isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

CSC CYBER SECURITY CENTRE

CIBERSEGURIDAD COMO CATALIZADOR DE LA GESTIÓN DEL CAMBIO

PERSONAS, PROCESOS Y TECNOLOGÍAS

X FORO DE LA CIBERSEGURIDAD

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

MAYO 2021

PROTAGONISTA
John McCumber (NIST)
Las palancas clave del CISO

FIRMA INVITADA
Susana Rey y Javier Lomas
Brechas de seguridad de datos personales

SECTOR PÚBLICO
Esther Muñoz (Madrid Digital)
Generar confianza y retener el talento

www.ismsforum.es

DANIEL LARGACHA

Director del Centro de Estudios de Ciberseguridad

ISMS FORUM

ismsforum.es

El escenario postcovid en el mundo digital

REPENSANDO LA DIGITALIZACIÓN

El 2020 marcará un antes y un después respecto a cómo la humanidad entiende la sociedad, el modo de vivir o de existir. Aunque el ansiado fin de esta pesadilla parece cada vez más cercano, el mundo que tendremos después será bastante diferente de como lo conocemos. Es fácil anticipar algunos aspectos que antes nos parecían lejanos y que tras la pandemia se quedar, como el teletrabajo, los entornos colaborativos, metodologías de trabajo más *agile*…. En cualquier caso, lo que subyace en los cimientos de las organizaciones es una profunda aceleración de la transformación digital que todas están acometiendo.

Es tan profundo el cambio, que no solo ha afectado a todo tipo de organizaciones (públicas y privadas, o en el ámbito profesional) sino que nos ha afectado a todos de forma individual: hemos cambiado gestos tan arraigados como la manera de pedir un taxi, consumir comida en un restaurante, ver la televisión, pedir cita para el médico o algo tan básico como pagar.

Probablemente, el futuro —ya casi presente— que nos depara será mejor. El éxito dependerá de cómo las organizaciones y los estados hagan frente a esta digitalización. Como todo nuevo camino, no va a estar exento de riesgos y el éxito dependerá de cómo se gestionen los ciberriesgos, ya que la confiabilidad de la tecnología va a depender directamente de la ciberseguridad de la que seamos capaz de dotarle.

Cualquier neófito puede pensar que el dilema de los ciberriresgos tiene una solución sencilla. Lo cierto es que no deja de ser parte de los viejos fantasmas del pasado, a los que todavía no hemos sido capaces de buscarle una solución (casi desde los últimos treinta años). La ciberseguridad no es un problema nuevo, no se está generando con las tecnologías que se están creando hoy en día. De hecho, la tecnología que se crea en la actualidad es mucho más segura que aquella que se creaba antaño.

DEPENDENCIA TECNOLÓGICA

Sin entrar en el debate acerca de si la tecnología puede ser más segura, la causa raíz es evidente. El punto de inflexión que nos ha llevado hasta la situación actual en cuanto a los ciberriesgos se ha ido cocinando lentamente en el seno de cada una de las empresas, gobiernos y el resto de las organizaciones. Todas ellas han ido incrementando de forma progresiva su "servidumbre" respecto a las tecnologías de información (apalancamiento tecnológico) hasta llegar al punto actual, en el que es casi imposible pensar en una sociedad del bienestar sin una dependencia casi completa de las TIC.

Aquí es precisamente donde reside el problema. El escenario actual no está exento de riesgos, que en el 2020 han provocado una avalancha de daños en las empresas y en la sociedad. Según el último informe IC3, elaborado por el FBI relativo a la delincuencia cibernética, los datos arrojan unas tendencias muy preocupantes. En el año 2020, el importe de las denuncias por fraude, robo digital de identidad y *ransomware* crecieron entre un

30% y un 350%. Además, atendiendo a las noticias, este año 2021 no parece que presente un cambio de tendencia. Pero si no queremos ir tan lejos, los datos publicados por el CCN-CERT indican que, en el año 2020, el número de incidentes que han tenido que gestionar se han incrementado en un 92% respecto al 2019.

BACK TO THE BASICS

A pesar de que la inversión en ciberseguridad ha experimentado un incremento en los últimos años, además de un aumento cercano al 50% que se espera para el 2022 según Gartner, aún queda mucho camino por recorrer. Muestra de ello son los datos de incidentes, que muestran que todavía no es suficiente. En 2017 —como quien dice, casi antes de ayer— tras el Wannacry se popularizó una tendencia de seguridad denominada *back to the basics*, convirtiendo el parcheado, el antivirus y el bastionado en actividades irrenunciables en las organizaciones. Este grave incidente hizo reflotar actividades que los profesionales hemos tratado de fomentar desde los orígenes de los planes directores de seguridad, con escaso éxito atendiendo a los resultados (parte del problema tendremos que asumirlo nosotros mismos).

El escenario en el que estamos inmersos actualmente es mucho complejo. Incidentes como el sufrido hace pocos días por Colonial Pipeline Co. muestran que lo básico no es suficiente. Resulta necesario reflexionar sobre la profundidad del problema y los devastadores efectos que pueden tener, y empezar de verdad a buscar una solución.

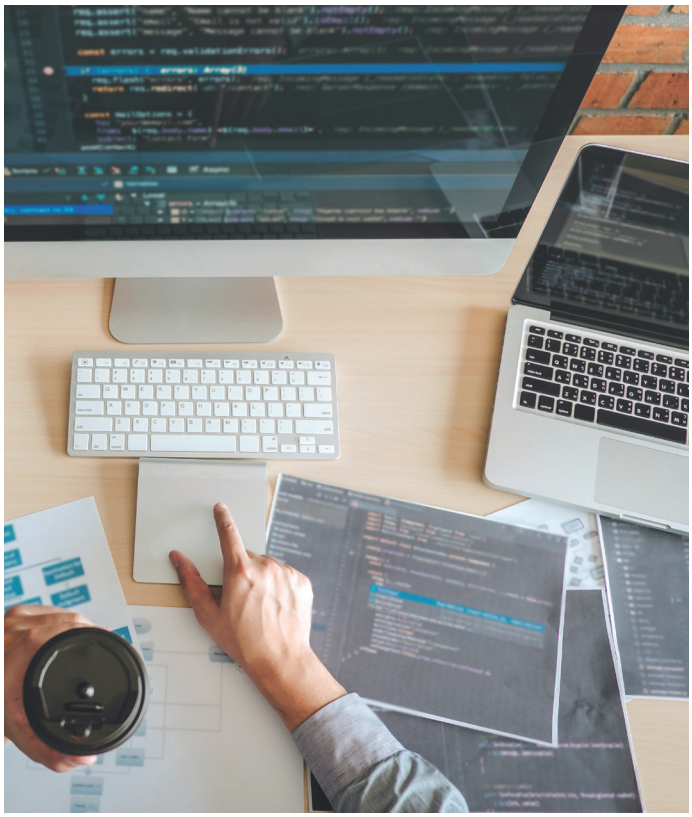
Las organizaciones están inmersas en acometer procesos de digitalización que implican cambios profundos en sus TIC, como la adopción de la nube o el traspaso de servicios *on-premise* a modalidad SaaS, entre otros. La adopción de estas nuevas tecnologías requiere de cambios profundos, no solo en las propias tecnologías, sino también en los procesos y en cómo se deben gestionar estas TIC. Aunque, por encima de todo, requiere que las organizaciones tengan un nivel de madurez elevado. De lo contrario, lo que se puede conseguir es crear un problema aún mayor, que puede ser de dimensiones descomunales si no se tiene en cuenta la incorporación de herramientas y servicios específicos de seguridad (la nube incorpora una seguridad por defecto, que probablemente no sea suficiente para muchas organizaciones).

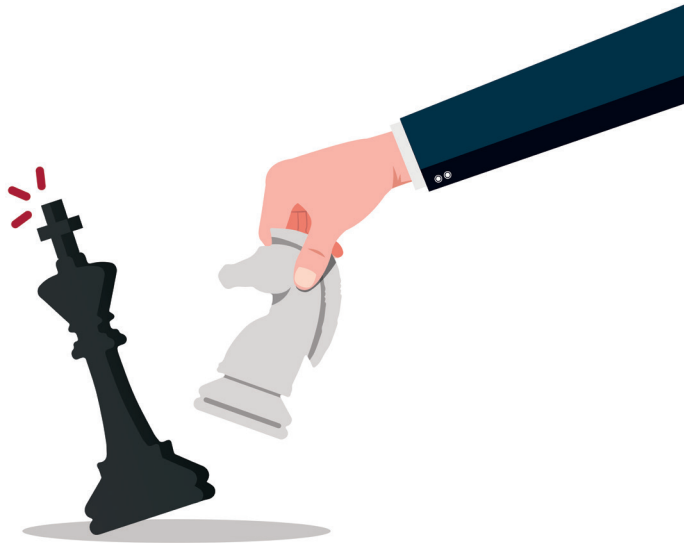
ECOSISTEMA DIGITAL, SEGURO Y FIABLE

Concluyendo, tenemos un sector de cibercrimen que cada vez ejerce mayor presión; unas organizaciones que, hasta hace poco tiempo, contaban con una aproximación de seguridad claramente insuficiente; y, para rematar, muchas están iniciando un salto a la digitalización, lo que requiere de cierta madurez y de un adecuado control, al menos desde el punto de vista de ciberseguridad, que todo apunta a que puede ser insuficiente.

Es el momento para hacer un parón y repensar entre todos los actores (empresas, gobiernos, proveedores de tecnología y el sector completo de la ciberseguridad) cómo construir un ecosistema digital más seguro y fiable. Es el momento, no tanto porque muchas organizaciones estén abrazando ese proceso de digitalización, sino porque, o somos capaces de construir un futuro digital o es posible que no haya futuro digital.

Desde hace diez ediciones, desde el ISMS buscamos crear estos entornos colaborativos, en los que todos los actores puedan encarar de la mejor manera los retos a los que se enfrentan en ciberseguridad.





REGIONAL CYBER SECURITY FORUM DE GALICIA

17 DE JUNIO DE 2021

isms GALICIA

CSC CYBER SECURITY CENTRE

XI ENCUENTRO DE CLOUD SECURITY ALLIANCE ESPAÑA

30 DE SEPTIEMBRE DE 2021

isms forum

CSAES cloud security SPAIN alliance℠

Alianza con el Clúster de Ciberseguridad de Madrid

PYME 3DSECURE

Desde que el Ayuntamiento de Madrid anunció su creación, ISMS Forum ha promovido y formado parte de la puesta en marcha del Clúster de Ciberseguridad de Madrid, una entidad que está promovida por el citado Ayuntamiento de Madrid, y que cuenta con la colaboración de la Comunidad de Madrid y el Instituto Nacional de Ciberseguridad.

El Clúster nace con la finalidad de sensibilizar y formar a empresas y ciudadanos en la importancia crítica de la ciberseguridad, así como reforzar el emprendimiento, incluyendo el desarrollo de nuevas empresas y el crecimiento de las ya existentes. Además de esto, entre sus objetivos están también el de contribuir a generar talento y mejorar la empleabilidad en este ámbito, así como posicionar a Madrid y su región como ciudad impulsora de la ciberseguridad.

Según se recoge en el plan estratégico aprobado por la Asamblea General de socios, las actividades a desarrollar se enmarcan en los siguientes ejes estratégicos:

» Formación, capacitación profesional y empleabilidad.
» I+D+i.
» Desarrollo y fortalecimiento empresarial.
» Difusión y sensibilización.

Como primera iniciativa, junto a ISMS Forum, el clúster ha presentado el proyecto Pyme 3DSecure a la consulta pública convocada por el Ministerio de Asuntos Económicos y Transformación Digital, cuyo objetivo es el de mejorar la postura de Ciberseguridad de las pymes. «

Nuevo esquema de certificación para productos, procesos y servicios

CONFIANZA FRENTE A RIESGOS DE TERCEROS

Cada vez es más evidente el incremento de la dependencia de las empresas con respecto a sus proveedores y a la cadena de suministro.

La responsabilidad y el deber de diligencia ha llevado a muchas organizaciones a la elaboración de nuevas políticas de externalización de servicios y de evaluación de las relaciones con terceros.

Cada vez es más importante ser capaces de analizar y evaluar los riesgos, así como controlar y supervisar a todas las entidades —terceros— que accedan a datos personales a lo largo de todo el ciclo de vida de la propia prestación de servicios. Incluso, uno de los objetivos que se plantean es llegar a determinar, de forma conjunta con los proveedores, el control relativo a esos riesgos.

Todo lo anterior hace reflexionar sobre la importancia de implementar un proceso de certificación que sea capaz de proporcionar confianza a todas las partes interesadas en que el producto, el proceso o el servicio cumpla con los requisitos especificados de ciberseguridad y privacidad.

En este contexto, ISMS Forum, en actuación y ejercicio de su rol para impulsar la concienciación y sensibilización de la comunidad, y a fin de proporcionar la necesaria confianza a todas las partes, propone un nuevo esquema de certificación.

Su objetivo es el de velar por un mínimo de cumplimiento exigible a los proveedores de servicios o de procesos en su modelo de prestación. «

Colaboración con la Universidad Complutense de Madrid

MÁSTER EN PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

ISMS Forum ha establecido una alianza con la Universidad Complutense de Madrid con el objetivo de desarrollar un nuevo programa del Máster en Protección de Datos y Seguridad de la Información, que permita a sus alumnos contar con la oportunidad de formarse, y adquirir conocimientos, tomando como fuente a los mejores profesionales del sector de la privacidad en España. Además, los alumnos pertenecientes a este máster tendrán podrán obtener de manera adicional las certificaciones Certified Data Privacy Professional (CDPP) y Certified Cyber Security Professional (CCSP), ambos títulos propios de ISMS Forum.

El objetivo principal del Máster en Protección de Datos y Seguridad de la Información es formar profesionales especializados en el ámbito de la privacidad y la ciberseguridad, de acuerdo a la normativa española de protección de datos de carácter personal y ciberseguridad. Este programa formativo permite obtener un dominio de los fundamentos principales, lo que permite que el alumno pueda aprovechar los conocimientos adquiridos tanto en el contexto nacional como en el europeo o el internacional.

El enfoque de las clases y actividades es eminentemente práctico, y se imparten en su inmensa mayoría por profesionales en ejercicio en este campo. Con este planteamiento, lo que se busca es ofrecer en todo momento una visión muy nítida de las mejores prácticas empleadas por las empresas en la realidad de su día a día. «

Convenio con el Business Continuity Institute

CONTINUIDAD DE NEGOCIO Y LA RESILIENCIA ORGANIZACIONAL

ISMS Forum ha firmado un convenio con el Business Continuity Institute, un organismo que está posicionado como líder mundial para los profesionales cuyas responsabilidades estén ligadas a la continuidad de negocio y la resiliencia organizacional. Su finalidad es la de establecer cauces para la realización, en común, de actividades de formación, asesoramiento, investigación y difusión de conocimiento.

Esta colaboración contempla la realización de actividades de divulgación, educativas y de investigación conjuntas, así como la elaboración de estudios y proyectos de investigación en aquellas áreas que se consideren de interés común.

Por otra parte, se incluye también el asesoramiento mutuo en cuestiones relacionadas con las actividades desarrolladas por ambas entidades, así como el intercambio de información y documentación, siempre dentro de los límites establecidos por la legislación relativa a la protección de datos, entre otros.

Como primeras iniciativas, ambas organizaciones han colaborado en el desarrollo del Proyecto de Gestión de CiberCrisis, organizado y promovido por ISMS Forum y el Departamento de Seguridad Nacional, así como la guía sobre continuidad de negocio en la pequeña y mediana empresa, que tiene previsto lanzarse próximamente. «

Los CISO tienen tres palancas clave: la tecnología, las políticas y procedimientos, y el factor humano

John McCumber. Fuente blog de (ISC)².

JOHN MCCUMBER,
Former Co-Chairperson,
National Institute of Standards
and Technology (NIST).

