Guiones de lecciones de NSE2 - Apuntes 1

calculo integral (Instituto Nacional de Educación Media Diversificada Manuel Murillo Toro)

FORTINET NSE Training Institute

Guiones de las lecciones de NSE 2-Español

Índice

Lección 1-Seguridad en la nube

¡Hola! En esta lección, exploraremos la misteriosa "nube", qué es en realidad, cómo surgió y algunas de los problemas de seguridad que nos encontramos allí.

En primer lugar, desmitifiquemos la nube. Es divertido que "la nube" tenga un nombre público extremadamente alto reconocimiento, pero pocos entienden lo que es en realidad.

Tradicionalmente, antes de la nube, las empresas y otras organizaciones adquirían sus propios sistemas informáticos para ejecutar el software de aplicación necesario para el funcionamiento de la empresa. Estos sistemas informáticos se ubicaban en las instalaciones de la empresa y eran gestionados por equipos de empleados. Aunque no siempre era así, a menudo había más de un sistema informático (o servidor) por aplicación principal.

Esta configuración era cara por el coste de capital de los equipos informáticos y el coste de mano de obra de los expertos residentes que lo mantenían todo en funcionamiento; pero merecía la pena. Estos sistemas aumentaron la productividad global y ayudaron a mantener la ventaja competitiva.

No hace mucho, alguien se dio cuenta de que, de todos sus sistemas informáticos, sólo unos pocos estaban completamente ocupados en un momento dado. La mayoría estaban inactivos, esperando a que llegara la siguiente transacción. En resumen: había muchos recursos desaprovechados.

Así que se desarrolló una nueva forma de utilizar el hardware de servidor llamada virtualización, que en realidad procede de una vieja tecnología de la informática mainframe que permite que un solo servidor ejecute simultáneamente los sistemas operativos y las aplicaciones de varios servidores. La virtualización consolida las cargas de trabajo en menos servidores, aumentando su utilización, y ahorra dinero.

No pasó mucho tiempo hasta que la mayoría de los centros de datos dejaron de ser hileras de hardware informático dedicado a aplicaciones específicas para convertirse en un conjunto -o pool- de recursos de hardware generales que ejecutaban aplicaciones virtualizadas. Era lo más inteligente.

Llegan unos ingeniosos empresarios que construyen enormes centros de datos, repletos de hardware informático generalizado, y ofrecen alquilar partes de esta infraestructura para que sus clientes puedan ejecutar allí sus aplicaciones virtualizadas, en lugar de en su propio hardware. Así nace la nube.

Este tipo de computación en nube se denomina Infraestructura como Servicio o IaaS. También hay otros tipos de nubes. Por ejemplo, algunos proveedores de nubes ofrecen la infraestructura para ejecutar aplicaciones con servicios gestionados, como bases de datos que el cliente no necesita parchear ni mantener, o incluso entornos de aplicación completos. Es lo que se conoce como software como servicio o SaaS. Si alguna vez ha utilizado el correo de Google, o algo parecido, entonces ha utilizado SaaS.

Además, entre IaaS y SaaS en términos de funcionalidad y responsabilidad se encuentra la Plataforma como Servicio o PaaS. Esto incluye servicios en los que el proveedor de la nube gestiona mucho más de la infraestructura subyacente, como el parcheo del sistema operativo, y abstrae gran parte del trabajo para los usuarios, que en este caso adquieren un entorno estable para ejecutar contenedores. PaaS es cada vez más frecuente.

En cualquier caso, trasladar el coste de que las aplicaciones se ejecuten en costosos activos de hardware propiedad de la empresa a un modelo en el que el precio es un coste operativo recurrente resulta muy atractivo para la mayoría de las organizaciones.

Veamos ahora lo que esto significa para la seguridad.

Cuando las aplicaciones se alojan en el propio centro de datos de una empresa, el panorama de la seguridad es sencillo: se coloca la tecnología de seguridad adecuada en los lugares adecuados para abordar los problemas de seguridad específicos.

Sin embargo, proporcionar seguridad a la nube no está tan claro. Podría decirse que está un poco nublado. En resumidas cuentas: la seguridad es una responsabilidad compartida entre el proveedor de la nube y el cliente que utiliza los servicios en la nube.

Diseñada en capas, la seguridad incluye tanto los componentes físicos como los lógicos.

La infraestructura en nube proporcionada por los proveedores de IaaS está protegida de varias maneras. Desde el punto de vista de la disponibilidad, la infraestructura está diseñada por el proveedor para estar altamente disponible, por lo que el tiempo de actividad de la infraestructura es responsabilidad del proveedor. Desde el punto de vista de la seguridad, el proveedor sólo es responsable de proteger la infraestructura que proporciona.

Como cliente, cuando instala una o varias aplicaciones virtualizadas en la infraestructura de nube del proveedor, es responsable de proteger el acceso, el tráfico de red y las aplicaciones de datos.

Ahora, la mayoría de los proveedores suministran algún tipo de herramientas de seguridad para que las distintas partes de la nube del cliente
entorno de aplicación puede estar protegido. Sin embargo, estas herramientas pueden plantear algunos problemas.

En primer lugar, estas herramientas tienden a proporcionar sólo unas pocas funciones de seguridad básicas, y son las mismas herramientas que los proveedores utilizan para asegurar la infraestructura subyacente. Si un atacante consiguiera eludir estas herramientas en el nivel de la infraestructura, probablemente también sería capaz de eludirlas en el nivel de la aplicación del cliente.

En segundo lugar, y quizás más importante, está el hecho de que muchas organizaciones operan en un mundo híbrido en el que algunas de sus aplicaciones permanecen alojadas en sus propios centros de datos, otras en la plataforma en nube IaaS del proveedor A, otras en la plataforma en nube del proveedor B y otras con múltiples proveedores de SaaS. Esto es lo que llamamos un entorno "multi-nube", y viene con un problema "multi-nube": soluciones de seguridad múltiples, independientes y descoordinadas, un problema en el que la complejidad puede escalar geométricamente con el número de proveedores de nube implicados.

Para empezar, el personal de seguridad altamente cualificado es escaso. Si a eso se añade la carga de integrar y hacer funcionar simultáneamente múltiples entornos de seguridad no integrados... puede ser un verdadero problema.

En Fortinet, tenemos soluciones de seguridad como FortiGate, FortiMail, FortiWeb, FortiSandbox, FortiInsight, y otras dentro del Fortinet Security Fabric que no sólo están en casa en el centro de datos de una empresa, proporcionando la misma seguridad consistente, sino que están optimizadas para todos los proveedores líderes de nube IaaS como Amazon AWS, Microsoft Azure, Google Cloud, VMware, Cisco ACI, Oracle Cloud e IBM.

Para terminar, hemos mostrado los fundamentos de cómo surgió "la nube", cómo se protegen los entornos en la nube y hemos descrito la estrategia de seguridad en la nube de Fortinet, que abarca desde entornos sencillos de solo nube hasta entornos complejos de varias nubes.

Gracias por su tiempo y no olvide responder al cuestionario que sigue a esta lección.

Lección 2-SD-WAN

¡Hola! En esta lección, explicaremos qué es SD-WAN y cómo ha evolucionado.

SD-WAN son las siglas en inglés de red de área extensa definida por software, y aprovecha la WAN corporativa, así como la conectividad multi-nube para ofrecer un rendimiento de aplicaciones de alta velocidad.

En el pasado, las empresas adquirían y gestionaban sus propios servidores para ejecutar aplicaciones y almacenar datos empresariales críticos. Como resultado, tenían gastos de capital iniciales y necesitaban emplear a un equipo de técnicos altamente cualificados para hacer funcionar estos servidores. Aunque resultaba caro, la ventaja competitiva que suponía frente a quienes no informatizaban sus empresas hacía que mereciera la pena. Uno de los primeros retos fue poner estos servidores a disposición de varias redes distribuidas geográficamente, llamadas redes de área local o LAN.

Tal vez recuerdes que una WAN es una red informática que abarca una gran área geográfica y que suele estar formada por dos o más LAN. Por ejemplo, si Acme Corporation abarcara varias ciudades y continentes, cada uno con su propia red de área local, ¿cómo conectarían estas LAN para que alguien en la oficina de Londres pudiera conectarse a un servidor de base de datos en Singapur? Tradicionalmente, las empresas conectaban sus LAN a través de un único proveedor de servicios dedicado. Aunque resultaba caro, podían controlar y asegurar esta conexión a la vez que proporcionaban acceso a recursos críticos. Sin embargo, este método tenía limitaciones. El punto único de conectividad estaba sujeto a frecuentes cortes, lo que lo hacía poco fiable. Además, como cada vez había más demanda para alojar aplicaciones empresariales en la nube, lo que se conoce como software como servicio (SaaS), la mayor latencia se convirtió en un problema. Las aplicaciones SaaS, como Salesforce, Dropbox y Google Apps, y una mayor dependencia de las videoconferencias y las conferencias de voz, contribuyeron a la congestión. Las empresas empezaron a aumentar su conectividad empleando múltiples proveedores, o buscando banda ancha más asequible y otros medios de conectividad a Internet. La tendencia hacia el aumento de las conexiones híbridas, y el crecimiento de las aplicaciones en la nube para respaldar las decisiones empresariales inteligentes subyacentes, dieron lugar a la primera generación de SD-WAN.

Las empresas añadieron varios enlaces de operador dedicados y un equilibrio de carga por tráfico de aplicación, en función del ancho de banda disponible. Aunque este enfoque parecía resolver algunos problemas de ancho de banda, añadía otro producto más para resolver otro reto de la red. Estos productos puntuales aumentan la complejidad de la infraestructura de red. ¿Por qué? Porque añadir varios productos de varios proveedores, cada uno de los cuales tiene consolas de gestión independientes y que a menudo no se integran totalmente con otros productos, se convierte en una pesadilla de gestión para los administradores de seguridad de TI. Aun así, la primera generación de SD-WAN resolvió una necesidad empresarial acuciante: sus técnicas básicas de equilibrio de carga permitieron a la red tomar decisiones empresariales inteligentes para las aplicaciones en enlaces WAN híbridos, incluidos los de proveedores de servicios, banda ancha y evolución a largo plazo o LTE, que es un estándar de comunicación inalámbrica de banda ancha para dispositivos móviles y terminales de datos.

La identificación precisa de las aplicaciones, la visibilidad del rendimiento de la red y la conmutación fiable del tráfico de aplicaciones entre los enlaces WAN de mejor rendimiento han convertido a SD-WAN en la tecnología WAN más solicitada por todas las empresas.

