Eye on Security

Transcripción

El panorama de amenazas en América Latina

Luke McNamara:
Bienvenido a otro episodio del podcast Eye on Security. Soy su anfitrión, Luke McNamara. Uniéndome hoy para una discusión sobre el panorama de amenazas en América Latina y cómo las organizaciones lo enfrentan, tengo a Ryan Goss, VP de América Latina y el Caribe y Juan Carlos García Caparrós, director de Mandiant Consulting para América Latina y el Caribe. Bienvenidos amigos, ¿cómo están

Ryan Goss:
Muy bien. ¿Cómo estás?

Luke McNamara:
Entonces, tal vez puedan contarme un poco sobre sus funciones y la organización de sus equipos y en qué se enfocan para resolver o abordar a los clientes. Ryan, comencemos contigo

Ryan Goss:
Como mencionaste, soy el vicepresidente para América Latina a cargo de todas las ventas y operaciones para la región y enfocado en hacer crecer realmente la empresa en este momento, donde tenemos una huella relativamente pequeña en la región. Así que realmente estamos enfocados en construir nuestra infraestructura de canales, ir tras las principales industrias en las que participamos mejor (sé que entraremos en eso un poco más tarde) y en la estrategia, ventas y marketing que hacemos en América Latina, siendo también muy importante la parte de los servicios de Mandiant.

Juan Carlos García Caparrós:
Hola, soy Juan Carlos. Soy el director de Mandiant Consulting para América Latina y el Caribe. Mi enfoque es, principalmente, ofrecer soluciones que pueden estar en la consultoría e implementación o incluso en el lado de los servicios administrados para resolver todas las situaciones que los clientes tengan hoy en día relacionadas con ciberseguridad.

Luke McNamara:
Así que hemos hecho, supongo, algunos de estos (podcasts) y ha sido una serie un poco informal en la que hemos analizado en las diferentes regiones, el panorama de amenazas y cómo las organizaciones se concentran en responder a esas amenazas. Y tal vez aquí es donde primero podemos comenzar esta discusión. Juan Carlos, empezaré por ti. Históricamente, ¿cuáles son los tipos de amenazas que hemos visto que enfrentan los clientes en América Latina? Estoy seguro de que ha habido muchas cosas que son muy similares a lo que vemos en diferentes regiones, los diferentes tipos de motivaciones de los

adversarios, el ciberespionaje, cibercrimen y hacktivismo, pero danos una idea de cómo se ve esto históricamente en América Latina.

Juan Carlos García Caparrós:
OK, América Latina no es muy diferente del resto del mundo. Los cibercriminales se están enfocando en monetarizar las vulnerabilidades que encuentran en la infraestructura de los clientes. Y también, por supuesto, hay otro tipo de ataques en los que quieren robar información para usarla o venderla o incluso con fines de espionaje.
Otro tipo de cosas que han ocurrido en los últimos años es el tipo de delincuentes que son patrocinados por Estados Nación, países que están interesados en hacer cambios importantes en otros países. No solo con el propósito monetario o financiero, sino mucho más allá. Así que pueden estar involucrados en elecciones o en otros asuntos políticos. Entonces, el panorama que podemos ver es muy amplio y la idea, en nuestro caso, es estar en la primera línea de batalla, para primero identificar cuáles son sus motivaciones, cuáles son sus técnicas y cómo podemos ayudar a los clientes a evitar este tipo de ataques.

Luke McNamara:
¿Hay ciertos aspectos de la actividad del adversario o tal vez la naturaleza de cómo se estructuran las organizaciones u otros aspectos del negocio y la sociedad, allí donde hay tipos particulares de amenazas que tal vez veamos más en América Latina que en otros lugares o ciertos matices de estas amenazas?

Juan Carlos García Caparrós:
Sí, una de las realidades que vivimos en América Latina es que la cultura de seguridad probablemente sea más baja que en otros países. Probablemente, si comparamos nuestra cultura de seguridad o nuestra cultura de riesgo, está menos desarrollada de lo que podemos ver en los Estados Unidos o en Europa. Ese es un gran problema porque muchas de las empresas y la gente están dispuestas a correr algunos riesgos y no están realmente preparadas para enfrentar a los criminales. Creo que es una gran diferencia con el resto de otras partes del mundo. Los cibercriminales son realmente inteligentes y están usando eso, aprovechándose de cosas como la pandemia, el COVID, y la gente es más débil que en otras épocas porque piensa en cosas diferentes y no están teniendo el cuidado suficiente para evitar eso.