John es un ejecutivo que cuenta con más de veinticinco años de experiencia en seguridad de la información y operaciones de ciberseguridad, adquisición, gestión y desarrollo de productos, así como en el impulso de políticas de seguridad corporativas y la implementación de la seguridad en el diseño de tecnologías de la información.

El proceso de transformación digital ha multiplicado la exposición a los llamados riesgos cibernéticos y se ha convertido en una brecha inexorable para las relaciones comerciales y la prestación de servicios entre empresas que, en sus relaciones con terceros, están sujetas a regulaciones específicas debido a su naturaleza (infraestructuras estratégicas, críticas, esenciales o digitales, entre otras). Además, son especialmente reseñables los riesgos asociados con la subcontratación a proveedores o servicios externos.

¿Se está planteando una revisión del *framework* a la luz del nuevo panorama de amenazas y el escenario ya permanente de teletrabajo?

El NIST siempre trata de mantener sus orientaciones actualizadas a la luz de las amenazas cambiantes y la evolución de la infraestructura. Los retos a los que se enfrenta cualquier organismo político, como el NIST, son garantizar que sus orientaciones sean viables en la práctica y, al mismo tiempo, lo suficientemente amplias como para mantener su aplicabilidad a medida que cambian las amenazas y la tecnología. Esto se consigue centrándose en las estructuras y las personas que se encargan de prever, diseñar, aplicar y gestionar el programa de ciberseguridad de una organización. Los diversos mecanismos se guían por estos elementos críticos para asegurar que el programa está trabajando para proporcionar eficazmente los controles de gestión de riesgos adecuados.

Si la orientación se convierte en una lista de comprobación detallada, como la *NIST Special Publication 800-53*, estos controles técnicos deberán actualizarse y ampliarse constantemente para abarcar un conjunto de controles que puedan ser implementados y validados por la organización usuaria. Las orientaciones, como los modelos de madurez, deben tener un carácter más amplio para garantizar la pertinencia durante un período más largo. La vigencia se define por la aplicación de la orientación y su uso en entornos operativos.

¿Cuál es su visión sobre el estado de madurez en ciberseguridad de las empresas?

Recientemente hemos tenido una perspectiva sobre la naturaleza y el estado de madurez de la ciberseguridad con el ataque de *ransomware* a *Colonial Pipeline*, del que se ha informado ampliamente. No puedo hablar en nombre de todas las empresas, ni siquiera de la mayoría, pero todas las organizaciones que he visitado como consultor tenían un subconjunto significativo de vulnerabilidades que debían ser abordadas. Muchas eran conscientes de estos problemas y un número significativamente menor estaba rastreando activamente sus vulnerabilidades en un registro de riesgos.

Los modelos de madurez emergentes se centran menos en estas vulnerabilidades específicas y más en los procesos establecidos para identificarlas, seguirlas y mitigarlas. Como consultor, no estaba tan interesado en si existía o no una vulnerabilidad específica, o un conjunto de vulnerabilidades, sino en si la organización era activamente consciente de ellas y tomaba medidas para mitigar el riesgo.

En la actualidad, el gobierno estadounidense ha desarrollado modelos de madurez para los sistemas y las personas, así como para las políticas y las prácticas. El programa del *Department of Homeland Security* se centra en el propio programa de ciberseguridad, mientras que la *DOD Cyberecurity Maturity Model Certification (CMMC)* se utilizará para validar a las empresas de la *Defense Industrial Base (DIB)*. Estos marcos y modelos emergentes están destinados a evaluar el propio programa de ciberseguridad de la organización.

> **Los modelos emergentes se centran en los procesos establecidos para identificar las vulnerabilidades, seguirlas y mitigarlas**

¿Qué puntos deben mejorar los CISO para ubicar a la ciberseguridad en el lugar adecuado?

Los CISO tienen un papel central en la madurez del programa de ciberseguridad de sus organizaciones, cada una con su propio punto de partida. La habilidad del CISO se juzga mejor por su capacidad para cambiar los procesos y a las personas hacia una postura de madurez. Los CISO necesitan evaluar efectivamente esta posición de partida e instaurar las políticas, los procesos y el plan de implementación para establecer una dirección.

Los CISO tienen tres "palancas" clave de las que tirar: la tecnología, las políticas y procedimientos, y el factor humano. Los CISO más eficaces que he tenido el privilegio de conocer eran expertos en saber de qué "palanca" tirar, cuándo y con qué intensidad.

La ciberseguridad no es un destino final, es un viaje continuo. Los CISO inteligentes se asegurarán de que las políticas y los procesos estén en vigor, y de que las personas adecuadas estén en su lugar para imple-

Sede del NIST (National Institute of Standards and Technology) ubicada en Gaithersburg, Maryland (Estados Unidos).

Debemos diseñar los controles necesarios para aliviar a los usuarios de toda la carga de la aplicación de la seguridad

mentar y gestionar su programa organizativo. Los más avispados también se aseguran de que las políticas y los procedimientos se prueben y documenten de forma recurrente.

¿Cuál debería ser la posición del CISO en el organigrama empresarial?

Seguimos bromeando con que CISO significa "*career is surely over*". El lugar que ocupan en el escalafón empresarial ha sido un tema muy debatido desde hace un par de décadas.

Hace veinte años, el cargo de CISO evolucionó a partir del reconocimiento profesional, llegando a debatir si debía tener visibilidad en la cúpula directiva. Sin embargo, la forma en que se ha implementado ha sido menos optimista: he visto a personas con el título de CISO ser empujadas hacia abajo en los escalones de la organización para sentarse en algún lugar por debajo del director de TI; otros que informan al consejo de administración... Mi opinión es que ni siquiera debería ser un papel organizativo, sino el de un asesor externo.

La ciberseguridad es un subconjunto de la ciencia la gestión de riesgos. Como tal, cualquiera que sea un empleado de la organización ya está trabajando desde una posición comprometida y le resultará difícil proporcionar —con franqueza— una orientación eficaz sobre la gestión de riesgos. Tal vez debería haber un CISO de la organización que realmente diseñe, implemente y gestione el programa de la empresa, pero estará influenciado por el CFO, el CIO, los líderes de TI, los líderes de ventas, los gerentes de programas y aquellos involucrados en la obtención de ingresos y encargados del cumplimiento de la misión.

Un asesor externo puede buscar y exponer vulnerabilidades potencialmente embarazosas, y hacer recomendaciones de riesgo sin preocuparse por todo: desde la gestión financiera hasta los recursos humanos. Creo que hay una necesidad vital de un asesor de riesgos externo, al menos mientras haya alguien, que es más que un CISO, que gestione el programa de la organización.

¿Cuáles son retos en cuanto a la gestión del talento en ciberseguridad?

El tema de la educación, la formación y la gestión del talento en el ámbito de la ciberseguridad seguirá siendo problemático en un futuro próximo. Estas cuestiones van mucho más allá de la profesión.

Hace más de cincuenta años cometimos el error de clasificar la mayor parte del trabajo de TI como lo que coloquialmente llamamos como de *white collar*. Como

tal, establecimos elevados requisitos académicos para muchos (si no la mayoría) de los trabajos de TI, como los primeros programadores y operadores de sistemas. Nuestro sistema educativo se adaptó a estos requisitos y creó una floreciente profusión de trayectorias profesionales bajo el manto general del trabajo en tecnologías de la información.

En Estados Unidos, muchas familias y personas están repensando cuál es el valor de una educación universitaria tradicional, especialmente a la luz de los continuos problemas creados por la creciente deuda universitaria que soportan las personas. Muchos profesionales están optando por vías educativas alternativas que incluyen certificaciones y "microtítulos".

Tras su experiencia en (ISC)², ¿qué opina de las certificaciones a nivel del CISO?

Creo que todavía no se ha creado una certificación precisa y completa para un CISO. Además de los innumerables deberes y responsabilidades inherentes a la función, hay una amplia lista de lo que denominamos *soft skills* que son necesarias para ser un CISO eficaz.

Soft skills ha sido el término utilizado para definir los rasgos interpersonales y de comportamiento que un individuo posee —o aprende— a medida que crece en conocimiento y madurez. Entre ellas se encuentran la actitud positiva, el pensamiento crítico, la ética, el trabajo en equipo y la capacidad de liderazgo. Ninguna de las certificaciones de ciberseguridad que he visto ha sido capaz de plasmar estos atributos en un examen. Prefiero llamarlos aptitudes profesionales, ya que no veo nada "blando" en ellos.

Estos comportamientos y aptitudes críticas tienen, al menos, tanto impacto en la eficacia de alguien como el CISO en cualquier habilidad técnica que se pueda probar, evaluar y certificar.

¿Debería existir una certificación de servicios, productos y procesos para empresas, o de su nivel de madurez en ciberseguridad?

Ha habido varios intentos notables de certificar, tanto a los procesos como a las organizaciones que proporcionan servicios, productos y procesos de ciberseguridad. Obviamente, esto es mucho más fácil en el caso de los productos y lo hemos visto en programas como el *FedRAMP* de la *US Government Services Agency (GSA)* para los proveedores de la nube.

Los modelos de certificación que intentan evaluar a toda una organización o consultoría tienen una tarea mucho más difícil. Las organizaciones están compuestas por muchas personas que van y vienen, y la mayoría busca avanzar en el grupo y en su carrera. Cualquier certificación de este tipo es, en el mejor de los casos, una instantánea en el tiempo. Queda obsoleta momentos después de su concesión, ya que sin duda ha habido cambios desde que se realizó la evaluación. El organismo certificador se ve entonces presionado para mantener la validez de su certificación a la luz de estos cambios. Además, cada explotación muy publicitada de las organizaciones, tanto públicas como privadas, seguirá poniendo en duda la legitimidad de estos sistemas.

> **En mi opinión, el papel del CISO ni siquiera debería ser organizativo, sino el de un asesor externo**

¿Los últimos acontecimientos han contribuido a mejorar la concienciación en ciberseguridad?

Escuché por primera vez esta pregunta a la luz de los ataques generalizados de virus a principios de los años 90. Me hubiese gustado decir que ya hemos superado la necesidad de una simple concienciación, pero la cuestión se plantea perennemente en los círculos gubernamentales, académicos e industriales.

El concepto de concienciación suele dirigirse a lo que llamamos el "usuario". A medida que nuestra profesión ha ido creciendo, seguimos depositando demasiada responsabilidad en aquellos para los que trabajamos. Nuestra profesión exige que diseñemos, implementemos y gestionemos nuestros sistemas informáticos, dispositivos tecnológicos y sistemas de control industrial para que funcionen de forma segura y eficaz para los usuarios previstos.

Es nuestra responsabilidad asegurarnos de que diseñamos los controles necesarios para aliviar a los usuarios de toda la carga de la aplicación de la seguridad. «

> **Ninguna de las certificaciones de ciberseguridad que he visto ha sido capaz de plasmar los soft skills en un examen**

"La prevención siempre es mejor que arreglar los fallos a posteriori"

LISA SHORT,
Digital Tech Transformation Strategist Analyst Design Ecosystems; Chief Research Officer, Global Foundation for Cyber Studies and Researchand Technology (NIST).

La profesora Lisa Short es una autoridad preeminente y líder de pensamiento en sistemas de tecnología digital y seguridad, pensamiento de diseño, economía del comportamiento, educación, cambio transformacional, blockchain y crypto. Como fundadora de Hephaestus Collective Ltd, P&L Digital Edge Ltd (Reino Unido), Mind Shifting, y Africa Agri Tech Ltd, Lisa está continuamente buscando nuevos enfoques multidisciplinarios para la transformación digital y el cambio tecnológico que ofrece un lugar mejor, más seguro, y más educado para vivir y trabajar.

Lisa Short ha sido nombrada CROfficer de la Global Foundation for Cyber Studies and Research (GFCyber) y es la presidenta de CySME, un grupo de interés especial centrado en la cibersalud de las pymes. Lisa también es miembro de la UK Cyber Security Association; del Peer Review Committee for The European Symposium on Usable Security (EuroUSEC), y del Advisory Council for the International CyberExpo (London). Ha sido reconocida como una de las mejores mujeres líderes del Top100 B2B Thought Leader in the World to Follow 2020 & 21.

¿Qué papel juega la ciberseguridad en un proceso de transformación digital?

En el mundo físico tenemos límites que podemos observar y realizar análisis de riesgos. En muchos sentidos, como líderes, podemos controlar el ritmo del cambio en nuestros propios entornos y elegir cómo se construye.

También se puede optar por cerrar las persianas y las cortinas y "el mundo" queda en gran medida vedado a la observación externa. Invitas a los amigos a entrar y mantienes a los enemigos fuera. También puedes eliminar físicamente los activos y la información.

El mundo digital, sin embargo, es invisible y no tiene límites. No puedes ver cuando alguien mira por las ventanas o por la puerta principal de tu vida, tu casa o tu negocio. A este reto se añaden las externalidades de las nuevas tecnologías, el trabajo a distancia y las empresas que requieren de una latencia de datos mínima para impulsar y dirigir las decisiones empresariales y la rentabilidad.

Estos retos deben tenerse en cuenta con hechos como los siguientes: actualmente, más del 82% de los ejecutivos de nivel C han reconocido que han tenido violaciones de datos en el último año; o que el 50% de todos los consejos de administración tienen el objetivo de prescindir del papel.

Dada la vertiginosa escalada de la economía digital, incluido el enorme volumen de datos que se añaden a cada momento, los riesgos, la previsión, la complejidad y la amplitud de las consideraciones se están moviendo más rápido que el ciclo de decisiones y el crecimiento de la capacidad de los líderes empresariales.

Incluir la seguridad digital y, de forma más proactiva, la resiliencia digital en la transformación sistémica significa que el marco y la arquitectura para la agilidad, la agudeza y la estrategia predictiva son fundamentales para el éxito, en lugar de una mentalidad de extensión. El sector debe incorporar la capacidad de aprendizaje automático y las oportunidades que ofrecen las tecnologías de vanguardia, como el *blockchain*, para permitir la agilidad y la seguridad que esperan las empresas y la economía.

¿Cuál debería ser el porcentaje de inversión en ciberseguridad dentro de TI?

Los presupuestos destinados a la ciberseguridad han permanecido estancados y en un nivel desproporcionadamente bajo del 6% del gasto en tecnología durante los últimos diez años. Sin embargo, el 64% de las empresas reconoce que este presupuesto no ha seguido el ritmo al que ha aumentado el riesgo o la estrategia para gestionar los paisajes de amenazas debido a la digitalización y las nuevas tecnologías. La pandemia y la aceleración de los ciberataques han obligado —en muchos sentidos— a las empresas a aumentar el gasto presupuestario durante el pasado año hasta un porcentaje ligeramente mejor: el 9%.

> **“ Hay que incorporar el aprendizaje automático y tecnologías de vanguardia como el *blockchain***

Sin embargo, las cifras exactas suelen ser difíciles, ya que los analistas también se esfuerzan por seguir el ritmo del crecimiento del mercado y la diversificación de lo que se incluye en el sector. La información está fragmentada y es confusa. A nivel mundial, se prevé que el gasto en infoseguridad —en 2021— sea de aproximadamente 124 000 millones de dólares. El gasto total del sector, incluyendo los rápidos costes del *ransomware*, ha disparado el coste real hacia el billón de dólares. No es sencillo contabilizar los ciberseguros, así como un gran porcentaje del gasto relacionado con la seguridad. Acciones como el despliegue de nuevo software o, incluso, el cambio a un modelo SaaS se consideran estrategias vinculadas a la TI y no a la seguridad. Esto se debe a que todavía nos centramos en detener las amenazas y no en diseñar sistemas de confianza.

¿Cuál es la inversión que se dedica actualmente a ciberseguridad en TI?

La verdadera pregunta debería ser cuál es el valor añadido que representa para una empresa, que tiene —de forma proactiva— un negocio digitalmente

sano y resistente como un activo, en lugar de uno que ve la ciberseguridad como un gasto. Para conseguirlo, es necesario un cambio de mentalidad y una inversión capitalizada que requiere una mejora continua y un programa de mantenimiento para que el activo se mantenga a la vanguardia y se revalorice.