Sin embargo, la seguridad seguía siendo un serio problema para las empresas. Incluso después de la adopción de SD-WAN, las empresas seguían enviando todo su tráfico de aplicaciones sensibles y críticas a los centros de datos por motivos de seguridad, o se veían obligadas a instalar una sofisticada

solución de cortafuegos para inspeccionar su tráfico directo de Internet.

acceso. Esto añadía otro producto puntual para la seguridad, lo que hacía la red aún más compleja, difícil de gestionar y retrasaba la adopción de la nube.

Las empresas necesitaban hacer frente a estos retos integrando las funcionalidades de seguridad y red en un único dispositivo SD-WAN seguro. Esto permitió a las empresas sustituir sus múltiples productos puntuales por un único y potente dispositivo de seguridad, con un coste reducido y una gestión sencilla. Una sólida postura de seguridad ayudó a las empresas a utilizar aplicaciones en la nube de forma más asequible, con menor latencia y con una conexión directa a Internet que garantiza un rendimiento óptimo de las aplicaciones y la mejor experiencia de usuario. Las continuas comprobaciones del estado del rendimiento de la red garantizaron la elección del mejor enlace WAN disponible, en función de los acuerdos de nivel de servicio de las aplicaciones definidos por el usuario. Si un enlace concreto se degradaba, el dispositivo SD-WAN sabía trasladar la conexión al enlace WAN de mejor rendimiento.

Hoy en día, en las SD-WAN seguras, los flujos de trabajo intuitivos de las políticas empresariales facilitan la configuración y gestión de las necesidades de las aplicaciones con la flexibilidad de priorizar las aplicaciones críticas para el negocio. Una consola de gestión centralizada proporciona una visibilidad y telemetría únicas para identificar, solucionar y resolver problemas de red con un mínimo de personal de TI. Los completos análisis sobre la utilización del ancho de banda, la definición de aplicaciones, la selección de rutas y el panorama de amenazas a la seguridad no sólo proporcionan visibilidad de la red ampliada, sino que ayudan a los administradores a rediseñar rápidamente las políticas, basándose en estadísticas históricas, para mejorar el rendimiento de la red y las aplicaciones.

En general, los resultados positivos de una solución SD-WAN segura son la simplificación, la consolidación y la reducción de costes, al tiempo que se proporciona el tan necesario rendimiento óptimo de las aplicaciones y la mejor experiencia de usuario para las aplicaciones empresariales, SaaS y de comunicaciones unificadas como servicio (UCaaS). Los análisis en tiempo de ejecución y la telemetría ayudan a los equipos de infraestructura a coordinar y resolver problemas de forma acelerada, lo que reduce el número de tickets de soporte y las interrupciones de la red.

Fortinet presentó el término Secure SD-WAN, cuyo núcleo es FortiGate®, el firewall de nueva generación (NGFW) de Fortinet. Además del dispositivo FortiGate®, la solución Secure SD-WAN incluye otras funciones de red avanzadas.

Gracias por su tiempo y no olvide responder al cuestionario que sigue a esta lección.

Lección 3: Seguridad de puntos finales

¡Hola! En esta lección aprenderemos sobre la seguridad de los puntos finales, qué es y cómo ha evolucionado.

Definamos lo que entendemos por punto final. En el pasado, se definía como cualquier dispositivo personal utilizado por un usuario final, como un ordenador de sobremesa, un portátil o un dispositivo de mano. Ahora, los puntos finales incluyen la Internet de las Cosas, o IoT, que abarca todo tipo de gadgets, como un termostato inteligente o un frigorífico en un hogar.

¿Cómo hemos protegido estos puntos finales y por qué es tan importante su seguridad? Los puntos finales siempre han sido un punto de entrada fácil en una red. ¿Por qué intentar burlar un cortafuegos cuando, mediante ingeniería social, se puede explotar a usuarios crédulos y descuidados? A medida que se han ampliado las conexiones en línea, el número de vectores de ataque se ha multiplicado en los puntos finales, dando a los atacantes más oportunidades que explotar.

Antes de que las redes estuvieran conectadas a Internet, los delincuentes recurrían a los disquetes para propagar programas maliciosos. Un disco infectado insertado en un ordenador infectaba ese ordenador. Más tarde, esto incluiría otros dispositivos de almacenamiento extraíbles, como CD, DVD y unidades portátiles conectadas por USB. Como se puede imaginar, este vector de ataque tenía un alcance bastante limitado. Los primeros productos de seguridad para puntos finales eran antivirus, o AV, que analizaban los dispositivos y el disco duro en busca de malware. Se basaban en firmas, lo que significa que el software antivirus buscaba características específicas, huellas dactilares o firmas del virus. Si encontraba algo que tenía esas características, podía poner el programa en cuarentena o eliminarlo.

Todo esto cambió cuando las redes domésticas y empresariales empezaron a conectarse a Internet. Los ciberdelincuentes tuvieron a su disposición muchos más vectores de ataque, como la suplantación de identidad por correo electrónico, los sitios web infectados, el uso de dispositivos propios en el trabajo (BYOD) y las redes sociales. Estas nuevas oportunidades multiplicaron el crecimiento del malware, que pasó de decenas de miles al año a cientos de miles al día. Además, los malhechores empezaron a explotar las lagunas de seguridad de los sistemas operativos, aplicaciones como el navegador web e incluso aplicaciones relativamente inertes como un documento de MS Word. Para agravar el problema de la ampliación de la superficie de ataque, cambió la propia naturaleza del malware. El malware polimórfico está diseñado para cambiar por sí mismo, imitando a los virus que mutan en el mundo natural. Esto significaba que el software antivirus basado en firmas ya no era totalmente eficaz.

Llegó la plataforma de protección de endpoints o EPP, que pretendía evitar los ataques de malware basados en archivos e implantar otros controles preventivos. El método se centraba en detener el malware antes de que se ejecutara e infectara el endpoint. El malware basado en archivos es un archivo descargado en un dispositivo que, al abrirse, ejecuta código malicioso o un script.

El EPP ofrecía muchos servicios centrados en la prevención, como antivirus, cortafuegos de dispositivos, filtrado web, protección de datos mediante cifrado y control de dispositivos. El control de dispositivos es una tecnología que proporciona seguridad integrada que detecta, autoriza y protege los dispositivos de almacenamiento extraíbles. El filtrado web es una tecnología que permite a los administradores de red controlar qué tipo de sitios se permite visitar.

Sin embargo, ninguna de estas técnicas resultó ser el remedio definitivo para las infecciones de los endpoints. En aquel momento, se pensó que el filtrado web era la solución porque se suponía que el malware nacido en la web procedía únicamente de sitios web lascivos. Quedaba la posibilidad de que el

malware se hiciera pasar por un anuncio en un sitio legítimo.

Dada la complejidad en constante evolución de los métodos de ataque y la ampliación de la superficie de ataque, los profesionales de la seguridad se dieron cuenta de que era imposible prevenir todas las infecciones de malware. Paralelamente al desarrollo del EPP, se desarrolló una nueva estrategia para defender el endpoint. Esa nueva estrategia se denomina detección y respuesta de puntos finales, o EDR.

EDR es un software utilizado para detectar, investigar y responder a actividades sospechosas en puntos finales. Comenzó como una herramienta de investigación forense digital, y proporcionó a los analistas de seguridad la información sobre amenazas y las herramientas necesarias para analizar un ataque e identificar los indicadores de compromiso, o IoC. De este modo, los analistas podían detectar programas maliciosos, algunos de los cuales permanecían en las redes sin ser detectados durante meses o años. En lugar de investigar un ataque para conocer su anatomía, la herramienta se utilizó también para detectar un ataque en curso en tiempo real. También se añadieron herramientas de corrección, que permitieron a los analistas solicitar más información de los puntos finales, prohibir procesos, aislar puntos finales y bloquear IP específicas. EDR se convirtió en una verdadera solución de detección y respuesta, pero no sin problemas.

Esta primera generación de EDR utilizaba sobre todo métodos manuales que consumían mucho tiempo y eran demasiado lentos para amenazas tan rápidas como el ransomware. La falta de integración con otro software de seguridad obstaculizaba su capacidad para responder de forma eficaz y oportuna. La configuración y el uso de EDR exigían conocimientos de alto nivel, y el análisis de multitud de alertas, muchas de las cuales eran falsos positivos, llevaba mucho tiempo a los analistas. Los proveedores mitigaron en parte estos problemas introduciendo una plataforma de detección y respuesta gestionadas, o MDR, que realizaba un triaje básico de las alertas y notificaba a los analistas por correo electrónico. Aun así, la EDR seguía siendo demasiado lenta y complicada para convertirse en una herramienta estándar en el arsenal del software de seguridad para puntos finales.

La EDR de segunda generación abordó estos problemas. Se diseñó para que se rigiera por políticas y se automatizara. A través de guías personalizables, los analistas pueden ordenar al EDR que solucione los problemas de forma inmediata y automática. De forma proactiva, los analistas pueden ordenar a EDR que responda de una forma específica si detecta un programa o script que se comporta de forma sospechosa. Las actividades maliciosas activan bloqueos automáticos para impedir la filtración de datos, el cifrado y los intentos de infiltración en la red. Puede detener y hacer retroceder el ransomware en tiempo real sin necesidad de retirar el dispositivo ni interrumpir la continuidad de la actividad.

Los profesionales de la seguridad no tardaron en darse cuenta de las ventajas de fusionar las tecnologías EDR y EPP, y la mayoría de las definiciones de EPP incluyen ahora ambas características. Un único agente integrado puede prevenir la mayoría del malware basado en archivos en la fase previa a la infección y la ejecución, al tiempo que detecta y responde al malware que ha eludido la prevención en la fase posterior a la infección. Una solución combinada de EPP y EDR también elimina los problemas de integración y simplifica la configuración y gestión para los analistas.

El software EPP y EDR incluye ahora otros controles preventivos para mejorar la higiene de la seguridad, como alertar a los analistas cuando los puestos finales no tienen el último parche de seguridad o están ejecutando aplicaciones inseguras. Al identificar vulnerabilidades críticas, los equipos de seguridad pueden mitigar las amenazas y aplicar parches virtuales o crear políticas que apliquen restricciones a los puntos finales hasta que se instale un parche de software. Además, el aprendizaje automático (ML) se incluye ahora como parte de las funciones AV mejoradas, lo que ayuda a detectar el malware en la fase previa a su ejecución.

Los productos de seguridad para puntos finales de Fortinet son FortiClient® y FortiEDRTM. El dispositivo FortiClient® está totalmente integrado con otros productos de seguridad que comparten datos de inteligencia y se gestionan de forma centralizada en lo que se denomina Fortinet Security Fabric.