Entonces, lo que podemos ver hoy es un gran incremento de malware, por supuesto, pero también ataques directos a través de phishing que se convierten en ransomware y cosas así. Esta es la escena que vemos. Casi todas las semanas tenemos un cliente que pide ayuda para resolver este tipo de situaciones. Y la cuestión aquí es que los clientes realmente ni siquiera saben qué tan bien preparados están para enfrentar ese tipo de ataques. No saben si hay presencia, si están realmente preparados para responder. Y, por supuesto, la madurez de la organización probablemente no esté lista para enfrentarse a este tipo de cibercriminales tan bien preparados. Creo que esto es lo principal.

Ryan Goss:
Juan Carlos mencionó el COVID, algo que también estamos viendo. Y creo que está en todo el mundo. Obviamente, la rápida transformación digital, pero en América Latina en particular debido a que sus equipos son tan limitados en términos de recursos, realmente han tenido que convertirse para hacer solo tareas básicas de TI de muchas maneras para facilitar esta t

ransformación, yendo todo al trabajo remoto. Y solo les está quitando su día a día. Ya tienen ciclos limitados para poder hacer su trabajo y no convertirse solo en bomberos y apagar incendios en todas partes. Se ha vuelto aún más difícil ahora con esto. Así que he visto un aumento mayor en la necesidad de automatizar, la necesidad de evaluar realmente y de tener la información al alcance de la mano cuando la necesitan.

Juan Carlos García Caparrós:
Además del incremento en los ataques que enfrentamos, provocado principalmente, porque se requirió que las empresas tuvieran más personas conectadas sin seguir realmente todas las mejores prácticas para estar protegidos. Tuvieron que reaccionar muy rápido para tener continuidad en sus negocios. Si a eso le sumamos, la complejidad de los cibercriminales, como colaboran, trabajando juntos para ser más eficientes y efectivos en sus ataques.

Además, existe otro problema: la falta de habilidades especializadas en ciberseguridad en América Latina. Se requieren demasiados profesionales que no pueden ser contratados por las empresas. Por eso las empresas están solicitando cada vez más, servicios como los que brindamos para poder resolver de la mejor forma sus problemas.

Luke McNamara:
Sí, ese es un punto del que tengo curiosidad por escuchar más. Porque creo que es interesante ver en diferentes regiones de dónde proviene el conjunto de habilidades específicas. En algunos lugares como los Estados Unidos, vemos mucho que, particularmente en el lado de la inteligencia de amenazas cibernéticas, por ejemplo, pueden provenir del gobierno o del ejército. Entonces, los conjuntos de habilidades que se han acumulado allí en organizaciones como esas, o en el sector financiero, donde sí tienen muchos recursos, eventualmente se transfieren a otros sectores y regiones, tal vez eso sea diferente para diferentes conjuntos de habilidades y componentes. Pero históricamente, ¿de dónde suele ven la gente? ¿De qué sectores suelen provenir las personas que tienen experiencia muy sólida en algunas de las capacidades básicas de ciberseguridad?

Ryan Goss:
Diría que probablemente no se diferencia de muchas cosas que vemos, incluso en los EE. UU. Es principalmente en el sector financiero, o en el sector Gobierno. Hay grandes industrias y empresas como Coca-Cola donde logran tener equipos fuertes y es en estas verticales de industria específicas donde vemos focos de fuerza. Y nuevamente, nos enfocamos principalmente en ese tipo de clientes, pero donde vemos mayor sofisticación y grandes presupuestos son, por mucho, la banca, las finanzas y el Gobierno.

Juan Carlos García Caparrós:
Otra área donde probablemente podamos encontrar ese tipo de habilidades o profesionales más relacionados con asuntos regulatorios, necesarios en algunas empresas cumplir con estos requisitos, es por ejemplo, la industria financiera, donde podemos encontrar profesionales especializados y también hay algunas universidades que están tratando de desarrollar este tipo de habilidades, pero aún es limitado. Entonces, por un lado, tenemos la industria financiera, pero también tenemos las empresas consultoras que están desarrollando sus propias habilidades especializadas. Pero todavía creo que hay una gran brecha entre lo que se requiere y lo que realmente tenemos en el mercado.