El lenguaje y el léxico tienen que cambiar al mismo tiempo que la seguridad cibernética, hacia la consecución de la confianza digital, que es esencial para las relaciones intrínsecas de las partes interesadas, los usuarios y las autoridades; y también a la consagración de la resistencia de la privacidad, los datos y la infraestructura digital.

La ciberseguridad es solo tener un mundo digital interconectado de confianza y alto funcionamiento. En cierto modo, es más fácil considerar que en Australia, a modo de ejemplo, una interrupción digital de cuatro semanas costaría 30 000 millones de dólares australianos, o el 1,5% del PIB total, y 163 000 puestos de trabajo. Por lo tanto, una inversión en confianza digital debería ser mayor que eso, y sin embargo en 2020 se registró una inversión de 5600 millones de dólares australianos. Los Estados Unidos gastan alrededor de 54 000 millones de dólares estadounidenses y el Reino Unido gasta casi un 50% menos que las principales democracias.

> **Las empresas tienden a ver la ciberseguridad como un coste, en lugar de un activo en el que invertir**

¿En su opinión, este porcentaje mejorará a lo largo de los próximos años?

Utilizando el mismo pensamiento tradicional, se prevé que el gasto adicional anual en el mercado de la ciberseguridad sea de aproximadamente un 12% o un 15%. Lo preocupante es que existe una tendencia desproporcionada hacia la seguridad "monetaria", que suele ser el bien más tangible para medir. Muchos analistas están luchando con la actividad cibercriminal sin precedentes, el impacto en la reputación empresarial (o la medición de la misma) y la falta de datos que generan las pequeñas y medianas empresas para proporcionar una imagen veraz del panorama completo.

Una vez más, el valor de la medición de la mejora predictiva, y la amenaza de oportunidades como un activo que puede ser valorado, se diluye entre la consistencia del enfoque de "miedo, incertidumbre y temor". Como resultado, las empresas tienden a ver la ciberseguridad como un coste y a buscar formas de minimizarlo, en lugar de un activo en el que invertir. La educación es clave para este cambio.

¿Qué KPI hay que impulsar y escalar a dirección?

Tengo una opinión muy diferente sobre los KPI. No se trata de indicadores clave de rendimiento, que generalmente son medidas retrospectivas. KPI significa mantener a la gente ideal. En términos de conducción y escalamiento para la gestión —ese debería ser el enfoque— la sociedad 5.0 es una evolución de la Cuarta Revolución Industrial, en la que el cambio es hacia un Internet de *Internet of Everything*, con propósito y conectado. Esto se presta a adoptar un liderazgo de seguridad y confianza que se centra en las asociaciones para crecer, desarrollar e integrar infraestructuras innovadoras de confianza cibernética y digital a un nivel fundacional básico, en lugar de limitarse a gestionar el riesgo.

Se trata de hacer de nuestras vidas un lugar mejor para vivir y trabajar, y para que las empresas tengan la oportunidad de prosperar. Para ello es necesario dar prioridad a la educación de las personas, y establecer una cultura dentro de las empresas en la que la salud digital y la confianza sean una forma de vida y no una elección.

¿Cuál es el papel de la nube en este proceso de evolución digital?

En términos generales, la nube se refiere a sistemas e información disponibles a distancia en el "espacio virtual" a través de Internet. Es una tecnología que permite, y posibilita, la transferencia de información, la disponibilidad de los datos y una increíble eficiencia y ganancia de oportunidades.

También hay varios modelos de despliegue de la nube que tienen diferencias significativas con respecto a un panorama de inteligencia de amenazas de ciberseguridad. Los modelos público, privado, comunitario, híbrido y empresarial tienen diferentes puntos de acceso, capacidades de intercambio, beneficios e impulsores de adopción. Todos tienen una base que requiere Internet y conectividad para que funcionen, y datos para alimentarlos. Cada uno de ellos tiene también una puerta principal por la que entran los datos, las partes interesadas identificadas, y una arquitectura que apoya lo que ocurre detrás de la puerta principal.

Las implicaciones para la confianza y la seguridad, empresarial y digital, son profundas e incluyen un amplio abanico de consideraciones como los problemas de conectividad, la integridad de los datos, los registros de auditoría, la velocidad de latencia, la ubicación del centro de datos, el cumplimiento de las normas entre jurisdicciones y la ingestión de datos.

En mi opinión, el sector digital carece actualmente de educación, adopción y despliegue de tecnologías *blockchain* que permitan un ecosistema virtual de confianza. La prevención siempre es mejor que arreglar los fallos a posteriori. Las características más destacadas de *blockchain* la sitúan en primera línea como solución funda-

cional para los sistemas virtuales y ciberfísicos en los que las personas y las empresas pueden confiar.

¿Cómo deberían progresar los entornos regulatorios, los transnacionales y los sectoriales, para mejorar el ecosistema de ciberseguridad?

Tengo dos opiniones al respecto, ya que una cultura de liderazgo cibernético y digital requiere madurez y el reconocimiento de la responsabilidad y la motivación. El sector ya cita la madurez de la demanda, la falta de inversión y el acceso limitado a las competencias como algunos de sus principales retos. Estos no están relacionados con los entornos normativos.

En muchos sentidos, la regulación controla a aquellos que no tienen madurez de liderazgo, que no se centran en la mejora proactiva y que siguen teniendo una mentalidad de recorte de costes y gastos. Un mayor enfoque en la urgencia de la educación y las oportunidades de los sistemas blockchain totalmente descentralizados, y sin confianza, son mucho más productivos que el cambio regulatorio burocrático y generalmente lento. A menudo también se puede argumentar que el cambio regulatorio, ya sea transnacional o internacional, implica muchos intereses creados y, a menudo, se produce después de que el caballo se haya desbocado.

¿Qué están desarrollando en las organizaciones en las que colaboras?

Estoy centrada al 100% en establecer un enfoque de ecosistema multidisciplinar que converja, acoja y priorice los mejores conocimientos del mundo de todos los grupos de interés, y que se centre en el uso de la tecnología blockchain, incluidos los smart contract y las métricas de responsabilidad para proporcionar confianza digital y personas cualificadas formadas.

Es evidente que el sector debe tener una mayor previsión, innovación y cohesión para trazar un camino que se adelante a la curva de riesgo, y eso no está ocurriendo actualmente. Estoy liderando el compromiso de la industria con el diseño tecnológico para producir una tecnología patentada que pueda medir la confianza y la responsabilidad de las credenciales como un activo. Mucho de lo que hacemos actualmente en la recuperación de activos y la gestión de ciberataques puede integrarse en el diseño de tecnología que se convierte en proactiva en lugar de reactiva.

¿Cómo será el futuro de las compañías que no afronten con garantías la ciberseguridad?

En la trayectoria actual, se espera que el coste global de las violaciones de datos, sin más (como los pagos por ransomware) supere los 6 billones de dólares en 2021 y los 10,5 billones en 2025. Se puede poner esto en perspectiva al darse cuenta de que la cantidad es mayor que el coste de todos los desastres naturales a nivel mundial en un solo año, y que se considera una amenaza mayor para la humanidad que las armas nucleares de destrucción masiva.

Lo interesante es que, sabiendo esto, la inversión en la prevención de estos resultados no deseados sigue siendo muy baja. Esto nos lleva a entender que los enfoques actuales no están funcionando para cambiar esa inversión. El 60% de las pequeñas empresas cierran en los seis meses siguientes a un ciberataque y, en adelante, los inversores son menos indulgentes con cualquier empresa que no esté preparada para las emergencias.

> **“El 60% de las pequeñas empresas cierran en los seis meses siguientes a un ciberataque**

La oportunidad llama a la puerta si un posicionamiento digital de confianza significa que los clientes y las partes interesadas le ven como un socio comercial que pueden ver como parte resistente de su futuro. La medición de los resultados positivos, y el crecimiento competitivo conseguido mediante la inversión en una huella digital saludable, solo puede producirse si las matrices de decisión se centran en el futuro.

A lo largo de los últimos años hemos podido ver a más mujeres en cargos importantes en este sector, ¿crees ha habido un avance en la reducción de la brecha de género?

No se ha retrocedido. La diversidad de género no se mide por el número de mujeres en el sector y el puesto que ocupan. Requiere un cambio de mentalidad prioritario hacia el respeto y una nueva narrativa.

La mejora incremental que se ha conseguido es insuficiente para superar la desventaja de género. Está determinada por la inclusión de oportunidades, la paridad en todas las áreas —incluida la salarial— y la ausencia de intimidación, acoso y abuso. El 48% de las mujeres en el área tecnológica sufren abusos. El Informe sobre el estado de las mujeres en la tecnología en 2021 es una constatación aleccionadora del verdadero estado de los desafíos de género que siguen siendo desmesurados e inaceptables.

El hecho de que, en la mayoría de los eventos y conferencias, los presentadores y ponentes principales sigan siendo predominantemente masculinos es indicativo de la necesidad urgente de cambio y de la falta de responsabilidad en el sector para adoptar prácticas de buena gobernanza. «

Ciberseguridad en el sector público

LOS RETOS DE GENERAR CONFIANZA Y DE RETENER EL TALENTO

El 8 de enero de 2020 se cumplían diez años de la publicación en el Boletín oficial del Estado, BOE, del Esquema Nacional de Seguridad (ENS). Esta ley establecía los principios básicos y requisitos mínimos que, de acuerdo con el interés general, permitían una protección adecuada de la información, comunicaciones y los servicios que las Administraciones Públicas ofrecían a los ciudadanos. Posteriormente se modificó y amplió su alcance para cubrir todos los sistemas del sector público.

ESTHER MUÑOZ FUENTES

Directora de Ciberseguridad, Protección de Datos y Privacidad

MADRID DIGITAL

comunidad.madrid

En la actualidad, el ENS es el principal marco de control y de medidas de seguridad (75 en concreto, de obligado cumplimiento), de tipo organizativas, operativas y de protección que toda entidad pública debe considerar. Bajo un enfoque de gestión de riesgos, ofrece toda una metodología de categorización de sistemas de información que permite clasificarlos según su criticidad, para determinar —desde el diseño— las medidas de seguridad a aplicar.

El ENS solo es obligatorio para el sector público. Sin embargo, muchas empresas en nuestro país lo implementan para mejorar la seguridad de sus sistemas de información. Además, existen guías muy prácticas —CCN-STIC desarrolladas por el Centro Criptológico Nacional (CCN-CERT)— que ayudan en la configuración e implementación segura de múltiples tecnologías. El ENS es una realidad desde hace más de diez años, y sus principios —gestión del riesgo, seguridad integral, seguridad como función diferenciada, y organización y gestión de la seguridad— siguen siendo relevantes; de hecho, cualquier empresa privada debe tenerlo en cuenta cuando gestiona su ciberseguridad.

El principal objetivo del ENS es generar confianza en los ciudadanos al utilizar los servicios electrónicos que la administración pone a su disposición. Además, para poder adaptarse a los tiempos, ya se anuncia una revisión de esta ley con el objetivo de actualizarla al marco legal y al contexto estratégico actual, flexibilizando ciertos aspectos y promoviendo la defensa activa; en particular incidiendo en la mejora de la monitorización, la cibervi-

gilancia, los observatorios de amenazas, etc. Todo ello unido a una estrategia de protección de sistemas y de redes basada en herramientas tecnológicas y procesos de ciberseguridad.

» INCIDENTES DE SEGURIDAD

Son bien conocidos los últimos incidentes que han afectado al sector público y privado, nacional e internacional, en los que los ataques de *ransomware* han puesto en jaque a muchas organizaciones con el consiguiente impacto en su reputación, en la vida de los ciudadanos y en sus balances financieros. Como referencia, en este 2021 podemos recordar los ataques al SEPE, al proveedor de servicios *cloud* ASAC (que ha afectado a múltiples ayuntamientos y entidades públicas) y, más recientemente, el caso de la distribuidora de carburantes Colonial en Estados Unidos, que ha provocado la declaración de estado de emergencia en algunos territorios de este país ante el riesgo de desabastecimiento. El panorama futuro no es mucho mejor: según el CERT-EU, en este primer cuatrimestre de año el número de víctimas de *ransomware* en Europa ha aumentado respecto a todos los indicadores de los cuatrimestres de 2020.

Es fácil vislumbrar los tiempos convulsos en materia de ciberseguridad que estamos viviendo. Los ataques y las amenazas se han incrementado de forma exponencial, aprovechando las vulnerabilidades en sistemas y redes que no han sido concebidos en origen para ser seguros, y cuya puerta de entrada suele ser la confianza, o la falta de conocimiento o de concienciación de los usuarios en el uso de la tecnología. A todo esto se une que los servicios en Internet que prestan las entidades públicas son cada día mayores y más diversos, la proliferación del teletrabajo y el mayor uso de servicios *cloud.* Todo ello ha conseguido que las principales defensas —el perímetro de seguridad o el antimalware del puesto y servidores— ya no sean ni las únicas ni las principales capas que debemos tener.

Esta nueva realidad trae consigo un mayor impulso de actividades de vigilancia digital, análisis de vulnerabilidades, detección de amenazas, revisiones proactivas de estado de la seguridad y, por supuesto, de concienciación, comunicación y divulgación hacia nuestros jefes, compañeros y usuarios; es decir, de actividades de prevención, detección, concienciación y formación. No solo se trata del análisis de la seguridad de los sistemas y redes, sino también del entorno exterior, de todo aquello que permita anticiparse, mejorar las protecciones y reducir la exposición al riesgo. Al mismo tiempo, hay que concienciar y formar a los usuarios para que se conviertan en la primera capa de defensa activa.

Todo ello no se consigue solo con tecnología, sino con organización, con procesos y con personas que conozcan el negocio y la tecnología, y que sepan de ciberseguridad. Este es uno de los grandes retos: disponer de suficiente talento capaz de gobernar, supervisar y controlar la ciberseguridad de una entidad pública. Pero que, además, tenga continuidad, ya que este es un sector donde la movilidad está a la orden del día.

» SIMILITUDES Y DIFERENCIAS

Por consiguiente, la realidad, las ocupaciones y preocupaciones de la ciberseguridad en una entidad pública no son muy diferentes a las del sector privado. La ciberseguridad es un pilar clave de la transformación digital de las organizaciones, fundamental para conseguir que los servicios telemáticos estén disponibles desde múltiples medios y canales, garantizando que las identidades y datos personales de los usuarios se traten siguiendo los principios que establece la RGPD.

> **La falta de talento en ciberseguridad afecta tanto el sector público como al privado**

Según el informe *Ascendant 2020-21* de madurez digital, en relación a la ciberseguridad existen muchas similitudes en cuanto a los proyectos —los abordados y los que están en proceso— centrándose en la implantación de sistemas multifactor en la autenticación, gobierno de identidades privilegiadas, potenciación de los servicios de SOC y EDR, o difusión y formación. Como principal diferencia, las entidades públicas están inmersas en procesos de certificación respecto al ENS de todos o parte de sus sistemas de información, ya que es de obligado cumplimiento para este sector.

Por último, insistir en lo relacionado a la falta de talento disponible en ciberseguridad, un aspecto que afecta tanto el sector público como al privado. La mayoría de las organizaciones no disponemos de las personas adecuadas, con las capacidades necesarias para los proyectos de ciberseguridad que tenemos que abordar. Esto nos avoca a depender de recursos externos, que contratamos a empresas especializadas que, a su vez, también sufren la carencia de ingenieros, analistas y técnicos en ciberseguridad. El resultado es un sector tensionado y con una elevada movilidad.