Gracias por su tiempo y no olvide responder al cuestionario que sigue a esta lección.

Lección 4 - Cortafuegos

En esta lección, aprenderá cómo se crearon los cortafuegos para proporcionar una seguridad de red rudimentaria y cómo evolucionaron hasta convertirse en cortafuegos de nueva generación para mantenerse al día con el panorama de amenazas en constante cambio.

Cuando las redes empezaron a crecer, a interconectarse y, finalmente, a conectarse a Internet, se hizo importante controlar el flujo del tráfico de red. Al principio, este control adoptó la forma de cortafuegos de filtrado de paquetes que examinaban las capas de protocolo más bajas, como las direcciones de red de origen y destino, los protocolos y los números de puerto. Las reglas de los cortafuegos utilizaban estos atributos para definir qué paquetes podían pasar. Si las direcciones de red, el protocolo y el número de puerto del paquete coincidían con los de una regla de filtrado de paquetes del cortafuegos, se permitía su paso. Si no, se rechazaba o bloqueaba silenciosamente.

El inconveniente de los cortafuegos de filtro de paquetes era que adoptaban un enfoque único para decidir si permitían o no el paso del tráfico, y los malos agentes podían saltarse las reglas del cortafuegos. ¿Qué impediría a un malhechor inyectar paquetes fraudulentos a través de protocolos y puertos aceptables, o explotar un fallo en el software de redes informáticas? Para contrarrestar esta debilidad, en los cortafuegos de segunda generación se desarrollaron criterios adicionales para bloquear o permitir el tráfico.

Los cortafuegos de segunda generación, llamados cortafuegos de estado, se diseñaron para observar estas conexiones de red a lo largo del tiempo. Observaban cómo se realizaban las nuevas conexiones de red y examinaban continuamente la conversación entre los extremos. Si una conexión no se comportaba correctamente, el cortafuegos la bloqueaba. Cualquier paquete que no perteneciera a una conversación conocida era descartado.

Aunque esto supuso una mejora, los cortafuegos de segunda generación seguían sin poder bloquear los paquetes no autorizados si utilizaban un protocolo aceptable, como HTTP. La explosión de la World Wide Web promovió HTTP como uno de los protocolos de red más utilizados. El problema es que HTTP se utiliza de muchas maneras, como contenido de texto estático, comercio electrónico, alojamiento de archivos y en muchos otros tipos de aplicaciones web. Como todas ellas utilizan el mismo número de puerto, el cortafuegos no es capaz de distinguirlas. Los administradores de red necesitaban distinguir entre estas aplicaciones web para bloquear las maliciosas y permitir las beneficiosas. Para determinar cómo se utilizan protocolos como HTTP, el cortafuegos debe profundizar en las cargas útiles de datos.

Los cortafuegos de tercera generación hacen precisamente eso. Aunque siguen siendo de estado, estos cortafuegos comprenden los protocolos de nivel superior y las aplicaciones que contienen, y controlan los distintos usos del mismo protocolo básico. Esto se conoce como filtrado de la capa de aplicación. Los cortafuegos que implementan el filtrado de la capa de aplicación pueden entender protocolos como HTTP, FTP, DNS y otros. En el caso de HTTP, puede diferenciar entre el tráfico del navegador a un blog, un sitio de intercambio de archivos, comercio electrónico, redes sociales, voz sobre IP, correo electrónico y muchos más.

Nuestras crecientes conexiones a través de Internet también precipitaron profundos cambios en la forma en que trabajamos, jugamos, nos entretenemos y comerciamos. Las empresas evolucionaron para aprovechar servicios multi-nube más baratos, y la comodidad de los dispositivos móviles y de IoT amplió drásticamente los bordes de la red, aumentando así la superficie de ataque. Los actores de las amenazas siguen cambiando en cuanto a métodos de ataque y sofisticación. Ahora los ataques proceden de usuarios, dispositivos y aplicaciones de confianza que propagan malware, tanto sin saberlo como con intenciones maliciosas.

Ahora, un cortafuegos debe prevenir los ciberataques en evolución en todos los extremos de la red y, al mismo tiempo, ofrecer seguridad, fiabilidad y rendimiento de la red. Esto nos lleva a las funciones de seguridad avanzadas que

se encuentran en el cortafuegos de nueva generación (NGFW). Al igual que la seguridad de un aeropuerto, un cortafuegos de nueva generación tiene varios puntos de control de seguridad. Al igual que un agente de seguridad examina su tarjeta de embarque como primera línea de defensa, un cortafuegos de nueva generación examina los paquetes y toma decisiones basadas en reglas para permitir o descartar el tráfico. A continuación, se comprueba su equipaje de viaje para ver si lleva algún contenido malicioso. Esto es similar a cómo un cortafuegos de nueva generación realiza una inspección profunda de paquetes (IPS). Si se encuentra contenido cuestionable en su bolsa de viaje, el control mejorado del aeropuerto apartará la bolsa para examinarla más a fondo. Esto es similar a cómo el cortafuegos de nueva generación envía el contenido malicioso a un sandbox para su posterior análisis.

A medida que las redes evolucionan e introducen nuevos retos, los cortafuegos de nueva generación también evolucionan. Por ejemplo, tienen la capacidad de controlar las aplicaciones, ya sea por clasificación o en función de quién sea el usuario. La seguridad a nivel de aplicación ayuda a proteger a los clientes que navegan por Internet de ataques y amenazas.

Los cortafuegos de nueva generación también adoptaron varios enfoques de segmentación que segregan usuarios, dispositivos y aplicaciones, que se ajustan a las necesidades empresariales. Al segmentar las redes en lugar de utilizar una red plana, el cortafuegos ayuda a eliminar un único punto de entrada, lo que facilitaba a los ciberdelincuentes introducirse en la red y propagar las amenazas por toda ella.

Los cortafuegos de nueva generación también ofrecen una inspección de alto rendimiento y una mayor visibilidad de la red, con una degradación mínima o nula, para soportar y proteger los centros de datos modernos y distribuidos que se encuentran dentro de una infraestructura de TI compleja e híbrida. Los centros de datos híbridos ofrecen a las empresas mayor agilidad, flexibilidad y escalabilidad bajo demanda, así como una superficie de ataque ampliada que requiere una estrategia de seguridad igualmente evolucionada. La inspección de alto rendimiento incluye aplicaciones, recursos informáticos, análisis, datos cifrados que se mueven por toda la infraestructura y almacenamiento de datos en varias nubes privadas y públicas.

FortiGate® es el cortafuegos de nueva generación de Fortinet. El dispositivo FortiGate® está totalmente integrado con otros productos de seguridad que comparten datos de inteligencia y se gestionan de forma centralizada en lo que se denomina Fortinet Security Fabric.

Gracias por su tiempo y no olvide responder al cuestionario que sigue a esta lección.

Lección 5-Wi-Fi

¡Hola! En esta lección, aprenderás sobre Wi-Fi y las implicaciones de seguridad de las redes inalámbricas.

Wi-Fi es una tecnología de conexión inalámbrica en red de área local de dispositivos basada en las normas IEEE 802.11. Empezó siendo pequeña, destinada sobre todo al uso industrial, y ha crecido hasta convertirse en la forma más común de conexión de todos nuestros dispositivos electrónicos personales en casa o en la oficina.

El desarrollo de Wi-Fi aprovechó muchos de los mismos protocolos y tecnología que Ethernet, con una gran diferencia. Todas las transmisiones se realizan a través del aire, lo que significa que, al igual que en una conversación verbal, cualquiera que esté escuchando puede oír lo que se dice.

Originalmente, los mecanismos de autenticación y privacidad de Wi-Fi eran muy débiles. La norma ofrecía una opción sencilla de cifrado llamada Wired Equivalent Privacy o WEP. WEP utilizaba una clave para cifrar el tráfico mediante el flujo de claves RC4. Sin embargo, si alguien disponía de las herramientas adecuadas y una máquina razonablemente potente, podía vulnerar la WEP con bastante rapidez. Se corrió la voz de que el Wi-Fi era inseguro y que la tecnología, que estaba empezando a crecer, tenía graves problemas.
Las partes interesadas se reunieron con el IEEE y la Wi-Fi Alliance para crear Wi-Fi Protected Access (WPA). Añadía funciones de seguridad adicionales, pero conservaba el algoritmo RC4, lo que facilitaba a los usuarios la actualización de sus dispositivos más antiguos. Sin embargo, seguía sin resolver el problema fundamental de seguridad.

También se introdujo un nuevo estándar, basado en el algoritmo Advanced Encryption Standard, o AES, del Instituto Nacional de Estándares y Tecnología (NIST), llamado Wi-Fi Protected Access 2 (WPA2). Era mucho más seguro que WEP. Además, se añadió a la tecnología una nueva autenticación de nivel empresarial, creando dos sabores de cada estilo de seguridad. El nivel de seguridad personal seguía utilizando una frase de contraseña compartida para la autenticación en red y el intercambio de claves. El nivel de seguridad empresarial utilizaba mecanismos de autenticación 802.1x, similares a los empleados en redes cableadas, para autenticar a un usuario y establecer el cifrado. Sin embargo, las frases de contraseña mal elegidas o débiles podían seguir dejando las redes vulnerables.

Lanzado en 2018, Wi-Fi Protected Access 3 (WPA3) introdujo un nuevo apretón de manos más seguro para establecer conexiones, un método más fácil para agregar dispositivos a la red, mayores tamaños de clave y otras características de seguridad.

Podría parecer que ya está, que la tecnología inalámbrica ya es segura y que no hay de qué preocuparse. Por desgracia, no es así. Los piratas informáticos han encontrado varias formas de explotar el comportamiento humano y seguir teniendo acceso a la información que desean.

Wi-Fi gratuito disponible, es una señal que todos buscamos cuando estamos en público, pero conlleva riesgos. Los hackers instalan puntos de acceso (AP) que actúan como honeypots en zonas públicas.
Los desprevenidos que se conectan a estas supuestas redes gratuitas no se dan cuenta de que el hacker tiene acceso a todo lo que hacen en línea.
Por ejemplo, si introduces las credenciales de tu cuenta y los datos de tu tarjeta de crédito, pueden conseguirlos. Desconfíe, aunque el nombre de una red parezca legítimo.

Además, nuestros dispositivos portátiles recuerdan las redes a las que nos hemos conectado en el pasado. En un esfuerzo por ayudarnos, buscan automáticamente esa red y vuelven a conectarse a ella cuando la ven. Esto significa que un pirata informático puede oír tu teléfono buscando la red Wi-Fi legítima del hotel a la que te conectaste el año pasado, configurar un punto de acceso falso que emita ese nombre de red y engañar a tu dispositivo para que se conecte. A menos que se dé cuenta de que su dispositivo está ahora conectado a Wi-Fi, puede pasar datos a través del AP falso, exponiendo de nuevo todo lo que está haciendo.