Luke McNamara:
Entonces, con estas amenazas, que nuevamente no son infrecuentes a lo que vemos en las diferentes regiones con estos mismos antecedentes y experiencia, así como en las diferentes industrias de la región. ¿Cuáles son los tipos de problemas por los que normalmente los clientes nos buscan? Y tal vez Ryan. Empezaré contigo en esto, ¿qué es lo que suelen buscar cuando se acercan a nosotros?

Ryan Goss:
Esa es una gran pregunta. Creo que obviamente ha habido iteraciones de FireEye. Por lo tanto, es una dinámica muy interesante de dónde estamos ahora, porque todavía tenemos clientes leales de mucho tiempo atrás, que nos compraron la solución de “sandbox” en línea y que han permanecido con nosotros durante toda nuestra evolución. Y tenemos algunos clientes que tienen casi todo nuestro portafolio de productos y que realmente han aprovechado los servicios, pero estos son pocos y distantes entre sí. Así que ahora, a medida que avanzamos en nuestra transformación, hemos incrementado nuestro portafolio, no solo en el lado de las soluciones, sino también en el lado de la consultoría. La reputación de FireEye del pasado es que somos una empresa élite y cara tanto en nuestras soluciones como en nuestros servicios y creo que esa percepción ha cambiado un poco con el cambio a la suscripción y ARR (Annual Recurring Revenue).

Así creo que realmente el área de inteligencia está tomando forma, en mi opinión. Nuestra oferta de inteligencia es una cosa, pero en realidad la Plataforma Helix es esa fuente de inteligencia y realmente el diferenciador para nosotros. Inevitablemente, diría que nos encontramos en peleas de cuchillo con otros proveedores, cuando trata oportunidades de punto final. Así que estamos tratando de diferenciarnos del resto, en términos de entregar esa ciberinteligencia también. Creo que eso está tomando forma y ese es el tipo de soluciones que están buscando.

Dejaré que Juan Carlos hable más sobre los servicios, pero mi percepción sobre los servicios y que no necesariamente ha cambiado en el tiempo que llevo aquí, los CA o evaluaciones de compromiso, son realmente una de nuestras fortalezas, y por supuesto, realmente nos reconocen como el líder. Por eso vienen mucho a nosotros. Ahora lo estamos haciendo mucho mejor con los retenedores de IR (Respuesta a Incidentes), donde realmente entendemos su valor y donde podemos responder rápidamente si así se necesita. Regresando a lo que dijo Juan Carlos en términos de los recursos limitados que tienen los clientes. Consideremos si es una evaluación de Swift o algo así. Ellos dicen: "Bueno, debemos asegurarnos de que estamos bien dentro de este protocolo y esta plataforma. Llamemos a Mandiant, porque son los mejores. Así que también recibiremos muchos de esos proyectos. Dejaré que Juan Carlos hable más sobre los servicios.

Juan Carlos García Caparrós:
Otra cosa que creo es que lo que mejor le queda a un cliente, dependerá del momento que esté pasando. Y lo que estoy tratando de decir con esto, es que si ya se encuentra comprometido o está siendo atacado o bien ya tiene una fuga de información, el tipo de servicios que va a requerir es totalmente reactivo. Y es aquí donde tenemos servicios como el de Respuesta a Incidentes, que es algo que hacemos muy bien, y probablemente seamos uno de los mejores en el mundo en hacerlo. Nuestro enfoque aquí es llegar con el cliente, traer un equipo especializado, entender el entorno y tratan de ayudarlo para evitar mayores daños,

identificando quién es el atacante y asegurando que el atacante saldrá de sus sistemas y que su persistencia desaparecerá.

Este es probablemente el principal servicio por el que somos reconocidos en el mundo. Por otro lado, cuando no hay un ataque, pero existe la posibilidad de que la organización esté o no comprometida, tenemos cierto tipo de evaluaciones que hacemos para revisar, si el cliente está comprometido, si el cliente está preparado para responder a ese tipo de ataques y tratar de definir con ellos cuál será su postura de seguridad. Creo que esto es más del lado proactivo para ayudar al cliente a definir cuál es el estado actual, cuál debería ser el estado futuro y qué deben hacer para cerrar esa brecha.

