QUÉ APRENDIMOS ACERCA DE LA CIBERSEGURIDAD EN 2017

4 lecciones para ayudarlo a dar forma a su estrategia en el próximo año

vmware® | intel®

Nuevas amenazas, nuevas oportunidades

Para el mundo de los negocios, el 2017 fue un año de cambios importantes. Las organizaciones comenzaron a mapear el panorama digital y plantear nuevas demandas... y los ataques malintencionados no se hicieron esperar. Fue un año en el que los líderes de TI y los negocios afrontaron una serie creciente de amenazas, al mismo tiempo que emergieron nuevas oportunidades para el crecimiento y la innovación.

¿Qué aprendimos en el camino? A continuación se presentan varios hechos clave que pueden servir de guía para las estrategias de seguridad en el 2018 y más adelante:

1. La superficie de ataque sigue creciendo
2. Los ataques están superando la protección
3. Las nuevas capacidades de amenaza exigen una nueva estrategia
4. La escasez de personal de ciberseguridad aumenta el riesgo

1 La superficie de ataque sigue creciendo

Los dispositivos, los usuarios, las aplicaciones y los datos se están multiplicando con rapidez. Si bien esto es bueno para los negocios (aumenta la flexibilidad, mejora la productividad y alienta la innovación), también crea más oportunidades para los atacantes malintencionados. Esto, a su vez, deja a los líderes de TI esforzándose para determinar de qué forma las nuevas iniciativas y tecnologías pueden exponer al negocio. Es una tarea que nunca termina.

Perseguir amenazas es inútil. Son simplemente demasiadas para rastrearlas. Las organizaciones de TI deben tomar una estrategia anticipativa única para su organización a fin de ir un paso por delante de los ataques emergentes. Este tipo de estrategia combina un conocimiento profundo de las vulnerabilidades específicas de un negocio con un conocimiento permanente de las tendencias en amenazas para ayudar a los equipos a crear una estrategia intuitiva para proteger el centro de datos. Esta estrategia, combinada con las herramientas adecuadas, permite a TI ganarle a las amenazas en su propio juego.

Se espera que el mercado de seguridad de la información tenga una tasa de crecimiento compuesto anual del 7,9 % y, de esta forma, alcance los $120,2 mil millones para el 2021[1]

1 Gartner, análisis de la previsión: Information Security, Worldwide, 3Q17 Update, Diciembre de 2017

2 Los ataques están superando la protección

A pesar del aumento del gasto en seguridad, la cantidad de infracciones sigue creciendo, y ningún negocio o sector es inmune.

El uso generalizado del cifrado está dificultando la detección de amenazas. Además, las amenazas avanzadas de estados nacionales han complicado aun más para los líderes en seguridad la tarea de proteger los datos y la infraestructura. En la actualidad, no se trata de "si" hay infracciones de seguridad, es simplemente es una cuestión de "cuándo".

Gastar más dinero no es la solución. Para proteger los datos, los usuarios y la marca, es necesario transformar la estrategia de seguridad.

+27,4 %

Aumento en el promedio anual de infracciones de seguridad en 2017[2]

+22,7 %

Aumento en el costo de ciberseguridad en 2017[2]

2 Accenture Security, '2017 Cost of Cybercrime Study,' diciembre de 2017

3 Las nuevas capacidades de amenaza exigen una nueva estrategia

A medida que los centros de datos, la tecnología de la nube, las aplicaciones y los dispositivos evolucionan, también lo hacen las amenazas. Las soluciones de seguridad tradicionales diseñadas para otra era no son suficientes para eliminarlas. Los atacantes modernos se camuflan y de formas imperceptibles. En lugar de perseguir las amenazas, TI debe concentrarse en la prevención para abordar los vectores de amenazas y reducir la superficie de ataque.

En el pasado, TI puso énfasis en una táctica generalizada de la búsqueda del mal. Sin embargo, en la actualidad, lo único que eso logra es distraer a la organización de evitar los ataques. Mediante el uso de estrategias tales como menor privilegio, TI puede mantener una actitud anticipativa incluso contra las amenazas más sofisticadas.

El concepto de menor privilegio le permite a un usuario, dispositivo, proceso o aplicación acceder únicamente a la información que necesita. Además, se controla cuidadosamente el estado deseado y los estados de ejecución de las aplicaciones, de manera que cualquier cambio se detecte rápidamente. Las alertas automáticas evitan las alteraciones y los cambios inesperados.

4 La escasez de personal de ciberseguridad aumenta el riesgo

En el 2017, ISACA publicó un informe de ciberseguridad donde se indicaba la existencia de una crisis laboral de trabajadores capacitados en seguridad. El 64 % de los líderes de negocios y TI sénior encuestados dijeron que menos de la mitad de los solicitantes están capacitados para un cargo vacante de seguridad. En la actualidad, existe un reconocimiento en todo el sector respecto de la falta de personas que sepan qué están haciendo para mantenerse a la vanguardia con la seguridad.[3]

El alto recambio en roles de seguridad también representa un problema en muchas organizaciones. Este recambio puede generar la pérdida de conocimiento institucional fundamental: generalmente, cuando los trabajadores se van de una empresa, se llevan con ellos habilidades e información valiosas. En su ausencia, es posible que otros no defiendan la expansión de soluciones y presupuestos de seguridad que la organización necesita.