No sólo estás expuesto cuando estás fuera de casa. Mucha gente configura su red en casa, pero nunca activa la seguridad. O si lo hicieron, fue hace mucho tiempo, posiblemente con WEP o WPA, y nunca actualizaron la contraseña. Los nuevos firmware de los routers inalámbricos domésticos ofrecen ahora funciones adicionales, como WPA3 o visibilidad de los dispositivos de la red. Es una buena idea mantener actualizada su seguridad y elegir frases de contraseña complejas y difíciles de adivinar. Como mínimo, cambia el identificador del conjunto de servicios, o SSID, y el nombre de usuario y contraseña por defecto del administrador. Además, vigila tu red doméstica y asegúrate de que reconoces los dispositivos que acceden a ella. Si un hacker entra en la red, tendrá acceso a todo lo que haya en ella. En ese momento, ya no se trata de leer el tráfico inalámbrico que envías, sino de saber qué dispositivos pueden comprometer y qué datos pueden obtener de ellos.

Los retos asociados a la Wi-Fi de clase empresarial siguen creciendo. Con IoT, BYOD y una fuerza de trabajo altamente móvil, es fundamental gestionar los puntos de acceso y, al mismo tiempo, hacer frente a las cambiantes amenazas de seguridad, ya sea en la oficina corporativa, en la oficina remota o en su hogar.

Fortinet ofrece un producto inalámbrico llamado FortiAP™. Es compatible con las últimas tecnologías Wi-Fi y se integra con FortiGate®, un cortafuegos de nueva generación, y es gestionado por él.

Gracias por su tiempo y no olvide contestar al cuestionario que sigue a esta lección.

Lección 6: Servicios de inteligencia de amenazas

En esta lección, aprenderá cómo los proveedores de seguridad recopilan información sobre amenazas y brindan acceso a ese conocimiento recopilado para detectar malos comportamientos en línea.

En los primeros días de los productos antivirus para terminales, los proveedores necesitaban una forma de catalogar todos los virus conocidos para que sus productos pudieran confirmar si un archivo contenía un virus o no. Su departamento de inteligencia de amenazas hizo esto tomando una muestra de cada virus conocido y generando una firma, que representaba el contenido del archivo. En otras palabras, una huella dactilar. Estas listas de firmas de virus se distribuyeron con software antivirus. A medida que pasaba el tiempo y se detectaban nuevos virus, el servicio de inteligencia de amenazas de cada proveedor distribuía actualizaciones a su lista de firmas de virus. Estas actualizaciones se emitieron regularmente y de diferentes formas. Las actualizaciones se publicaron mensualmente, trimestralmente o, en algunos casos, solo una vez al año.

A medida que los desarrolladores de malware ganaron experiencia, su malware se volvió más sofisticado e incluyó mecanismos para evadir el escaneo clásico basado en firmas al poder cambiar el contenido de sus archivos a voluntad. Debido a que el contenido del archivo cambió, sus firmas también cambiaron, lo que permitió que el malware pasara sigilosamente por los productos antivirus más antiguos. Esto dio lugar a que un solo tipo de malware se convirtiera en una familia de malware completa de quizás cientos de miles de archivos diferentes, también conocidos como malware polimórfico, y cada uno de ellos realizaba los mismos malos comportamientos. Este problema también ocurre cuando los kits de malware de bricolaje se ponen a la venta en la dark web, sin mencionar la proliferación de organizaciones de malware como servicio. ¡El cibercrimen tiene su propio modelo de negocio!

Ahora tenemos un nuevo problema: el enfoque clásico de firma uno a uno en el que cada archivo de malware conocido está representado por una firma en el archivo de firma obviamente no va a escalar bien, dado el potencial de que la cantidad de nuevas variaciones de malware contará en millones o más cada día. Para manejar esta nueva capacidad del malware de transformarse en nuevas formas, los servicios de inteligencia de amenazas de los proveedores crearon formas de detectar familias enteras de malware usando solo una firma. Esto se hace en una variedad de formas diferentes, pero todas detectan puntos en común en la familia de malware.

Hasta ahora, hemos estado hablando de malware que se ha visto y, por lo tanto, es conocido por los investigadores de amenazas de los proveedores. ¿Qué pasa con las variaciones de malware que aún no se han visto? Los métodos de detección basados en firmas no funcionarán. Para detectar este tipo de amenazas, los proveedores crearon productos de sandboxing, que toman un archivo sospechoso y lo colocan en un entorno donde se puede analizar de cerca su comportamiento. Si el archivo hace algo malicioso mientras está en la zona de pruebas, se marca como malware. Esto se conoce como detección heurística y busca comportamientos anómalos fuera de lo común. De hecho, los proveedores crean algoritmos heurísticos patentados que pueden detectar muestras polimórficas de malware nunca antes vistas.

Según el producto de sandbox en particular y su configuración, el propietario del sandbox puede propagar este nuevo conocimiento no solo a través de su propio entorno de seguridad de red, sino también enviar los detalles al servicio de inteligencia de amenazas del proveedor para que pueda compartirse en todo el mundo y proteger más. gente.

Más allá del sandboxing, el futuro de la detección de malware previamente desconocido incluye el uso de inteligencia artificial y aprendizaje automático por parte del servicio de inteligencia de amenazas para calificar rápidamente el potencial de amenaza de seguridad de los archivos a medida que atraviesan la red. Y no se trata solo de archivos. El servicio de inteligencia de amenazas cataloga el conocimiento sobre los ataques existentes o emergentes, incluidos los mecanismos específicos del ataque, la evidencia de que el ataque ha ocurrido, también conocido como Indicadores de Compromiso o IoC, las implicaciones del ataque, la atribución del adversario y sus posibles motivaciones.

A medida que las técnicas utilizadas por los malos actores continúan evolucionando y se vuelven más sofisticadas, es más importante que nunca compartir la inteligencia de amenazas en tiempo real, en todo el entorno de seguridad de la red. Si algunos componentes de seguridad conocen el ataque mientras otros esperan actualizaciones periódicas de firmas, los atacantes pueden evadir las defensas y causar daño. Los productos de seguridad y los servicios de inteligencia de amenazas que pueden actuar juntos en tiempo real tienen la mejor oportunidad de detener estos ataques.

Y el intercambio de inteligencia sobre amenazas no se detiene con la línea de productos de cada proveedor. Aunque pensaría que después de realizar el trabajo necesario para recopilar, analizar y catalogar información sobre amenazas, cada proveedor mantendría esa información en secreto. Casi todos los proveedores comparten esta información con la comunidad de seguridad en general. Esto sucede a través de membresías formales en organizaciones como Cyber Threat Alliance, equipos de respuesta a emergencias informáticas (CERT) locales, nacionales e internacionales, así como numerosas asociaciones privadas de confianza con otros proveedores, investigadores de seguridad independientes y fuerzas del orden. Este intercambio de información sobre amenazas en tiempo real permite una imagen más completa del ataque, porque ningún proveedor individual tendrá todos los datos, y no es la inteligencia de amenazas lo que distingue a los proveedores,

Aquí es donde sobresale Fortinet. Nuestro servicio de inteligencia de amenazas se conoce como FortiGuard® Labs. Centenares de investigadores de FortiGuard® Labs, que abarcan diez disciplinas de seguridad distintas, exploran el panorama de las ciberamenazas y buscan proactivamente nuevas vías de ataque todos los días para descubrir (e idealmente evitar) las amenazas emergentes. La protección de seguridad comprobada y certificada por FortiGuard® Labs brinda servicios integrales de seguridad, actualizaciones y protección para la gama completa de soluciones Fortinet Security Fabric.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.

Lección 7: VUELA

Hola. En esta lección, veremos la orquestación, automatización y respuesta de seguridad (SOAR). SOAR es un término candente en la industria de la seguridad, por lo que es importante no solo saber qué es, sino también estar familiarizado con los problemas y desafíos que aborda SOAR. Pero antes de llegar a eso, primero examinemos los conceptos básicos.

¿Qué es SOAR? SOAR conecta todas las demás herramientas en su pila de seguridad en flujos de trabajo definidos, que se pueden ejecutar automáticamente. En otras palabras, SOAR le permite aumentar la eficiencia de su equipo mediante la automatización de procesos manuales repetitivos.

La automatización es muy importante en el mundo de la seguridad actual porque los equipos de seguridad están desbordados. A medida que se desarrollan nuevas herramientas para hacer frente a un panorama de amenazas en constante evolución, los analistas que utilizan esas herramientas tienen que alternar entre ellas para realizar sus tareas diarias.

Una tarea común del día a día es responder a las alertas. Con más herramientas de seguridad vienen más alertas, que se abordan en una serie de procesos manuales y cambios de contexto, es decir, cambiar de una herramienta a otra. Más alertas para responder cada día significa que tiene menos tiempo para dedicar a cada alerta, lo que aumenta la probabilidad de cometer errores. La degradación del rendimiento frente a una avalancha de alertas se denomina fatiga de alertas.

Una forma obvia de mitigar la fatiga de las alertas es simplemente contratar más analistas. Sin embargo, debido a la escasez de habilidades en ciberseguridad, simplemente no hay suficientes analistas calificados para contratar. Entonces, si contratar más analistas no es una opción, ¿cómo resolvemos la fatiga de alertas? Sencillo, con SOAR.

Como se mencionó, SOAR une las herramientas en su pila de seguridad. Al extraer datos de todas estas fuentes, SOAR reduce el cambio de contexto con el que tienen que lidiar los analistas. Por lo tanto, los analistas pueden realizar todos sus procesos de investigación habituales directamente desde la interfaz de origen. Además, esos procesos se pueden traducir de forma manual o automática en un libro de jugadas, que es un conjunto de pasos similar a un diagrama de flujo que se puede repetir a pedido. Al usar un libro de jugadas, puede asegurarse de que se sigan todos los pasos de su procedimiento operativo estándar. También tiene datos sobre exactamente qué se hizo, cuándo y quién lo hizo. Esta capacidad se denomina orquestación y automatización.