Es importante apostar por retener el talento, apreciando la experiencia y el conocimiento de los especialistas en ciberseguridad. Esta es una disciplina transversal a toda la TIC de una organización. Es fundamental disponer de un equipo que conozca el negocio TIC y su impacto en la organización para responder de forma eficaz y eficiente ante un incidente de seguridad. De ello depende la continuidad del negocio y la confianza de nuestros ciudadanos y usuarios. «

TONI GARCÍA

CISO, CIO y CDO en LETI Pharma y Miembro de la Junta Directiva

ISMS FORUM

ismsforum.es

Continuidad de negocio y ciberseguridad

EL IMPACTO EN LAS PYMES

La continuidad de negocio es una actividad que incluso a las grandes empresas les resulta difícil acometer. La necesidad de establecer controles de ciberseguridad se ha incrementado exponencialmente debido al riesgo, cada vez más evidente, que implica para las compañías. Los escenarios de continuidad de negocio desencadenados por un incidente de ciberseguridad nos afectan a todos. Haber pensado en ello con anterioridades, resulta cada vez más importante.

Los planes de continuidad de negocio —que en su mayoría están basados en la ISO 22301:2019 Sistemas de Gestión de Continuidad de Negocio— son necesarios en aquellas compañías que ponen énfasis en la gestión de riesgos corporativos. En el momento que le ponemos nombre parece muy complicado, pero pongámoslo en contexto: hacer una correcta gestión de *stocks* no deja de ser valorar el riesgo de tener o no tener los productos que necesitamos, y esto no deja de ser algo relacionado con gestionar aquellos aspectos sobre los que no tenemos una certeza cierta.

Desde el punto de vista de estos riesgos, por desgracia, los eventos disruptivos —baja frecuencia y alto impacto— se producen cada vez con mayor asiduidad. Esto se analiza asociando estos eventos en escenarios como:

» **Indisponibilidad de personas.** La actual situación, fruto de la pandemia, podía contemplarse como un evento de baja probabilidad, pero hemos visto que no es así.

» **Indisponibilidad de la infraestructura.** Del mismo modo, la capacidad de acceder a un edificio o zona de trabajo también se ha visto alterada, especialmente cuando se maneja la posibilidad de un confinamiento.

» **Indisponibilidad de proveedores.** Especialmente de aquellos que pueden ser críticos para nuestro negocio y que, sin ellos, no podríamos continuar nuestra actividad, ya sea por la ausencia de materias primas, por

los servicios logísticos que prestan o por cualquier otro motivo. No contar con estos productos o servicios puede afectar gravemente a nuestro negocio.

» **Indisponibilidad tecnológica.** Todos dependemos de la tecnología en mayor o menor medida. Hablar de digitalización ya no es novedad, la comunicación bidireccional con nuestros clientes, la información crítica de la compañía, las cuentas, etc., todo esta digitalizado por los beneficios que eso implica en situaciones normales.

TENER UN PLAN B

Sin necesidad de incluir más argumentos a la situación que estamos viviendo, es evidente que hablamos de escenarios que no son nuevos. Precisamente, lo que cambia es haber pensado en ellos y en la manera que tenemos de afrontarlos. Los riesgos que pueden desencadenar todos estos eventos cada día ganan más peso. De esta forma, cada vez se hace más imprescindible tener un plan B para todos ellos.

En el caso de los riesgos tecnológicos, durante estos últimos años se han visto agravados por el ingente incremento en el número de ciberataques que, cada vez más, podríamos denominarlos como de "pesca de arrastre". Se lanzan masiva e indiscriminadamente y pueden afectar tanto a grandes corporaciones internacionales, como a medianas y pequeñas empresas, y también, como no, a particulares.

De hecho, este escenario de sensación de vulnerabilidad generalizada ha hecho necesario que, concretamente las pymes, deban contemplar de forma clara la necesidad de protegerse frente a estos riesgos, y establecer planes que les permitan reaccionar de manera rápida y adecuada frente a ataques malintencionados.

ANÁLISIS Y ACCIONES

Establecer unos mínimos controles no tiene por qué ser especialmente costoso, aunque sí muy necesario, ya que es lo que va a evitar el importante impacto que tiene para una compañía el perder su información o el acceso a ella.

Algunos puntos de análisis básicos pasan por:

» **Identificar aquellos días o periodos críticos.** Presentación de cuentas, impuestos u otras actividades que son 100% necesarias realizar en un determinado momento y que, en caso de no hacerse, pueden poner en riesgo una licencia o acarrear una multa.

» **Ser conscientes de qué información es importante para el negocio.** No tiene por qué protegerse todo el primer día, solo aquello que realmente es primordial, y poco a poco poder ampliarlo al resto si realmente es necesario.

» **Cruzar las dos anteriores y establecer puntos críticos de fallo.** Básicamente, qué tengo que hacer y qué necesito para ello. Esto, que puede parecer obvio, no lo suele ser y normalmente obliga a las empresas a tener que tomar decisiones en caliente y de forma acelerada, que no estaban planificadas con anterioridad.

En cuanto a las acciones a realizar, siguen siendo igual de básicas:

» Copias de seguridad periódicas, automatizadas y aisladas. De poco sirve hacerlo a mano, porque se trata de una actividad que puede resultar poco importante en el día a día… lógicamente, hasta que pasa algo. No depender de recordar hacer este tipo de actividades es básico, pero, del mismo modo, que esas copias no sufran la misma suerte que los datos originales también es importante. Hay que garantizar que esta información esté aislada o, por lo menos, en una ubicación distinta. Esto puede salvarnos de más de un susto.

> **Expresiones como "a mí no me pasará" o "yo no soy importante" han quedado relegadas al pasado**

» Configurar adecuadamente las redes, tanto las físicas como las inalámbricas. Desde la tienda más pequeña hasta la compañía más grande tienen una infraestructura de red montada, ya sea porque ofrecen wifi a sus clientes o porque necesitan conectar dispositivos inteligentes. Sea cual sea el caso, es importante poner las medidas necesarias para que, aunque cerremos la puerta, no estemos dejando otras abiertas.

» Establecer controles de acceso robustos, como el doble factor de autenticación. Todas las empresas tienen un correo electrónico, una herramienta de mensajería instantánea junto con su red social u otros canales de comunicación. Ya ser trate de herramientas corporativas o particulares, prácticamente todas permiten habilitar el doble factor de autenticación, que incluye algo que sabemos (el usuario y contraseña) y algo que tenemos (nuestro teléfono móvil). La excusa de "no es cómodo" pasó a la historia cuando, de media, consultamos el teléfono alrededor de cien veces al día. Es decir, cada diez minutos. Es un dispositivo que está completamente integrado en nuestro día a día y siempre a nuestro alcance.

Estas recomendaciones, que son muy básicas, a la hora de la verdad no siempre se cubren. Se refieren a los principales puntos de entrada por donde se puede sufrir un incidente de seguridad. Ser conscientes de ello es el primer paso, pero poner medidas es el segundo y, el más necesario.

Expresiones como "a mí no me pasará" o "yo no soy importante" han quedado relegadas al pasado. Estar preparado para lo que pueda venir no implica ser demasiado precavido o no arriesgar, se trata más bien de poder tomar esos riesgos en lo que realmente es importante, nuestro negocio, y ser conscientes de ello. «

Brechas de seguridad de datos personales

UNA VISIÓN PRÁCTICA

Raro es el día que no vemos alguna noticia sobre ramsonware, exfiltraciones de datos, pérdidas millonarias e incluso sanciones. Ya nadie puede poner en duda que todos somos víctimas potenciales de sucesos semejantes y es su gestión adecuada la que va a permitir minimizar el impacto en nuestras organizaciones, también en el ámbito de la privacidad.

SUSANA REY BALDOMIR

Delegada de Protección de Datos Grupo EUSKALTEL

ISMS FORUM

ismsforum.es

JAVIER LOMAS SAMPEDRO

Delegado de Protección de Datos Grupo CODERE

ISMS FORUM

ismsforum.es

En mayo de 2018 se hizo exigible el RGPD. Como responsables y encargados del tratamiento de datos personales en nuestras organizaciones, una de las principales novedades fue la doble obligación de, en determinadas circunstancias, notificar los incidentes de seguridad a las autoridades de control y a las personas físicas afectadas. Esta obligación está emparentada con otras semejantes, cada vez más presentes en la normativa de la Unión Europea, que está potenciando el desarrollo seguro de la economía digital: LPIC, ENS, directiva NIS.

Estas exigencias nacen de la experiencia acreditada de que, si los afectados comparten lo aprendido en los incidentes reales, las organizaciones podrán aspirar a mantenerse seguras o, al menos, alertas frente a un número creciente de amenazas, externas e internas. En un mundo hiperconectado, los incidentes no son algo privado. No hay islas de autogestión que no tengan influencia sobre los demás.

Desde hace tiempo se han venido produciendo iniciativas para establecer vías o espacios donde compartir información, tanto técnica como de gestión, entre los profesionales de la ciberseguridad. Compartir lecciones aprendidas siempre ha resultado muy útil, pero al realizarse de forma privada y en base a redes de confianza personales, se ha dejado fuera a muchas empresas y profesionales, y, sobre todo, a las autoridades.

A través de estas obligaciones de comunicación, las empresas pueden compartir todo ese conocimiento sin miedo a quedar expuestas a un escrutinio público no deseado y, de esta forma, dejar fluir las lecciones aprendidas a organizaciones públicas y privadas para evitar que sean las víctimas futuras de incidentes similares.

De aplicar esta misma experiencia a la privacidad, la obligación de notificar las brechas de seguridad pasaría a ser un instrumento de ayuda y apoyo a las empresas que las están sufriendo, y de prevención para el resto. Todo ello sin olvidar la comunicación directa a las personas físicas afectadas para ayudarles en la salvaguarda de sus derechos y que puedan tomar las medidas necesarias para minimizar el impacto. Además, el eco público va concienciando a la sociedad sobre los riesgos e importancia de una gestión adecuada de la seguridad en la vida diaria.

INFORMACIÓN ÚTIL Y PRECISA

Desafortunadamente, en muchos casos solo el riesgo de sanción sirve de incentivo para impulsar este conocimiento colectivo sobre la gestión de brechas de seguridad. Cuando en 2018 la Agencia Española de Protección de Datos, en colaboración con ISMS Forum, publicó la *Guía para la gestión y notificación de brechas de seguridad,* ya se buscaba "*facilitar la interpretación del RGPD en lo relativo a la obligación de notificar (...) de modo que la notificación a la autoridad competente se haga por el canal adecuado, contenga información útil y precisa*".

La norma está planteada para que los responsables deban entender cada brecha, establecer si han de notificarla, gestionarla adecuadamente y comunicar la información necesaria. Mientras hacen frente al incidente, deben ir acreditando con cuidado la labor durante la crisis, y hacerlo de un modo impecable para no exponerse a la amenaza de un procedimiento sancionador. Todo ello en el plazo límite de 72 horas.

Tres años después de la publicación de aquella primera guía, con alguna actualización realizada por parte de la Agencia, sigue siendo perfectamente útil para sus fines, pero adolece de la falta de ejemplos y casos prácticos que solo se pueden generar con los años de rodaje entre profesionales del sector. Desde la DPD Community, un grupo de estos profesionales, hemos considerado que este es un buen momento para sacar una guía práctica, una verdadera herramienta de consulta por y para profesionales, que complemente lo doctrinal de la primera y que se utilice de forma conjunta.

ANTES, DURANTE Y DESPUÉS

Todo ello organizado en base a las fases *antes, durante y después*. Para el antes tenemos la fase de ***planifica***. Desde la perspectiva de la anticipación diligente, será fundamental revisar qué cumplimos y cómo acreditarlo. El famoso *Accountability*: RAT, análisis de riesgos y evaluaciones de impacto, medidas de seguridad y mejora continua, políticas de seguridad y códigos de conducta, auditorías, etc. En esta fase se hablará de medidas técnicas y organizativas, aunque ese no será su foco.

Aquello que, previamente a sufrir el incidente, no tengamos incorporado y rodado en nuestra organización, difícilmente se podrá corregir en plena crisis, donde los tiempos se precipitan y las tensiones se incrementan a falta de una adecuada planificación.

Uno de los mensajes clave es que la mera notificación de una brecha no supone una sanción por parte de la AEPD, aunque sí resultaría de la falta de diligencia. Además, debemos cuidar y anticiparnos al máximo para evitar el impacto reputacional. Si la brecha transciende, se deberá en parte a nuestra acción u omisión.

En el segundo bloque, la fase de ***gestiona***, revisaremos la importancia de que la organización esté preparada para afrontar el incidente de seguridad de forma rápida, ordenada y eficaz, minimizando sus consecuencias también sobre terceras partes. Esto será analizado con detenimiento por la AEPD: si estamos preparados para detectar, analizar, contener, mitigar y recuperar una brecha, será más fácil mantener la calma durante la crisis.

Por supuesto, las brechas se ***notifican*** a la autoridad de control y a las personas afectadas, incluyendo los análisis del riesgo que puedan suponer para ellas. Será determinante que, como organización que trata datos personales, se tenga en mente a las personas físicas y sus datos, cómo protegerlos y cómo se pudieran ver afectados en sus derechos fundamentales. Además, habrá que tener en cuenta las posibles obligaciones de notificación más allá de la AEPD: autoridades de control de otros países (ICO), otras legislaciones (LPIC, NIS, ENS, etc), obligaciones contractuales, etc.

Por último, completaríamos con ***resuelve***, dando seguimiento a su evolución y evaluación por parte de la Agencia, lo que podría desembocar en la indeseada consecuencia de la apertura de un expediente sancionador. Tampoco debemos olvidar la gestión ulterior de la comunicación a los afectados: aclaraciones, reclamaciones de daños a terceros, ciberseguros, etc. Todo ello culminando en la gestión del posible daño reputacional que también habrá que administrar y reparar.

> **Esta Guía reunirá la experiencia y el aprendizaje de todos los profesionales de ciberseguridad y la privacidad**

Esta Guía no estaría completa si no se nutriera de la experiencia y el aprendizaje de todos, que podremos compartir en la ***encuesta*** que lanzaremos, dirigida tanto a profesionales de la ciberseguridad como de la privacidad. El objetivo es compartir fortalezas y debilidades, así como nuestra evolución como gestores de este tipo de incidentes, determinada por las nuevas reglas impuestas por el RGPD. Esto nos permitirá conocer la posición y capacidad que tiene cada una de nuestras organizaciones ante estas inevitables y permanentes amenazas; revelando lo preparados que realmente estamos para una gestión adecuada y las debilidades que deberemos corregir si queremos hacer de la notificación de las brechas de seguridad una herramienta útil de mejora.

MAX HEINEMEYER

Director of Threat Hunting

DARKTRACE

darktrace.com/es

Inteligencia artificial y *ransomware*

DETECCIÓN DE WASTEDLOCKER

Desde que se descubrió por primera vez —en mayo de 2020— el *ransomware* WastedLocker se ha convertido en una ciberamenaza de renombre. Es especialmente conocida por sus sofisticados métodos de ofuscación, así como por sus fuertes demandas de rescate. Recientemente se detectó un ataque a una organización agrícola en los Estados Unidos, mediante la tecnología de IA de autoaprendizaje que intervino cuando fallaron las herramientas tradicionales.

El ransomware WastedLocker "*lives off the land*" (vive de la tierra) utiliza herramientas y protocolos de uso común para integrarse en su entorno. Esto hace que sea extremadamente difícil de detectar para las empresas que hacen uso de una seguridad heredada, que depende normalmente de reglas y firmas establecidas. Además, un tiempo de retención cada vez menor significa que los humanos que responden solo luchan por contener la variante de *ransomware* antes de que se produzca el daño.

Sin embargo, cuando en diciembre del pasado año los ciberdelincuentes atacaron una organización agrícola con WastedLocker, la tecnología de inteligencia artificial (IA) de autoaprendizaje fue capaz de detectar e investigar el incidente en tiempo real.

