Enfrentando a la Amenaza del Ransomware

Una Guía Sobre Amenazas y Recomendaciones para Escuelas y Universidades

Introducción

Los ataques de ransomware y de malware han estado llamando poderosamente la atención de los medios. Los gobiernos y organizaciones locales de Escocia, Estados Unidos y Japón han sido víctimas de estos ataques, y al menos en uno de los casos se reportó una interrupción de alto perfil que cobró gran relevancia. Estos ataques ahora se han extendido a los sectores público y privado.

Si bien los detalles exactos de estos ataques aún son escasos, destacan una vez más el impacto operativo que un ataque de malware puede tener en las organizaciones. Y los titulares refuerzan el hecho de que los métodos de seguridad actuales no están logrando brindar los niveles de protección y resiliencia necesarios, y que es ineludible hacer una mayor inversión para identificar y cerrar las brechas que permiten el éxito de los ataques.

En este documento encontrará los principios rectores que sustentan una estrategia de seguridad, así como cinco recomendaciones específicas para su implementación. No es posible ofrecer garantías de ningún tipo, pero estamos convencidos de que adoptar estos principios y seguir las recomendaciones ayudará a las instituciones a evitar los ataques potenciales y, en caso de que ocurrieran, poder identificarlos y mitigarlos efectivamente.

Tres Principios Rectores

Se puede encontrar un gran número de guías y de marcos de seguridad reconocidos para ayudar a las organizaciones a mejorar su seguridad. El Cybersecurity Framework, dado a conocer por el National Institute of Standards and Technology (NIST), el resumen de los “10 Pasos Hacia la Seguridad Cibernética” del Communications Electronics Security Group (CESG), y los 20 principales controles de seguridad críticos del SANS Institute son sólo tres ejemplos notables de los recursos que se encuentran disponibles.

Al combinar los consejos contenidos en este documento y nuestra propia experiencia práctica, creamos los siguientes principios para sustentar la estrategia de seguridad de una institución.

1 Sensibilizar a los Usuarios

El eslabón más débil de la postura de seguridad de una organización es su personal: la comunidad de usuarios. Y no es que el personal se comporte de una manera maliciosa siempre, sino que sencillamente son humanos y pueden ser engañados por un correo electrónico de phishing bien diseñado.

Por lo tanto, es necesario que se le recuerde regularmente a los usuarios la necesidad de ser cautos cuando abren los archivos adjuntos que vienen con sus correos electrónicos o cuando pulsan los enlaces contenidos en ellos. Se requiere de una educación constante para garantizar que la seguridad ocupará siempre en lugar preponderante en la mente del personal.

2 Asumir que ya se Han Registrado las Brechas

De que una institución sufrirá una brecha de seguridad no hay duda; por tanto la pregunta no es "si" sino "cuándo".

En nuestra experiencia, muchas organizaciones ya han sido víctimas de un ataque y sencillamente aún no lo saben. Para solucionar esto, las organizaciones deben hacerse la siguiente pregunta: Si supiera que va a ser atacadas, ¿implementarían la seguridad de manera distinta? Al ver a la seguridad desde esta perspectiva, las instituciones pueden comenzar a entender cómo podría propagarse un ataque después de que se registrara el compromiso inicial y, lo más importante, cómo puede detectarse el ataque cuando ya está dentro del perímetro de la red.

3 Dar prioridad a la Higiene Cibernética

A medida que la industria se concentra en las amenazas sofisticadas de ransomware y de malware, es fácil pasar por alto la importancia de los controles de seguridad fundamentales, como es la aplicación regular de parches al software y la rigurosa gestión de contraseñas.

De acuerdo con el Reporte de Investigaciones sobre Brechas de Datos 2015 de Verizon, el 99.9 por ciento de los ataques exitosos aprovechó las vulnerabilidades que se habían publicado hacía más de un año en el sitio web de CVE (Common Vulnerabilities and Exposures).

Por lo tanto, las organizaciones deben adoptar un enfoque efectivo e integrado hacia la seguridad.

Cisco y nuestros socios pueden explicar el valor de una estrategia digital, ayudarle a desarrollar la suya y, por supuesto, ayudar a ejecutarla. Por favor, consulte la sección de este documento donde se explica cómo podemos ayudarle. Esperamos tener la oportunidad de hacerlo. Para obtener más información, o programar una visita a Cisco para ver en acción nuestra tecnología digital, por favor póngase en contacto con su gerente de cuenta local de Cisco.

Protección Durante los Ataques

Muchas de las estrategias de seguridad recomendadas se enfocan totalmente en el uso de tecnologías más bien defensivas para bloquear las amenazas antes de que puedan provocar daños.

Incluso si se adopta este enfoque, el malware puede aún traspasar las defensas. Entonces, si no se realiza un monitoreo constante para detectar una brecha y no se segmenta la red para evitar que una amenaza se propague, un mayor número de usuarios estaría en riesgo.

