ambas áreas interactúan en los comités, en los planes de inversión, en las pruebas y en los proyectos.
Hay que conseguir que ambas áreas estén sincronizadas y trabajen como un equipo, más allá de que tengan liderazgos distintos o estén unificadas. Unificar los esfuerzos en ciberseguridad para disminuir los riesgos, y en las áreas de continuidad a la hora de restablecer los servicios críticos en función de esas amenazas.

> **El grado de especialización, la madurez en ciberseguridad y continuidad no tiene nada que ver con el valor de la marca**

Otra de las amenazas claras está relacionada con la gestión de la ciberseguridad en proveedores
Efectivamente, ha habido algunos casos especialmente llamativos en los últimos meses y este tipo de amenazas ha pasado a un primer plano. Una de las lecciones que debemos aprender es que no se debe extrapolar la reputación, o el valor, de una marca a ámbitos tan diferentes como la especialización en ciberseguridad. La garantía de que un proveedor sea resiliente se consigue a través del esfuerzo y de contar con una estratega adecuada, y eso no tiene nada que ver con el valor de su marca o el tamaño de su organización.
Muchas veces hablamos de grandes marcas que pareciera que tienen que ser especialistas en absolutamente todo lo que hacen y no necesariamente es así. Porque una marca tenga mucha reputación, incluso aunque sea en el ámbito de la tecnología o de la seguridad, no significa que sean expertos en lo que quieren vender ni que tengan un modelo de resiliencia y continuidad impoluto. Seguramente, una empresa de menor tamaño, especialista en este ámbito, cuente con un modelo perfecto en cuanto resiliencia y continuidad de negocio.
Especialmente cuando hablamos de proveedores, asociamos el valor de la marca al grado de ciberseguridad y de residencia que puedan tener. Esa garantía como proveedor en la cadena de suministro se otorga a través de pruebas reales en su modelo de resiliencia y de ciberseguridad, garantizando que la aplicación interna sea consistente. Esto es lo único que garantiza que la cadena de suministro no salga perjudicada. Asociar eso a un valor de marca es erróneo.

UN ENTORNO ESPECIALIZADO

La comunicación entre profesionales es clave en materia de ciberseguridad. Entidades como ISMS Forum favorecen el necesario intercambio de conocimiento en un entorno especializado y agnóstico. Potenciar la colaboración entre los profesionales que trabajan en empresas cliente, y también entre proveedores especialistas en la materia, resulta fundamental.
El CISO de una empresa tiene un conocimiento muy claro de su organización y de cómo llevar adelante la ciberseguridad, pero un proveedor especializado cuenta con un alto grado de experiencia acerca de cómo desplegar este tipo de tecnologías y estrategias. Fomentar la interacción entre ambos roles es muy interesante.

¿La capa directiva de las empresas es consciente de todos estos riesgos?
El grado de conocimiento de las empresas en cuanto a los riesgos existentes depende mucho de la interacción que exista entre el CISO y el responsable del negocio, del trabajo que se haga para contextualizar el escenario de amenazas, los riesgos existentes y la estrategia adecuada para poder darles respuesta.
Lo que sí es evidente es que la inversión en ciberseguridad tiene un retorno claro, aunque para hacerlo más "visible" es importante que toda la estrategia de protección ante amenazas esté muy ligadas a negocio, para que se vea claramente ese retorno. En el momento en el que nos alejamos del negocio, y nos volvemos muy técnicos, perdemos ese vínculo.
Cuanto más unidas estén ambas áreas (CISO y negocio), y trabajen de forma más conjunta, mayor visión tendrá el negocio del retorno de estas inversiones.

¿Hacer públicos los incidentes de seguridad puede ayudar a visibilizar este retorno?
Lógicamente, todo esto ayuda mucho a la hora de incrementar el grado de sensibilidad en torno a este tipo de amenazas, lo que afecta también a la inversión en este ámbito por parte de las empresas.
En cualquier caso, lo que sí es necesario es mejorar la gestión de las comunicaciones ante un incidente de seguridad. Es importante contar con una estrategia adecuada de comunicación durante todo el ciclo de vida del incidente, cuando se produce o se descubre, durante las distintas etapas de su gestión, cuando se cierra y, por supuesto, también más allá, durante el período que se abre tras la finalización. Además, esta comunicación debería afectar a todas las partes interesadas, tanto de forma interna en la organización como también a clientes, accionistas o los proveedores. La comunicación es un aspecto importante dentro de la disciplina de la continuidad de negocio. «

15 OCT

X ENCUENTRO DE CLOUD SECURITY ALLIANCE

isms forum
INTERNATIONAL INFORMATION SECURITY COMMUNITY

CSAES cloud security SPAIN alliance SM

La certificación de seguridad de los sistemas OT

EL PAPEL DE LA COLABORACIÓN PÚBLICO-PRIVADA

Tradicionalmente, el desarrollo de los sistemas OT** (operational technology **o tecnologías en el ámbito operativo) ha corrido en paralelo, y de forma independiente, al de los sistemas IT. De hecho, durante años ha sido considerados distintos porque sus funciones, y su propia idiosincrasia, así lo aconsejaban.

Los sistemas OT fueron diseñados pensando en la continuidad de negocio. Si alguna de las dimensiones de la seguridad era tenida en cuenta, era la disponibilidad, ya que se concebían como sistemas aislados trabajando en entornos controlados, que no requerían la implementación de medidas relacionadas con la integridad o la confidencialidad. Lo importante era mantener la producción de manera permanente, ya que, en caso de parada afectaría a la producción industrial, lo que conllevaría inevitablemente perjuicios económicos.

Este diseño, basado en la producción y en entornos aislados, tradicionalmente no ha hecho necesarias medidas de protección tales como control de acceso a los sistemas, antivirus, defensas perimetrales o generación de eventos, entre otras. Además, la imposibilidad de la parada de los sistemas de manera frecuente, debido a los perjuicios económicos que conlleva, impide actualizaciones periódicas de los sistemas operativos y de las aplicaciones, con el consiguiente riesgo ante vulnerabilidades que puedan presentar.

SUBSANAR LOS *GAPS*

No obstante, la creciente interconexión entre los sistemas OT e IT ha cambiado radicalmente el enfoque de la seguridad y, en la actualidad, los procesos de certificación exigen el mismo nivel de seguridad para ambos sistemas. Estas carencias por diseño en el ámbito de OT hacen imperativo consensuar, en un documento formal, las medidas compensatorias necesarias para eliminar estos vacíos o, al menos, mitigarlos.

Desde la Oficina de Coordinación de Ciberseguridad (OCC), dependiente del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad del Ministerio del Interior del Gobierno de España, estamos convencidos de que la existencia de un documento de este tipo facilitaría los procesos de consultoría y certificación. Además, darían a los CISO directrices claras para subsanar los *gaps* de seguridad que presentan los sistemas de operación industrial.

Actualmente, la OCC lidera un proyecto para confeccionar una guía en la que están trabajando diferentes acto-

res de la ciberseguridad española, entre los que se encuentran representantes de la Administración pública, fabricantes, consultores, universidades, asociaciones de profesionales del sector y operadores de servicios esenciales, principalmente.

Esta guía pretende ser un compendio de las carencias de seguridad en los sistemas de operación industrial identificadas por los actores implicados en su confección. La metodología para su confección se basa en la elaboración de un catálogo de las insuficiencias de seguridad identificadas, así como en la definición de las medidas compensatorias necesarias que se deben aplicar para subsanar cada una de ellas.

Tanto el citado catálogo como las medidas a aplicar, están siendo reportadas a la OCC por los actores implicados mediante la remisión de un documento formalizado donde se contemplan los aspectos a los que hemos hecho referencia. Además, también se encuesta sobre el periodo de moratoria que se considera necesario para exigir a los fabricantes, desde la Administración, medidas de protección al mismo nivel que los sistemas IT, entendiendo que, en esta interconexión de sistemas, el precario nivel de seguridad de los sistemas de operación podría comprometer al resto de los sistemas.

» COLABORACIÓN PÚBLICO-PRIVADA

La previsión es que, una vez recibidos todos los formularios, se realice una síntesis de la información aportada para poder elaborar un borrador que deberá ser consensuado por todos los participantes. Este consenso es realmente el elemento más importante del proceso, porque con él se pretende dar la fuerza necesaria al documento para su adopción generalizada en los procesos de consultoría y auditoría. De igual forma, debería servir para el establecimiento de las estrategias de seguridad por parte de los CISO en sus ámbitos de actuación, y en su caso, por parte de la Administración en la elaboración de una norma de obligado cumplimiento.