También contamos con otro tipo de servicios para ayudar a la organización a transformarse, para capacitarse o para crear una cultura de seguridad en la organización. Así como también la entrega de servicios administrados para gestionar las capacidades de defensa del cliente. No solo en monitoreo, sino también en la detección, en la respuesta e incluso en la recuperación para cubrir todo el espectro de ciberseguridad.

Luke McNamara:
Una cosa que creo hemos visto mucho, en particular, en este año, impulsada por la velocidad de los ataques de ransomware y la naturaleza de cómo se han transformado realmente en 2020, es que muchas organizaciones han elevado la discusión de seguridad al nivel C- suite en el Consejo Directivo en formas que tal vez no habían hecho en el pasado.

Tengo curiosidad por su descripción de las organizaciones que están buscando esa respuesta reactiva, y tal vez no están pensando en invertir en seguridad o que tal vez están más restringidas en su función de seguridad y de TI en lugar de llevar una discusión más amplia dentro de la empresa, así como de las organizaciones que están pensando en esto de manera más proactiva, ¿han visto un cambio en esta conversación sobre seguridad, Si es que se está elevando más al Consejo Directivo?, ¿cómo lo están abordando y cómo quieren pensar al respecto en el futuro?

Ryan Goss:
Están llegando ahí. Queda un largo camino por recorrer. Y muchas de las discusiones que tengo con todos en mi equipo giran exactamente en torno a eso. Volviendo a mi analogía, la pelea a cuchillo, especialmente a medida que nos adentramos en otras soluciones como inteligencia y validación, pero si nos quedamos a ese nivel de operación, será muy difícil. Entonces, creo que ese es uno de los beneficios de FireEye Mandiant y la inteligencia de primera línea que tenemos, y en los mensajes que continuamos entregamos y que realmente nos ayudarán a llegar allí. En muchas de las discusiones que tenemos, inicialmente no nos metemos en bits y bytes y velocidades y feeds y todas esas cosas a las que eventualmente tienes que llegar, pero si llegas allí de inmediato, va a ser muy duro. Entonces, hemos hablamos del asunto de la transformación, y realmente como un buen ejemplo, Juan Carlos ha mencionado la regulación.

En Brasil, el equivalente del GDPR es LGPD y es igual de rígido. Esta regulación está impulsando inversiones que antes no existían y las personas que están en la línea con esto son el nivel Ejecutivo. Así que este es un ejemplo claro de cómo se eleva la conversación.

Pero nuevamente, el mejor diferenciador que tenemos, no solo del lado de Mandiant sino del lado de la inteligencia, es cuando realmente podemos brindar este entendimiento estratégico y no solo ponerlo en términos técnicos, hablar de como ¿Cuál es su riesgo? ¿Estás expuesto al riesgo o no? ¿Puede demostrar cuál es su nivel de riesgo? ¿Puede mostrarle al Consejo Directivo, a sus jefes y a sus Ejecutivos que las inversiones que se han realizado están haciendo lo que deberían estar haciendo? Eso no sucede de la noche a la mañana.

Obviamente, estamos ganando mucha más tracción en ese sentido en términos de llegar no solo al CISO sino también más arriba, pero definitivamente es un proceso y todo tiene que ver con el nivel de madurez que las empresas tienen y en el algunas piensan: "Está bien, la seguridad la veremos cuando pase. Solo tienes que estar allí para marcar la casilla sin entrar en demasiados detalles". Incluso esto puede venir de un Gobierno. Juan Carlos está en México y lamentablemente en este momento, la tendencia desde arriba es planificar la austeridad y hacer todo lo más eficiente posible, lo más barato posible. Y eso obviamente también afecta la seguridad. Y no necesariamente tendrá ningún nivel de discusión de alto nivel cuando eso esté sobre la mesa.

Entonces, cada país es diferente. Algunos están mucho más en sintonía como Brasil debido a LGPD en comparación con lo que está sucediendo en México en este momento, pero eso obviamente cambiará en un par de años cuando las cosas sean fluidas. Pero desde nuestro nivel, a nivel profesional, definitivamente hay mucho más interés en alcanzar ese nivel ejecutivo y superior.

Luke McNamara:
Hemos hablado de inteligencia un par de veces aquí y desde el lado de la inteligencia, sería negligente si no hiciera una pregunta más sobre eso. Creo en mi mente, uno de los ejemplos mas notables que hemos visto históricamente, es un conjunto de actores de amenazas que realizan actividades en una región en particular, de cierto tipo, que quizás históricamente no se esperaría, como el caso de los actores de amenazas de Corea del Norte que apuntan a las finanzas en toda América Latina.