La investigación es otra capacidad crucial de SOAR. Cuando aparece una alerta sospechosa, los equipos pueden realizar sus tareas de investigación, como verificar las fuentes de inteligencia de amenazas para obtener una reputación o consultar un sistema de administración de información de seguridad (SIM), para eventos relacionados desde dentro de la plataforma SOAR. La información obtenida de esta investigación determinará los pasos de mitigación requeridos. Entonces, dado que SOAR es un banco de trabajo unificado de todas sus herramientas de seguridad, también puede tomar esos pasos de mitigación desde dentro de SOAR. Por ejemplo, desde SOAR puede bloquear el tráfico de una dirección IP maliciosa en su firewall o eliminar un correo electrónico de phishing de su servidor de correo electrónico. Al incorporar sus procesos estándar en libros de jugadas, puede reemplazar los procesos manuales repetitivos y que consumen mucho tiempo con la automatización a la velocidad de la máquina.

La implementación de SOAR en su ecosistema hace más que solo centralizar sus procesos de respuesta a incidentes: optimiza una operación completa. La optimización da como resultado respuestas optimizadas a la velocidad de la máquina, lo que permite a los equipos mejorar la colaboración y administrar mejor la ola interminable de alertas. Esto se debe a que SOAR permite a los usuarios asignar alertas a diferentes analistas o equipos en diferentes etapas del proceso de respuesta, y para que los usuarios asignados agreguen información a la alerta mientras trabajan en ella, de modo que otros que hagan referencia a esa alerta más adelante tendrán información adicional. contexto sobre la investigación.

Expliquemos los libros de jugadas con más detalle. Los equipos usan libros de jugadas, a veces llamados flujos de trabajo, como una forma de responder a alertas o incidentes de la misma manera cada vez. Los libros de jugadas funcionan al unísono con los equipos de seguridad al seguir los pasos que un analista normalmente implementaría al responder a un incidente. Los libros de jugadas realizan las tareas repetitivas, como compilar datos en un informe o enviar correos electrónicos, y pueden pausar cuando se necesita supervisión humana, como implementar un bloqueo de firewall. Los libros de jugadas son la clave para la capacidad de automatización de SOAR, lo que permite a los equipos mejorar su velocidad de respuesta y consistencia, mientras mantienen la autoridad humana sobre el proceso. En última instancia, el uso de un libro de jugadas puede reducir la carga de trabajo del analista y reducir las posibilidades de error.

Las investigaciones de phishing son uno de los casos de uso más comunes para SOAR implementado por los clientes. Sin SOAR, un analista dedicará tiempo a investigar el remitente de un correo electrónico de phishing y los indicadores clave ubicados dentro de los encabezados o el cuerpo del correo electrónico. Realizar estas investigaciones generalmente significa tiempo dedicado a ingresar dominios y URL en una plataforma de inteligencia de amenazas. Si los analistas determinan que un correo electrónico es dañino, deberán dedicar más tiempo a investigar su servidor de correo electrónico y su SIM, determinar quién recibió el correo electrónico, determinar quién hizo clic en él, eliminarlo, etc. Con un libro de jugadas de investigación de phishing, los pasos iniciales de investigación se toman automáticamente, tan pronto como se informa el correo electrónico de phishing. De esta manera, los analistas serán alertados solo de aquellos correos electrónicos que el libro de jugadas determine que son sospechosos.

Así que ahí lo tiene, una introducción a SOAR, qué es, qué problemas aborda y cómo ayuda. El producto SOAR de Fortinet se llama FortiSOAR™ y abarca todas estas características y más.

Gracias por tu tiempo. ¡Y no te olvides de hacer el cuestionario!

Lección 8—Control de acceso a la red

¡Hola! En esta lección, le presentaremos el control de acceso a la red (NAC) y le explicaremos cómo ha evolucionado.

NAC es un dispositivo o máquina virtual que controla el acceso de los dispositivos a la red. Comenzó como un método de autenticación y autorización de red para dispositivos que se unían a la red, que sigue los estándares IEEE 802.1X. El método de autenticación involucra a tres partes: el dispositivo cliente, el autenticador y el servidor de autenticación. El autenticador podría ser un conmutador de red o un punto de acceso inalámbrico que separa la red protegida de la red desprotegida. El cliente proporciona credenciales en forma de nombre de usuario y contraseña, certificado digital o algún otro medio al autenticador, que envía estas credenciales al servidor. Dependiendo del resultado de la autenticación, el autenticador bloqueará el dispositivo o le permitirá acceder a la red. Otro método para controlar el acceso a una red, especialmente una red disponible públicamente, es un portal cautivo. Si alguna vez se conectó a una red en un aeropuerto, hotel o cafetería, es posible que recuerde haber interactuado con una página web que le pedía que aceptara los términos legales antes de otorgar acceso.

Más tarde, NAC evolucionó para adaptarse al acceso de invitados, Traiga su propio dispositivo (BYOD) e Internet de las cosas (IoT). Por un par de razones, los dispositivos BYOD e IoT presentaron nuevos desafíos de seguridad. Uno, los BYOD son de propiedad personal, no activos de una organización. Por lo tanto, MIS no controla lo que se ejecuta en estos dispositivos, por ejemplo, software antivirus o aplicaciones no seguras. Dos, los dispositivos IoT son hardware con un sensor que transmite datos de un lugar a otro a través de Internet, expandiendo drásticamente la superficie de ataque. Las organizaciones compran dispositivos habilitados para IoT de otros proveedores, y estos dispositivos se conectan nuevamente a las redes de los proveedores para proporcionar información sobre el uso del producto y las necesidades de mantenimiento. Las organizaciones toleran esta situación porque los dispositivos IoT les ahorran tiempo y dinero. Por ejemplo, si una impresora tiene poco tóner, el proveedor podría notificar al administrador de la red por correo electrónico o incluso entregar un nuevo cartucho de tóner automáticamente. En un hogar inteligente, los dispositivos IoT regulan el calor y la humedad, controlan de forma remota las cerraduras de las puertas, monitorean lo que hay en el refrigerador e incluso ayudan con sus listas de compras.

La evidente comodidad de estos dispositivos los ha hecho muy populares y numerosos. Sin embargo, la variedad de dispositivos, la falta de estándares y la incapacidad de asegurar estos dispositivos los convierte en un conducto potencial para que el contagio ingrese a la red. Muchos dispositivos IoT carecen de los ciclos de CPU o la memoria para alojar el software de autenticación y seguridad. Se identifican mediante un secreto compartido o un número de serie único, que se inserta durante la fabricación. Pero este esquema de autenticación es muy limitado: si se conoce el secreto, es probable que no haya forma de restablecerlo y, sin la capacidad de instalar software de seguridad, hay poca visibilidad de esos dispositivos. Afortunadamente, NAC evolucionó para resolver estas debilidades.

Cuando MIS introduce NAC en una red, lo primero que hace NAC es crear perfiles de todos los dispositivos conectados. Luego, NAC permite el acceso a los recursos de la red según el perfil del dispositivo, que se define por función. Esto es similar a otorgar a las personas acceso a información confidencial en función de su necesidad de saber. Por ejemplo, NAC permitiría la conexión de una cámara IP a un servidor de grabadora de video en red (NVR), pero evitaría que se conecte a un servidor financiero. Según su perfil, un NVR no tiene por qué comunicarse con un servidor financiero. Cuando se otorga el acceso de esta manera, la red se segmenta por función del dispositivo. Si un dispositivo está comprometido, el malware puede infectar solo aquellos objetos que

el dispositivo puede conectarse. Por lo tanto, la cámara IP comprometida del ejemplo anterior podría infectar el servidor NVR, pero no el servidor financiero.

Si bien NAC demostró ser muy eficaz en la gestión de numerosos dispositivos desprotegidos, tuvo deficiencias en su evolución. Algunas soluciones NAC se diseñaron para ayudar con la incorporación de BYOD en redes inalámbricas, pero funcionaron mal en la parte cableada de la red. Se desarrollaron otras soluciones para trabajar dentro de un entorno de un solo proveedor, pero no podían perfilar automáticamente los dispositivos de terceros. Algunos tenían buena visibilidad en redes pequeñas y simples, pero no escalaban bien en redes grandes y distribuidas.

Hoy en día, la mayoría de las soluciones NAC han corregido estas limitaciones. Tienen una visibilidad más completa de la red y son mejores para categorizar dispositivos automáticamente. Funcionan de manera efectiva tanto en Ethernet como en redes inalámbricas. Muchas soluciones NAC tienen una arquitectura centralizada que mejora la gestión de dispositivos en redes grandes y multisitio. Fundamentalmente, NAC también debe integrarse en el marco de seguridad, de modo que cuando se detecte una infracción, NAC notifique automáticamente al centro de operaciones de seguridad (SOC) y se coordine con otros dispositivos de seguridad para neutralizar la amenaza.

Fortinet ofrece una solución de control de acceso a la red, denominada FortiNAC™. Contiene todas las características identificadas en esta lección.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.

Lección 9: Caja de arena

¡Hola! En esta lección, explicaremos qué es un sandbox, por qué se inventó y cómo ha evolucionado.

Un sandbox, dentro del contexto de la seguridad informática, es un sistema que confina las acciones de una aplicación, como abrir un documento de Word o un navegador, a un entorno virtual aislado. Dentro de este entorno virtual seguro, el sandbox estudia las diversas interacciones de las aplicaciones para descubrir cualquier intento malicioso. Entonces, si sucede algo inesperado o peligroso, solo afecta a la zona de pruebas y no a las otras computadoras y dispositivos en la red.

La tecnología Sandbox generalmente es administrada por el equipo de seguridad de la información de una organización, pero la utilizan los equipos de operaciones de red, aplicaciones y escritorio para reforzar la seguridad en sus respectivos dominios.

Los actores de amenazas explotan vulnerabilidades en aplicaciones legítimas para comprometer el dispositivo y, desde allí, se mueven a través de la red para infectar otros dispositivos. La explotación de una vulnerabilidad desconocida se conoce como ataque de día cero. Antes del sandboxing, no había medios efectivos para detener un ataque de día cero. Los firewalls y el software antivirus podían detener las amenazas conocidas, pero eran indefensos frente a los ataques de día cero.

Un sandbox proporcionaba un entorno virtual aislado que imitaba varios dispositivos informáticos, sistemas operativos y aplicaciones. Permitió que las amenazas potenciales se desarrollaran dentro de la seguridad de estos sistemas virtuales. Si el sandbox concluyó que el archivo o la actividad sospechosa era benigna, no se necesitaban más acciones. Sin embargo, si detecta una intención maliciosa, el archivo podría ponerse en cuarentena o la actividad podría detenerse en el dispositivo real.