> **Darktrace Antigena habría respondido a este ataque bloqueando instantáneamente el tráfico C2**

DETALLES DEL ATAQUE

Después de que un empleado fuese engañado para que se descargara una actualización falsa del navegador, la inteligencia artificial detectó que había un escritorio virtual que realizaba conexiones inusuales con destinos externos. Once minutos más tarde se realizaron una serie de escaneos inusuales, mientras el atacante buscaba posibles objetivos de Windows adicionales.

El atacante utilizó una credencial administrativa ya existente para autenticarse contra un controlador de dominio, iniciando un nuevo control de servicio sobre SMB *(server message block)*. Varias horas después, durante la madrugada, utilizaron una cuenta de administrador temporal para pasar a otro controlador de dominio. En ese momento, la tecnología de inteligencia artificial de Darktrace puso en marcha un proceso de investigación automático sobre el incidente e inmediatamente generó un resumen de alto nivel.

BLOQUEAR Y CARGAR

El atacante logró establecer conexiones administrativas y remotas exitosas con otros dispositivos internos. Poco después se detectó una transferencia de archivos .csproj sospechosos. Darktrace Antigena habría respondido a este ataque bloqueando instantáneamente el tráfico C2. Se trata de la primea solución de respuesta autónoma del mundo. Está basada en la galardonada ciber IA y es capaz de responder a ciberataques en cuestión de segundos. La tecnología funciona como un anticuerpo digital que genera de manera inteligente respuestas dirigidas y proporcionales cuando se produce algún incidente que suponga una amenaza en la red, el correo electrónico o entornos de la nube.

Darktrace Antigena emprende acciones contra las ciberamenazas en curso, deteniendo los ataques antes de que provoquen daños. Antigena reacciona en segundos, tomando decisiones autónomas —basadas en un comportamiento combinado— en tiempo real que se actualizan repetidamente mediante una observación continua de las amenazas a medida que se desarrollan.

CONFIAR EN LA IA

Es evidente que el *ransomware* se ha desarrollado mucho durante este año y los cibercriminales están creando constantemente nuevos TTP (tácticas, técnicas y procedimiento) de ataque. A medida que el tiempo de retención se reduce a horas en lugar de días, los equipos de seguridad confían cada vez más en la inteligencia artificial. Estas tecnologías ayudan a evitar que las amenazas se intensifiquen ante los primeros signos de compromiso y también permiten contener ataques incluso cuando ocurren de noche o durante el fin de semana.

Sin el uso de la inteligencia artificial, este atacante habría cifrado archivos confidenciales, impidiendo las operaciones comerciales en un momento crítico y, posiblemente, infligiendo enormes pérdidas financieras y de reputación. ⋘

Data-Centric oriented SASE

CLOUDIFICACIÓN DE LAS ORGANIZACIONES

Apoyándose en la plataforma Forcepoint Cloud Security Gateway, Forcepoint DLP permite extender la capacidad de protección de información más allá de la solución SASE, aplicarla sobre otros canales de comunicación o incluso proteger la información sensible en el puesto de usuario frente a posibles fugas hacia repositorios locales.

La arquitectura SASE *(secure access service edge)* representa la evolución de las plataformas actuales de seguridad con el objetivo de hacer frente a los nuevos desafíos que van apareciendo. Esta arquitectura ha de entenderse como una solución *cloud,* que integra múltiples tecnologías en una propuesta única:

» Se utilizan tecnologías avanzadas de análisis de contenido que permiten proteger a los usuarios frente a las amenazas externas, así como establecer controles en el uso de Internet.

» Busca controlar el acceso y el uso de aplicaciones *cloud* por parte de los usuarios, ya sean corporativas o no. Incluso puede utilizarse para el control del denominado *shadow IT*, o tecnología en la sombra, y facilitar el acceso a aplicaciones corporativas privadas.

» Ofrece tecnologías que permiten proteger el activo más valioso de las organizaciones: la información.

PROTEGER

El control y protección de la información es una característica transversal de la arquitectura SASE. De hecho, estos controles se aplican en el acceso a la web pública y a las aplicaciones corporativas en la nube, pero también a las aplicaciones privadas. De este modo es posible establecer políticas de uso adecuado de la información sensible de la organización en los diferentes ámbitos de protección. Precisamente por eso, por la importancia capital que tiene la protección de la información en las organizaciones, es por lo que se hace necesario adoptar una orientación *data-centric* —o de protección del dato— en las arquitecturas SASE.

La propuesta de Forcepoint en el ámbito de la prevención de fugas de información — Forcepoint DLP— presenta una serie de especiales características, como sus capacidades avanzadas de detección y protección de la información, su multicanalidad o su capacidad de aplicación de políticas adaptativas en función del comportamiento del usuario. Esta tecnología forma parte de la solución Forcepoint Cloud Security Gateway, integrada de forma transversal y consolidada con el resto de las tecnologías de protección de usuarios y de aplicaciones que ofrece este producto SaaS.

IDENTIFICAR

Una tecnología DLP *(data loss prevention),* diseñada para detectar potenciales brechas de seguridad en los datos, debe disponer de técnicas avanzadas que permitan la identificación de información. Sin ellas, la solución no va a ser capaz de reconocer los datos sensibles, algo que normalmente resultará en innumerables falsos positivos.

Metodologías como la búsqueda de palabras o patrones preconfigurados pueden servir para realizar una prueba, pero no son soluciones reales. Por el contrario, es recomendable utilizar técnicas de identificación de información sensible que hacen que la tecnología DLP aporte un gran valor a la solución SASE, como:

» Utiliza patrones con algoritmia y análisis de contexto.

» Técnicas de finger printing o huellas de información que permiten detectar información estructurada y no estructurada y las partes que la componen.

» Tecnologías relacionadas con la identificación de caracteres en imágenes

» Etc.

LUCAS REY

Channel Sales Manager

FORCEPOINT

forcepoint.com/es

> El control y protección de la información es una característica transversal de la arquitectura SASE

EXTENDER LA PROTECCIÓN

Además, es importante tener en cuenta que la tecnología permite extender esta capacidad de protección de información más allá de la solución SASE, y aplicarla sobre otros canales de comunicación como pueden ser el correo electrónico, los puestos de los usuarios y los repositorios de información.

Por último, ahondando en la filosofía de convergencia tecnológica, el mismo agente de puesto de usuario permite también la conexión con la plataforma SASE para, de forma adicional, proteger la información sensible en este punto frente a posibles fugas de información hacia, por ejemplo, repositorios USB, discos locales, etc. «

MIKE ANDERSON

Chief Digital and Information Officer

NETSKOPE

netskope.com/es

La colaboración como terapia

CONFLICTO ENTRE REDES Y SEGURIDAD EN EUROPA

La rivalidad entre los departamentos de redes y seguridad puede impedir que las empresas obtengan los resultados esperados de sus proyectos de transformación digital. Acabar con este lance es un paso crítico en este tipo de procesos, y la creación de equipos interfuncionales es un comienzo

Aunque la transformación digital es un término que puede aplicarse a una enorme variedad de proyectos, el patrón general pasa normalmente por replantear las arquitecturas de red y de seguridad, lo que va a gestionar nuevos flujos de trabajo y también diversos riesgos.

Tal es su importancia que este tipo de proyectos podría recibir una dotación de hasta 6,8 billones de dólares en todo el mundo entre 2020 y 2023, según IDC. Sin embargo, la falta de colaboración entre los departamentos de redes y seguridad podría abrir un cisma perjudicial.

Es más, según una investigación realizada por Censuswide para Netskope en el mercado europeo, el 54% de los CIOs cree que esta ausencia de cooperación impedirá a su organización alcanzar los beneficios de la transformación digital, como pueda ser la implementación de una estrategia SASE, basada en la convergencia de redes y seguridad.

> **El problema reside en un desacuerdo entre las figuras del CIO y del CISO, cuyas prioridades chocan entre sí**

EL ORIGEN DE LA RIVALIDAD

La investigación muestra que las diferencias entre estos departamentos no radican en que tengan objetivos diferentes. Por un lado, hay que tener en cuenta que ambos trabajan para apoyar el aumento de la productividad, impulsar la infraestructura e incrementar la visibilidad y el control. Tampoco es debido a una posible falta de colaboración, ya que el 85% están o han colaborado en un proyecto de transformación digital; ni tan siquiera en un problema de ideología subyacente, teniendo en cuenta que el 82% afirma que "la seguridad está integrada en la arquitectura de la red".

El problema reside en un desacuerdo entre las figuras del CIO y del CISO, cuyas prioridades chocan entre sí.

EQUIPOS INTERFUNCIONALES

Ante este escenario, cómo se puede plantear una solución al problema. La creación de equipos interfuncionales puede ser la respuesta. De este modo, modelos como DevOps —para la construcción, despliegue y ejecución de un producto o software— han demostrado su eficacia y ya se replican a otros niveles, también en el ámbito de la seguridad:

» SecOps (seguridad + operaciones de TI)

» DevSecOps, donde la seguridad de las aplicaciones y la infraestructura se diseñan desde el principio.

En los últimos años se han formado también "Tiger Team", encargados de abordar retos empresariales concretos como el de habilitar y asegurar el trabajo remoto por la COVID-19.

Por tanto, la creación de equipos interfuncionales podría acabar con la división entre red y seguridad. En este sentido, convertir los centros de operaciones de red y de seguridad (NOC y SOC) en un centro de operaciones de seguridad y redes (SNOC) sería un gran paso en la dirección correcta.

DIGITAL TRANSFORMATION NEEDS A MORE PERFECT UNION

Investigación realizada entre febrero y abril de 2021. Se ha entrevistado a 2675 profesionales de TI en América del Norte (Canadá y Estados Unidos), Europa (Francia, Alemania y Reino Unido) y América Latina (Argentina, Brasil, Chile, Colombia y México).

Puede descargar los resultados globales de la investigación haciendo clic **aquí.**

Si no puedes ganarlos...

AJEDREZ Y CIBERSEGURIDAD

RAÚL GORDILLO

Regional Sales Manager

PCYSYS

pcysys.com

Gary Kasparov explica que Deep Blue no le ganó en el año 1997 porque fuera mejor que él jugando al ajedrez, si no porque, al disponer de un mayor número de movimientos y combinaciones en un menor tiempo, cometió menos errores (soportando mejor la presión). De ahí viene el título de este artículo: "Si no puedes ganarlos, únete a ellos".

Los que habéis asistido últimamente a alguna de mis presentaciones en PCYSYS (acrónicmo de Proactive Cyber Systems), sabréis que incluyo un par de referencias al mundo del ajedrez tan de moda últimamente gracias a la serie Gambito de Dama.

El motivo por el que lo hago es intrínseco a la compañía: desde Arik Liberzon, fundador y CTO; hasta Amitai Ratzon, nuestro CEO, que interviene en esta X edición del Foro de la Ciberseguridad y que, junto con Gary Kasparov, explicó perfectamente en una entrevista que podéis ver en este vídeo de Youtube las posibilidades que ofrece la tecnología la hora de realizar pruebas automáticas de penetración y elevar el nivel de validación de seguridad en las empresas.

PenTera es una solución completa de *pen testing* totalmente automatizada. Esta plataforma, que permite la automatización de la validación del riesgo a nivel corporativo, permite realizar pruebas continuas de penetración, consiguiendo mejores resultados en un menor tiempo, comparado con las pruebas manuales tradicionales. Su objetivo es abarcar todos los activos de una compañía, analizando y comprobando sus vulnerabilidades, sus fallos de configuración, la eficacia de las medidas de seguridad de la red y de las políticas de *passwords*. Además, busca también explotar éticamente todas las brechas de seguridad que suponen un claro riesgo para la compañía, hacerlo en el menor espacio de tiempo y de forma automática. Todo ello sin necesidad de tener conocimientos de *hacking* ético o ser un maestro de ajedrez.

» ANTICIPARSE A LOS MOVIMIENTOS

Como comenta Arik Liberzon, es increíble el paralelismo que existe entre un tablero de ajedrez y la ciberseguridad. Él lo sabe bien, ya que lo vivió desde niño. Su abuelo, Vladimir Liberzon, fue un gran maestro de ajedrez Ruso e Israelita, que le inculcó el interés por el juego. Si somos capaces de anticiparnos a los movimientos de los oponentes, varios pasos por delante, podremos defender y proteger nuestras piezas (activos), para ganar la partida.

Ese es el objetivo de PenTera: ofrecer a cada CSO *(chief security officer)* un gran maestro a su lado en forma de un software inteligente de *pen testing*. La posibilidad de realizar *machine-based pen testing* de forma automática, que continuamente piensa y actúa como un *hacker,* es la mejor forma de asegurar a las compañías que tienen sus ciberdefensas lo más ajustadas y fuertes posible, tal y como deberían ser.

Las líneas de defensa deben adaptarse a las amenazas al mismo ritmo que avanzan las técnicas de ataque, campañas, vulnerabilidades, etc.

> **Las líneas de defensa deben adaptarse a las amenazas al mismo ritmo que avanzan las técnicas de ataque**

El hecho es que, hoy en día, más del 95% de la inversión en tecnología de ciberseguridad se realiza en tecnologías de defensa, que no tienen la capacidad de evolucionar y alinearse con la perspectiva y forma de actuar en la mente de un *hacker*. Estos ciberdelincuentes tienen en cuenta diferentes vectores de ataque y, además, lo hacen en varios pasos de la *kill chain* en lugar de buscar solo vulnerabilidades conocidas pero que, en multitud de ocasiones, no son explotables ni producirán un daño a la organización.

Por último, aquellos que hayan asistido a la sesión de Amitai Ratzon, ya sabréis cuál es la otra analogía que utiliza con el ajedrez... Si no habéis podido asistir, ya sabéis dónde me podéis encontrar. «

JAVIER CARRERAS

Southern Europe Sales Manager

RECORDED FUTURE

recordedfuture.com

Tempus fugit

RETOS DIARIOS DE LOS EQUIPOS DE SEGURIDAD

Tiempo, o más bien la falta de éste, es sin lugar a duda uno de los mayores problemas con los que se encuentran todos los equipos de seguridad, independientemente de su tamaño, especialización o de la organización para la que trabajen. En este breve artículo voy a poner sobre la mesa algunos ejemplos concretos de situaciones que ocasionan esta falta generalizada de tiempo a la que se enfrentan los profesionales de la seguridad.

Los equipos de operaciones se ven abrumados por el número de vulnerabilidades existentes, que tratan de priorizar haciendo uso de los datos tradicionales de criticidad publicados en la NVD (National Vulnerability Database), el repositorio del gobierno de Estados Unidos en cuanto a los datos de gestión de vulnerabilidades basados en estándares, y representados mediante el protocolo de automatización de contenido de seguridad (SCAP).

En 2020 se publicaron 18.335 vulnerabilidades nuevas. De ellas, solo 2.761 fueron clasificadas como de baja severidad. De este modo, la mayoría de las organizaciones simplemente aplica los parches basándose en estos niveles de gravedad. Pero, si tenemos en cuenta que un 85% de las vulnerabilidades detectadas tienen un nivel de severidad entre medio y alto, ¿por dónde empezamos?

Además, para incidir en este tema, solo un 5,5 % de todas las vulnerabilidades llega realmente a explotarse. Al no disponer de un contexto adecuado sobre la información del *exploit*, las empresas terminan desperdiciando una cantidad considerable de recursos solucionando vulnerabilidades de bajo riesgo, al tiempo que ignoran las que son más importantes.

> **Para mitigar el riesgo de forma eficaz hay que moverse igual de rápido que los autores de las amenazas y sus tácticas**

INFORMACIÓN INSUFICIENTE

Por otro lado, estudiar miles de eventos resulta abrumador, incluso para el técnico respuesta a incidentes más experimentado. Al disponer de información insuficiente, es difícil determinar qué alerta representa un incidente crítico y cuál puede ser simplemente una redundancia o un falso positivo. Se desperdician horas y horas en examinar alertas irrelevantes, mientras que los verdaderos positivos pueden estar colándose por las fisuras.