La OCC, así como antes el extinto Centro Nacional de Protección de Infraestructuras y Ciberseguridad, ahora Centro Nacional de Protección de Infraestructuras Críticas, han apostado decididamente por la colaboración público-privada. De hecho, se han establecido modelos de trabajo donde se pretende involucrar a los actores del ámbito privado en la elaboración de normas y procedimientos, teniendo en consideración sus intereses y necesidades. Esto permite establecer unas normas más justas y adecuadas para el desarrollo de las actividades para las que han sido dictadas.

Por último, pero no menos importante, un aspecto a considerar es la coordinación entre los distintos actores en ciberseguridad de la Administración pública española y, en algunos casos, europea.

La entrada en vigor de la Directiva NIS, y el Real Decreto-ley 12/2018 que la transpone en España, ha motivado que las distintas administraciones comiencen a dictar normas que pretenden regular el sector en el ámbito de sus respectivas competencias. Esto ha generado un alto volumen de normativa en la que, en ocasiones, se exigen diferentes requisitos para el mismo requerimiento, incluso en algún caso, se contraponen. Esto ha generado, en estos últimos años, un desconcierto en los operadores a la hora de intentar satisfacer los requisitos legales.

En España, la transposición de esta normativa europea se ha realizado con cierto orden, gracias a que ya teníamos normativa similar desde el año 2011 con la Ley de Protección de Infraestructuras Críticas. Otra de las razones que han contribuido a simplificar esta transposición en España han sido los esfuerzos que están realizando los ciberactores estatales, entre los que destaco especialmente al Centro Criptológico Nacional (CCN) y al Instituto de Ciberseguridad Español (INCIBE), para reconocer la normativa propia existente y coordinarla con la que se está generando como consecuencia de la mencionada transposición. Conseguir una normativa coordinada, coherente, sencilla y eficaz, es el objetivo que todos nos hemos marcado. «

ALBERTO FRANCOSO

Jefe del Servicio de Análisis de la Ciberseguridad y la Cibercriminalidad de la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior

> **En la actualidad, la creciente interconexión entre los sistemas OT e IT ha cambiado radicalmente el enfoque de la seguridad**

INVERSIONES EN SEGURIDAD

Por una parte, la Administración es consciente de la enorme inversión que se ha realizado por parte de los operadores, en sistemas que están diseñados para una vida útil de entre veinte y treinta. De esta forma, no se puede obviar que, durante los próximos años (al menos a medio plazo) tendremos que tener en cuenta esta situación a la hora de securizar los sistemas. Pero, por otro lado, la demanda del sector, especialmente de los operadores, pasa por que los fabricantes incorporen medidas de seguridad en la fabricación de los nuevos productos de operación industrial. Por lo tanto, desde la Administración se debería pensar en establecer un periodo de carencia razonable a la obligación del cumplimiento de la normativa, en tanto en cuanto los operadores pueden sustituir los viejos sistemas OT por otros más modernos y los fabricantes pueden adaptar sus productos a las nuevas demandas.

ROBERTO BARATTA

Director of Loss Prevention, Business Continuity and Security & DPO at ABANCA & Board Member

ISMS FORUM

ismsforum.es

Resiliencia digital en la Nueva Normalidad

EVALUAR RIESGOS Y GESTIONARLOS

El perímetro de los servicios digitales desapareció hace años, cuando el cliente, el usuario o el individuo se dio cuenta de cuándo y qué tecnología utiliza, y para qué servicios específicos necesita o desea utilizar. Las empresas y organizaciones, salvando a unas pocas muy reacias, todavía se encuentran unos pasos atrás de este escenario eminentemente digital.

En la actualidad, vivimos tiempos increíbles. Más allá de la necesidad de lidiar con un escenario en el que debemos crecer exponencialmente en un contexto de transformación digital (incluso sin tener una idea clara de lo que significa), garantizando un contexto de negocio seguro, confiable y eficiente; sino que, además, nos despertamos hace pocos meses teniendo que resolver un escenario de pandemia global que ni las más finas teorías conspirativas hubieran podido imaginar.

DÓNDE ESTAMOS Y DÓNDE ESTAREMOS

En esta nueva situación, todos —individuos, organizaciones y empresas— nos vemos obligados a avanzar muy rápidamente y a volver a poner sobre la mesa los oxidados planes de digitalización que habíamos pensado hace tiempo. Esto significa aumentar los riesgos, teniendo en cuenta la necesidad que se ha planteado para hacer las cosas apresuradamente, en un escenario especialmente complejo que, además, está aquí para quedarse.

> **Es hora de tomar un café y sentarse para averiguar dónde estamos y dónde se espera que estemos en el futuro próximo**

En el actual escenario, los problemas de seguridad cibernética son los mismos, pero ahora han aumentado con el uso masivo de servicios y comunicaciones en remoto.

» La continuidad operativa y las operaciones comerciales se vuelven críticas cuando la curva ascendente de la adopción digital comienza a apuntar al cielo a ritmos nunca antes vistos.

» La gente necesita concienciación y formación, ya que los estafadores están por todas partes y ya son digitales.

» Los vendedores y proveedores están ofreciendo soluciones y servicios listos para usar, mientras que ellos también se ven afectados.

» Por su parte, la privacidad está en todas partes, lo que requiere un alto nivel de perspectiva de cumplimiento e interacción con el cliente.

Por lo tanto, es hora de tomar un café y sentarse para averiguar dónde estamos y dónde se espera que estemos en el futuro próximo: el próximo mes, trimestre, año... en términos de asegurar las capacidades digitales, la gestión de riesgos y la respuesta a incidentes.

RESILIENCIA ORGANIZACIONAL

Comencemos a revisar lo que realmente importa en cualquier organización. ¿Qué procesos y servicios son relevantes para los números, para la reputación y para la perspectiva de cumplimiento?

Hoy en día nos enfrentamos a un problema de índole sanitario que afecta de forma directa a las personas, que son lo más importante. El bienestar y la salud de los empleados, clientes y contratistas es una prioridad. Sin embargo, al mismo tiempo, debemos centrarnos en qué procesos son clave para desarrollar la misión de la organización, y cuáles tienen más impacto en la planificación financiera y estratégica. Además, también hay que tener en cuenta aquellas piezas relevantes, que son las que los sustentan: personas, infraestructura, cadena de suministro y datos. Si se adopta un enfoque detallado, esas piezas son los elementos esenciales de un sistema de información, que, junto con los procesos, constituyen el núcleo empresarial de una organización digital.

El desarrollo de un programa de resiliencia para una organización digital incluye la evaluación de los procesos críticos desde diferentes perspectivas (financiera,

de reputación, tecnológica, de seguridad, de continuidad...), los sistemas y servicios que los soportan (infraestructura, aplicaciones, comunicaciones...), los terceros y proveedores que participan en su mantenimiento (vendedores, *outsourcing*...) y, por supuesto, las personas involucradas (equipos críticos).

Solo si se dispone de esa información detallada será posible evaluar los riesgos a los que se enfrentan esos procesos y, por tanto, gestionarlos: aceptarlos, mitigarlos o transferirlos.

HIGIENIZACIÓN DE LA TI

En este punto, los marcos de control adquieren un nivel adicional de relevancia. El enfoque tradicional de los controles de seguridad, privacidad, continuidad y otros riesgos tecnológicos significativos debe ser revisado para que sea más efectivo y, sobre todo, más ágil. La aplicación de los controles en diferentes capas —la tecnología, los procesos y las personas que mantienen la coherencia y la eficiencia adecuada— no es una tarea sencilla. Además, teniendo en cuenta que no todo puede prevenirse, y que no todos los procesos y sus piezas tienen la misma prioridad y pertinencia, resulta fundamental mejorar todas las capacidades de detección y respuesta tempranas.

El concepto de "Higienización de la TI" aparece de repente, recordando a los gerentes de Tecnología de la Información —comenzando por el CIO y el CTO— la tarea que no se ha enfrentado con anterioridad. Se trata solo de un recordatorio de lo que ya sabían, pero en la actualidad es algo que está surgiendo de forma acelerada. Esa tarea incluye la obsolescencia, la aplicación de parches para hacer más robustos los sistemas, la gestión de la vulnerabilidad, el diseño y el desarrollo seguro, así como el control, la supervisión y el seguimiento.

> **El concepto de "Higienización de la TI" aparece de repente, recordando la tarea que no se ha enfrentado con anterioridad**

Además, siguiendo ese concepto, cerca del nivel operacional, pero, al mismo tiempo, vigilando el negocio, deben ubicarse las unidades de control, tales como el CISO, el oficial de protección de datos, de continuidad del negocio, de riesgo informático... Todos ellos deben prestar atención a sus capacidades para poder informar de forma precisa, completa y rápida sobre los riesgos a la organización, así como poder ofrecer las mejores opciones para gestionarlos reaccionando con los niveles de control adecuados.