Muchos de los primeros sandboxes no lograron integrarse estrechamente con otros dispositivos de seguridad dentro de la red. Si bien un sandbox podría identificar y derrotar un ataque de día cero, esta inteligencia de amenazas vital no siempre se compartió con los otros dispositivos de seguridad de la red de manera oportuna. Sin embargo, la falta de comunicación y coordinación tuvo menos que ver con un defecto de la tecnología sandbox que con una arquitectura de seguridad construida sobre soluciones puntuales. Las soluciones puntuales, que no podían integrarse completamente en los productos de otros proveedores, significaban que el centro de operaciones de seguridad (SOC) requería una consola de administración para cada producto. Por lo tanto, los intentos de agregar datos de inteligencia de amenazas fueron difíciles y requirieron mucho tiempo.

El sandbox de segunda generación surgió para corregir el enfoque aislado y fragmentado. Los sandboxes se equiparon con más herramientas de integración o se asociaron con otros proveedores de productos para mejorar la integración. Como resultado, podrían compartir inteligencia sobre amenazas con otros dispositivos de seguridad, como firewalls, puertas de enlace de correo electrónico, puntos finales y otros dispositivos de sandbox de manera más efectiva. El nuevo enfoque de la seguridad de la red permitió a los analistas correlacionar la inteligencia de amenazas de forma centralizada y responder a las amenazas desde un único panel de vidrio. Además, un entorno de seguridad de red integrado podría compartir información con un servicio de inteligencia de amenazas en la nube, que podría enviarse a otras redes.

Hoy en día, los actores de amenazas están innovando técnicas de automatización e inteligencia artificial (IA) para acelerar la creación de nuevas variantes y exploits de malware, y para descubrir vulnerabilidades de seguridad más rápidamente.

con el objetivo de evadir y abrumar las defensas actuales. Para mantener el ritmo y acelerar la detección de estas nuevas amenazas, es imperativo que se agregue el aprendizaje de IA al proceso de análisis de amenazas de la zona de pruebas.

Los ataques impulsados por IA requerían un sandbox de tercera generación basado en un estándar de análisis de amenazas. Además, necesitaba cubrir la superficie de ataque en expansión de las empresas debido a la transformación digital. La transformación digital se refiere al movimiento de datos comerciales, aplicaciones e infraestructura a la nube.

El desafío del análisis de amenazas basado en estándares surgió debido a la lucha por interpretar y comprender los métodos de amenazas cibernéticas, lo que obstaculizó las respuestas efectivas. MITRE, una organización sin fines de lucro, propuso el marco ATT&CK que describe categóricamente las características estándar del malware. Muchas organizaciones adoptaron MITRE ATT&CK como estándar para el análisis de amenazas. Por lo tanto, se hizo necesario que los productos de seguridad adoptaran el marco MITRE ATT&CK. Proporcionó a los dispositivos de seguridad un lenguaje común en el que identificar, describir y categorizar las amenazas, que se podían compartir con otros dispositivos de proveedores y comprender fácilmente.

Por último, a medida que más empresas adoptan la transformación digital, hay nuevas organizaciones o partes de organizaciones expuestas a ataques. Un ejemplo de ello es la industria de tecnología operativa (OT), que incluye servicios públicos, fabricación, petróleo y gas, y muchos otros. Tradicionalmente, OT mantuvo sus redes operativas internas y separadas de sus redes comerciales corporativas, pero cada vez más las redes OT acceden a redes corporativas y de proveedores externos. Otro ejemplo son las organizaciones que ofrecen aplicaciones, plataformas e infraestructura como servicios en la nube pública: AWS y Azure, por nombrar algunos. Albergan aplicaciones para otras empresas, a las que se accede a través de Internet. Estas nuevas áreas requieren una protección similar contra las amenazas de día cero para minimizar la interrupción del negocio y los riesgos de seguridad. Como resultado,

El producto sandbox de Fortinet se llama FortiSandbox™ e incorpora todas las últimas tecnologías discutidas aquí. Colabora con otros productos de seguridad para promover una defensa común que se puede administrar desde un único panel de vidrio, que Fortinet llama Security Fabric. El servicio de inteligencia de amenazas proporcionado por Fortinet se llama FortiGuard® Labs.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.

Lección 10—Información de seguridad y gestión de eventos

¡Hola! En esta lección, explicaremos qué es la gestión de eventos e información de seguridad (SIEM) y cómo ha evolucionado con el tiempo.

Introducido en 2005, SIEM analiza alertas de seguridad en tiempo real. Fundamentalmente, los SIEM hacen tres cosas:

Uno: Recopile, normalice y almacene eventos de registro y alertas de la red y los dispositivos de seguridad, servidores, bases de datos, aplicaciones y terminales de la organización en una ubicación central segura. SIEM recopila información no solo de dispositivos físicos, sino también de dispositivos virtuales, tanto en las instalaciones como en la nube. Los investigadores habían determinado que iniciar sesión en todos los sistemas para verificar los eventos de registro relevantes era cada vez más imposible. Además, si sus registros no estaban seguros, no tenía garantía de que un atacante no hubiera eliminado las entradas para ocultar sus actividades.

Dos: ejecutar análisis avanzados de los datos, tanto en tiempo real como a través de datos históricos, para identificar posibles incidentes de seguridad que deberían ser investigados por un ser humano. Los incidentes potenciales se priorizan por riesgo, gravedad e impacto. Con el tiempo, estos análisis de seguridad han pasado de emplear reglas simples de correlación cruzada a monitorear anomalías en el comportamiento del usuario, observar indicadores conocidos de compromiso (IoC) y aplicar modelos sofisticados de aprendizaje automático.

Tercero: Acreditar que todos los controles de seguridad a cargo del SIEM están establecidos y son efectivos. Si bien el mantenimiento de la seguridad por sí mismo debería impulsar los requisitos de seguridad y el nivel adecuado de inversión, en realidad, para muchas organizaciones, el principal impulsor para comprar SIEM ha sido el cumplimiento normativo.

Las primeras dos décadas del siglo XXI han visto una avalancha de nuevos requisitos de cumplimiento, tanto legislativos como patrocinados por la industria. Algunos ejemplos son el estándar de la Industria de Tarjetas de Pago (PCI), la Ley Sarbanes-Oxley de 2002, la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) y el Reglamento General de Protección de Datos (GDPR) en 2018. Empresas, hospitales y otras organizaciones ignore el cumplimiento por su cuenta y riesgo, y los infractores pueden incurrir en multas punitivas.

A medida que los ataques cibernéticos se volvieron más sofisticados y sigilosos, las demandas de información sobre un ataque cibernético (sus características, propósito y el alcance de la penetración de la red) se volvieron más urgentes. Otro hecho alarmante fue que los equipos de seguridad muy a menudo no descubrieron las infracciones hasta muchos meses después de que ocurrieron, y luego fueron descubiertas con más frecuencia por un tercero que por la seguridad interna. La seguridad de TI necesitaba una imagen holística de la actividad de la red, y los datos en tiempo real recopilados por SIEM llenaron esta necesidad. En la segunda etapa de desarrollo, los proveedores de SIEM agregaron capacidades de detección de amenazas con inteligencia de amenazas integrada, análisis histórico y en tiempo real, y análisis de comportamiento de usuarios y entidades (UEBA). Y, más recientemente, el aprendizaje automático se ha convertido en parte del conjunto de herramientas de SIEM, y es particularmente necesario cuando se examinan grandes cantidades de datos.

Otro tema que dificultó una mayor aceptación del SIEM por parte de las organizaciones fue el esfuerzo que supuso su instalación, integración y uso. La tecnología era compleja y difícil de sintonizar, era difícil identificar los ataques y exigía un alto nivel de habilidad por parte del usuario para saber lo que estaba buscando. A pesar de todas sus capacidades, SIEM no era una tecnología de configuración y olvido. Esta situación se agravó

por otros dos hechos. Uno, la seguridad de TI adolece de una cantidad insuficiente de profesionales calificados, y dos, el enfoque aislado utilizado en los centros de operaciones de red (NOC) y los centros de operaciones de seguridad (SOC) típicos aumenta la complejidad y provoca una falta de visibilidad de la red. Un entorno compuesto por soluciones multiproveedor de un solo punto con diferentes sistemas operativos, ciclos de parches, protocolos y lógica, funcionaba en contra de la interoperabilidad y la simplificación. El resultado fue una mayor demanda de recursos de TI escasos, una mayor posibilidad de error humano y una menor visibilidad de la seguridad de la red. Entonces, si bien SIEM hizo grandes avances al pasar de una plataforma de información a un centro de inteligencia de amenazas, permaneció paralizado por limitaciones tanto externas como internas.

La escasez sistémica de personal capacitado fue el ímpetu para una mayor automatización y aprendizaje automático en los dispositivos SIEM posteriores. La inteligencia artificial detecta tendencias y patrones en enormes cantidades de datos más rápidamente que incluso el ser humano más inteligente. Además, se gana tiempo y precisión al configurar SIEM para responder y remediar automáticamente. Los desarrollos recientes en SIEM también han integrado NOC y SOC, estableciendo así a SIEM como el centro neurálgico de todas las operaciones de red y seguridad. Entonces, desde un solo panel de vidrio, la seguridad de TI gana visibilidad en toda la red. SIEM simplifica la implementación y la integración a través de un motor de configuración de dispositivos y descubrimiento de activos en tiempo real y de autoaprendizaje. Esta herramienta establece un inventario de dispositivos de red, aplicaciones, usuarios y servicios comerciales. A continuación, crea una topología que muestra cómo se interconecta cada objeto, estableciendo así una línea de base del comportamiento normal de la red. Al determinar la normalidad y con la ayuda del aprendizaje automático, el comportamiento anormal puede alertar a los analistas de un ciberataque, que luego puede detenerse antes de que ocurra una infracción.

En un par de décadas, SIEM ha evolucionado de una plataforma de información a un centro de inteligencia de amenazas, a un centro completamente integrado y automatizado para operaciones de red y seguridad.

El producto SIEM de Fortinet se llama FortiSIEM™ y abarca todas estas características, además de otras.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.

Lección 11: Firewall de aplicaciones web

¡Hola! En esta lección, hablaremos sobre los firewalls de aplicaciones web (WAF) y cómo han evolucionado con el tiempo. ¿Qué es un WAF y en qué se diferencia del firewall perimetral tradicional?

Un WAF es un dispositivo o software que monitorea el tráfico HTTP/HTTPS y puede bloquear el tráfico malicioso hacia y desde una aplicación web. Se diferencia de un cortafuegos de borde tradicional en que apunta al contenido de aplicaciones web específicas y al nivel de la aplicación, mientras que los cortafuegos de borde crean puertas de enlace seguras entre la red de área local y los servidores externos al nivel de la red. Específicamente, al inspeccionar el tráfico HTTP, un WAF puede detener los ataques que se originan en las fallas de seguridad de las aplicaciones web, como la inyección de SQL, las secuencias de comandos entre sitios, la inclusión de archivos y las configuraciones incorrectas de seguridad. Dado que gran parte de nuestro tiempo, tanto en el trabajo como en el hogar, lo dedicamos a interactuar con aplicaciones web y servidores web, el WAF se convierte en un componente vital en nuestro arsenal contra los malos actores y sus esquemas maliciosos en línea.

