Gestión priorizada de vulnerabilidades técnicas con base en indicadores de riesgo.

Víctor Manuel Castellanos Bernal, Daniel Cruz Moscoso
Estudiantes Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes. Bogotá, Colombia
Diciembre 2019

1. Introducción

Una vulnerabilidad tecnológica hace referencia al estado de un activo o proceso de tecnologías de la información a estar expuesto a la posibilidad de un ataque, degradación o daño, ya sea físico o lógico. Una vulnerabilidad por sí misma no representa la materialización de un ataque, únicamente representa un riesgo al que se encuentra expuesto el activo o proceso. Las vulnerabilidades normalmente se presentan por errores de código, fallas en el diseño de software, problemas en la implementación o malas prácticas de configuración de activos que permiten que actividad maliciosa sea ejecutada por medio de un "*exploit*" (Software o acciones para explotar una vulnerabilidad).

Las organizaciones actualmente son conscientes del crecimiento continuo de las vulnerabilidades, y reconocen que parte de la continuidad de negocio depende de una gestión de riesgos de TI Efectiva prestando especial atención a la aplicación de actualizaciones de seguridad recomendada por los fabricantes y a la aplicación de parches de remediación que operan como controles preventivos ante riesgos de posible explotación de debilidades en los sistemas de TI.

La falta de capacidades para una correcta ejecución de un programa de gestión de vulnerabilidades puede llevar a las organizaciones a afrontar graves daños económicos y reputacionales, como en el caso de Equifax en 2017 que represento la fuga de datos de miles de usuarios del sistema financiero tras la explotación de una vulnerabilidad que no había sido cerrada luego de más de 3 meses de su publicación, generando perdidas para Equifax por 575 millones de dólares[1].

Según un estudio de TripWire Inc. las vulnerabilidades que no se remedian en un tiempo prudente representan la causa raíz de las fugas de información más críticas en los últimos días. En un estudio realizado en mayo de 2019 por Tripwire en alianza con Dimensional Research consultó a 340 profesionales en seguridad informática acerca de las tendencias en gestión de vulnerabilidades, encontrando que en efecto al menos el 27% de los entrevistados había sufrido una fuga de información como resultado a una vulnerabilidad sin remediar.

[1] Equifax Data Breach: How to Protect Your Credit, Bank Accounts, Alexandra Silets, WTTW. Fuente : https://news.wttw.com/2017/09/19/equifax-data-breach-how-protect-your-credit-bank-accounts

Es importante no confundir gestión de vulnerabilidades con escaneo de vulnerabilidades. El escaneo de vulnerabilidades consiste en usar un software para identificar vulnerabilidades en redes, infraestructura informática o aplicaciones. La gestión de vulnerabilidades es el proceso que se genera a partir del escaneo de vulnerabilidades, teniendo en cuenta también otros aspectos como aceptación de riesgos, remediación y control de activos

El constante crecimiento del delito cibernético y los riesgos asociados están obligando a la mayoría organizaciones a centrar más su atención en la seguridad de la información.

El proceso de gestión debe ser parte del esfuerzo de una organización para controlar los riesgos de seguridad de la información. Este proceso permitirá que una organización obtenga una visión general continua de vulnerabilidades en su entorno de TI y los riesgos asociados con ellas. Al identificar y mitigar vulnerabilidades en el entorno de TI una organización puede evitar que los atacantes penetren en sus redes y roben información.

En Latinoamérica este tipo de situaciones se ve de manera más fuerte en las pequeñas y mediana empresas, en un estudio realizado por “Brother International Corporation”[2] a 800 negocios que están haciendo uso de tecnologías de la información para soportar sus operaciones demostró que efectivamente el 69% de estos encuestados admitió estar preocupado por la seguridad de la información, sin embargo, el 40% de estos encuestados admitió no haber implementado ninguna medida para mitigar los riesgos que puedan representar brechas de seguridad en sus empresas.