De igual manera, la mayor dificultad para los analistas de inteligencia de amenazas, o *threat hunters*, es la cantidad de recursos que tiene que invertir en cada una de ellas. Se dedica demasiado tiempo en tareas como recopilar, contextualizar y analizar manualmente datos inconexos para poder extraer inteligencia aplicable.

Con el objetivo de poder mitigar el riesgo de forma eficaz, es importante moverse igual de rápido que los autores de las amenazas y sus tácticas (TTP, tácticas, técnicas y procedimientos). Teniendo en cuenta el escenario actual, resulta evidente que el laborioso proceso de investigación manual da lugar a huecos importantes en su análisis, y también a amenazas no identificadas, lo que pone en riesgo a la organización.

EN TIEMPO REAL

Otro ejemplo de la baja eficiencia de estos análisis manuales lo podemos observar si nos centramos en algo que está muy de moda en la actualidad: la vigilancia digital. Hablamos de monitorizar, constantemente y en tiempo real, las campañas de *phishing*, las fugas de propiedad intelectual o de las credenciales, así como la posible suplantación de identidad de nuestros VIP. Todos estos procesos pueden suponer una inversión en recursos muy importante que no podemos despreciar.

Hay muchos más ejemplos en esta misma línea, como la baja optimización de los análisis de riesgos de terceros dentro de los equipos de GRC, independientemente de que, además, solo devuelven una foto estática.

Si se ha sentido identificado con alguna de estas casuísticas, no desespere. Lamentablemente no podemos dotar de más horas al día, pero existen soluciones de inteligencia de seguridad que le permitirán dar una respuesta más rápida y certera a estas y otras problemáticas. «

Gestión de identidades y accesos

CARLOS FERRO

Vicepresidente SEEMEA

THYCOTIC CENTRIFY

thycotic.com

ASEGURAR LA NUBE CORPORATIVA

La pandemia ha acelerado muchos procesos de digitalización y ha descubierto la necesidad de mejorar los accesos remotos, tanto de empleados como de terceros, a nuestros sistemas. En un mundo cada vez mas dinámico, la única constante es la identidad de los que deben acceder a la información y sistemas críticos.

La pandemia de la COVID-19 ha acelerado los proyectos de transformación digital y la migración a la nube de multitud de empresas. Las cifras hablan por sí solas. El 90% de las empresas están adoptando esta tecnología de alguna manera y el 80% de los presupuestos de TI se centran ahora en soluciones en la nube. En cualquier caso, aunque la nube ha permitido aumentar la agilidad y la eficiencia, y ha reducido los costes para muchas empresas, la velocidad con la que las organizaciones han enfrentado estos procesos de migración también ha abierto nuevos riesgos de seguridad.

» IDENTIDADES Y LOS ACCESOS PRIVILEGIADOS

Tanto por la adopción a la nube como por la necesidad de permitir el acceso remoto a la información critica, los conceptos de perímetro o entornos de confianza comienzan a desdibujarse y se hacen cada vez más dinámicos.

De hecho, tienen como única constante las identidades que acceden a esta información.

Precisamente, un informe de Verizon de 2020 destaca que las credenciales están involucradas en el 77% de las filtraciones en la nube. Estos datos deberían hacer saltar todas las alarmas en cualquier empresa que opere en la nube, ya que ponen de manifiesto que las soluciones de seguridad tradicionales ya no son suficientes. Ahora entran en el escenario dos nuevas claves: las identidades y los accesos privilegiados.

Los antiguos conceptos de identidades o accesos privilegiados han evolucionado más allá del entorno de TI. Cada vez hay más identidades que son críticas teniendo en cuenta la información sensible que gestionan y debemos tratarlas como tal. Por ello, la gestión de identidades privilegiadas (PAM) ha evolucionado para aumentar la postura de seguridad sobre estos aspectos a través de con controles de autenticación, autorización, accesos más sólidos para los usuarios, así como su monitorización y trazabilidad.

Estas tecnologías han evolucionado y sus necesidades también. De esta forma, el analista internacional KuppingerCole estima que el mercado crecerá mas de 100% en los próximos cuatro años, alcanzando una cifra de negocio cercana a los 5.400 millones de dólares en 2025. Y es que, en el futuro, todas las identidades serán privilegiadas.

> **Más del 60% de las identidades digitales no pertenecen a personas y requieren una gestión diferente para asegurarlas**

» GESTIÓN *CLOUD* DE IDENTIDADES

Un dato especialmente llamativo es que más del 60% de las identidades digitales —y, por ende, de las identidades privilegiadas—no pertenecen a personas y requieren una gestión diferente para asegurarlas. Hablamos de dispositivos autónomos, sistemas, base de datos, etcétera que se identifican e interactúan entre sí para compartir y distribuir información sensible. Por lo tanto, son vulnerables frente a ataques dirigidos, tal y como como se ha visto en los últimos cinco años.

Desde ThycoticCentrify, la fusión de dos lideres en gestión de Identidades, estamos trabajando para dar respuesta a estas nuevas necesidades. Según la consultora Gartner, somos líderes en la gestión *cloud* de identidades, ya que proporcionamos la plataforma mas completa y granular del mercado. Esto nos permite acelerar los procesos de implementación e integración con los sistemas existentes, potenciar las inversiones ya realizadas y acompañar a nuestros clientes en el proceso de transformación digital en entornos TI y TO. «

DIDIER SCHREIBER

Marketing Director Southern Europe

ZSCALER

zscaler.com

Internet, la nueva red corporativa

CLOUDIFICACIÓN DE LAS ORGANIZACIONES

Durante mucho tiempo, la red empresarial era similar a un castillo, aislado del mundo exterior por un foso perimetral que era una red de área local (LAN), y con un puente levadizo que era una red de área amplia (WAN) defendida desde dentro de los muros del castillo. Un camino de entrada, un camino de salida, con pocas razones para que los datos y los usuarios salieran. La seguridad parecía sencilla.

La red empresarial actual es algo mucho más grande y amplia. En un momento en el que las empresas siguen adoptando servicios en la nube y soportando flujos de trabajo más móviles y flexibles, el alcance de la red se extiende mucho más allá de los muros del castillo y dentro de Internet. El modelo cliente/servidor tradicional, y los modelos de seguridad en las instalaciones, ya no son los más efectivos, o los más responsivos, teniendo en cuenta la cambiante topología de la red. Además, cada vez más, el panorama de las amenazas es mayor y más complejo.

Proteger el perímetro del castillo ya no es suficiente. La noción de este borde que limita el radio de acción de los usuarios tiene que ir mucho más allá, rodeando Internet y las ubicaciones externas que la gente visita fuera de las defensas que protegen a la organización.

> **Cuando Internet es la red empresarial, el castillo fortificado y lugar de negocio pueden estar en cualquier lugar del mundo**

LA TRANSFORMACIÓN DE LA NUBE

Cuando se observan los niveles de tráfico WAN actuales, es evidente que casi todo el volumen de datos fluye hacia y desde Internet. Esta realidad, combinada con el creciente número de dispositivos que utilizamos diariamente, conforma un escenario en el que se ha incrementado de forma exponencial el número de objetivos y rutas de actuación para los cibercriminales, los creadores de *malware* y los defraudadores.

No hay más que ver algunos ejemplos de todas los servicios y aplicaciones que utilizamos cada día en nuestro lugar de trabajo —que ya no está alojado *in situ* o en otra sucursal conectada mediante una línea alquilada— como pueden ser el correo electrónico, la Intranet corporativa, herramientas como Microsoft 365, el CRM…

Esta transformación de la nube ha sido impulsada por el auge de los dispositivos móviles y de los usuarios remotos. No cabe duda de que ha ayudado a fomentar una cultura de acceso a servicios y datos en cualquier momento, desde cualquier dispositivo y lugar. Respondiendo a esta tendencia, la productividad empresarial y los servicios de comunicaciones han migrado —diría que con gran éxito— hacia la nube, fuera del tradicional ordenador de sobremesa.

UN PERÍMETRO ALREDEDOR DE INTERNET

Si tenemos en cuenta el escenario descrito, es evidente que la seguridad necesita una estrategia similar. El entorno ha cambiado y el antiguo método de apilar dispositivos de seguridad en el centro de datos, y de crear un foso de protección, ya no es efectivo.

En Zscaler estamos siendo testigos de cómo se está produciendo esta *cloudificación* de las organizaciones, un fenómeno que está ocurriendo en algunas de las empresas más grandes y complejas del mundo. Internet se está convirtiendo en su red corporativa. La forma en la que estamos respondiendo a este escenario es colocar —de forma efectiva— un perímetro alrededor de Internet mediante el que proteger a los usuarios accediendo a esta red en cualquier lugar y desde cualquier dispositivo.

Por último, es importante también tener en cuenta que este no es un aspecto únicamente relacionado con TI, sino que es un asunto de transformación empresarial, en el que la seguridad tiene que ser un elemento principal.

Cuando Internet es la red empresarial de una empresa, su castillo fortificado y lugar de negocio pueden estar en cualquier lugar del mundo. ⋘

CERTIFICACIÓN DE DELEGADO DE PROTECCIÓN DE DATOS - CDPD

ISMS Forum se constituye como Entidad de Certificación de manera definitiva desde el 11 de octubre de 2018 en virtud del Esquema de Certificación para Delegados de Protección de Datos impulsado por la Agencia Española de Protección de Datos (AEPD) y siguiendo el procedimiento de acreditación de ENAC.

ACREDITACIÓN DE PRE-REQUISITOS

Se debe remitir la Solicitud de certificación, Solicitud de Convocatoria de Examen y el modelo de Justificación de Prerrequisitos a fin de realizar una valoración previa por parte del Comité Certificador.

PRÓXIMA EDICIÓN

MADRID

Viernes 18 de junio
Oficinas de ISMS Forum, C/Segre, 29, 1ºB
28002, Madrid.
De 10:00 a 14:00h.

BARCELONA

Miércoles 23 de junio
ICAB de Barcelona, C/Mallorca, 281
08037, Barcelona
De 10:00 a 14:00h.

Escríbenos a info.cdpd@ismsforum.es para más imformación.

CCSP: CERTIFIED CYBER SECURITY PROFESSIONAL

Certified Cyber Security Professional (CCSP) nace con el objetivo de ser la primera certificación española dirigida a los profesionales del ejercicio de gobierno de la ciberseguridad. La obtención de la certificación acredita un alto nivel de especialización en ciberseguridad y reconocimiento del ejercicio de la profesión.

PRÓXIMA EDICIÓN

Jueves, 3 de Junio
Jueves, 10 de Junio
Oficinas de ISMS Forum, C/Segre, 29, 1ºB
28002, Madrid.
Horario: 10:00 a 13:00h.

CDPP: CERTIFIED DATA PRIVACY PROFESSIONAL

Certified Data Privacy Professional (CDPP) acredita un alto nivel de especialización en la normativa española en materia de Protección de Datos de carácter personal, tanto en un contexto local, como en un contexto europeo e internacional, así como un dominio de los fundamentos que rigen la Seguridad de la Información.

PRÓXIMA EDICIÓN

Jueves, 1 de Julio
Viernes, 2 de Julio
Oficinas de ISMS Forum, C/Segre, 29, 1ºB
28002, Madrid.
Horario: 09:30 a 12:30h.

Escríbenos a certificacion@ismsforum.es | www.ismsforum.es

Una cuestión de seguridad

CONECTAR USUARIOS Y APLICACIONES

FEDERICO DIOS

Pre-sales Senior Manager

AKAMAI

akamai.es

El axioma "el trabajo es lo que haces, no dónde lo haces" nunca había sido tan cierto como ahora. Ya nadie cuestiona desde dónde trabajas, sino cuáles son tus resultados. Parece que algo nos ha enseñado esta pandemia.

Durante estos meses, la reacción de las organizaciones al desafío de asegurar el acceso remoto de sus empleados se ha desarrollado en tres fases:

» El pánico de tener a toda la plantilla trabajando desde casa, generalmente ampliando una VPN a toda prisa.

» Parchear una red que podía utilizarse como punto de entrada para las ciberamenazas y asegurar unas conexiones remotas, a las que accedía toda la plantilla, mejorando la mejor protección de los puntos finales, añadiendo más defensas contra DDoS para las pasarelas VPN (que de repente se convirtieron en el eje de toda la empresa) y actualizando las herramientas anti phishing.

» Por último, el reconocimiento de que debía haber una forma más inteligente de actuar.

Conectar a una organización entera a través de redes privadas virtuales no era sostenible desde el punto de vista del rendimiento o la seguridad. Nacía la necesidad de conectar datos y usuarios desde cualquier lugar y, sin embargo, seguían encerrados en el envío de tráfico por túneles virtuales, ubicaciones fijas y cuellos de botella. A medida que el mundo se reabre, un entorno de trabajo híbrido será lo habitual y el reto será mantener la flexibilidad sin comprometer la seguridad.

El nuevo enfoque debe facilitar un trabajo eficaz sin tener que hacer malabarismos con múltiples conexiones VPN a medida que las aplicaciones migran de los centros de datos a la nube. Hay que enrutar el tráfico a través de un sistema de seguridad central para volver a salir a la nube, en lugar de ir directamente hasta allí. No hay que olvidar que los ciberataques RDP crecieron un 768% en 2020.

En lugar de conectar las máquinas a las redes, debemos centrarnos en conectar a los usuarios con las aplicaciones, con soluciones como *zero trust* y autenticación multifactor (MFA) para reducir drásticamente el riesgo y mejorar el rendimiento. ⋘

Estrategias *zero trust* y SASE

CÓMO DESESTABILIZAR UN SOC

PEDRO MARTÍNEZ BUSTO

Responsable de Desarrollo de Negocio

HPE ARUBA

arubanetworks.com

Un estudio del Instituto Ponemon sobre las mejores prácticas en materia de seguridad revela que más del 70% de los encuestados optarían por una solución *cloud*, combinando los mejores proveedores —en lugar de uno único— para diseñar una infraestructura *zero trust* y SASE.

El objetivo es generar un marco de políticas consistente para todas las soluciones de seguridad. Además, facilita que las compañías evolucionen a su ritmo, desde las arquitecturas de red existentes (focalizadas en el centro de datos y con seguridad basada en un perímetro tradicional) a una centrada en la nube y apoyada en los principios de *zero trust* y SASE.

Las políticas basadas en arquitecturas *zero trust* enfocan la seguridad bajo la premisa de que cualquier dispositivo conectado a la red corporativa puede ser una amenaza. Es evidente que este tipo de estrategias se están adoptando de forma masiva. Además, cuentan con la ventaja de que se apoyan en tecnologías ya existentes, por lo que no es preciso el desarrollo de nuevas herramientas.

Con esta estrategia, cada usuario recibe el nivel mínimo de acceso necesario para el desempeño de sus tareas y no va a tener acceso a toda la red. La información de contexto permite —a través de mecanismos avanzados de autenticación— delimitar quién accede, a través de qué tipo de dispositivo y desde dónde, para controlar los accesos a los datos, a las aplicaciones, a otros dispositivos, etc. Esta información contextual permite asociar toda una serie de atributos a ese perfil que permitan su rápida identificación de forma automática.

Zero trust, combinado con herramientas basadas en inteligencia artificial para el análisis del comportamiento de la red, permite plantear estrategias de defensa más robustas: sabiendo cómo se comporta de forma natural una red y los dispositivos que están conectados a ella, se puede determinar si cualquier variación en ese comportamiento puede ser indicativa de algo sospechoso. Esto permitirá aislar los dispositivos dudosos para evitar que la totalidad de la red pueda ser comprometida. ⋘

El fin de las VPN

ARQUITECTURAS SEGURAS MEJORADAS

La tecnología VPN está diseñada para proporcionar acceso y proteger los datos en tránsito fuera de la red corporativa tradicional. Se despliega más como un habilitador de negocios que como una herramienta de ciberseguridad, ofreciendo la capacidad de extender la red corporativa a los usuarios en cualquier lugar, en casa, en un avión, en un hotel...

