CIBERSEGURIDAD DE LA RED

Prevenga vulneraciones de su red informática para mantener su servicios e infraestructura protegida

La seguridad informática continúa creciendo debido a la dependencia que tienen las empresas de las tecnologías de procesamiento de la información. Estas tecnologías administran información crítica para las organizaciones y deben asegurar que la información está completamente íntegra, tiene niveles de confidencialidad adecuados y está disponible cuando se requiera.

IIA lleva adelante un Análisis de Seguridad de la Red que permitirá reconocer los activos informáticos más importantes, determinar las vulnerabilidades a las que se está expuesto y recomendar acciones que ayuden a mitigar el riesgo.

Con estas acciones y a través de un reporte, el cliente podrá identificar activos, conocer las vulnerabilidades y corregir los problemas encontrados.

1. Activos Informáticos

Primero, se lleva a cabo una evaluación que permita identificar los activos críticos en la red. Realizando escaneos de la red en conjunto con entrevistas a los responsables de la operación se determinan cuáles son los elementos críticos de los sistemas TI que podrían dañar el negocio en caso de no estar disponibles. Las aplicaciones o sistemas pueden ser desde ERP, sistemas contables o de facturación hasta estaciones de trabajo de personal crítico.

2. Recolección de Información

Luego de identificar los activos críticos se lleva a cabo La etapa de recolección de información relevante para el análisis. En esta etapa se usan herramientas que recolectan información durante un período de tiempo para luego ejecutar reportes que apoyan la labor de análisis. También se obtienen las versiones de firmware, Sistema Operativo y Software que se están ejecutando, así como las configuraciones que están operando.

3. Análisis de la información

Con la información disponible, se realiza un análisis para identificar las vulnerabilidades que se detectan en los sistemas y software que están operando en la red. Se determina el nivel de exposición que tiene cada una de estas vulnerabilidades y por último se estima el impacto que estas vulnerabilidades pueden llegar a tener. Esto permitirá al cliente tener una visión específica del grado de riesgo a la que sus activos están expuestos y cuáles sistemas son los que se deben priorizar.

4. Recomendación de acciones

La etapa final del proceso se refiere a documentar los descubrimientos obtenidos en cada etapa del proceso de tal forma que el cliente pueda usar la información para revisar sus procedimientos y sistemas de seguridad presentes.

El reporte incluye también recomendaciones de acuerdo a las vulnerabilidades encontradas, de tal forma que el cliente pueda tomar medidas de mitigación adecuadas que eviten que las vulnerabilidades sean explotadas.

Evaluación de Ciberseguridad en la Red

Item

Identificación, Análisis y Reporte desde 50 Activos críticos

Reporte

- ☑ Activos críticos
- ☑ Vulnerabilidades identificadas
- ☑ Priorización según riesgo
- ☑ Recomendaciones

CONTÁCTENOS

Para más información 228401000 - División Internet

30 AÑOS | Generando soluciones TI integrales para su empresa