ENFOQUE ÁGIL

En resumen, la denominada Nueva Normalidad requiere de un enfoque ágil, y trae consigo la oportunidad de revisar nuestras organizaciones y comprobar nuestra estrategia y planes digitales centrándose en lo que es realmente valioso para la empresa, especialmente en términos de resistencia.

Significa estructurar esa revisión respondiendo a tres preguntas difíciles.

» ¿Qué es importante para que la organización se mantenga estable, en funcionamiento y monitoreada? w.

» ¿Qué tecnología y servicios la apoyan? Sistemas de información.

» ¿Qué riesgos y amenazas están claramente identificados y qué control debemos reforzar? Cibernética y continuidad. «

La seguridad en IoT

VISIBILIDAD, SUPERVISIÓN Y SEGMENTACIÓN

El mundo está cada vez más conectado, y nuestros dispositivos también. El monitor de actividad de la pulsera que llevo sube los datos a mi móvil y este, a su vez, controla el sistema de entretenimiento de los coches conectados que tengo aparcados. Este mismo móvil es, además, una herramienta de comunicación indispensable para mi negocio. Con él consulto mis contactos, gestiono el correo electrónico, participo en videoconferencias y hago muchas otras cosas.

Cada vez más dispositivos se suman al mundo conectado: timbres, termostatos y hasta frigoríficos que comparten datos e instrucciones con teléfonos inteligentes y otros aparatos. Toda esta red (el llamado Internet de las cosas) y miles de millones de objetos ahora incorporan microchips y comparten datos por Internet. Además, con la llegada del 5G el número de dispositivos conectados se ha disparado.

La conectividad inalámbrica a gran escala ya es una realidad, pero la interconexión de tantos dispositivos y objetos entraña graves riesgos, ya que el nivel de seguridad de una red viene dado por su eslabón más débil. En el mundo conectado, un sensor que apenas cuesta un dólar puede estar conectado a una red valorada en mil millones. Los objetos llevan microchips integrados que actúan como sensores y miden parámetros como el calor o el desgaste. Son pequeños, ligeros y económicos, pero suelen carecer de sistemas de seguridad.

En un caso de *hacking* muy sonado, los atacantes se infiltraron en la red digital de un casino a través del termostato del acuario del vestíbulo, lo que les permitió hacerse con los datos personales de los clientes que más gastaban. Sin la protección adecuada, los sensores del IoT son sumamente peligrosos.

HAY QUE PONERSE FIRMES

Es lógico que a los directivos se les haga la boca agua pensando en las oportunidades comerciales que ofrece un mundo conectado, aunque también deben ser conscientes de los riesgos de seguridad. En reuniones de alto nivel, los CIO y los CISO deberían ponerse firmes e insistir en la importancia de las evaluaciones de riesgos, la visibilidad y la segmentación.

A medida que la conectividad ubicua se extienda los riesgos se multiplicarán, y las empresas necesitarán herramientas de inteligencia artificial y aprendizaje automático avanzadas para llevar un seguimiento de todos estos dispositivos. También les hará falta tecnología capaz de someter los dispositivos conectados a un análisis de amenazas. Los directores de información, y

los responsables de protegerla, tienen el deber de concienciar sobre los riesgos de la conectividad y explicar qué soluciones y presupuestos se necesitan para garantizar la seguridad.

La terminología es buen punto de partida. Para mí, IoT es un término publicitario que crea una falsa sensación de seguridad. Los empresarios suelen asociarlo a artículos de consumo como Fitbits y frigoríficos, y no se imaginan que tiene que ver con el Internet de las cosas industrial (IIOT), que controla robots, líneas de producción y otras redes industriales como las compuestas por tecnología operativa (TO) y sistemas de control industrial (ICS). Estas redes se utilizan, por ejemplo, en las centrales nucleares, que en su día fueron víctimas del famoso ataque Stuxnet. Estos sistemas ya están completamente segmentados, pero habría que tener en cuenta otro aspecto: la ventaja de un dispositivo inteligente es, en parte, que puede conectarse a otros y crear sistemas aún más inteligentes.

En un mundo en el que todo esté más conectado, los dispositivos IoT de consumo podrían utilizarse para penetrar en redes industriales. Supongamos que una empresa instala una máquina expendedora inteligente en sus oficinas y la conecta a Internet por wifi para que el proveedor la reponga cuando sea necesario. Lo más probable es que la máquina esté en la misma red que el sistema que controla la climatización del edificio y otras funciones. El problema es la vulnerabilidad a los errores humanos. En un momento dado, para ahorrar tiempo, podrían establecerse conexiones provisionales que luego nunca lleguen a desconectarse, o tal vez se tome la decisión de conectar las redes industriales y empresariales, lo que también entraña un riesgo.

En estos casos, algo tan sencillo como una falsa actualización del software cargada a una máquina expendedora autónoma podría acabar enviando código a una planta de producción y paralizar su actividad, haciéndole perder millones de dólares. Esto es algo que podría ocurrir. De hecho, ya ha habido casos de redes de cajeros en los que se ha inyectado código para redirigir los fondos.

» EL REMEDIO: LA VISIBILIDAD

Otra complicación añadida es que los dispositivos conectados utilizan un sinfín de protocolos y lenguajes para enviar y recibir datos. Aunque el software dotado de inteligencia artificial y aprendizaje automático es capaz de leer e interpretar estos lenguajes, el trabajo no se acaba nunca: a diario surgen nuevos dispositivos y servicios cuya supervisión solo será eficaz si el software se evalúa con frecuencia.

Para proteger una red, es importante identificar qué actividades son indispensables y tomar medidas para protegerlas. En el caso de las empresas manufactureras, lo más importante es la línea de producción, la maquinaria esencial debe estar segmentada y tener una conexión a Internet independiente de la que utilizan, por ejemplo, los departamentos de marketing, ventas y contabilidad. Para la mayoría de las empresas, solo entre el 5% y el 10% de sus operaciones son de importancia crucial. Segmentar estos activos es vital para que las operaciones estratégicas estén a salvo de los ataques.

Uno de los mayores riesgos del mundo conectado es que algo aparentemente inofensivo —como un sensor IoT integrado en un timbre o un acuario— podría acabar metiéndose en un flujo de comunicación equivocado, convertirse en un punto de entrada y acabar ocasionando graves perjuicios a una empresa.

Para hacer frente a estos riesgos, la segmentación debe formar parte de la estrategia de conexión de cualquier empresa. Habrá que definir el propósito de todos los dispositivos y objetos conectados a la red, y establecer restricciones para que cada uno se conecte únicamente a las partes de la red necesarias para su función. Con 5G, la segmentación se consigue con la técnica del *network slicing*, que divide los datos móviles en varios flujos aislados: si vemos un vídeo, seguramente lo hagamos en un flujo distinto al que se utiliza para una conexión telefónica. Así, el sistema se divide en secciones más manejables y, dado que las operaciones se segmentan y se mantienen separadas unas de otras, se refuerza la seguridad.

Para aplicar la segmentación a su negocio de manera global, las empresas deben analizar constantemente sus conexiones, sus dispositivos y sus objetos conectados, del primero al último, y saber exactamente para qué sirve cada uno.

> **La segmentación debe formar parte de la estrategia de conexión de cualquier empresa**

» CONECTIVIDAD UBICUA

El término IoT trivializa la conectividad y quita importancia a sus riesgos. Se puede interpretar de muchas maneras, desde la conexión de una impresora doméstica a un ordenador, hasta los sistemas de gestión de edificios y contadores inteligentes o, incluso, la relación con las redes industriales. Esta confusión complica la tarea de proteger y segmentar todos los objetos conectados a la red.