El antecesor de WAF es el firewall de aplicaciones que se desarrolló por primera vez en la década de 1990. Aunque en gran medida es un cortafuegos basado en la red, podría tener como objetivo algunas aplicaciones o protocolos, como el Protocolo de transferencia de archivos (FTP) y el shell remoto (RSH), que es un programa informático de línea de comandos. El debut de la World Wide Web en 1991 fue el gran estallido del universo de Internet, que se ha estado expandiendo a un ritmo acelerado desde entonces. La misma accesibilidad y apertura de Internet permitía a cualquiera buscar y explorar, pero también permitía que los malos actores lo usaran para sus propios y sórdidos propósitos.

A medida que más personas y organizaciones se convirtieron en víctimas de espionaje, robo y otros delitos, desarrollar una defensa contra los ataques cibernéticos basados en HTTP se convirtió en una prioridad principal. WAF no podía confiar en los métodos de cortafuegos de borde tradicionales que basaban las decisiones en una lista de bloqueo de direcciones de red y bloqueaban ciertos protocolos y números de puerto. Como todas las aplicaciones web usaban HTTP y el puerto 80 o 443, este enfoque no era muy útil.

Veamos un método de ataque común llamado inyección SQL. Imagine que tiene un negocio en línea y los clientes y socios inician sesión en su sitio para comprar productos y servicios. Una página de inicio de sesión típica solicita una identificación de usuario y una contraseña. Una persona, llamémosle John Smith, escribe su ID de usuario, jsmith, y su contraseña. Esta información se verifica en una base de datos back-end. Si la contraseña es verdadera, John Smith entra, pero si la contraseña es falsa, no lo hace. Ahora, un mal actor probablemente no sepa la contraseña de John. Siempre podía adivinar, pero eso podría llevar mucho tiempo. En cambio, para la contraseña, el mal actor escribe "abc123 o 2+2=4". Cuando las credenciales de John se envían a la base de datos para su verificación, es probable que la contraseña "abc123" sea falsa; sin embargo, la expresión 2+2=4 es verdadera. Debido a esta falla, el mal actor pudo ingresar a algunos sitios.

Con la creciente popularidad de Internet, pronto la gran cantidad de aplicaciones web y su creciente complejidad hicieron obsoleto el enfoque basado en firmas. Además, la cantidad de falsos positivos (alertas de ataques que en realidad eran conexiones legítimas) creció en proporciones que superaban la capacidad de los equipos de seguridad de TI. En la próxima generación, los WAF se volvieron más inteligentes: había un elemento de aprendizaje por parte del firewall. El WAF aprendería el comportamiento de la aplicación para crear una línea de base que podría usar para evaluar si los intentos de acceder a las aplicaciones fueron normales o irregulares, y

por lo tanto sospechoso. También introdujo el monitoreo de sesiones y la heurística, lo que permitió que el firewall detectara variantes de firmas conocidas. Este fue un paso adelante, pero debido a que el aprendizaje de la aplicación fue supervisado por la seguridad de TI, la defensa no pudo mantenerse al día con el número cada vez mayor de mutaciones de métodos existentes o nuevas vulnerabilidades. Además, no había defensa contra las vulnerabilidades de día cero, que explotaban una debilidad desconocida en el código de una aplicación.

El giro lógico en el desarrollo de WAF fue el aprendizaje automático sin supervisión humana. Ahora, el análisis de comportamiento podría realizarse a la velocidad de una máquina y podría adaptarse a los atributos siempre cambiantes de la amenaza. Se aumentaron otras funciones de seguridad en el cortafuegos. Entre estos activos se encontraban la defensa contra la denegación de servicio (DDoS), la reputación de IP, el antivirus y la prevención de pérdida de datos (DLP). El cortafuegos podría detener cualquier acción que violara el comportamiento HTTP aceptable. Podría identificar al usuario y correlacionar la acción que estaba intentando realizar con sus permisos, y detener cualquier acción que fuera más allá del alcance de su función. El WAF también se diseñó para compartir información y colaborar con otros dispositivos de seguridad en la red, como otros firewalls y sandboxes. Esto sirvió para integrar el cortafuegos en una defensa colectiva entrelazada en lugar de trabajar de forma independiente. Y el sandboxing permitió que el material sospechoso se probara de manera segura y aislado de la red. Los ataques de día cero podrían exponerse y ponerse en cuarentena en estos entornos de espacio aislado, y sus firmas podrían compartirse con otros dispositivos en la red. Además, estos nuevos descubrimientos podrían cargarse en un centro de inteligencia de amenazas en Internet, donde podrían comunicarse a otras redes.

Fortinet tiene un WAF llamado FortiWeb™. FortiWeb™ se puede integrar con FortiGate® y FortiSandbox™. FortiGuard® Labs es el centro de inteligencia de amenazas de Fortinet, que puede proporcionar actualizaciones vitales para FortiWeb™ y otros productos de Fortinet Security Fabric.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.

Lección 12: Gateway de correo electrónico seguro

¡Hola! En esta lección, explicaremos qué es una pasarela de correo electrónico segura y cómo ha evolucionado.

El correo electrónico fue una de las primeras actividades que la gente hizo cuando el mundo se puso en línea en la década de 1990. Se necesitaba muy poco ancho de banda porque la tecnología permitía muy poco. ¡También fue fácil, rápido y ni siquiera costó un sello postal! Era tan fácil y económico que se convirtió en un medio para enviar un mensaje a muchas personas a un costo mínimo o gratuito.

Algunos de esos envíos masivos provenían de negocios legítimos y eran equivalentes a volantes publicitarios enviados por correo, pero otros envíos masivos eran enviados por personajes más nefastos. Este fue el comienzo del spam: el acto de enviar mensajes irrelevantes y no solicitados en Internet a una gran cantidad de destinatarios.

Las personas podían enviar y recibir mensajes con poca verificación o responsabilidad. Por lo tanto, ofrecieron el anonimato. Inicialmente, la gente veía el spam más como una molestia que como una amenaza. Pero en 1996, America Online (AOL) acuñó el término phishing para describir la práctica fraudulenta de enviar correos electrónicos que pretenden ser de una fuente confiable, para inducir a las personas a revelar información personal.

Por ejemplo, algunos de ustedes pueden haber conocido al Príncipe Salomón de Abadodo, u otro personaje astuto, que quería compartir su riqueza con ustedes. Otros malhechores registraron nombres de dominio que se parecían sorprendentemente a los nombres de empresas u organizaciones legítimas y se hicieron pasar por esa empresa en un correo electrónico, instándolo a hacer clic en un enlace o un archivo adjunto que contenía malware.

La técnica de phishing se basó en la ingenuidad humana, el descuido o la distracción para que funcionara. Una de las primeras respuestas de las empresas fue educar a los empleados sobre las tácticas de phishing. Sin embargo, si bien la educación puede haber reducido las vulnerabilidades de phishing, no eliminó la amenaza. Había que hacer algo a nivel del servidor de correo y del proveedor de servicios de Internet (ISP). En respuesta, las empresas instalaron filtros de spam en los servidores de correo para detener los correos electrónicos de spam y phishing.

Los filtros de spam se basan en la identificación de palabras o patrones específicos en los encabezados o cuerpos de los mensajes. Para usar un ejemplo simple, la palabra efectivo es común en el correo electrónico no deseado. Si un profesional de TI agregara la palabra efectivo al filtro de spam en el servidor de correo de su empresa, el filtro eliminaría cualquier correo electrónico que contuviera esa palabra.

Los ISP también implementaron filtros de spam. Además del filtrado, los ISP recurrieron al fortalecimiento de los métodos de autenticación. A fines de la primera década del siglo XXI, los ISP comenzaron a implementar el Marco de políticas de remitente (SPF), que tomó forma lentamente durante esa década, pero no se propuso como estándar hasta 2014.

SPF es un método de autenticación de correo electrónico que detecta direcciones de remitentes y correos electrónicos falsos.

Sin embargo, por cada medida defensiva implementada por negocios, organizaciones e ISP legítimos, los malos actores introdujeron una contramedida que eludió la última defensa.

Volviendo a nuestro ejemplo simple, los spammers podrían pasar por alto fácilmente nuestra palabra filtrada, efectivo, traduciéndola como c@sh o alguna otra variante. Y aunque los filtros se volvieron más sofisticados para detectar patrones de spam, eran demasiado estáticos y fáciles de burlar.

El spam y el phishing son demasiado lucrativos para que los malhechores se den por vencidos fácilmente. De hecho, el número de ataques de phishing ha crecido enormemente desde principios de siglo. En 2004, se registraron 176 ataques de phishing únicos. En 2012, este número aumentó a 28.000. Y no es de extrañar; el phishing era lucrativo. Entre dinero perdido y daños, los ataques causaron una pérdida de $500 millones a empresas e individuos. Más recientemente, durante el primer trimestre de 2020, el Grupo de trabajo antiphishing (APWG) registró 165 772 sitios de phishing detectados.

Se necesitaba una mejor defensa. Las puertas de enlace seguras de correo electrónico (SEG) surgieron para proporcionar una defensa más rigurosa. Además del filtro de spam, los SEG agregaron escáneres antivirus, emulación de amenazas y sandboxing para detectar archivos adjuntos y enlaces maliciosos en tiempo real. Incluso si la educación de los empleados y el filtro de spam fallaran, una de estas otras herramientas podría detectar y neutralizar la amenaza. Sin embargo, la cantidad de falsos positivos y el gran volumen de ataques abrumaron a los equipos de seguridad, que se empantanaron en la remediación manual.

Los SEG continúan evolucionando a medida que evolucionan las amenazas.

Hoy en día, los SEG incorporan una mayor automatización y aprendizaje automático, lo que alivia las demandas impuestas a los centros de operaciones de seguridad (SOC). La prevención de pérdida de datos (DLP) también está disponible para detectar y detener la salida de datos confidenciales.

En algunos casos, un SEG se integra con otros dispositivos de seguridad de red, como firewalls de borde y segmentación. Estos dispositivos forman colectivamente un tejido integrado de seguridad que los profesionales de la seguridad pueden administrar de forma centralizada desde un único panel de vidrio y actualizarse continuamente utilizando inteligencia de amenazas, a medida que se conocen nuevos métodos y contagios.