Ryan Goss: Correcto.

Luke McNamara:
Y nuevamente, siempre hay una tendencia a que las organizaciones, especialmente con recursos limitados, se enfoquen en los actores de amenazas que están afectando actualmente a su sector o que están actualmente activos en su región. Pero creo que ese escenario va al punto de que, si estás tratando de pensar en riesgos potenciales, al menos debes tener algo de conciencia de cuáles son los otros actores de amenazas, quiénes están llevando a cabo campañas globales, cuáles son sus capacidades y cuáles son esas primeras señales de advertencia de una amenaza hacia un objetivo.

Cuando pensamos en cómo las organizaciones de América Latina se están acercando a la inteligencia de amenazas, situaciones como esas, son esas llamadas de atención al valor de la inteligencia de amenazas, una especie de sistema de alerta temprana, aunque todavía hay mucho enfoque en los IOC, los indicadores tácticos y los casos de uso en el SOC.

Ryan Goss:
Sí, diría que, desafortunadamente, sigue siendo una forma muy táctica de usarlo, Hay excepciones. Tenemos clientes que son muy maduros y han invertido no solo en una solución de ciberinteligencia, sino quizás en varias. El desafío sigue siendo, todavía más en el lado táctico, cómo hacer que esa información sea mucho más accionable en tiempo real, con ese nivel de empleado que no necesariamente tiene todo el conocimiento, como Juan Carlos ha señalado, y que están muy enfocados queriendo ver, como dijiste, IOC o binarios que si no están ahí, entonces consideran que la solución no es valiosa para ellos.

Creo que hemos recorrido un largo camino. Ahora no está tan definido y están entendiendo el valor de entender las tendencias de otras partes del mundo, los TTP y todo ese tipo de cosas que realmente pueden darles una señal de advertencia temprana como "Oye, tenemos que hacer algunos ajustes aquí debido a lo que está sucediendo", asociando la información. Esto es un proceso continuo y creo que cuantos más proveedores de inteligencia continúen ingresando al mercado se podrán ver la diferenciación, y es entonces cuando nos volveremos mucho más interesantes.

Pero es frustrante porque aunque podemos demostrar, más allá de toda duda razonable, que somos una muy buena solución de inteligencia, los presupuestos o el alcance son muy limitados y saber (desde el punto de vista del cliente) cómo va a usar esa inteligencia, a veces se vuelve difícil. Pero esto es una discusión en curso y yo diría que cada año, tenemos más y más proyectos, hay más y más RFPs mucho más profundos con los requisitos que están ahí. Así que me gusta dónde estamos, pero debo decir que es un área de gran crecimiento para nosotros. No sé si quieres agregar algo Juan Carlos.

Juan Carlos García Caparrós:
Sí, diré que la ciberinteligencia es, por seguro, una forma de tener un enfoque proactivo para estar listo para responder. Pero hay una situación que puede ser complicada, ya que muchas de las organizaciones reciben toneladas de información, toneladas de ciberinteligencia y el problema, que Ryan ya mencionó, es que esta inteligencia no es accionable y eso se debe a que no tiene contexto. Por lo tanto, es necesario tener algún filtro adicional con el fin de crear un contexto específico para las organizaciones. De lo contrario, es demasiada información que no hace fácil tomar decisiones basadas en eso.

La otra cosa es que no se da la colaboración entre las distintas organizaciones. Los bancos, no se hablan entre si, no comparten información, manteniéndose en sus islas de información y esto es una de las cosas que se requiere suceda, al igual que con las empresas de ciberseguridad, las cuales deberían compartir más información para poder colaborar. Por supuesto, hay situaciones comerciales que no permite que eso suceda con mucha facilidad, pero es la única forma, porque los cibercriminales, realmente si colaboran entre ellos, y por esa razón, a veces están incluso más preparados que los buenos para responder mejor. Por lo tanto, la ciberinteligencia contextual es, para mí, el siguiente paso a seguir.