La estrategia de seguridad de Cisco se fundamenta en un acercamiento arquitectónico que protege y remedia durante el ciclo completo, esto es antes, durante y después de un ataque. Si las tecnologías defensivas no logran bloquear una amenaza, se despliega entonces una capacidad adicional dentro de la red para identificar y contener rápidamente la actividad maliciosa.

La tecnología de seguridad de Cisco® abarca cada una de estas tres etapas de un ataque. Ha demostrado ser capaz de ayudar a proteger contra las amenazas del ransomware y el malware como las que se han reportado recientemente.

Antes del ataque

El vector de ataque inicial que utiliza el ransomware y el malware es frecuentemente el correo electrónico. Los correos electrónicos de phishing pueden no ser sofisticados o estr altamente dirigidos, pero pueden ser lo suficientemente convincentes para hacer que un usuario desprevenido pulse en un vínculo o abrir un archivo adjunto.

Bloquear este tipo de amenaza requiere echar mano de varios controles. Una solución de seguridad debe ver cómo están construidos los correos electrónicos entrantes, determinar quién los está enviando e inspeccionar su contenido (incluyendo los URLs que pudieran incluir para determinar si se enlazan a sitios maliciosos conocidos).

El Cisco Email Security Appliance es capaz de aplicar estos múltiples controles. Es ideal para mitigar las amenazas potenciales de los correos electrónicos cuando intentan entrar a la red de una institución.

La operación del Email Security Appliance apoyada por la abundancia de datos y la analítica de datos del equipo de inteligencia de amenazas Cisco Talos. Los miembros de este equipo utilizan una vasta capacidad de inteligencia de seguridad basada en la Web, que observa y analiza casi el 30 por ciento del tráfico del correo electrónico del mundo. Desde esta abundancia de datos, se puede detectar las nuevas amenazas e integrar sus conocimientos en los productos de seguridad de Cisco.

Durante del ataque

Para afianzarse, el ransomware y el malware a menudo utilizarán un programa tipo dropper. Estos programas recuperan un ejecutable malicioso y lo instalan en la máquina de la víctima.

Si el correo electrónico es el vector de ataque, el dropper será parte del archivo adjunto que una víctima se sentirá tentado a abrir. Cuando se activa, el dropper establece una conexión para recuperar el ejecutable del malware. Esta opción brinda la oportunidad de bloquear la infección.

Los ejecutables del malware muy a menudo se recuperan de sitios con la peor reputación. La solución Cisco OpenDNS Umbrella utiliza técnicas de DNS para evitar la recuperación de los ejecutables maliciosos a través de algún puerto o protocolo. Simplemente bloquea las respuestas del DNS asociadas con los dominios maliciosos. La inteligencia detrás de la decisión de bloquear las respuestas del DNS viene, como lo hace con el Email Security Appliance, de la recopilación y análisis de más de 80 mil millones de consultas DNS al día. La solución OpenDNS Umbrella utiliza la minería de datos y técnicas avanzadas de clasificación. Puede identificar y bloquear rápidamente los dominios con amenazas nuevas y emergentes.

Después del ataque

Al usar la red como un sensor, usted tiene visibilidad completa de la actividad de la red mediante el monitoreo del comportamiento NetFlow. Cisco NetFlow captura los metadatos de cada conversación que se realiza en la red: quién está hablando con quien, a través de qué protocolo, y por cuánto tiempo. Cuando se suma y analiza, esta información puede brindar conocimientos de lo que es el comportamiento normal. También ayuda al personal de TI a identificar patrones de actividad cuestionables, como la propagación de malware por la red, lo que de otro modo pasaría inadvertido.

Usar así a NetFlow convierte a toda la red en un sensor de seguridad. Usted recibe conocimientos que simplemente no podría ser posible con los dispositivos de seguridad tradicionales implementados en ubicaciones específicas. NetFlow tiene el apoyo de una amplia gama de switches estándar Cisco Catalyst® y Cisco Nexus®, así como del portafolio de ruteadores de Cisco.

Una arquitectura complementaria, la red como un ejecutor, utiliza la tecnología Cisco TrustSec® y el Cisco Identity Services Engine (ISE) para ofrecer segmentación de la red definida por software. Las etiquetas de grupos de seguridad (SGTs) Cisco TrustSec aplican el control de acceso por roles e independiente de las topologías. La segmentación de la red puede implementarse mucho más fácilmente que depender de direcciones IP o de la segmentación basada en VLAN, además de que puede automatizarse.