Por eso prefiero hablar de "conectividad ubicua", un término que hace hincapié en el hecho de que los dispositivos están interrelacionados. El IoT se presenta como una lucrativa oportunidad comercial, sin mencionar los peligros que supone. El concepto de conectividad ubicua deja más claro a los directivos que la conectividad tiene sus riesgos y que, por tanto, es importante que la visibilidad, la supervisión y la segmentación formen parte de sus estrategias de seguridad. «

GREG DAY

Vicepresidente y Director de Seguridad en Europa, Oriente Medio y África

PALO ALTO NETWORKS

paloaltonetworks.es

Democratizar el *threat intelligence*

PREVENIR O MITIGAR LOS CIBERATAQUES

En concepto threat intelligence *suele asociarse a elementos de las películas de James Bond: genios criminales y naciones-Estado conspirando para robar dinero y sembrar el caos, armas cibernéticas capaces de causar estragos, y oscuros callejones en los que se reúnen turbios malhechores... Por suerte para los que estamos al pie del cañón, gestionando la realidad cotidiana del* threat intelligence, *esta analogía no va más allá.*

El *threat intelligence* moderno es algo más que el ámbito en el que se mueve la élite de los agentes secretos. Más bien al contrario, la implementación de la "inteligencia" es un deporte de equipo, que afecta las operaciones cotidianas de manera mensurable. Aunque existen analistas expertos que comprenden las herramientas, técnicas y procedimientos utilizados por los sofisticados actores de las amenazas, y que son capaces de acceder a los selectos foros de la *dark web*, el trabajo que realizan solo es efectivo cuando se pone en manos de aquellos que están en la primera línea de los sistemas de defensa.

Los miembros del SOC, del equipo de respuesta a incidentes, del de gestión de vulnerabilidades, entre otros, pueden utilizar la inteligencia que recopilan para detectar y bloquear los ataques que se produzcan y evitar que se repitan más adelante. Así mismo, los líderes del sector de la seguridad pueden obtener conocimientos sobre las tendencias emergentes y el aumento del nivel de riesgo. La inteligencia puede impulsar una estrategia de seguridad proactiva cuando se pone a disposición de los equipos y tecnologías que mejor la pueden aprovechar.

> **Hay que poner la inteligencia al servicio de los equipos y tecnologías que mejor la pueden aprovechar**

» CONVERTIR DATOS EN INFORMACIÓN

El *threat intelligence* es el conocimiento que permite prevenir o mitigar ciberataques. Se basa en datos y proporciona un contexto que permite informar tus decisiones sobre aspectos de seguridad respondiendo a preguntas tales como quién te está atacando, cuáles son sus motivos y capacidades, y qué indicadores de riesgo se deben controlar en el sistema. Gartner lo define como un conocimiento empírico que incluye contexto, mecanismos, indicadores, implicaciones y asesoramiento sobre acciones en relación a una amenaza o riesgo existente o emergente para sus activos.

Las mejores soluciones de *threat intelligence* son aquellas que utilizan el aprendizaje automático para automatizar la recopilación y el procesamiento de información, integrarse con las soluciones ya existentes, y recibir datos no estructurados de diferentes fuentes para convertirlos en información contextual sobre indicadores de riesgo (IOC), y sobre tácticas, técnicas y procedimientos (TTP) de los atacantes.

El *threat intelligence* se divide en tres subcategorías:

» **Estratégica.** Tendencias generales pensadas para un público no especializado.

» **Táctica.** Descripción general de las tácticas, técnicas y procedimientos de los atacantes para un público más especializado.

» **Operativa.** Información técnica detallada sobre campañas y ataques específicos.

Hay que tener en cuenta que el *threat* intelligence solo es útil cuando proporciona el contexto que necesitas para tomar decisiones informadas y medidas acertadas, que es para todo el mundo, y que las personas y las máquinas trabajan mejor en colaboración. Vamos a desarrollar cada uno de estos puntos.

» CONTEXTO

Hoy en día, el sector de la ciberseguridad se enfrenta a muchos desafíos: atacantes cada vez más tenaces y retorcidos, avalanchas de datos irrelevantes, falsas alarmas en diversas soluciones de seguridad no conectadas, y una carencia de habilidades técnicas. Algunas organizaciones intentan incorporar fuentes de datos sobre amenazas a su red, pero no saben muy bien qué hacer con toda esa información: aumenta la carga de

trabajo de los analistas que, a menudo, no cuentan con las herramientas necesarias para decidir qué es prioritario e irrelevante.

El *threat intelligence* tiene que ser práctica, es decir, entregada en un formato que sea comprensible para su destinatario. Una manera de conseguir esto es integrarla de forma sencilla con todas las soluciones de seguridad ya existentes en el entorno. La extensión para navegador Recorded Future, por ejemplo, establece una capa por encima de todas las soluciones web de seguridad para proporcionar acceso a información —tales como calificaciones del riesgo, CVE, *hashes*, dominios y direcciones IP— directamente en el sitio web.

UNIVERSAL

El *threat intelligence* no es un ámbito separado pensado exclusivamente para los analistas de más alto nivel, aporta valor a todas las funciones de seguridad en organizaciones de todos los tamaños. Operaciones, respuesta a incidentes, gestión de vulnerabilidades o de riesgos, prevención del fraude, planificación o la toma de decisiones por parte de la dirección se benefician de la información contextual que aporta.

No obstante, para poder aprovechar estos beneficios sin añadir carga de trabajo, el *threat intelligence* tiene que integrarse con las soluciones y flujos de trabajo en los que ya se confía, y que son accesibles. Cuando se utiliza como una función aislada dentro de un sistema de seguridad más amplio, y no como una pieza esencial que multiplica la efectividad de todas las demás funciones, muchas de estos beneficiaros no tienen acceso a ella cuando la necesitan.

En raras ocasiones, los equipos de operaciones de seguridad pueden atender todas las alertas que reciben. El *threat intelligence* se encarga de filtrar y priorizar de manera automatizada las alertas y demás amenazas. Los equipos de gestión de vulnerabilidades pueden centrarse en las más críticas, valiéndose del *threat intelligence* para determinar cuáles suponen un mayor riesgo en función del panorama de amenazas externas. Así mismo, la prevención del fraude, el análisis de riesgos y otros procesos de alto nivel pueden ser enriquecidos con los conocimientos claves sobre los atacantes y sus tácticas, técnicas y procedimientos.

TRABAJO EN CONJUNTO

La capacidad de las máquinas para procesar y clasificar los datos brutos es varias órdenes de magnitud superior a la de los seres humanos. A la inversa, los seres humanos somos capaces de realizar análisis intuitivos y con visión de conjunto de una manera mucho más efectiva que cualquier inteligencia artificial, siempre que no se vean lastrados por la necesidad de realizar una actividad de investigación tediosa y de procesar volúmenes ingentes de datos. Cuando se combinan las capacidades de ambos, cada uno de ellos trabaja de manera más eficiente, ahorrando así tiempo y dinero, reduciendo el agotamiento y el desgaste, y mejorando la seguridad en general.

A la hora de construir un sistema de defensa efectivo es fundamental aprovechar, de la manera más eficiente posible, los miembros altamente cualificados de nuestro equipo. Un *threat intelligence* integral ayuda a los equipos de seguridad a identificar amenazas con mayor antelación y a resolver los incidentes más rápido.

Tanto si estás creando tu iniciativa de *threat intelligence*, como si llevas muchos años trabajándola, el principal objetivo es reducir el riesgo de manera eficiente. «

JAVIER CARRERAS

Southern Europe Sales Manager

RECORDED FUTURE

recordedfuture.com

ENRIC MAÑEZ

Responsable Seguridad Enterprise

AKAMAI

akamai.es

Nunca confiar, siempre comprobar...

TRES MEDIDAS SENCILLAS PARA MANTENER TU EMPRESA SEGURA

Recientemente, un asistente a un foro me preguntó si realmente yo pensaba que había algún modo de proteger a las empresas de los ataques de los delincuentes de hoy en día. Mi respuesta fue clara: si una empresa sigue los pasos adecuados, reducirá al mínimo su riesgo de ser atacada.

Los nuevos procesos e iniciativas empresariales han ampliado las superficies de ataque. Las aplicaciones, los usuarios y los dispositivos operan ahora fuera de las lindes de control corporativas tradicionales, difuminado lo que solía ser un perímetro de seguridad fiable. De esta forma, para proteger la actividad del negocio los sistemas de seguridad y las redes empresariales deben evolucionar.

Es ingenuo pensar que todas las empresas son capaces de asumir una transformación completa al modelo de seguridad *zero trust* de la noche a la mañana. La mayoría de las organizaciones necesitan un tiempo para implementar los cambios de red y de seguridad que supone dicha transformación.

> **Es ingenuo pensar en hacer una transformación completa al modelo zero trust de la noche a la mañana**

Para ponerla en marcha hoy mismo, podemos aplicar tres medidas que sirven de base para el cambio hacia un modelo de seguridad cuyo mantra es "nunca confiar, siempre comprobar".

Evaluar. La primera consiste en evaluar las amenazas para ganar visibilidad del entorno actual y determinar en qué medida están expuestos actualmente los dispositivos a amenazas como el *malware* o el *phishing*. Muchas redes ya han sufrido ataques de este tipo, y por ellas circula malware activo que ha pasado desapercibido eludiendo las medidas de seguridad existentes.