Luke McNamara:
Dos áreas que me vienen a la mente en nuestra discusión, con algunas de las cosas que ustedes mencionaron y que tengo curiosidad por saber es cuál ha sido el nivel de respuesta y el interés de las organizaciones en América Latina, sobre capacitación y la validación, particularmente quizás para algunas organizaciones que históricamente no han invertido tanto

en seguridad y tal vez tengan muchas menos deudas de seguridad cuando se trata de averiguar qué cosas quieren tirar y pasar por ese proceso de mirar los controles y saber qué está funcionando bien. Todo el contexto de validación, pero también en la capacitación, ¿verdad? Para abordar tal vez el tema de la escasez de mano de obra, o tal vez donde haya falta de experiencia en ciertas áreas. ¿Cómo piensan las organizaciones sobre estas cosas?

Ryan Goss:
Supongo que empezando por el punto de validación. Es similar a lo que hablamos sobre inteligencia. Si nos remontamos a la adquisición de Verodin, comenzamos a hablar sobre eso y realmente comenzamos a aprender sobre que significa BAS (Breach and Attack Simulation) y qué diferencia a Verodin y de ahí poder evangelizar. Y esa es la palabra, mucha evangelización en este punto, porque desafortunadamente algunos de los proveedores de BAS llegaron primero y entonces pusieron la mesa y esto es lo que parece. Nos metimos en este tema y lleva tiempo. Ya hemos pasado por ese proceso. Tenemos, nuevamente volviendo al nivel de madurez, clientes que están realmente en sintonía con lo que es una verdadera validación y conocen todos los casos de uso que podemos proporcionar y el nivel de granularidad y detalle que se pueden obtener es realmente impresionante.

Ahora, a veces se remontan (los clientes) a simplemente marcar la casilla y tener un mínimo como, "Oigan, ¿tienen alguna herramienta para verificar el BAS?", Otros proveedores también están usando el término validación, "Oh, sí, lo tenemos." y así se convierte inmediatamente en un ejercicio de precios, por lo que estamos en el proceso de llevarlos a un punto en el que vean la diferencia y puedan presupuestarla.

Con respecto a tu segundo punto, entrenamiento. Este es un problema continuo para ellos (los clientes), porque sucede mucho. Han invertido mucho tiempo en capacitar a su gente, desde un nivel muy inicial, pero a gente inteligente. Cuando decimos nivel de madurez, no nos referimos al nivel de inteligencia de las personas, sino a la experiencia que han tenido. Entonces van los contratan y los preparan para ser contribuyentes sólidos y luego (estos recursos) obtienen una oferta de trabajo en otro lugar y se van, regresando a la empresa de nuevo al punto de partida.

Por eso, creo que una cosa es la educación y la capacitación, pero otra cosa es tener a una compañía como FireEye Mandiant detrás de ellos para ayudarlos a obtener el nivel de madurez requerido en su programa (de ciberseguridad) del que Juan Carlos comentó antes y esto es realmente importante. La capacitación es definitivamente difícil y también hay muchas empresas locales que ofrecen capacitación. Por lo tanto, no diría que la capacitación es necesariamente una gran parte de nuestro portafolio, pero sí ofrecemos capacitación cuando es parte de un negocio más grande y, obviamente, capacitación específicamente para nuestros productos, o bien en proyectos que buscan elevar realmente el nivel de madurez de todo el programa de seguridad, incluidos los empleados y sus habilidades específicas.

Juan Carlos García Caparrós:
Me gustaría agregar que la capacitación está bien, pero solo si tiene un objetivo. Lo que realmente importa es crear una cultura de ciberseguridad basada en riesgo. La capacitación es algo que no funcionará cuando solo se usa para cumplir un requisito o un requerimiento regulatorio. La formación tiene que estar enfocada en crear esa cultura de ciberseguridad y tiene muchas fases. Una de estas fases, que muchas empresas olvidan al final, es probar si

esa formación realmente funciona. Si realmente hace una diferencia, si realmente crea esa cultura, que permita tener simulaciones de ataques, probar cómo reaccionará la gente y probar si el plan de recuperación es realmente algo que va a funcionar. Por lo tanto, esto tiene que ver con la capacidad de resiliencia empresarial de la organización.

Entonces, la pregunta no es si te van a atacar, sino la pregunta es cuándo esto sucederá. Las empresas tienen que estar preparadas para resolverlo. Preparadas en los controles, preparadas en los procesos, preparadas en la tecnología, pero aún más preparadas en la forma en que la personas van a reaccionar para recuperarse de ese ataque. Creo que este es el punto principal de la capacitación, y no solo aprobar un requisito regulatorio o corporativo.