Muchas empresas utilizan las VPN para conceder acceso a la red a empleados, terceros, proveedores, invitados... cualquiera que pueda comprometer un punto de entrada a la VPN. Esto, en sí mismo, es un grave descuido de seguridad.

En los últimos años, hemos visto docenas de vulnerabilidades de VPN explotadas en importantes violaciones corporativas y gubernamentales. Las VPN se han convertido en un objetivo. Los *hackers* saben que, si pueden penetrar a través de una VPN, no tienen que preocuparse por los controles de seguridad tradicionales, como los cortafuegos. Ahora tienen acceso completo a la red de la empresa. Además, las VPN suelen estar mal configuradas, lo que crea vulnerabilidades que pueden ser explotadas por los atacantes.

En lugar de una arquitectura de seguridad de "castillo fuerte", que supone que todo lo que está dentro del perímetro de la red es seguro, las organizaciones deben comprender qué recursos deben estar disponibles dentro de la red corporativa y qué usuarios necesitan realmente acceder a esos recursos. También deben planificar cuidadosamente una política básica de mínimos privilegios para evitar conceder acceso cuando no sea necesario.

El modelo de *zero trust* —que se basa en denegar el acceso por defecto a cualquier persona o sistema a menos que sea necesario— representa un avance constructivo hacia una arquitectura más segura. Este enfoque, combinado con la evolución de la arquitectura de seguridad, permite a menudo sustituir las VPN por una mejor gestión de los accesos privilegiados.

La optimización de las alertas y la supervisión, así como la capacidad para aislar las cosas, es realmente importante. También resultan fundamentales para construir la arquitectura segura que hoy en día necesitan las empresas. «

WILLIAM CULBERT

Director
Southern Europe

BEYOND TRUST

beyondtrust.com/es

Seguridad desde el inicio

ENFOQUES *SHIFT LEFT*

La nueva normalidad ha traído aparejada el teletrabajo. Aunque ya era una opción en muchas empresas, en el escenario actua resulta de lo más usual en la mayoría de las organizaciones, lo que ha provocado que los equipos de trabajo estén más distribuidos que nunca. Hace unos años esto hubiera sido impensable, pero las posibilidades que ofrecen las tecnologías *cloud* han facilitado esta transición, por otra parte obligatoria debido a los confinamientos en medio mundo. El impacto del *cloud* es claro: IDC lo sitúa en un 90% de las empresas.

Pero no todo es color de rosa. Un sistema que funciona solamente *online,* y al que puede acceder cualquier usuario y desde cualquier lugar, es muchísimo más vulnerable que los sistemas tradicionales... si no se protege adecuadamente.

Los sistemas basados en la nube demandan su propia estrategia de seguridad. El problema aparece cuando se adaptan enfoques tradicionales de red a un entorno *cloud* nativo. Para empezar, hay que tener en cuenta que la seguridad en la nube sigue el modelo de responsabilidad compartida, es decir, los proveedores tienen su parte de trabajo a la hora de proteger la infraestructura, pero las empresas y los usuarios también deben asegurarse de que sus activos están seguros. Si una de las dos partes falla, la información se pondrá en riesgo.

Los ciberdelincuentes lo saben. Esta es una de las razones por las que la seguridad debe integrarse desde el inicio del desarrollo de cualquier aplicación, no añadirse después. Es lo que se llama *shift left*, una práctica orientada a detectar y prevenir defectos desde el inicio, con el objetivo de mejorar la calidad desplazando a la izquierda las tareas tan pronto como sea posible.

Haciendo números, este enfoque resulta hasta seis veces más barato que incluir la seguridad una vez diseñada la aplicación, y hasta quince veces más efectivo en costes que lo que supone realizar cambios en la fase de comprobación para integrar los protocolos de seguridad. «

JOAN TAULÉ

Vicepresidente
Sur de Europa

CROWD STRIKE

crowdstrike.com/es

ENRIQUE VALVERDE

Sales Engineer Cytomic

CYTOMIC

cytomic.ai/es

Malware fileless

TRES MEDIDAS SENCILLAS PARA MANTENER TU EMPRESA SEGURA

La ciberseguridad es una carrera armamentística en la que las herramientas defensivas y el entrenamiento empujan a los creadores de amenazas a adoptar técnicas de intrusión aún más sofisticadas y evasivas para entrar en las redes de las víctimas. Un ejemplo de ello es el *malware* sin archivo o *malware fileless*, que nunca toca el almacenamiento de la víctima.

Parte de la razón por la que los programas informáticos maliciosos de tipo *fileless* se han convertido en una técnica de ataque tan popular es que resulta sumamente difícil identificarlos con precisión, así como bloquear las etapas iniciales de esos ataques sin provocar accidentalmente falsos positivos e impedir que las mismas herramientas realicen actividades legítimas.

Aunque la mayoría del *malware fileless* comienza con algún tipo de archivo *dropper*, hay que tener en cuenta que existen variantes más evasivas que realmente no requieren un archivo. Generalmente, estas instancias se originan de dos maneras: explotando una vulnerabilidad de ejecución de código en una aplicación; o, la más común, utilizando credenciales robadas para abusar de las capacidades de una aplicación conectada a la red para ejecutar comandos de sistema.

DEFENDERSE DEL *MALWARE FILELESS*

El uso de este tipo de *malware* no hará más que crecer en prevalencia en el futuro, ya que herramientas como PowerSploit facilitan que incluso los ciberdelincuentes novatos lancen ataques evasivos. El modo adecuado para combatir esta amenaza es centrarse en el despliegue de soluciones de seguridad EPP y de detección y respuesta en los *endpoints* (EDR), capaces de identificar los indicadores que existen únicamente en la memoria.

También es fundamental promover prácticas de contraseñas robustas en toda la empresa, respaldadas por una autenticación multifactor (MFA) siempre que sea posible. Esto permitirá evitar que el robo de credenciales pueda iniciar un ataque.

Combinadas, estas estrategias pueden ayudar a reducir significativamente el riesgo de sufrir una brecha de seguridad ocasionada por un *malware fileless* más allá de la red.

MARC VAN ZADELHOFF

CEO

DEVO

devo.com

La pregunta de los 5TB

CÓMO DESESTABILIZAR UN SOC

Uno de nuestros clientes me habló acerca de "la pregunta de los 5TB". Permíteme mostrarte cómo funciona. El CISO recibe una pregunta sencilla del CEO, que va a requerir al menos 5TB al día de ingesta adicional de datos y análisis para poder darle una respuesta satisfactoria. La primera vez que esto le ocurrió a uno de nuestros clientes, el SOC de su empresa se saturó.

Pregunté a otros clientes sobre su "pesadilla de 5TB por día". Para mi sorpresa, descubrí que esto ocurre muy a menudo, y muchas veces la pregunta es de 50TB. Vamos con algunos ejemplos de estas preguntas:

» Un banco europeo tenía un buen SIEM en su SOC. El CIO preguntó, "¿Podemos detectar el fraude en tarjetas de crédito?". Responder a esta cuestión supuso un aumento de 15TB diarios.

» Un fabricante de ropa deportiva realizó una ingesta de gran cantidad de logs. Después, la parte de negocio preguntó si eran capaces de detectar tanto posibles fraudes como malware a través de las webs de e-commerce. Resultado: pasaron de solo 3TB a más de 50TB al día.

» Una organización de defensa, con varios SIEM en su stack tecnológico, fue requerida para detectar una filtración externa dentro de los veinte minutos posteriores a la ocurrencia. Para ello tuvieron que escalar a 40TB al día.

¿Por qué añadir más datos en tu SIEM, o a tu solución de gestión de *logs*, significa dar lugar a nuevos problemas? Principalmente por tres razones:

» El SIEM no puede escalar.

» La solución de seguridad solo es eficiente cuando se utilizan principalmente logs de seguridad.

» El proveedor utilizará esta situación para intentar subir el coste.

Para responder a estas preguntas sorpresa es necesario contar con una arquitectura nativa en la nube, una estructura amigable en cuanto a coste y precio, y una parte analítica que cubra las necesidades de la empresa. Como CISO, ¿estás totalmente preparado para responder a estas preguntas "sorpresa" de 5TB, 25TB o 50TB?

DevOps y seguridad

POR QUÉ ES IMPORTANTE EL ENCAJE

JESÚS MARTÍN OYA

General Director

FASTLY

fastly.com/es

DevOps nació para fomentar la necesaria colaboración entre los equipos de desarrollo y de operaciones, con el objetivo de agilizar los procesos de lanzamiento de software desde el diseño hasta el despliegue. Esto notorio que, desde que naciera en 2009, la adopción de esta metodología se ha ido intensificado año tras año. En la actualidad, uno de los retos que existen en esta metodología está en integrar también la seguridad como agente activo en los ciclos de vida de software y *apps*.

Los ciberataques se están moviendo a la capa de aplicación. Cuando se trabaja en ciclos de distribución rápidos, la posibilidad de contar con un equipo de seguridad —que también forme parte de los bucles de DevOps— hace posible contar con la necesaria visibilidad y el acceso a los datos que permitan responder (dentro de los tiempos de ejecución) a las anomalías. Además, y esto es muy importante, hacerlo antes incluso de que pasen a ser amenazas reales.

Estamos también ante una tendencia en auge: hacer cada vez un mayor uso de los microservicios, desplazando a las arquitecturas más monolíticas. El aumento de esta práctica contribuye a que los equipos busquen respaldo en API basadas en Internet, en ocasiones desacopladas entre sí, que dejan las puertas abiertas a brechas de seguridad.

Los WAF *(web application firewall)* de generaciones anteriores no son capaces de detectar estas tipologías de amenazas por sí mismos. Las protecciones proactivas generan *feedback* sobre su uso, con capacidad de llamar la atención sobre eventos que con otros protocolos quedarían desatendidos. Al mismo tiempo, establecen bucles reales entre *DevOps* y seguridad.

La colaboración —que se denomina DevSecOps— contribuye además a la necesaria priorización de tareas. Los informes de tipos de ataques y objetivos en tiempo real son la principal fuente de información que guía la integración de estas tres áreas, empujando la toma de decisiones y la ejecución de tareas en el momento exacto en que aparece una sospecha o ataque real. «

La campaña UNC2452

EL ATAQUE A SOLARWINDS

JONATHAN RENDAL

Consulting Sales Engineer

FIREEYE

fireeye.com

FireEye ha descubierto una campaña a nivel global identificada como "UNC2452". Los actores que están vinculados a ella accedieron a las redes de numerosas organizaciones, tanto públicas como privadas a través de la cadena de suministro de las actualizaciones de software.

Los primeros indicios se remontan a la primavera del año 2020 y hoy en día la campaña sigue estando activa. Las acciones posteriores al compromiso de la seguridad de sus objetivos ha incluido el movimiento lateral y el robo masivo de datos. El gobierno de los Estados Unidos informa que esta ha sido realizada por el SVR, el Servicio de Inteligencia Exterior de Rusia.

» SUNBURST

Es un grupo de *malware* que está detrás de esta campaña, y que permite al actor acceder a organizaciones de todo el mundo. Los atacantes lograron el acceso remoto a los entornos de las víctimas mediante la inserción de código malicioso en las actualizaciones legítimas del software de monitorización y gestión de TI SolarWinds Orion. Tras el acceso inicial, el actor fue capaz de utilizar otras técnicas más sofisticadas para escalar privilegios dentro de la organización. Sus principales motivaciones son el espionaje mediante la exfiltración de datos. Hasta ahora no se han descubierto indicadores vinculados a extorsión, *ransomware* o delitos financieros.

FireEye ha identificado esta campaña como UNC2452. La campaña es obra de un actor altamente cualificado y muy paciente, que tiene una huella de *malware* ínfima: priorizan ante todo el sigilo y prestan una gran atención a la seguridad operativa. En abril de este año el gobierno estadounidense atribuyó esta campaña al Servicio de Inteligencia Exterior de Rusia.

Entre las víctimas de esta campaña se encuentran múltiples entidades gubernamentales, empresas privadas de sectores como la consultoría, tecnología, sanidad o *telco,* además de empresas energéticas (petróleo y gas) de Norteamérica, Europa, Asia y Oriente Medio. Es posible que haya aun más víctimas en otros países y sectores sin identificar. En esta guía, le mostramos las estrategias de defensa y recomendaciones de bastionado frente a este actor. «

Asegurar la innovación digital

TRANSFORMAR LAS ORGANIZACIONES

RENEE TARUN

CISO adjunta y VP Information Security

FORTINET

fortinet.com

Uno de los cambios más profundos que están viviendo las organizaciones ha sido el aumento de la dependencia de las aplicaciones para apoyar todos los aspectos del negocio.

Esta tendencia ha conducido a una serie de cambios estructurales críticos, como la adopción de infraestructuras basadas en la nube, la incorporación de aplicaciones y servicios SaaS y la necesidad de proporcionar conexiones rápidas, flexibles y seguras a estos recursos a cualquier usuario, desde cualquier dispositivo y desde cualquier lugar.

Por otra parte, la pandemia mundial que estamos viviendo aceleró de forma clara la adopción de soluciones innovadoras en el ámbito del teletrabajo, con el fin de satisfacer la necesidad de mantener el distanciamiento social al tiempo que se seguían desarrollando las operaciones de negocio.

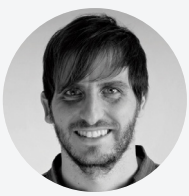
Otras acciones, como la implementación de actualizaciones de la red o la ampliación de sus perímetros, están diseñadas para mejorar la eficiencia de la empresa y la experiencia del cliente.

Competir en el contexto actual, que es eminentemente digital, también implica la necesidad de desplegar nuevos sistemas y soluciones, aumentando la complejidad de los entornos de red y su operativa, y exponiendo a la organización a nuevos ciber riesgos. Entre ellos, caber destacar el despliegue de productos de seguridad puntuales, que fragmentan la visibilidad y reducen el control, o la incorporación de toda una variedad de dispositivos nuevos a la red (IoT, terminales móviles, *cloud* distribuida, etc.) que no contemplan la seguridad en su diseño o que requieren herramientas de seguridad especializadas.

Al integrar la seguridad en todas las áreas de la red, los CISO pueden garantizar que su equipo se adapte dinámicamente a los desafíos y responda con agilidad ante la adversidad. Derribar los muros tradicionales entre la red y la seguridad, y crear una estructura de ecosistema más integrada y automatizada, debería ser una prioridad para los CISO que quieren estar preparados para cualquier eventualidad y triunfar en el nuevo mercado digital. «

Protección de Datos

ENTENDER, PROTEGER Y CONCIENCIAR



EDUARD SESERAS

Experto en Seguridad de Datos

HELP SYSTEMS

helpsystems.com

Lamentablemente, a la hora de proteger la información corporativa no existe una solución perfecta. La mejor defensa posible es tener visibilidad y proteger los datos durante todo su ciclo de vida, además de implementar una estrategia de seguridad por capas.

En cualquier caso, se puede plantear un modelo de protección de los datos basado en tres pasos:

» Entender los tipos de datos almacenados, saber dónde residen y clasificarlos por tipología, departamento, grado de confidencialidad, etc. Esto permitirá aplicar a cada tipo de dato los controles adecuados y enfocar los esfuerzos en aquellos que resultan más crítico.

» Un error que se suele dar con frecuencia es tratar todos los datos de la misma forma. De hecho, muchos proyectos de data loss prevention (DLP) fallan por no clasificar los datos antes. En lo posible, lo más recomendable es realizar ese proceso de clasificación de los datos en el momento de su creación.

» Proteger el flujo de datos, tanto dentro como fuera de su organización. La operación del Negocio obliga a que sus datos sean compartidos entre empleados, enviados a clientes, proveedores o terceros, y, al hacerlo, quedan más expuestos. Cuando se intercambian datos confidenciales o personales es importante utilizar cifrado, sanitización de documentos, redacción adaptativa (para eliminar malware o enmascara información sensible que no debe ser enviada), canales de envío seguros y auditados, además de la posibilidad de revocar el acceso a la información enviada. Para ello se puede hacer uso de las tecnologías de DLP y managed file transfer.

