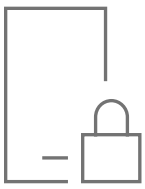
Microsoft Security

Mantenerse al día con un panorama cambiante de ciberseguridad

Contenido

Introducción

Sobre todo, los CISO deben enfrentarse a un panorama de ciberseguridad de mayor complejidad.



El papel de un CISO nunca ha sido fácil, pero parece que cada día se vuelve más desafiante. La descripción del trabajo es bastante completa:

- ✓ proteger los activos digitales de la organización
- ✓ promover buenas prácticas de seguridad en todo el negocio
- ✓ comprender las necesidades y los riesgos de las unidades de negocio individuales
- ✓ interactuar periódicamente con los ejecutivos de alta dirección y la junta directiva para ayudarles a administrar de forma estratégica el riesgo

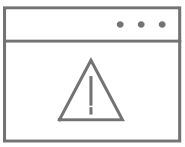
Sobre todo, los CISO deben enfrentarse a un panorama de ciberseguridad de mayor complejidad. Los días de proteger los activos detrás de un perímetro fortificado terminaron hace mucho tiempo. Los datos residen en la nube, en los puntos de conexión y en toda la cadena de suministro, lo que amplía en gran medida la superficie de ataque.

Y ahora, los CISO deben ocuparse de las nuevas realidades del trabajo creadas por una pandemia global. Un mundo en el que repentinamente se les exige a todos los empleados que trabajen desde casa aumenta significativamente la seguridad de los dispositivos de punto de conexión, los datos y la infraestructura de red.

Por lo tanto, es fundamental para los CISO mantenerse al día con las amenazas emergentes y, lo más importante, cómo las estrategias de protección contra amenazas está evolucionando para ayudar a mantener a las organizaciones seguras.

Amenazas emergentes

Muchos bandidos en línea se sienten atraídos por una nueva generación de técnicas de ataque "sin malware".



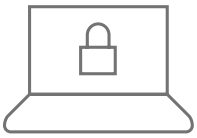
Al igual que la distancia más corta entre dos puntos es una línea recta, los delincuentes cibernéticos harán el menor esfuerzo necesario para comprometer los sistemas y filtrar los datos. Por lo tanto, no debería sorprender a nadie que muchos bandidos en línea se sientan atraídos por una nueva generación de técnicas de ataque "sin malware". ¿Por qué escribir malware cuando se puede penetrar en un sistema con código ejecutado a partir de memoria o credenciales comprometidas?

"Se me ha informado de más de una infracción donde el atacante usó enfoques libres de malware, como adivinar la contraseña de un escritorio remoto para primero obtener acceso al entorno", dijo Chris Clements, vicepresidente de Arquitectura de soluciones de Cerberus Sentinel, una consultoría de ciberseguridad. "Luego, los atacantes utilizaron las funciones integradas del sistema para escalar sus privilegios y darles un control total sobre todos los sistemas y datos de la red".

Estos ataques pueden ser devastadores", agregó Clements, **"ya que los atacantes están imitando las mismas actividades que realizan los administradores de TI legítimos, por lo que el antivirus no está diseñado para detenerlas".**

Técnicas avanzadas de suplantación de identidad (phishing)

La suplantación de identidad (phishing) sigue siendo una amenaza popular, con actores de amenazas que adoptan tácticas avanzadas para evitar las defensas de red tradicionales.



La suplantación de identidad (phishing) sigue siendo una amenaza popular, con actores de amenazas que adoptan tácticas avanzadas para evitar las defensas de red tradicionales. Se esconden detrás de la ofuscación de paquetes, el cifrado, las cargas útiles de varias fases y el DNS de flujo rápido, donde las redes de bots ocultan sitios de entrega de suplantación de identidad (phishing) detrás de una red de hosts comprometidos que actúan como proxies.

Los ataques de ransomware también están evolucionando. Los operadores más sofisticados penetrarán un objetivo y, a continuación, buscarán un socio que pueda implementar su ransomware en el objetivo de forma personalizada. Por ejemplo, se sabe que los desarrolladores del ransomware LockerGoga, que necesita derechos administrativos para ejecutarse, analizan minuciosamente las defensas de un objetivo y que ni siquiera se molestan en ocultar su mala aplicación porque saben que esas defensas no lo detectarán.

Los atacantes también usan herramientas ya instaladas en un sistema, como PowerShell, para propagarse en una red y ampliar la infestación. Estos intrusos "viven de la tierra" una vez que penetran en un sistema, utilizando herramientas y utilidades disponibles públicamente para lograr sus fines. Estos ataques son difíciles de detectar porque los defensores parecen ser una actividad de red normal.

Aumento de las vulnerabilidades remotas

De acuerdo con KnowBe4, un proveedor de concienciación sobre seguridad, los ataques por correo electrónico relacionados con el coronavirus alcanzaron un 600 % durante el trimestre que finalizó el 30 de marzo de 2020.

A medida que más empleados se ven obligados a trabajar desde casa debido a la epidemia de COVID-19, los trabajadores remotos plantean otra mayor vulnerabilidad a las organizaciones. La rapidez del cambio al trabajo remoto para muchas organizaciones provocó que muchos equipos de seguridad tuviesen que ponerse al día para garantizar que las directivas y protecciones estuvieran vigentes. No es de sorprender que los malos actores también aprovechen la pandemia a través de la ingeniería social. De acuerdo con KnowBe4, un proveedor de concienciación sobre seguridad, los ataques por correo electrónico relacionados con el coronavirus alcanzaron un 600 % durante el trimestre que finalizó el 30 de marzo de 2020.