2. Problema

El objetivo de presentar estos datos es describir la problemática general de seguridad que están enfrentando diferentes empresas en múltiples sectores frente al desarrollo de capacidades tecnológicas y humanas que permitan la remediación oportuna de vulnerabilidades sobre activos de información críticos tecnológicos para el desarrollo de sus actividades de negocio:

Número creciente de vulnerabilidades

La cantidad de vulnerabilidades ha venido como mínimo manteniéndose y con tendencia a incrementarse a diario, como se puede evidenciar en la siguiente ilustración tomada del centro de estadísticas del NIST en la que se describe la cantidad de parches y severidad publicados desde el 2001 hasta lo que va transcurrido del 2019:

[2] ¿A que se enfrentan las pymes en 2019? . Fuente : https://www.dinero.com/economia/articulo/a-que-se-enfrentan-las-pymes-en-2019-en-latinoamerica/268226

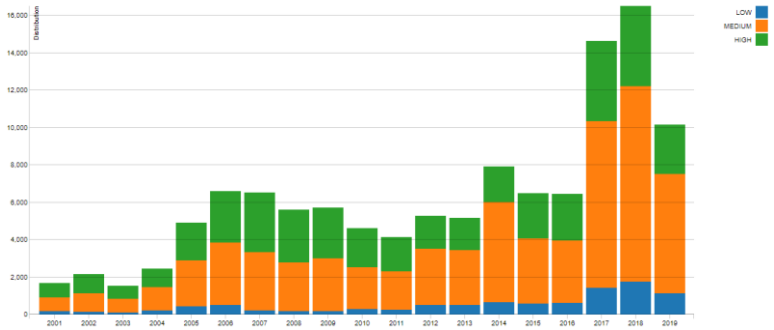

Imagen 1. CVSS Severity Distribution Over Time (NIST, 2019)

Las organizaciones no saben priorizar sus vulnerabilidades

De acuerdo con un estudio titulado: "*Security Report for In-Production Web Applications*" realizado por la empresa Rapid 7, El tiempo promedio para remediación de vulnerabilidades en general es de 38 días a partir de liberación del parche por el fabricante.

De acuerdo con estudios realizados por ServiceNow en su reporte de estado de vulnerabilidades y amenazas en consultas realizadas a más de 300 profesionales de seguridad de la información y ciberseguridad entre las razones más comunes para no cerrar de manera oportuna vulnerabilidades sobre los sistemas de información de identificaron causas como:

No se cuenta con una estrategia de priorización de implementación de parches.

No se cuenta con el personal y conocimiento suficiente para realizar el cierre de vulnerabilidades.

Los resultados de las herramientas de escaneo de vulnerabilidades tradicionales no brindan visibilidad clara sobre las amenazas vigentes que aprovechan estas vulnerabilidades en el contexto organizacional.

3. Propuesta de solución

Con el fin de dar solución a los inconvenientes identificados en el proceso de gestión de vulnerabilidad, se plantea definir un servicio con las capacidades requeridas para apoyar la gestión de vulnerabilidades técnicas en las organizaciones por medio de la adquisición de servicios consultivos con recursos y herramientas especializadas que den un tratamiento priorizado a las vulnerabilidades identificando sus fuentes de amenazas relevantes y niveles de riesgo que representan para la organización.

La solución se centra en tres pilares fundamentales: personas, procesos y tecnología.

Tecnología

En la parte tecnológica se cuenta con una infraestructura centralizada la cual soporta los procesos asociados a la prestación del servicio.

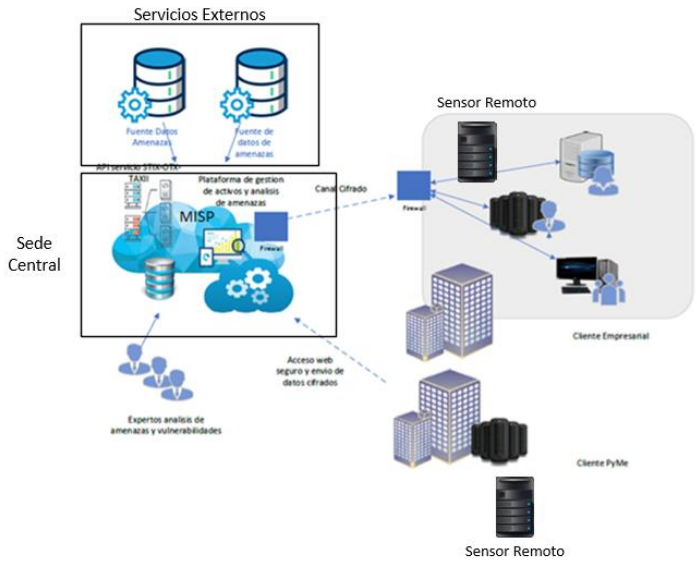

Imagen 2. Infraestructura tecnológica de la solución

En la sede central se cuenta con los siguientes servicios:

- Servidor central de gestión de vulnerabilidades: este recibe y consolida la información obtenida por parte de los sensores remotos. Los sensores remotos realizan toda la labor de identificación de activos y análisis de vulnerabilidades dentro de la infraestructura de cada uno de los clientes.

- Servidor de monitoreo de amenazas: Este dispositivo cuenta con una API de integración con las fuentes abiertas de amenazas en tiempo real.

- Servidor de correlación de datos: Este dispositivo toma los resultados de análisis de vulnerabilidades, clasificación de activos, explotación de vulnerabilidades de acuerdo a fuentes abiertas de inteligencia de amenazas, y genera un reporte priorizados de vulnerabilidades cuyos factores de riesgo se basan en la explotación real de vulnerabilidades y el análisis de riesgo asociado al activo.

- Servidor de alertas: Su labor principal es la recepción de información por parte del servidor de monitoreo de amenazas para la generación de alertas en el caso de identificación de explotación real de una vulnerabilidad.

La sede central establece una conexión con fuentes de datos de inteligencia de amenazas por medio del servidor de monitoreo de amenazas. Estas fuentes de datos son alimentadas en tiempo real por parte diversas comunidades e individuos que desempeñan sus labores en ciberseguridad. De las fuentes de datos de inteligencia de amenazas se obtienes los datos que permiten identificar la explotación de una vulnerabilidad y los mecanismos usados por parte de los atacantes.

Personas

El recurso humano que soportaría la operación se describe a continuación con el rol que desempeñaría y sus responsabilidades dentro de la organización.

Rol	***Responsabilidades***
Director de operaciones	- Supervisar la actividad del equipo técnico y consultivo. - Reclutar, contratar, entrenar y evaluar al personal. - Gestionar el proceso de escalación y revisión de los informes de proyectos - Realizar un análisis de capacidad del personal de acuerdo con los datos de implementación y proyección de servicios - Gestionar tareas administrativas y financieras.
Consultor en seguridad	- Revisar el descubrimiento de activos y los datos de evaluación de vulnerabilidad en los servicios. - Implementar y refinar continuamente casos de uso basados en resultados de investigación de amenazas (Inteligencia de amenazas). - Investigar nuevas técnicas de ataque y alineación de la estrategia de vulnerabilidades de los clientes de acuerdo con los hallazgos de inteligencia de amenazas. - Cumplir con las metodologías y procedimientos establecidos para la ejecución y control de servicios. - Desarrollar la prestación del servicio para los clientes que adquieran la solución ofrecida por la organización.
Ingeniero de infraestructura	- Gestionar y configurar la infraestructura asociada a tecnologías y soluciones (STIX Server, SOAR, plataforma gestión de vulnerabilidades, tickets, gestión de activos y análisis de datos.) - Reportar al director de operaciones planes de mejora sobre la arquitectura de la infraestructura tecnológica que soporta el servicio. - Apoyar incidentes de tecnología de infraestructura que ocurran en la Organización. - Garantizar el correcto funcionamiento de los activos tecnológicos de la organización.
Gerente de proyectos	- Gestión y planeación de recursos para la ejecución de proyectos manejados por la organización. - Dirección y organización del equipo de proyecto asignado para la prestación de servicio. - Seguimiento continuo sobre los avances y riesgos asociados a los proyectos durante la prestación de servicio. - Generación de reportes de cumplimiento, costos y calidad en la ejecución de cada proyecto manejado por la organización.

Procesos operativos

Los procesos operativos asociados a la prestación del servicio se resumen a continuación:

Fase de Alistamiento:
Son analizados los requerimientos para la prestación del servicio:

Perfilamiento de usuario: Tipo de organización, tamaño, sector económico, razón social, misión y visión.

Levantamiento arquitectura de red de la organización.