Se puede efectuar un control gratuito durante un mes y recibir un informe personalizado sobre las amenazas que están activas actualmente en su entorno, así como una serie de sugerencias —pensadas a medida— para combatir este tipo de amenazas avanzadas. Se trata de un proceso rápido y fácil de implementar que apenas supone cambios en la red.

Cambio de mentalidad. El segundo y más importante, conlleva un cambio de mentalidad. El acceso a la red debe limitarse exclusivamente a las aplicaciones que cada persona necesite. El acceso pleno incrementa su exposición a las amenazas. Para realizar este cambio de forma operativa, es aconsejable comenzar con las aplicaciones que permiten una transición más sencilla, como las de tipo web, y publicarlas conforme a los principios de la seguridad *zero trust*.

Una vez hecho esto, se debe realizar una evaluación de la arquitectura *zero trust* para desarrollar un plan integral de migración del estado actual a un marco "confianza cero". Esto incluye la categorización de los distintos perfiles de usuarios y aplicaciones, así como el desarrollo de un plan gradual personalizado para todas las soluciones (incluidas las locales heredadas).

Prescindir de las VPN. En tercer lugar, debemos sustituir la VPN tradicional para ciertos grupos de usuarios. No podemos confiar en los puntos finales de forma incondicional. Hay que prescindir de los métodos de acceso tradicionales (como los segmentos wifi o Ethernet corporativos con privilegios, o las VPN), a fin de desligarlos de la confianza que se les atribuye en las capas internas. Debemos otorgar los accesos basándonos en los principios de seguridad *zero trust* a los grupos de usuarios de alto riesgo, como los contratistas.

A continuación, hay que determinar un plan para suprimir gradualmente el acceso heredado de todos los usuarios.

Es fundamental adaptar la estrategia de seguridad de la empresa de forma continua, según los cambios que se vayan produciendo en el panorama empresarial y de amenazas. La migración a una arquitectura de seguridad *zero trust* permite proteger las aplicaciones, los usuarios y los dispositivos de una manera sencilla y eficaz, y puede lograr dicha transformación de forma progresiva, empezando por estas tres tareas básicas y prácticas que evitarán posibles amenazas. «

El ciberdelito como desafío empresarial

DETECTAR, COMPRENDER, CONTENER Y ELIMINAR

Mientras las organizaciones de toda España siguen luchando contra los trastornos que está causando la reciente pandemia de COVID-19, resulta fundamental no dejar de lado otra amenaza que no es reciente, pero que puede causar también grandes problemas y pérdidas: el ciberdelito.

Aunque durante los últimos meses las organizaciones han centrado gran parte de sus esfuerzos en equipar al personal para el trabajo remoto, así como a adaptar sus procesos de negocio a la "nueva normalidad", los ciberdelincuentes han estado también ocupados perfeccionando sus estrategias de ataque y mejorando sus armas para aprovechar el nuevo escenario de ataque que ha proporcionado el teletrabajo.

DELITOS ELECTRÓNICOS

En general, podemos definir dos categorías principales para clasificar a delincuentes cibernéticos: electrónicos (eCriminals) y gubernamentales (nation-state organizations). Aquellos que pertenecen al primero de estos grupos, los eCriminals, suelen estar interesados en obtener ganancias financieras, mientras que los delincuentes catalogados como gubernamentales están más centrados en obtener acceso a la propiedad intelectual de las distintas industrias, incluidas las empresas que operan en los sectores de telecomunicaciones, financiero o sanitario.

De entre todas las amenazas de ciberseguridad, las que se encapsulan en el ámbito del eCrime son las que han experimentado un nivel de incremento más elevado desde que apareció la pandemia por COVID-19 a principios de este año. De hecho, el equipo de inteligencia de CrowdStrike ha detectado un aumento especialmente importante en todo lo relacionado con los delitos electrónicos —de más del 330%— desde el comienzo de este año en comparación con lo ocurrido en 2019.

EL DESAFÍO 1-10-60

Combatir adversarios de este nivel de sofisticación requiere contar con una serie de armas capaces de prevenir, detectar y responder a las amenazas con rapidez y agilidad. Desde CrowdStrike se insta a las organizaciones a seguir la regla denominada "1-10-60" a la hora de combatir eficazmente las ciberamenazas más sofisticadas:

» Ser capaces de detectar las intrusiones en menos de un minuto.
» Investigar y comprender todas estas amenazas en menos de 10 minutos.
» Contener y ser capaces de eliminar al adversario del entorno en menos de 60 minutos.

Aquellas organizaciones que son capaces de cumplir esta regla 1-10-60 aumentan de forma importante las probabilidades de erradicar al adversario antes de que el ataque se extienda por toda la organización y se convierta en una auténtica brecha de seguridad, minimizando el impacto. La única forma de hacer frente a este desafío es la inversión en una serie de herramientas que proporcionen autentica visibilidad, detección, análisis y remediación a lo largo de todos los activos de la compañía. A través de estas soluciones, los responsables de seguridad de las organizaciones podrán tener —de una forma más sencilla— una visión mucho más cercana a la realidad acerca de las amenazas presentes, lo que les permitirá tomar rápidamente las decisiones más acertadas.

LA ANTIGUA NORMALIDAD

Los expertos creen que pasarán todavía muchos meses antes de que Europa vuelva a la "antigua normalidad", pero, aun así, la amenaza del ciberdelito perdurará. Desde Crowdstrike animamos a las empresas a dedicar esfuerzos ahora, y plantearse cuál es el nivel de eficacia de sus actuales medidas de protección, considerando que, en la actualidad, cuentan con una plantilla trabajando mayoritariamente de forma remota.

Si las empresas dedican ahora tiempo y esfuerzos a comprender cómo evolucionan estas amenazas de ciberseguridad, podrán estar en las mejores condiciones para prevenir un ataque ahora y en el futuro. «

> **La forma de hacer frente es la inversión en herramientas que proporcionen visibilidad, detección, análisis y remediación**

Analizar y perfilar los comportamientos

TRISTAN REED

International Presales Coordinator

CYTOMIC

cytomic.ai/es

IOC Y LIBRERÍA THREAT HUNTING

El primer paso para contener y erradicar un ciberataque es, sin duda, una detección temprana del incidente. De hecho, toda estrategia de ciberseguridad tiene que ser capaz de detectar lo antes posible la actividad anómala, identificarla y reaccionar rápidamente ante el incidente. Es aquí donde entran en juego una serie de herramientas avanzadas capaces de amplificar las capacidades del SOC (s*ecurity operations centers*) para poder distinguir entre la actividad esperada y las acciones anómalas que indiquen la presencia de una amenaza.

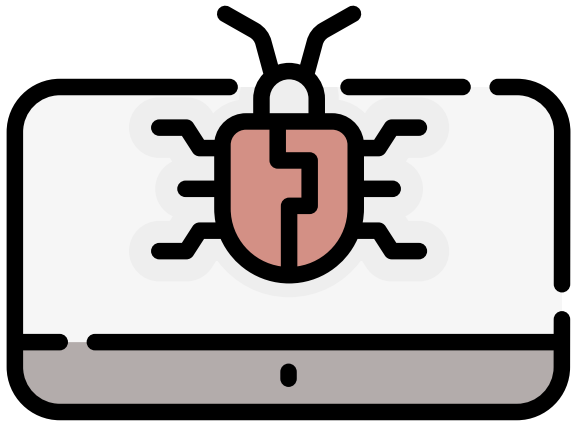
Para ello, es indispensable apoyarse en soluciones punteras y en recursos que proporcionen una visibilidad total del entorno y de lo que ocurre en él, algo que resulta fundamental para proteger cualquier infraestructura TI ante amenazas de ciberseguridad.

IDENTIFICAR LOS ATAQUES

Por un lado, de cara a agilizar la remediación de toda esta actividad anómala, hay que llevar a cabo un análisis avanzado de todos los eventos de seguridad para reunir su información en los IOC (indicadores de compromiso), que identifican ataques o vulnerabilidades, y es la evidencia de que una brecha de seguridad ha tenido lugar. Los IOC pueden identificar archivos o conductas previamente catalogadas como maliciosas: un email con intenciones de *phishing*, un archivo con *malware*, una filtración de datos, una distribución de IP para un uso relacionado con el cibercrimen, etc. Los IOC ayudan a analizar la naturaleza del daño y reaccionar ante él, bien sea eliminándolo o mitigando su efecto. Además, también son útiles para hacer un diagnóstico certero de lo que ha pasado y saber dónde radicó el problema.