Cuando la red se utiliza como un ejecutor, las SGTs responden a las amenazas de forma dinámica. Por ejemplo, un usuario al conectarse a la red se le asigna una etiqueta asociada con su rol (por ejemplo, finanzas). La etiqueta se utiliza para aplicar las políticas de acceso que se han acordado. El usuario puede acceder solamente a aquellos servicios disponibles para los miembros del departamento de finanzas. Si se infecta el dispositivo de ese usuario con malware y comienza a mostrar un comportamiento cuestionable en la red (que la red reporta como si fuera un sensor), la etiqueta del usuario puede cambiarse dinámicamente a una etiqueta “en cuarentena”. Las políticas de control de acceso podrían ya estar predefinidas dentro de la red para limitar el acceso a esos dispositivos que contengan la etiqueta “en cuarentena”. El ataque potencial de malware se contendrá rápidamente sin ninguna intervención administrativa manual.

Resumen y Recomendaciones:

Una estrategia de seguridad exitosa requiere de una institución para dar prioridad a varias acciones.

Lo primero y más importante, los aspectos básicos que deben cuidarse son la educación y sensibilización del usuario, y la higiene cibernética a través de la gestión de parches y de la protección de contraseñas. Pero en segundo lugar, pero no por eso menos importante, es adoptar un acercamiento arquitectónico hacia la seguridad que abarque al ciclo completo del ataque.

Las organizaciones pueden comenzar a adoptar dicho método mediante la implementación de las siguientes cinco recomendaciones.

1. Crear una cultura de seguridad.

La educación de los usuarios es un principio de seguridad importante y es fundamental para desarrollar una cultura de seguridad robusta. Sin embargo, la cultura de la seguridad va más allá de la capacitación de rutina sobre el tema. Debe estar inmersa en la vida diaria de los usuarios. Como todas las cosas en el mundo de la seguridad, debe probarse y, en el contexto del ransomware y el malware, las instituciones deben realizar campañas de phishing de prueba para medir la efectividad de la educación que han recibido los usuarios. La cultura de seguridad de Cisco se ha desarrollado a lo largo de muchos años. Ahora se fundamenta en un programa maduro y estructurado que opera en todo el negocio.

2. Considere a la seguridad como una arquitectura.

Con mucha frecuencia, la seguridad se aplica a un nivel de proyecto o en respuesta a un incidente de seguridad. Este enfoque puede llevar al desarrollo de una multitud de tecnologías con integración limitada, lo que se deriva en una falta de visibilidad y protección. Lo que recomendamos a las organizaciones es adoptar un acercamiento arquitectónico a la seguridad. Deben considerar cómo deben aplicarse los controles de seguridad en el entorno y cómo pueden trabajar juntos para mitigar el riesgo. Este acercamiento asegura una capacidad de seguridad más integrada y efectiva que pueda alinearse mejor para gestionar el riesgo y el impacto para el negocio.

3. Revise la segmentación de la red.

La mayoría de las redes siguen construyéndose con un modelo de seguridad plano. Aunque la segmentación puede implementarse por conveniencia operativa, a menudo sólo existe la aplicación limitada de las políticas de seguridad entre los segmentos. La falta de aplicación de políticas entre los segmentos abre la puerta para que los ataques que violan la tecnología perimetral defensiva aprovechen fácilmente la incursión inicial y se propaguen por toda la red. Las organizaciones deben revisar su segmentación de red actual y explorar oportunidades de implementar políticas de seguridad robustas entre los segmentos.

4.Mejore la visibilidad del tráfico de la red.

Dentro del perímetro de la red, pocas organizaciones tienen un conocimiento claro de los patrones de flujo que sigue el tráfico. Al capturar los datos de NetFlow, las organizaciones pueden tener información valiosa del comportamiento normal de la red. Pueden identificarse rápidamente las amenazas y contenerlas.

5. Desarrolle una capacidad de operaciones de seguridad.

Es costoso implementar y operar un Centro de Operaciones de Seguridad de tiempo completo, pero es esencial para identificar y contener rápidamente los incidentes. Existe una tendencia importante hacia el uso de proveedores especializados para contar con una capacidad de operaciones de seguridad totalmente administrada. Las organizaciones deben auditar su capacidad operativa actual y explorar si debe complementarse con los recursos y la experiencia de terceros.

¿No está seguro por dónde comenzar? Los servicios de seguridad de Cisco brindan acceso a la red y a los expertos en seguridad, así como monitoreo continuo y soporte administrativo.

Autores

Este documento fue escrito por los equipos de Educación y Seguridad de Cisco Reino Unido. Los equipos cuentan con más de 20 años de experiencia trabajando con instituciones educativas en sus programas tecnológicos. Su objetivo es desarrollar entornos tecnológicos seguros donde se desarrollen negocios eficientes y rentables; que promuevan la enseñanza, el aprendizaje y la investigación de alta calidad; y que puedan brindar las bases para que los campus digitales apoyen el trayecto de los estudiantes.

Oficinas Centrales en América
Cisco Systems, Inc.
San Jose, CA

Oficinas Centrales en Asia Pacífico
Cisco Systems (USA) Pte. Ltd.
Singapur

Oficinas Centerales en Europa
Cisco Systems International BV Amsterdam
Holanda

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números telefónicos y fax están listados en el sitio de Cisco en www.cisco.com/go/offices.