"Los atacantes son oportunistas y usarán cada ocasión que tengan para sacar ventaja de las emociones más intensas de las personas durante situaciones de crisis, como esta, al tratar de tentarlos a hacer clic en un vínculo malintencionado o descargar un archivo adjunto con malware", dijo Stu Sjouwerman, CEO de KnowBe4.

Defensores atribulados

El panorama de amenazas en expansión pone más presión en los CISO para que modernicen las operaciones de seguridad con el fin de reducir las ineficiencias.

El panorama de amenazas en expansión pone más presión en los CISO para que modernicen las operaciones de seguridad con el fin de reducir las ineficiencias, aumentar la visibilidad en toda la organización y ser más proactivos en la identificación y protección contra las amenazas.

Tradicionalmente, los equipos de seguridad se han encargado de supervisar dominios específicos, sin interacción ni integración. Estos silos pueden impedir que los defensores vean el contexto completo de un ataque hasta que sea demasiado tarde. Los atacantes actuales se mueven tan rápido que en el momento en que los equipos de operaciones de seguridad reconocen la magnitud total de un problema, sus sistemas ya están comprometidos.

Este desafío se ve exacerbado por una combinación cada vez mayor de productos y servicios de seguridad. Por lo general, estos productos utilizan diferentes portales, esquemas de datos y metodologías. La supervisión manual de los datos de esos productos puede retrasar los tiempos de respuesta e incluso pasar por alto los elementos de un ataque en sí.

Un aumento de los productos de seguridad y los datos que recopilan y analizan a menudo crea fatiga de alertas. Los analistas de seguridad no pueden priorizar el volumen de alertas que reciben para abordar las amenazas mayores. Toda la inteligencia que están recopilando no es procesable. Sin las herramientas adecuadas que les ayuden a responder de forma proactiva, antes o mientras se produce una infracción, y para bloquear las amenazas persistentes, los defensores están en una desventaja distinta cuando luchan contra adversarios.

Una nueva era de protección contra amenazas

La seguridad basada en la identidad es un componente clave de un marco de seguridad emergente conocido como Confianza Cero.

La protección contra amenazas está evolucionando para abordar estos desafíos, con métodos y tecnologías emergentes diseñados para fortalecer las defensas tradicionales.

Por ejemplo, los controles de red comenzaron a dar paso a la identidad como un medio para proteger los sistemas y los datos. Cuando el paradigma de defensa centrado en el perímetro y la arquitectura de TI compartía un rango de direcciones IP comunes, los controles de seguridad estaban orientados a la red. A medida que las plataformas de nube y móviles han ido sacando los datos del perímetro, las protecciones de seguridad también deben extenderse fuera de la red. En consecuencia, las organizaciones están explorando formas de rediseñar sus defensas en torno al contexto y la identidad.

Con el paradigma del perímetro, una vez que iniciaba sesión en un sistema, se consideraba al usuario como totalmente confiable. Con el paradigma de la identidad, el acceso a un sistema se limita a lo que el usuario necesita para hacer su trabajo y cualquier comportamiento anómalo desencadenará alertas. La seguridad basada en la identidad es un componente clave de un marco de seguridad emergente conocido como Confianza Cero. Este modelo se basa en la premisa de que la confianza no debe darse por sentada dentro o fuera de la organización. Todo debe comprobarse antes de cualquier tipo de acceso.

Más herramientas para la defensa en profundidad

Los equipos de seguridad ahora pueden implementar capacidades avanzadas de "caza" para erradicar infracciones sofisticadas.

La protección contra amenazas modernas requiere controles de seguridad que se correlacionan continuamente y analizan variables pertinentes casi en tiempo real, y deciden si se debe conceder o denegar el acceso a una identidad. Esta necesidad está aumentando la urgencia de que las organizaciones adopten la automatización, la inteligencia artificial (IA) y el machine learning (ML) a través de sus pilas de seguridad.

La IA y el ML desempeñan roles críticos en las operaciones de ciberseguridad porque permiten analizar cantidades masivas de datos en busca de patrones de actividad sospechosas y señales de amenaza que los analistas humanos no pueden ver hasta que es demasiado tarde. Los algoritmos de ML pueden convertir los datos sin procesar de varias fuentes en incidentes que brindan a los defensores el tipo de visibilidad que necesitan para entender todo el contexto de un ataque y crear una respuesta dirigida.

La IA, el ML y la automatización también ayudan a las organizaciones a ser menos reactivas y más proactivas en la identificación y respuesta a las amenazas. Los equipos de seguridad ahora pueden implementar capacidades avanzadas de "caza" para erradicar infracciones sofisticadas o comprender mejor cómo se comportan los activos de su organización. Este enfoque aumenta la capacidad de una organización para defenderse de los ataques persistentes y bloquear a los atacantes, con lo que evitan que puedan sacar ventaja de los datos y los sistemas.

El trabajo de la CISO no se torna cada vez más fácil. Sin embargo, con una visión clara del panorama de ciberseguridad cambiante y el acceso a métodos de defensa en evolución, podrán dormir un poco mejor por la noche.

Obtenga más información sobre cómo la IA, la automatización y la integración ayudan a mantener seguros a los usuarios, los puntos de conexión, las aplicaciones en la nube y los datos.

Microsoft