> **Hay que realizar un análisis avanzado de todos los eventos de seguridad para reunir su información en los IOC**

En este punto es muy importante contar con un proveedor con soporte de búsqueda retrospectiva y en tiempo real en los IOC, así como reglas YARA en el *endpoint*. YARA es una herramienta que ayuda a identificar y clasificar muestras de *malware,* de manera similar a cómo lo hacen los antivirus tradicionales.



Ante un incidente de seguridad, buscar IOC mejora la identificación de dispositivos que están siendo atacados y, además, ayudar a tomar las medidas pertinentes para contener la brecha rápidamente. De esta manera, el equipo de TI tiene una mayor visibilidad del entorno y de lo que ocurre, lo que le permite adelantarse al problema y ponerle freno.

Por otro lado, para cumplir los estándares de efectividad a la hora de responder ante los incidentes, hay cinco pasos que se deberían seguir:

» Preparar un plan sólido de *incident response* que ayude a evitar las brechas.

» Una vez detectada la amenaza, determinar la causa del incidente para contenerlo.

» Hacer un "triaje", o protocolo de intervención, así como análisis de la situación.

» Contener el daño, erradicarlo y recuperarse ante él.

» Por último, aplicar los cambios adecuados a la estrategia de ciberseguridad para evitar que vuelva a ocurrir.

VISIBILIDAD E INTELIGENCIA

Es muy importante contar con las últimas tecnologías para poder actuar con proactividad en base a analítica de comportamiento a escala desde la nube. Herramientas como lo servicios basados en las librerías de Threat Hunting (Cytomic Orion), capaces de analizar y perfilar en tiempo real los comportamientos, o investigar y certificar todos los procesos que tienen lugar en el sistema informático buscando posibles anomalías.

Los indicadores IOC son útiles y muy necesarios para proteger de forma proactiva la ciberseguridad en cualquier organización y eliminar el peligro antes que se convierta en un incidente real. «

Modelo de seguridad *zero trust*

FORCEPOINT PRIVATE ACCESS

ELENA CERRADA

Country Manager

FORCEPOINT

forcepoint.com/es

El principio sobre el que se basa zero trust es que nada debe ser de confianza y siempre debe ser verificado. Básicamente, este es un modelo de seguridad de red basado en un proceso estricto de verificación de identidad. Este marco impone que solo los usuarios y dispositivos autenticados y autorizados pueden acceder de forma segura a la red, a las aplicaciones y a los datos. Al mismo tiempo, protege esas aplicaciones y usuarios frente a amenazas avanzadas que procedan de Internet.

Fue en 2010 cuando Forrester Research presentó la arquitectura *zero trust*, un modelo de seguridad basado en la ausencia de confianza, especialmente como sistema de protección, frente a los enfoques más tradicionales que históricamente se han centrado en la protección del perímetro de la red. Básicamente, se trata de llevar el foco hacia la verificación de identidad, con el objetivo de proteger los datos independientemente de donde estén ubicados.

Zero trust utiliza una verificación de identidad estricta para cada persona o entidad que intenta acceder a los recursos de red, independientemente de si se encuentra en la oficina enlazada por el perímetro de red o si accede a la red de forma remota. El principio sobre el que se basa es que nada debe ser de confianza y siempre debe ser verificado.

ENFOQUE EN LA NUBE

El propósito de Forcepoint es dar respuesta a los retos de seguridad del mercado, en nuestro caso España y Portugal, a través de una cultura de colaboración estrecha, poniendo un gran esfuerzo por ejecutar una estrategia compartida, focalizada, y con el objetivo de aportar a nuestros socios un valor único y diferencial.

Forcepoint pone a disposición de sus clientes soluciones de *zero trust* que brindan —de forma segura—acceso remoto a aplicaciones internas en centros de datos y nubes privadas virtuales, todo ello sin las complejidades, cuellos de botella y riesgos de que las VPN comprendan el comportamiento, la intención, el contexto y el riesgo de una acción específica que usuario trae a la empresa.

Es el caso de Forcepoint Private Access, que permite implementar un control detallado sin exponer las redes internas, y libera a los usuarios remotos de tener que trabajar de manera diferente o sufrir un rendimiento más lento en la nube. A diferencia de otros proveedores que ofrecen productos de acceso privado, Private Access protege las aplicaciones y las redes internas contra dispositivos y redes remotas potencialmente comprometidas, al tiempo que evita la pérdida de información confidencial o propiedad intelectual.

ZERO TRUST Y SASE

Además, la seguridad *zero trust* que propone Private Access libera a los usuarios de tener que trabajar de manera diferente cuando están en remoto y la convergencia de seguridad de SASE (*secure access service edge*) mantiene a las personas, los datos y los sistemas seguros. El modelo SASE está especialmente relacionado con la convergencia: en un momento en el que las organizaciones están más distribuidas que nunca, colocar pilas de hardware en cada ubicación, o usar productos dispares para los trabajadores remotos, crea agujeros para los atacantes, tiene un coste económico elevado, y resulta una carga para los escasos recursos de TI.

Las soluciones SASE proporcionan un "todo en uno" para ofrecer un modelo de seguridad avanzada que incluye tanto la protección web, como de la red y de los datos, así como el análisis del comportamiento de las aplicaciones y de los usuarios dondequiera que trabajen. Todo ello entendiendo la intención y el riesgo, y adaptándonos al *time-to-market*.

Teniendo en cuenta el escenario actual, las mayores oportunidades para Forcepoint en España se están dando en gran cuenta, un segmento en el que el potencial es muy grande y la aproximación con una propuesta integral de seguridad puede resolver sus necesidades de forma efectiva. En cualquier caso, también estamos detectando un importante interés en este tipo de soluciones por parte de organizaciones del segmento *mid market* o incluso pymes, áreas en las que estamos creciendo.

Retos de seguridad para el *enterprise of things*

VISIBILIDAD Y CONTEXTO DE LOS DISPOSITIVOS

JORGE HERMOSILLO WORLEY

Director Southern Europe-Balkans-Israel

FORESCOUT

forescout.com

En la actualidad, los dispositivos que se manejan a diario, o que están instalados, en las empresas representan un reto de seguridad muy importante para cualquier organización. Tanto en términos de cifras (miles de millones) como en lo referente a tipos (IT, OT, IoT, BYOD), lo que conocemos como *enteprise of things* o EoT está en plena expansión. Todos (empleados, proveedores, contratistas, *partners* y clientes) pueden conectarse a *datacenters* o a la nube desde cualquier lugar, tanto si es seguro como si no lo es, y esto añade complejidad a los entornos de red.

Las empresas modernas necesitan una planificación detallada, además de una serie de medidas que se lleven a cabo de forma automática, con las que sea posible proteger los dispositivos y a la propia empresa. Además, hay que tener en cuenta que muchos de estos sistemas de la EoT no son propiedad de la empresa, ni están gestionados por ella y, cada vez más, residen fuera del perímetro corporativo.

Según un reciente análisis del "EoT" realizado por Forescout, el mayor riesgo procede de los dispositivos del Internet de las cosas (IoT) que, no solo son difíciles de supervisar y controlar, sino que además, generan vulnerabilidades, ya que conectan la capa de lo cibernético con la de lo físico, que hasta ahora estaban separadas. De hecho, los dispositivos IoT pueden suponer puertas de entrada a las redes, así como objetivos prioritarios de *malware* especializado.

> **Para ser eficaz, una solución debe ofrecer una visibilidad total de los dispositivos sin necesidad del uso de agentes**

PLANIFICACIÓN POR PARTE DE LOS CISO

Es evidente que hay tendencias de ciberseguridad que exigen un mayor grado de planificación por parte de los CISO. En cualquier caso, entre el reto de lidiar con el creciente número de vectores de ataque y, al mismo tiempo, garantizar el cumplimiento de las numerosísimas normativas vigentes, los CISO no dan abasto.

Precisamente, el objetivo de los avances en segmentación de la red es permitir a las empresas automatizar la detección de amenazas y su aislamiento sin afectar a sus operaciones. Si se limitan los riesgos, se maximiza el control y se asegura la implementación eficaz de controles en toda la red. De esta forma, las empresas podrán preparar y gestionar de manera más satisfactoria la inevitable nueva ola de ciberamenazas.

Sin embargo, la clave es la prevención. Esto implica que, para ser eficaz, una solución debe ofrecer una visibilidad total de los dispositivos sin necesidad del uso de agentes, una supervisión continua y una respuesta automática a las amenazas.

CASOS DE USO

En España, desde Forescout trabajamos con G2K, con empresas del IBEX-35 y con clientes de todos los tamaños y de cualquier vertical, tanto en los sectores de finanzas, tecnología, sanidad, servicios, manufactura, energía, entretenimiento, educación y administración pública.