¿La organización cuenta con una tecnología que soporte la gestión de vulnerabilidades técnicas?

a). Si el usuario no cuenta con la herramienta se proveen los sistemas satélites que se conectan por canales seguros al sistema central de gestión de vulnerabilidades del servicio.

b). Si el usuario cuenta con la herramienta se realiza el análisis y se toman los resultados en CSV o XML para normalizarlos e integrarlos con las fuentes colaborativas de inteligencia de amenazas

Identificación de procesos críticos.

Definición de estrategia de servicio para asesoría en gestión de vulnerabilidades.

Fase implementación del servicio:

Levantamiento del inventario de activos:
Por medio de un sensor que hace parte del servicio ofrecido se hace la búsqueda máquinas “activas” en la red.

De acuerdo con el reporte del sensor de acuerdo a la tarea de escaneo de red se genera una asociación de los dispositivos detectados con procesos de negocio.

Se da una categorización de criticidad y riesgo a cada uno de los activos, identificando también el nivel de confidencialidad de los datos de acuerdo con la información obtenida del dueño de los procesos o activos.

Identificación de vulnerabilidades:

Se ejecuta el análisis de vulnerabilidades técnicas sobre el inventario de activos identificados sobre la fase previa:

a). El usuario cuenta con una herramienta de análisis de vulnerabilidades

Se realiza el escaneo con su herramienta y se solicitan los resultados en formato XML o CSV.

b). El usuario no cuenta con una herramienta de análisis de vulnerabilidades: Se realiza escaneo con herramienta propuesta dentro del servicio con integración definida hacia las bases de datos de amenazas.

Generar informe de vulnerabilidades priorizado:
Entrega de reporte de vulnerabilidades con priorización basada en riesgos:

Se toman los resultados del análisis de vulnerabilidades, el inventario de activos, vulnerabilidades realmente explotadas y pasan por una correlación con datos de información de base de datos de amenazas.

Se espera que tras la correlación se obtenga un informe de las amenazas más significativas la organización objetivo y que afecten en mayor medida los activos que soportan sus procesos de negocio críticos.

Generación de un plan de remediación de las vulnerabilidades con prioridad más alta.

Actividades de remediación:
Definición de roles, responsabilidades, hitos, actividades y riesgos asociados al plan de remediación, con metodología de ejecución de tareas propuesta por el proveedor de servicios.

Cierre de proceso:
Certificación remediación - Identificación de vulnerabilidades:

Análisis de vulnerabilidades técnicas.
Generación de reporte diferencial.
Análisis de ROI

Conclusiones y recomendaciones

Las empresas a nivel Colombia y en general en el mundo carecen de capacidades tecnológicas, procesos específicos y personal dedicado para dar una gestión oportuna a las vulnerabilidades técnicas en un tiempo adecuado para prevenir exposición a los Ciber-atacantes.

Cada día toma más relevancia aprovechar las capacidades que ofrecen tecnologías emergentes como “Cloud Computing”, automatización – RPA, Tecnologías para la orquestación de seguridad, respuesta y automatización de incidentes (SOAR por su sigla en inglés) para dar gestión a procesos como la gestión de vulnerabilidades, este tipo de procesos aunque son técnicos por naturaleza y con una responsabilidad organizacional de áreas de TI o Seguridad Informática, apoyan las personas, procesos y tecnologías que soportan el cumplimiento de los objetivos de negocio de las organizaciones.

Siempre que el retorno de inversión de seguridad o ciberseguridad sea el adecuado para una organización, es necesario contar con estas capacidades o este tipo de servicios bajo la modalidad que se ajuste a las capacidades de cada organización, por ejemplo, a través de un CSIRT, CERT, SOC, por medio de un servicio especializado o capacidades organizacionales internamente desarrolladas.

Las fuentes de datos de inteligencia de amenazas pueden apoyar otros procesos asociados a operaciones de seguridad, esto teniendo en cuenta que no solo brindan datos de vulnerabilidades, también permiten perfilar atacantes, detectar sitios maliciosos y herramientas asociadas a brechas de seguridad. Esto permitiría identificar de forma proactiva amenazas que puedan afectar la infraestructura tecnológica y definir procedimientos proactivos en caso de detectar una amenaza que ya se encuentra perfilada en bases de datos de inteligencia de amenazas.