» Concienciar a los empleados y proveerles de alternativas seguras para su trabajo, como archivos y carpetas compartidas, email seguro y envío de archivos de gran tamaño. Si no lo hace, los empleados buscarán una vía alternativa y no segura, exponiéndolo a un riesgo mayor.

La seguridad de los datos debe ser la parte central de la estrategia de seguridad, pero también es importante complementarla con dos capas más, en el ámbito de la infraestructura y también de la gestión de identidades y accesos. «

Enfoque confianza-cero

RETOS EN LA RELACIÓN CON CLIENTES

La transformación digital llegará de la mano del 5G, la IA, el IoT o el *cloud*. Aunque son muchas las oportunidades que estas tecnologías brindan a nuestra sociedad también surgen nuevos escenarios de riesgo para la seguridad. En este contexto de retos y oportunidades, la confianza será clave como eje fundamental tanto para gobiernos, empresas y clientes.

Los fabricantes de tecnología como Huawei nos enfrentamos a un reto común: cómo seguir siendo *partners* de confianza para el futuro. En lo que se refiere a la relación con clientes, en el nuevo ciberespacio no se debe confiar o desconfiar de nadie por defecto, esto es lo que llamaríamos confianza-cero. La seguridad debe crearse en este entorno de confianza-cero a partir de dos pilares fundamentales:

El primero es el de los hechos definidos en estándares. En este sentido, cabe destacar las recomendaciones del Toolbox 5G, que la UE formuló a los Estados miembros para valorar los riesgos existentes en las redes de quinta generación, y aplicar medidas destinadas a reforzar la seguridad en el despliegue de esta tecnología. Estas recomendaciones abogan por criterios técnicos para determinar qué procesos y actores son seguros. Estos criterios, medibles y cuantificables, van en línea con la idea de confianza-cero y previenen contra posibles restricciones impuestas a proveedores y empresas debido a su país de origen o a cuestiones geopolíticas externas a criterios puramente técnicos.

El segundo se basa en verificaciones independientes, como la utilización de esquemas de certificación en los que un tercero independiente realiza una auditoría para verificar que los estándares mencionados se cumplan y garanticen la seguridad de la cadena de valor.

Huawei demuestra su firme compromiso con la ciberseguridad y la confianza. Para ello, cuenta con más de 270 certificaciones globales de seguridad e informes de aseguramiento independientes. Entre todas, cabe destacar las 59 certificaciones Common Criteria, informes de auditoría NESAS y certificaciones EuroPriSe o ePrivacyseal. «

GONZALO ERRO

Privacy and Cyber Security Officer

HUAWEI

huawei.com

Superficie de ataque

HERRAMIENTAS DE *SCORING*

Estamos frente a la tormenta perfecta: una superficie de ataque expandida, amenazas más sofisticadas producto de la transformación digital, las dificultades en la gestión de la cadena de suministro y una serie de consecuencias graves, como la discontinuidad del negocio a raíz de ciberataques.

Aquellas compañías que estén mejor preparadas para enfrentar dichos desafíos serán las que dispongan de una completa visibilidad de su superficie de ataque. Por eso es recomendable:

» Implementar herramientas que simplifiquen el análisis de riesgo. Las soluciones de rating como SecurityScorecard informan, con grados que van de la A a la F, del nivel de riesgo potencial. Lo hacen de una manera objetiva y permiten la unificación de los criterios de evaluación.

» Optimizar la labor de los equipos de seguridad mediante herramientas que automaticen las alertas y las acciones en respuesta a eventos de seguridad.

» Evaluar de forma continua la postura de seguridad mediante herramientas de rating que monitorizan nuestra situación y la de nuestros vendors.

Las herramientas de *scoring* identifican las vulnerabilidades de nuestros proveedores y, además, permiten compartirlas con ellos para crear planes de acción conjuntos a fin de lograr el mínimo nivel exigido para homologarlos.

La calificadora de riesgo Fitch, utilizando la plataforma de *scoring* SecurityScorecard, ha publicado recientemente un trabajo donde relaciona el nivel de calificación de entidades crediticias con su *performance* en *ratings* de ciberseguridad. Aunque los grandes bancos suelen tener mejores calificaciones de riesgo crediticio, no pensemos que el tamaño de las compañías son un predictor de ciberhigiene. Aquellas que no lo abordan apropiadamente, sufren brechas que afectan a su operatividad y calificación de riesgo.

Necesitamos disponer de visibilidad continua de la superficie de ataque, que incluya tanto a nuestra organización como a las terceras partes. Esta monitorización agilizará la gestión y la comunicación entre las diferentes áreas. Para lograrlo, recomiendo integrar herramientas de *scoring* transparentes a nuestro *dashboard* de seguridad. «

ROBERTO HEKER

Director

NEXTVISION

nextvision.es

JESÚS DÍAZ

Cortex
SE Manager

PALOALTO NETWORKS

paloaltonetworks.com

Hacia el SOC autónomo

ELIMINAR AL HUMANO DE LA ECUACIÓN

Hay muchas películas en la historia del cine que enfrentan a humanos contra máquinas y, en la mayoría de ellas, el humano termina saliendo victorioso. Sin embargo, se trata tan solo de una entelequia cinematográfica y la realidad es bien distinta: cuando una máquina está programada para realizar una tarea automáticamente, es invencible.

Esta realidad es justamente la que aprovechan los atacantes actuales, automatizando sus operaciones para generar multitud de variantes y acciones. Este modo de actuar, en el mejor de los casos se traducen en miles de eventos en los SIEM, con los que han de lidiar manualmente los defensores (o sea la gente de SecOps en los SOC). Para ello deben invertir incontables horas en su gestión, sin que ello evite que se dejen escapar las amenazas más serias que vuelan bajo el radar.

Por tanto, resulta crítico automatizar tanto como sea posible la operativa del SOC sacando al humano de las tareas repetitivas. De este modo, podrá centrar su talento en el descubrimiento y gestión de los ataques más serios.

Para ello, es fundamental que el SOC autónomo cuente con dos piezas interrelacionadas:

» Por un lado, un data lake que recoja y correlacione la información desde cualquier fuente de red, nube o endpoint, sobre el que aplique algoritmos de inteligencia artificial (normalmente machine learning) que diferencien los comportamientos usuales de los anómalos e identifiquen las amenazas más complejas de forma automática.

» La segunda pieza es un orquestador de seguridad que, conectado a ese data lake central y al resto de la infraestructura de seguridad, sea capaz de ingerir los incidentes y enriquecerlos contra las diferentes fuentes de inteligencia para validar su gravedad. Además, que actúe en consecuencia, bloqueando máquinas, generando reglas automáticas en los cortafuegos o modificando configuraciones en nube pública.

Volviendo a la analogía del cine, Sarah Connor no podrá jamás vencer a Terminator en la vida real si no cuenta con armas similares. Eso es justamente lo que Cortex de Palo Alto Networks propone. «

DAVID CONDE

Head of
SOC/CERT

S21SEC

s21sec.com/es

Cyber Profiling

CYBER PROFILING

Protegerse sí es posible, si se identifica previamente al cibercriminal. Cuando las organizaciones son víctimas de un ciberataque suelen prestar más atención a la mitigación rápida del incidente y, generalmente, no se molestan en averiguar quién ha podido ser el responsable. Conocer el perfil del criminal y qué le ha motivado es vital para saber cómo se ha podido manejar la información filtrada y, de este modo, medir el posible impacto del ciberataque para establecer el mejor método de actuación.

Desde el punto de vista forense, realizar perfiles cibercriminales puede ayudar a comprender qué fines persiguen, además de conocer su procedencia y poder tomar medidas de contención proporcionales a sus ataques. Para ello, se aplican un conjunto de teorías y análisis relacionados con el perfil criminológico y el perfil del criminal, para intentar averiguar qué le mueve realmente y cuál es su *modus operandi*.

» PATRONES DE COMPORTAMIENTO

Por suerte, resulta más sencillo identificar las motivaciones de los cibercriminales en el ámbito de la ciberseguridad. A diferencia de otros crímenes, en este tipo de actuaciones existen ciertos patrones de comportamiento —tanto a nivel psicológico como a nivel de despliegue de artefactos en un incidente— que revelan el objetivo que hay detrás de los actores maliciosos. Entre las motivaciones más frecuentes se pueden destacar las económicas, las emocionales, aquellas que responden a una necesidad de autoafirmación o autorespeto, sexuales, políticas, ideológicas y religiosas.

Los perfiles más comunes pueden agruparse según sus objetivos, motivaciones y capacidades. Los cuatro grandes grupos para destacar son los ciberterroristas, los *hacktivistas*, los actores con patrocinio estatal y los ciberdelincuentes.

A pesar de que no son los únicos perfiles de ciberactor, estos conforman los principales perfiles de riesgo cibercriminal para cualquier organización, ya sea pública o privada. De este modo, se hace más importante que nunca tomar medidas acordes con el objetivo de protegerse tanto de sus numerosas campañas como de la mejora progresiva de sus capacidades. «

Estrategia de datos y *cloud*

TI, DEVOPS Y SEGURIDAD

La nueva normalidad —o el mundo durante la pandemia y, según parece, después de la pandemia— ha acelerado la transformación digital. La oportunidad es enorme. A nivel nacional se está planteando la reconversión de la economía gracias a la digitalización.

Este es un proceso que se basa fundamentalmente en los datos y en la provisión de capacidades *as a service* (como servicio), lo que resumimos en una palabra a veces sobrecargada: *cloud*.

Todas las organizaciones se encuentran en algún punto de un viaje hacia la nube y esta tendencia hacia un escenario *multicloud* nos dirige hacia un nivel de complejidad muy grande, lo que compromete también la resiliencia de las organizaciones y genera una mayor exposición a riesgos de seguridad ciber. Lógicamente, hay más puntos de fallo y una superficie expuesta a ataque más grande.

Los costes imprevistos —o los no visibles— de consumo en el modelo *cloud*, el exigente ritmo de innovación requerido y la determinación y profesionalización de los ciber delincuentes son algunos de los desafíos del día a día de los responsables de TI.

Estudios de analistas confirman que las iniciativas de transformación digital que tienen una estrategia de datos clara y definida, alineada con la estrategia de negocio, tienen cinco veces más posibilidades de éxito. Dicha estrategia de datos debe dotar de transparencia para reducir la complejidad, empujando la innovación y unificando la postura relativa a la seguridad. Todo ello para poder garantizar el cumplimiento, la privacidad y los riesgos, gestionando en tiempo real las amenazas y ayudando a diagnosticar y responder a los ataques.

Splunk es la columna vertebral de datos para el nuevo entorno tecnológico, necesaria para acelerar la transformación basada en el *cloud* y para potenciar las estrategias de datos integrales de los equipos de TI, DevOps y seguridad. Es la que va a permitir que puedan operar e innovar más ágilmente, optimizando costes, securizando lo que más importa y reduciendo tiempo de parada. «

MARCO BLANCO

Country Manager

SPLUNK

splunk.com

Riesgos de terceros

MONITORIZACIÓN CONTINUA Y CUESTIONARIOS DE SEGURIDAD

Desde hace tiempo, los profesionales de la ciberseguridad y el riesgo han entendido las debilidades que plantean los cuestionarios de seguridad a la hora de convertirse en un barómetro preciso del riesgo de terceros. Son difíciles de validar y su procesamiento requiere mucho tiempo, tanto para el proveedor como para la organización. Además, incluso asumiendo que las respuestas a los cuestionarios de seguridad son precisas o veraces, están ancladas a un solo punto en el tiempo.

Obviamente, esto es lo que ha llevado a muchas empresas a buscar un seguimiento continuo para reforzar sus programas de gestión de riesgos de terceros (TPRM, *third-party risk management*). Pero las organizaciones no pueden simplemente cambiar una cosa por otra. Cada forma de evaluación ofrece una visión ligeramente diferente del estado de riesgo de un proveedor. La autoevaluación proporciona una mirada más completa —de adentro hacia afuera— del entorno del proveedor, mientras que la monitorización continua proporciona una vista precisa y oportuna, de afuera hacia adentro. El poder real de los programas de TPRM necesita de un enfoque que integre ambos medios de evaluación. Una buena analogía aquí sería compararlo con las prácticas contables. Mientras que la autoevaluación aportaría más una mentalidad de balance a la evaluación, la monitorización continua proporciona el estado de flujo de efectivo continuo. Cuando está bien integrado, el poder combinado de amabas acciones puede ayudar a mejorar la TPRM en cinco frentes importantes:

» Visión más holística y validada del riesgo de terceros.
» Actualizaciones frecuentes sobre cambios en la postura frente al riesgo.
» Requiere una autoevaluación menos frecuente.
» Reduce la carga de los proveedores cuando responden cuestionarios.
» Facilita los proveedores de nivel de formas más sofisticadas.

En conclusión, las organizaciones pueden obtener grandes beneficios si pueden fusionar con éxito los resultados de los cuestionarios de seguridad y la monitorización continua de TPRM. Pero a menudo es más fácil decirlo que hacerlo. «

VICENTE DE LA MORENA

Country Manager

RISKRECON

riskrecon.com

Seguridad en contenedores

MITRE ATT&CK *FOR CONTAINERS*

GREG YOUNG

Vicepresidente de Ciberseguridad

TREND MICRO

trendmicro.es

Proteger contenedores no significa asegurar las aplicaciones, pero con un nombre diferente. Este entorno utiliza microservicios para orquestar el almacenamiento, la red y la seguridad; tres cosas interesantes para los delincuentes. De este modo, hay que tener en cuenta la independencia que conlleva esta nueva tecnología, así como la seguridad de toda la canalización, que se traduce en una nueva superficie de ataque.Kubernetes y Docker se emplean para orquestar todos estos contenedores y microservicios. Los atacantes explotan esa complejidad para evitar la detección, ganar privilegios y moverse lateralmente. Esta complejidad es la pieza más pequeña de un conjunto que incluye, como mínimo, la red, la carga de trabajo, el sistema operativo, la aplicación y el contenedor.

UN *FRAMEWORK* PARA CONTENEDORES

Los constructores, los equipos de operaciones y los de seguridad necesitan un único lenguaje para entender el riesgo asociado a los contenedores. Mitre ATT&CK Framework sigue evolucionando, añadiendo perfiles de ataque conocidos y nuevas técnicas. Recientemente ha incluido Mitre ATT&CK Matrix for Containers, con características como:

» Incluye un recurso discreto para ataques que involucran contenedores.

» Los ataques a nivel de orquestación y de contenedor están en una sola vista, permitiendo a los analistas del SOC seguir un ataque en contenedores desde un único marco de trabajo.

» MITRE hizo un llamamiento a la comunidad para obtener la mejor información sobre la seguridad y los ataques a contenedores, alimentando un marco para reflejar la realidad a la que se enfrentan los SOC. Muchos criterios de evaluación de las herramientas de seguridad no han tenido suficiente información del mundo real, y esto es un error.

La colaboración en materia de conocimiento y experiencia en ataques reales es clave y facilita que la comunidad de seguridad trabaje para ayudar a las empresas a estar protegidas contra los ataques utilizando, como lenguaje común, bases de conocimiento como ATT&CK. Aplaudamos la iniciativa. «

PARTNERS

Platinum Sponsors

Check Point SOFTWARE TECHNOLOGIES LTD. · DARKTRACE · Forcepoint · netskope · OneTrust Privacy Management Software · PCYSYS · Recorded Future® · thycotic · zscaler™

Gold Sponsors

Akamai · aruba · BeyondTrust · CROWDSTRIKE · CYTOMIC · DEVO · fastly · FIREEYE · FORTINET · helpsystems · HUAWEI · NEXTVISION & SecurityScorecard · paloalto NETWORKS · riskrecon · S21SEC · splunk> · TREND MICRO