Un reto habitual que nos solemos encontrar es la carencia de visibilidad y contexto de los dispositivos IT, IoT y OT que están conectados a la red del cliente. Además, sin la tecnología adecuada, es imposible identificar y clasificar con precisión a todos estos dispositivos. Este escenario provoca que no se superen las auditorías de seguridad y, además, que se eleven los costes debido a la necesidad de realizar un inventario de forma manual.

Uno de los casos de uso más habituales para nuestra plataforma es lo que conocemos como control de acceso a la red (NAC) de nueva generación. En Forescout aportamos una solución para ello y ayudamos a nuestros clientes a obtener visibilidad y clasificación automática de todos los dispositivos que estén conectados a la red, ya sea en entornos de campus, IoT, OT, centros de datos o de la nube.

Aprovechar el potencial de SASE

COMPONENTES DE SEGURIDAD EN TODOS LOS ENTORNOS

JOHN MADDISON

EVP de Productos y CMO

FORTINET

fortinet.com

La evolución de la tecnología y la innovación en todos los ámbitos está derivando en toda una serie de nuevos desafíos para las empresas, incluidas las configuraciones de red que cambian dinámicamente y la rápida expansión de la superficie de ataque. Esto ha dado lugar también a la creación de niveles adicionales de protección y control de acceso para dar respuesta a los requerimientos de empresas y usuarios.

Durante los últimos tiempos, SASE (*secure access service edge*) se ha convertido en un tema prioritario para todo tipo de organizaciones. Las empresas requieren, cada vez más, de un acceso inmediato, ininterrumpido y seguro a los recursos y datos basados en la red y en la nube, y especialmente a las aplicaciones que son críticas para el negocio. Además, este acceso debe ser independientemente de la ubicación de los usuarios.

Sin embargo, hay dos cosas críticas que hay que recordar cuando se realiza la selección e implementación de una solución SASE. La primera es que debe integrarse fácilmente en una estrategia de seguridad más grande. Si no es así, simplemente se está creando otro conjunto de soluciones de seguridad independientes, que requieren atención y recursos adicionales. La segunda es que cualquier solución SASE no solo debe satisfacer las necesidades actuales de acceso y flexibilidad, sino que también debe admitir una estrategia de redes basada en la seguridad, para que pueda adaptarse rápida y automáticamente a los nuevos cambios de red y a los requisitos empresariales. Al mismo tiempo, debe proporciona una seguridad y un rendimiento robustos, y mejorados continuamente.

COMPONENTES DE SEGURIDAD

Para sacar el máximo rendimiento de los beneficios que aporta SASE, es básico que las organizaciones entiendan e implementen los componentes de seguridad en todos sus entornos:

» **Una solución SD-WAN funcional.** SASE comienza con una solución SD-WAN que incluye elementos tales como la selección de ruta dinámica, capacidades WAN de auto reparación, así como el necesario cuidado con la consistencia y experiencia de usuario para aplicaciones de negocio.

» **Un cortafuegos NGFW (físico) o FWaaS (basado en la nube)**. SASE requiere incluir una pila completa de seguridad que abarque tanto los escenarios físicos como los basados en la nube.

» **Acceso a la red de confianza cero.** Se utiliza principalmente para identificar a los usuarios y dispositivos, y así poder autenticarlos ante las aplicaciones. Dado que ZTNA (*zero trust network access*) es más una estrategia que un producto, incluye varias tecnologías que trabajan juntas, empezando por la autenticación multifactorial (MFA) para identificar a todos los usuarios. En el aspecto físico, la ZTNA debe incluir el control de acceso seguro a la red (NAC), la aplicación de políticas de acceso y la integración con la segmentación dinámica de la red para limitar el acceso a los recursos de la red. En el ámbito de cloud, ZTNA necesita microsegmentación con inspección de tráfico para las comunicaciones seguras este-oeste entre los usuarios, así como la seguridad siempre activa para los dispositivos tanto dentro como fuera de la red.

> **SASE no solo debe satisfacer las necesidades actuales de acceso y flexibilidad, también debe admitir una estrategia de redes basada en la seguridad**

» **Una salida segura a la web.** Se utiliza para proteger a los usuarios y los dispositivos de las amenazas a la seguridad en línea mediante la aplicación de políticas de seguridad y cumplimiento de Internet, y el filtrado del tráfico malicioso. También puede hacer cumplir las políticas de uso aceptable para el acceso a la web, asegurar el cumplimiento de las regulaciones y prevenir la fuga de datos.

» **Un CASB.** Un servicio basado en la nube permite a las organizaciones tomar el control de sus aplicaciones SaaS, incluyendo la seguridad del acceso y la eliminación de los desafíos del *shadow* IT. Esto debe combinarse con la DLP en las instalaciones para garantizar la prevención integral de la pérdida de datos. «

SAMUEL BONETE

Regional Sales Manager

NETSKOPE

netskope.com/es

Protección de entornos colaborativos

RENDIMIENTO Y SEGURIDAD A PARTES IGUALES

A lo largo de los últimos meses, el uso de las herramientas de colaboración ha aumentado drásticamente. Por ejemplo, según datos de Aternity, entre el 17 de febrero y el 14 de junio de este año, el manejo de Microsoft Teams creció un 894%, mientras que el de Zoom lo hizo un 677%.

En estos momentos, más de 75 millones de usuarios en todo el mundo utilizan Teams a diario y, además, Microsoft ha aprovechado este impulso para introducir una serie de innovaciones y hacer más funcional el producto. Ahora bien, poco a poco se va incrementando el riesgo de que, a medida que los usuarios se van sintiendo más cómodos con la tecnología, vayan también descuidando la seguridad y la protección de la información confidencial.

> **Las funcionalidades de seguridad a menudo no llegan a cubrir todos los requisitos de los actuales modelos de colaboración**

DATOS SEGUROS

Cuando se realiza una videollamada se comparte mucho más que vídeo. Estas interacciones llevan implícita la difusión de información sensible. En la mayoría de los casos se asume que la seguridad está activada por defecto, pero… ¿Esto es realmente así?

Según el modelo de responsabilidad compartida de la nube, la seguridad es una opción. Por ejemplo, dentro de Microsoft Teams hay una capacidad limitada de controles en línea y en tiempo real, lo que significa que hay pocas opciones a la hora de evitar que algo suceda. De esta forma, resulta fundamental que la gestión de la seguridad y la protección de datos dentro de Teams signifiquen, por defecto, que el departamento de seguridad tiene que gestionar las políticas a través de múltiples productos, dando lugar a importantes demandas de recursos y niveles de inconsistencia.

Las funcionalidades de seguridad nativas a menudo no llegan a cubrir todos los requisitos y, además, no facilitan la gestión de políticas granulares y corporativas. Existen siete señales clave, que se deben seguir para garantizar una protección eficaz en entornos de colaboración:

» La capacidad de hacer cumplir las políticas corporativas en múltiples plataformas.
» La aplicación de políticas granulares fijadas por el usuario, la ubicación, el acceso…
» Controles en línea para proteger los datos en tránsito y en reposo.
» Seguridad en tiempo real para bloquear y prevenir la exfiltración de datos.
» Distinción entre instancias del uso de la nube (por ejemplo, empresa A *versus* empresa B) para prevenir que las aplicaciones autorizadas sean un punto débil en la protección de datos.
» Reconocer formatos de datos para permitir a los equipos de seguridad bloquear, por ejemplo, el intercambio de datos personales en canales de colaboración.
» Detección proactiva de *malware* y otras amenazas.

EVOLUCIONAR CON LAS APLICACIONES

Teniendo en cuenta el constante desarrollo que están sufriendo las aplicaciones de colaboración, mejorando rápidamente sus características y funcionalidades, las medidas de seguridad que se plantean por parte de las empresas tendrán que seguir esa misma línea de agilidad si quieren mantenerse al día.

Por poner un ejemplo, una de las últimas funcionalidades anunciada por Teams es la posibilidad de transcribir completamente las conversaciones de video/audio. Esta funcionalidad seguro que será muy aplaudida, pero también resultará crítico que estos cambios de formato automatizados para los datos no creen nuevas formas de filtración de información sensible.

La colaboración y las funcionalidades en cuanto a seguridad deben evolucionar de forma conjunta, e ir de la mano con nuestra nueva forma de trabajar. «

Defensa contra amenazas internas

FERNANDO ANAYA

Country Manager

PROOFPOINT

proofpoint.com/es

UN TERCIO DE ATAQUES SON CAUSADOS POR EMPLEADOS

La mayoría de las ciberdefensas están enfocadas en mantener a raya las amenazas del exterior. Una visión acertada si se tiene en cuenta la gran cantidad de amenazas externas existentes, que van desde los denominados ataques BEC (*business email compromiso)*, que se han convertido en un negocio multimillonario, hasta todo tipo de *malware* que puede dañar significativamente a la organización.