Fortinet tiene un SEG, llamado FortiMail®. FortiMail® incluye todas las características discutidas aquí, además se integra con firewalls y soluciones de sandboxing. Puede administrar de forma centralizada todos estos dispositivos con FortiManager® y actualizar su inteligencia de amenazas con FortiGuard® Labs, que es el centro de investigación e inteligencia de amenazas global de Fortinet.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.

Lección 13—Filtro web

¡Hola! En esta lección, veremos el filtrado web y el desarrollo de esta tecnología.

Durante los primeros días de Internet, había pocas o ninguna restricción sobre los sitios web que podía visitar. Desafortunadamente, algunos de esos sitios tenían malware que podía infectar la computadora de navegación. O, a veces, un sitio web contenía contenido que otros objetaban. Lo que constituye contenido objetable puede ser controvertido, pero estas dos razones (seguridad y contenido objetable) dieron el impulso para el desarrollo de la tecnología de filtrado web.

Entonces, ¿qué es un filtro web? Es una aplicación que examina las páginas web entrantes para determinar si parte o todo el contenido debe bloquearse. El filtro web toma estas decisiones en función de las reglas establecidas por la organización o la persona que instaló la aplicación. Hay una interfaz correspondiente que le permite configurar las reglas y determinar qué se bloquea y qué pasa. Un filtro web también puede establecer diferentes reglas para diferentes tipos de usuarios. Por ejemplo, en casa un padre puede querer hacer cumplir reglas más estrictas para los niños que para los adolescentes y adultos.

En los Estados Unidos, las bibliotecas fueron las primeras en instalar filtros web en sus computadoras de acceso público en respuesta a la presión de la comunidad. El gobierno federal aprobó la Ley de protección de Internet para niños (CIPA) en 2004, que exige que todas las computadoras de una biblioteca pública tengan filtros web, si esa biblioteca acepta fondos federales para computadoras con acceso a Internet. Estas medidas fueron recibidas con una recepción mixta. A medida que el filtrado web se extendió de las bibliotecas a las escuelas, algunos argumentaron que censurar la información, sin importar cuán ofensiva fuera, contradecía la misión de las bibliotecas y la educación. Es más, a veces los filtros no eran lo suficientemente sofisticados para distinguir entre el arte y una fotografía lasciva, o los filtros bloqueaban la literatura por una palabrota.

Si bien la motivación inicial fue proteger a los niños, después de que se desarrolló la tecnología, se hizo evidente su utilidad para otros fines. La información puede ser censurada por motivos religiosos, políticos o ideológicos. Además, las fechorías anteriores de un gobierno podrían borrarse del registro digital. Aún así, en el otro lado del libro mayor, la navegación se hizo más segura mediante el desarrollo de filtros que podían bloquear adware, spam, virus y spyware. Hoy en día, el filtrado web constituye la primera línea de defensa contra los ataques basados en la web. Además de las estaciones de trabajo de los clientes, los servidores web y los ISP, se agregaron filtros web a otros dispositivos de red, como firewalls, servidores proxy, tecnología sandbox y puntos de acceso inalámbrico.

¿Cómo funciona un filtro web? Un filtro web puede consultar una base de datos de URL que enumera sitios web y dominios que se sabe que albergan malware, phishing y otras herramientas dañinas. Con más de mil millones de sitios web activos en Internet, esta puede ser una tarea onerosa. Las URL que se encuentran en esta lista traviesa también se conocen como lista de denegación. También puede haber una lista de permitidos, que es una lista autorizada de URL. Otro método que se puede utilizar es un filtro que busca una palabra clave o un contenido predefinido. Como se señaló anteriormente, el problema con este método es la cantidad de falsos positivos; es decir, puede bloquear inadvertidamente contenido legítimo, como el art. El aprendizaje automático puede, con el tiempo, superar esta deficiencia. Otros tipos de filtros web, como el motor de búsqueda de Google, utilizan el aprendizaje automático para ayudarlo a encontrar lo que está buscando. Al igual que otros dispositivos de seguridad de red,

Fortinet ha integrado filtros web en varios de sus productos: por ejemplo, FortiClient®, FortiGate® y, para puntos de acceso inalámbrico, FortiAP™.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.

Lección 14—SASE

¡Hola! En esta lección, le presentaremos Secure Access Service Edge SASE y le explicaremos cómo ha evolucionado.

SASE es una tecnología que combina la red como servicio con capacidades de seguridad como servicio. SASE se entrega a través de la nube como un modelo de consumo como servicio, para respaldar el acceso seguro para las redes empresariales híbridas y distribuidas de hoy.

La seguridad de la red es una prioridad principal para la mayoría de las organizaciones, sin embargo, han surgido nuevos desafíos. La innovación digital rápida y disruptiva ha traído consigo:

- un borde delgado en expansión definido por ubicaciones de sucursales pequeñas que están conectadas a la red central
- una cantidad creciente de usuarios fuera de la red que acceden al centro de datos central
- una experiencia de usuario desafiante para usuarios fuera de la red
- una superficie de ataque en expansión
- Requisitos de cumplimiento multinivel y
- ciberamenazas cada vez más sofisticadas

A medida que los entornos de trabajo han evolucionado, también lo han hecho el comportamiento de los usuarios y los requisitos de protección de terminales. Los usuarios ya no acceden a la información desde una estación dedicada dentro de un perímetro de red predefinido confinado a una oficina corporativa. En cambio, los usuarios acceden a la información desde una variedad de ubicaciones, como en el hogar, en el aire y desde los hoteles. También acceden a esa información desde diferentes dispositivos, como estaciones de trabajo de escritorio, computadoras portátiles, tabletas y dispositivos móviles. A esta complejidad de la red se suma el surgimiento de Bring-Your-Own-Device, donde los usuarios acceden a los sistemas empresariales a través de dispositivos personales que no forman parte de la infraestructura empresarial.

Las organizaciones de hoy requieren que sus usuarios tengan acceso seguro inmediato y continuo a la red y los recursos y datos basados en la nube, incluidas las aplicaciones críticas para el negocio, independientemente de la ubicación, en cualquier dispositivo y en cualquier momento. Las organizaciones deben proporcionar este acceso de una manera escalable y elástica que integre sitios de red de borde delgado y usuarios remotos en la infraestructura central, y que favorezca un modelo operativo ajustado como servicio.

Encontrar soluciones que cumplan con estos requisitos es un desafío,

Las razones de esto son claras.

Si bien las redes han evolucionado para admitir los flujos de trabajo de usuarios y puntos finales remotos, muchas soluciones de seguridad de red obsoletas siguen siendo inflexibles y no se extienden más allá del centro de datos para cubrir el perímetro de red en constante expansión y, por lo tanto, la superficie de ataque. Con la llegada de nuevas redes de borde delgado, este desafío se ve exacerbado.

En segundo lugar, estas soluciones para redes convergentes y supervisión de seguridad requieren que todo el tráfico, ya sea que provenga de ubicaciones de borde delgado o usuarios fuera de la red, pase por el centro de datos central para su inspección.
Esto resulta en:

-Alto costo

- Complejidad
- Exposición al riesgo elevado
- Latencia y una experiencia de usuario deficiente al acceder a aplicaciones y datos basados en múltiples nubes

Por último, el entorno de red de varios bordes de la actualidad ha puesto de manifiesto las limitaciones de las soluciones solo de VPN, que no pueden admitir la seguridad, la detección de amenazas y la aplicación de políticas de acceso a la red de confianza cero presentes en la red corporativa local. Las soluciones solo de VPN no pueden escalar para admitir la creciente cantidad de usuarios y dispositivos, lo que genera una seguridad inconsistente en todos los perímetros.

Se requiere una nueva solución escalable, elástica y convergente para lograr un acceso seguro y confiable a la red para usuarios y terminales. Uno que aborda la seguridad de muchas organizaciones híbridas, definida por sistemas y usuarios repartidos por la red corporativa y remota. Esa solución es SASE.

Una solución SASE proporciona capacidades de red y seguridad integradas, que incluyen:

- Peering, que permite la conexión a la red y el intercambio de tráfico directamente a través de Internet sin tener que pagar a un tercero.
- Un firewall NGFW de próxima generación o un firewall como servicio FWaaS basado en la nube, con capacidades de seguridad que incluyen el sistema de prevención de intrusiones IPS, antimalware, inspección SSL y Sandbox.

- Una puerta de enlace web segura para proteger a los usuarios y dispositivos de las amenazas de seguridad en línea mediante el filtrado de malware y la aplicación de políticas de cumplimiento y seguridad de Internet.
- Zero Trust Network Access ZTNA, que garantiza que no se confíe automáticamente en ningún usuario o dispositivo. Cada intento de acceder a un sistema, ya sea desde el interior o desde el exterior, se cuestiona y verifica antes de conceder el acceso. Consta de varias tecnologías, incluida la autenticación multifactor MFA, NAC de control de acceso a la red seguro y aplicación de políticas de acceso. Data Loss Prevention DLP evita
- que los usuarios finales trasladen información clave fuera de la red. Estos sistemas informan la inspección del contenido de las aplicaciones de mensajería y correo electrónico que operan en la red.

- Sistema de nombres de dominio DNS, que sirve como la guía telefónica de Internet y proporciona a SASE capacidades de detección de amenazas para analizar y evaluar dominios de riesgo.

Estos servicios ofrecen:

- Rutas optimizadas para todos los usuarios a todas las nubes para mejorar el rendimiento y la agilidad
- Seguridad certificada de nivel empresarial para fuerzas de trabajo móviles,
- Seguridad consistente para todos los bordes, y
- Gestión consolidada de seguridad y operaciones de red.

Aunque está clasificado como basado en la nube, existen casos de uso comunes de SASE, que pueden requerir una combinación de soluciones físicas y basadas en la nube. Para que SASE se implemente de manera efectiva en este escenario, la conectividad segura con controles de acceso a la red debe extenderse desde la infraestructura WAN física hasta el borde de la nube. Por ejemplo, para implementar el acceso a SASE en las sucursales, es posible que SASE dependa de dispositivos de red físicos, como extensores inalámbricos (LTE y 5G) y cableados (Ethernet) o puntos de acceso Wi-Fi.

El objetivo de SASE es respaldar las necesidades de acceso seguro y dinámico de las organizaciones actuales. El servicio SASE adecuado permite a las organizaciones ampliar la seguridad y las redes de nivel empresarial a:

- El borde de la nube, donde los usuarios remotos fuera de la red acceden a la red, y el
- borde delgado, como las sucursales pequeñas

La solución SASE basada en la nube de Fortinet se llama FortiSASE™.

Gracias por su tiempo, y por favor recuerde tomar el cuestionario que sigue a esta lección.