Luke McNamara:
Ese es un punto excelente, tener eso divorciado de una estrategia más amplia en torno a la mitigación de riesgos y los procesos y controles y la experiencia, y luego el componente de personas de lo que tiene una organización para hacer frente a las amenazas cibernéticas, creo que es muy importante.

Terminando aquí. Tengo curiosidad por las cosas con las que dejaría a la audiencia, cosas que buscar a medida que avanzamos en 2021. Ryan, ha mencionado, por ejemplo, la regulación y cómo ha tenido un impacto o ha dado forma a lo que las organizaciones piensan sobre la seguridad. Obviamente, COVID-19, que con suerte saldremos de eso en 2021 (toco madera). Puede haber aspectos como los que, Juan Carlos señaló desde el principio, donde las organizaciones han tenido que cambiar la forma en que realizan negocios. Y puede haber continuas evoluciones en torno a eso que tengan implicaciones de seguridad y que puedan impulsar ciertos controles o procesos de seguridad. Y puede haber una evolución que no amenace el panorama. Es posible que veamos surgir nuevos actores de amenazas en América Latina o apuntar hacia América Latina. Así que tengo curiosidad por saber cuáles son sus pensamientos y predicciones para 2021.

Ryan Goss:
En realidad, mencionaste un par de ellos y todo se relaciona con lo que hemos estado hablando a lo largo, en lo que respecta a COVID y la rápida aceleración de la transformación digital hacia la nube. Lo hemos visto en este período de COVID en 2020 y solo aumentará a medida que avancemos en 2021, ya que el presupuesto se ha centrado en esa transformación. Así que veremos mucho de eso y sí, más y más regulaciones estarán en línea. Y diría solo el modelo mientras seguimos hablando sobre la falta de recursos.

Por lo tanto, los requisitos de MSSP, nuestra necesidad de tener socios de MSSP sólidos, no solo para nosotros, sino también para los usuarios finales, cómo compran y realmente como pueden subcontratar muchas de esas cosas, es realmente importante para ellos. Y creo que, para nosotros, como empresa, con nuestra transformación, hay muchas oportunidades ahora y estamos bajando un poco el mercado objetivo y realmente nos enfocaremos más en la pequeña y mediana empresa donde antes no era viable para nosotros, pero ahora lo es. Y creo que veremos mucha más acción en esta pequeña y mediana empresa. Y, por supuesto, también en la cima de la pirámide. ¿Juan Carlos?

Juan Carlos García Caparrós:
Agregaré que algo que podemos esperar es ver más ataques. Esto no va a terminar pronto.

Los cibercriminales, hacen sus cosas con todo el tiempo disponible. Pueden estar preparando un ataque durante días, meses e incluso años, y nadie puede darse cuenta de lo que está sucediendo. Tienen todo el tiempo del mundo para atacar una organización. Y una cosa que es segura es que la pandemia del COVID-19 ayudó a los delincuentes a tener más tiempo sin ser notados. Por eso es importante que la empresa tenga las capacidades para detectar, responder y recuperarse al mismo tiempo, al mismo nivel, al mismo nivel de madurez que mencionó Ryan.

Y la otra cosa es que la seguridad no es un asunto técnico, es un asunto de decisión empresarial. Las empresas deben entender que no es solo una cuestión técnica, o es cuestión de tener cuidado con los datos, sino que va más allá. Puede destruir completamente una empresa, puede destruir su reputación, puede sacar a una organización del negocio muy fácilmente, y es por eso por lo que la seguridad no es solamente responsabilidad del CISO o la persona encargada de TI, es responsabilidad de cada persona y de cada ejecutivo de la organización. La seguridad debe estar en su ADN, no solo para informar o responder sobre lo que requiere la organización, sino incluso en sus propias vidas. Así creo que esta es la forma en que necesitamos ver la ciberseguridad en estos días.

Luke McNamara:
Sabias palabras para terminar con esto. Caballeros, gracias por su tiempo. Ha sido una conversación fantástica, gracias a ambos.

Ryan Goss:
Gracias.

Juan Carlos García Caparrós:
Gracias.

Obtenga más información visitando https://www.fireeye.com/mandiant/advantage.html.