No obstante, hay que tener en cuenta que no todos los ataques son perpetrados por agentes externos. Según las principales conclusiones del Informe Global 2020 sobre el Coste de las Amenazas Internas publicado por Proofpoint, en los últimos dos años han aumentado en un 47% las amenazas internas. Además, casi un tercio de los ciberataques tiene hoy su origen en el interior de la organización. Las consecuWencias de todos estos ataques con origen interno pueden ser igual de perjudiciales que los de origen externo: solo en 2019, costaron una media de 11,45 millones de dólares a organizaciones globales, lo que supone un aumento del 31% con respecto a los 8,76 millones de dólares que se registraron en 2018.

RAPIDEZ EN LA DETECCIÓN

A diferencia de l que ocurre con otros ataques comunes, las amenazas internas suelen pasar desapercibidas. Además, cuanto más tiempo tarden en detectarse, las repercusiones serán mucho más graves y costosas. Según el citado informe, los incidentes que duraron más de 90 días costaron una media de 13,71 millones de dólares al año a las organizaciones, mientras que aquellos que se pudieron contener en menos de 30 días costaron aproximadamente la mitad: unos 7,12 millones de dólares. Otro dato: se tarda una media de 77 días en contener un incidente interno.

Aun así, la organización dispone de la posibilidad de identificar y contener estos ataques rápidamente. Para una empresa resulta crucial conocer a sus trabajadores, sus motivaciones y su relación con los datos y la red corporativa.

No existe un único modelo de amenaza interna. Algunos ataques pueden deberse a un comportamiento negligente del usuario, ya que en la actual situación de teletrabajo muchos pueden estar más inquietos o distraídos y, por tanto, ser más propensos a cometer errores. Pero también hay empleados malintencionados que ven en la exfiltración de datos una revancha simple y eficaz ante cualquier circunstancia que le haga estar a disgusto con su empresa.

De hecho, según los datos del informe, más del 60% de estos incidentes provocados por amenazas internas fueron resultado del descuido de un empleado o de un colaborador externo, y el 23% fueron causados por ciberciminales infiltrados. Un total del 14% de todos los incidentes de amenazas internas implicaron el robo de credenciales por parte de ciberdelincuentes.

> **En la actualidad, casi un tercio de los ciberataques tiene su origen en el interior de la organización**

DEFENSA ACTIVA

De igual forma que los motivos pueden marcar el método de ataque, también permiten dar con la respuesta adecuada. Una defensa efectiva debe ser flexible, robusta y multicapa, capaz de combinar de forma adecuada tanto a personas, como procesos y tecnología. La respuesta vendría a través de diferentes factores, como implementar una solución integral de administración de acceso privilegiado, establecer un sistema de confianza cero entre tecnología y empleados, o añadir procesos claros y completos con los que gestionar los accesos.

Teniendo en cuenta que el mayor factor de riesgo son las personas, hay que tenerlas muy presentes y deben estar en el centro de la estrategia de seguridad, creando una cultura adecuada a través de la educación continua sobre las amenazas internas. «

La migración a la nube

¿QUÉ VA MAL Y POR QUÉ?

JOSÉ DE LA CRUZ

Director Técnico

TREND MICRO

trendmicro.com/es

El espacio *cloud* ha evolucionado durante casi una década. Aunque durante todo este tiempo se ha ido adquiriendo una mayor experiencia, que está permitiendo abordar mejor los proyectos de migración e incrementar la probabilidad de éxito, los arquitectos de soluciones e ingenieros de seguridad se siguen enfrentando a una serie de desafíos cuando analizan las migraciones a entornos cloud.

ARRASTRAR Y SOLTAR

En muchas ocasiones, la falta de una estrategia y de una planificación adecuada, desde el principio, es síntoma de un problema mucho más amplio que se suele dar en muchas organizaciones: realmente no hay una estrategia clara en torno a la nube, solo esfuerzos tácticos a corto plazo. No se tienen en cuenta las dificultades que se pueden encontrar a la hora de migrar una serie de *apps* a la nube, ni siquiera si es necesario y deseable hacerlo.

> La automatización es un ingrediente clave para asegurar el éxito de los procesos de migración

Estos problemas, además, se ven agravados por la existencia de silos organizativos. Cuando mayor sea el tamaño de la organización, más grandes y establecidos serán sus equipos individuales, algo que suele derivar en que la comunicación entre ellos se convierta en un gran reto. Incluso hay casos en que sí se cuenta con un equipo dedicado a la nube para trabajar en un proyecto determinado, pero es posible que no hable con otros departamentos asociados a tecnologías como DevOps o seguridad, por ejemplo.

El resultado es que, en muchos casos, las herramientas, aplicaciones, políticas y otros elementos simplemente se trasladan desde los entornos *on premise* a la nube. Esto termina siendo costoso, ya que las organizaciones no cambian realmente nada, solo añaden un intermediario extra sin aprovechar los beneficios que ofrecen las herramientas *cloud* nativas como, por ejemplo, los microservicios, los contenedores, y *serverless*.

Además, a menudo se carece de visibilidad y de control. Las empresas no entienden que, por ejemplo, es necesario supervisar todos sus contenedores y sanear las API. Asímismo, no se le suele dar la autoridad necesaria a los equipos *cloud* en ámbitos como la gobernanza, la gestión de costes o la asignación de políticas. De esta forma, simplemente, las cosas se descontrolan. A menudo, la responsabilidad compartida no se entiende bien, especialmente en el nuevo entorno del ciclo de vida DevOps, por lo que la seguridad no se aplica en las áreas adecuadas.

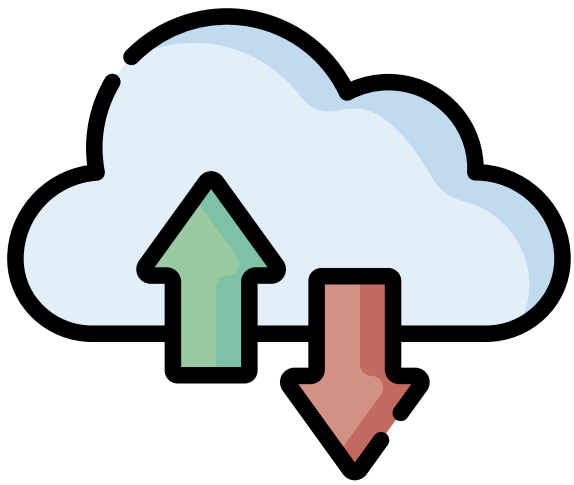
HACERLO BIEN

Lo que es evidente es que estos problemas no son fáciles de resolver. Desde la perspectiva de seguridad, todo parece indicar que aún tenemos que educar al mercado sobre la responsabilidad compartida en la nube, especialmente cuando se trata de nuevas tecnologías, como *serverless* y contenedores. Cada vez que hay una nueva forma de desplegar una *app*, parece que se cometen los mismos errores una y otra vez, y las empesas siguen suponiendo que los proveedores *cloud* son los que se encargan de la seguridad.

En este ámbito, la automatización es un ingrediente clave para asegurar el éxito de los procesos de migración. Las organizaciones deberían automatizar todo lo posible, para dar más coherencia a los proyectos y conseguir un mayor control sobre los costes. Al hacerlo, deben darse cuenta de que esto puede requerir de un rediseño de las *apps*, además de un cambio en las herramientas que utilizan para desplegarlas y gestionarlas.

En última instancia, es posible que se puedan migrar *apps* a la nube en un par de clics, pero el gobierno, la política y la gestión que deben acompañar a esto a menudo se olvidan. Por esa razón, es muy importante contar con objetivos estratégicos claros, y una planificación cuidadosa que permita asegurar resultados más exitosos.

Puede que no sea muy atractivo, pero es el mejor camino a seguir. «



26 NOV

XXII INTERNATIONAL INFORMATION SECURITY CONFERENCE

isms forum

dpi DATA PRIVACY INSTITUTE

csc CYBER SECURITY CENTRE

isc IOT SECURITY CENTRE

CSAES cloud security SPAIN alliance℠

PARTNERS

Platinum Sponsors

paloalto NETWORKS

Recorded Future®

Gold Sponsors

Akamai

cipher a PROSEGUR company

CROWDSTRIKE

FORTINET

Forcepoint

FORESCOUT

netskope

CYTOMIC

proofpoint

TREND MICRO

vmware

isms forum

INTERNATIONAL INFORMATION SECURITY COMMUNITY

www.ismsforum.es

@ISMSForum

ISMS Forum