Esta escasez de talento pone en desventaja a la empresa, ya que su capacidad para responder a los nuevos desafíos depende de las personas capaces y dispuestas a afrontar esos retos. Sin profesionales capacitados que puedan detener la creciente cantidad de ataques, las organizaciones son blancos fáciles para las amenazas.

Una formación permanente y procesos establecidos, estrechamente vinculados con automatización y marcos, pueden ayudar a las organizaciones a retener el talento y reducir los riesgos.

3 ISACA, State of Cybersecurity 2017, 2017

En algunos casos, el equipo de seguridad se ve presionado por las expectativas de la organización, que a veces pueden resultar excesivas. Entonces, al afrontar el carácter inevitable de una intrusión o buscar un mayor desafío, los líderes y operadores de seguridad pasan de un trabajo al otro con notable frecuencia. Este recambio tiene un impacto desgastante sobre el conocimiento institucional, ya que los expertos y aquellos muy solicitados avanzan hacia puestos lucrativos (o se los despide como consecuencia de una infracción), y no queda nadie que defienda la expansión de presupuestos y programas de seguridad.[4]

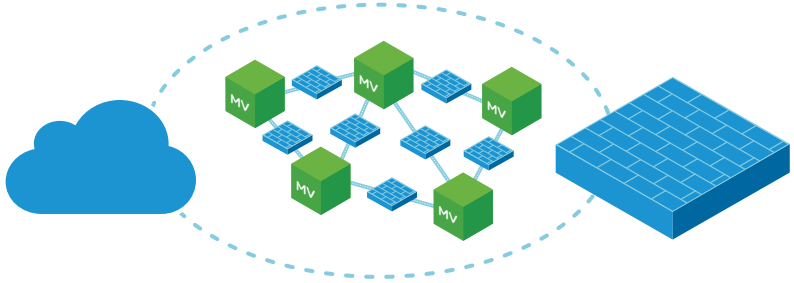
4 Gartner, How to Respond to the 2018 Threat Landscape, noviembre de 2017

Tome medidas estratégicas: Las recomendaciones de VMware para 2018

Si bien el panorama de amenazas puede resultar intimidante, está lejos de ser imbatible. Estas mejores prácticas de los profesionales de seguridad de VMware le servirán de ayuda para fortalecer su postura de seguridad y proteger su organización durante los próximos meses y años.

Enfóquese en la detección y la prevención

El establecimiento de un comportamiento conocido de la aplicación sirve como valor de referencia para la prevención y la detección de amenazas. Si dicho comportamiento llegase a desviarse de esta configuración "reconocida como buena", se pueden activar automáticamente medidas de respuesta.



Utilice la segmentación para reducir la superficie de ataque

Mantener por separado las cargas individuales y las máquinas virtuales evita que las amenazas se propaguen rápidamente. La creación de enclaves le permite limitar el alcance de una amenaza. La microsegmentación, habilitada mediante la virtualización de redes, detiene la propagación lateral y le quita efectividad a los ataques. Si neutraliza la capacidad de las amenazas de utilizar el tráfico horizontal, puede detectar, aislar y eliminar un ataque antes de que se propague.

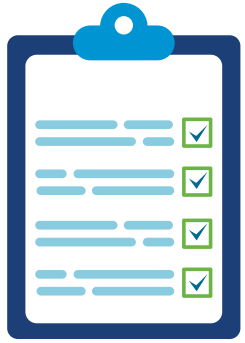
Tome medidas estratégicas: Las recomendaciones de VMware para 2018

Utilice inteligencia ante amenazas

Las mejores soluciones de inteligencia ante amenazas son exclusivas de cada negocio. No existe una estrategia universal. Una estrategia personalizada puede proporcionar una alerta de confianza elevada que genere una respuesta de acción de parte del equipo de TI.

Mantenga una higiene cibernética básica

Utilice la aplicación de parches y el fortalecimiento de sistemas para mantener las amenazas a raya. La seguridad de la información debería priorizar los esfuerzos de aplicación de parches en las operaciones de TI y compartir por qué se aplican dichos parches. Esto ayuda a aumentar la cooperación y disminuir los desacuerdos. Utilice parches donde pueda y detección en todas partes.



Planifique la adquisición de nuevas tecnologías de seguridad

No todas las soluciones de seguridad funcionarán para su negocio. TI debe asegurar que la nueva tecnología trate amenazas específicas dentro del negocio y que el personal existente sea capaz de administrarla. Si los profesionales de la seguridad no saben cómo utilizar una herramienta, no vale la pena hacer la inversión.

Proteja su negocio para hoy, mañana y siempre

En cualquier negocio, la seguridad de los datos siempre ha sido importante; y hoy es más importante que nunca. A medida que el panorama de amenazas sigue evolucionando, TI debe anticiparse a las amenazas y ser previsor siempre.

VMware e Intel transforman la seguridad suministrando medidas de seguridad integrales basadas tanto en software como en hardware en la infraestructura de aplicaciones y los terminales. Esto maximiza la visibilidad y el contexto de la interacción entre los usuarios y las aplicaciones, alinea las políticas y los controles de seguridad con las aplicaciones que protegen y, a su vez, posibilita la inserción de servicios de seguridad de terceros adicionales para brindar protección inteligente adicional.

COMIENCE LA TRANSFORMACIÓN DE LA SEGURIDAD

Más información sobre las soluciones de VMware >

Encuéntrenos en línea:

vmware® | intel®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304, USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com/latam