Gestión de Vulnerabilidades

De un escaneo reactivo a una gestión estratégica del riesgo

LA PROBLEMÁTICA

El proceso de identificar, clasificar y mitigar vulnerabilidades es un aspecto central de cualquier programa de seguridad Corporativa, sin embargo en una Compañía típica con uno o múltiples servidores, se pueden llegar a detectar decenas o cientos de vulnerabilidades, sumado a esto, cada día se descubren entre 10 a 30 nuevas vulnerabilidades.

Cada una de estas vulnerabilidades es una amenaza potencial, que de ser explotada implica un altísimo costo para la Compañía, en la medida en que comprometa la reputación de la marca, la información critica de clientes, colaboradores, accionistas o proveedores, o cualquier otro activo y que puede afectar seriamente la continuidad del negocio.

Muchas Organizaciones usan escaneos activos tradicionales que requiere una exploración remota de cada dispositivo conectado a la red. Pero este enfoque a menudo es limitado por que:

- Se presentan limitaciones de acceso a activos críticos cuando el escaneo es disruptivo y puede afectar la disponibilidad de esos activos.
- Se escanea parcialmente debido a que no todos los activos son rastreables fácilmente ni están conectados a la red (como dispositivo móviles y activos en la nube).
- Sobre información, ya que los reportes sobre vulnerabilidades pueden ser extensos y sin un análisis crítico, pueden ser abrumadores o arrojar gran cantidad de falsos positivos lo cual representa mayor consumo de tiempo y recursos.
- Los escaneos típicos pueden priorizar las vulnerabilidades basados en los activos o rankings predefinidos de amenazas, sin tener en cuenta el contexto de la red particular de la empresa, esta metodología no considera el contexto de la red y puede llevar al equipo de seguridad a solucionar aspectos no amenazante e ignoran los críticos.

Debido a estas limitaciones, la mayoría de las organizaciones sólo escanean algunos segmentos de sus redes, exponiendo a los activos críticos a vulnerabilidades por largos periodos de tiempo, debido a esto, el alcance de la gestión de la vulnerabilidades se vuelve insuficientes.

www.ransecurity.com /RANsecurity @RANsecurity

RAN ARGENTINA Av. Rivadavia 877 - Piso 5° (C1002AAG) C.A.B.A. Teléfono: (+54 11) 5353 9999
RAN CHILE San Sebastián 2812 Of. 312 (7550151) Las Condes, Santiago de Chile. Teléfono: (+562) 3223 9532
RAN PERU - Los Zorzales 160. Piso 3. San Isidro, Lima. Teléfono: (+51 1) 712 4764

expertos@ransecurity.com

¿Por qué Gestión de Vulnerabilidades?

Mas que un reporte de vulnerabilidades

Transforme datos sobre vulnerabilidades en inteligencia de remediación priorizada y específica, para que pueda actuar con rapidez minimizando riesgos y eliminando vectores de ataque.

Más rápido y efectivo

Estamos 100% enfocados en la seguridad informática, nuestro equipo cuenta con experiencia y herramientas para gestionar eventos y reducir al máximo falsos positivos, haciendo más eficiente la operatoria de la gestión de vulnerabilidades.

Flexibilidad, escalabilidad y adaptabilidad

al contexto de cada Organización, ya los riesgos críticos son diferentes en cada caso. Mas allá de un parcheo, exploramos múltiples opciones de remediación y prevención antes que el ataque ocurra.

Disminución de amenazas que se puede ver

Compruebe el cambio y la mejoría en la posición de su Empresa frente a amenazas persistentes y técnicas avanzadas d evasión desde la primera semana. Podemos medir y presentar la efectividad de la gestión.

LA SOLUCIÓN

Más allá de un escaneo es necesario la combinación entre herramientas dinámicas para el descubrimientos de vulnerabilidades, conocimiento experto sobre el panorama de amenazas, priorización de riesgos para actuar en lo realmente importante evitando perdidas de tiempo y dinero, así como un seguimiento y medición continua sobre las actividades realizadas para minimizar el riesgo que enfrenta día a día la Organización,

La Gestión de Vulnerabilidades como una poderosa herramienta de mitigación de riesgos

Nuestro enfoque permite detectar, priorizar, documentar y gestionar vectores críticos de amenazas, basado en un inventario automatizado, priorización y análisis del riesgo, permitiendo a su equipo de seguridad descubrir y remediar las vulnerabilidades críticas de inmediato.

1. Relevamiento de activos informáticos

Más allá del parcheo

El primer paso de la gestión de vulnerabilidades consiste en identificar todos los activos informáticos dentro de la red, mapearlos y asignar parámetros específicos de criticidad para la continuidad del negocio.

2. Descubrimiento continuo de vulnerabilidades.

Los datos actualizados mantienen la estrategia de seguridad

Una vez identificados los activos críticos se ejecutan escaneos hacia los sistemas para descubrir las vulnerabilidades encontradas, nuestro equipo experto puede asesorarte en la identificación de falsos positivos y el correcto relevamiento de vulnerabilidades a tratar.

3. Análisis de contexto.

Los riesgos críticos son diferentes en cada Organización.

Integramos la criticidad de cada activo con las vulnerabilidades detectadas, como resultado se da una priorización a cada vulnerabilidad según el entorno particular de cada Organización. Definimos conjuntamente un plan de acción y asignamos mediante un sistema de tickets automatizado los responsables para su solución.

4. Priorizando riesgos

Optimizando recursos y tiempo

¿Qué pasa con las vulnerabilidades que no se pueden parchar? El análisis de vulnerabilidades no se limita al parcheo, por eso nuestro expertos te asesoran en la implementación de controles alternativos y determinación del impacto que genera una vulnerabilidad de difícil tratamiento en los sistemas afectados.

5. Seguimiento y documentación.

Midiendo la efectividad del programa para garantizar la seguridad

El programa se mantiene vigente y fresco para minimizar la ventana de tiempo de vulnerabilidades mediante el descubrimiento de un ***Mapa de Criticidad de Vulnerabilidades***, el seguimiento a los tickets asignados y la verificación de la ejecución de acciones recomendadas.

Conoce cómo convertir la Gestión de vulnerabilidades en un potente programa estratégico de Gestión del riesgo.

No dudes en contactarnos: expertos@ransecurity.com