ESET® INTELLIGENCE LABS

Servicios confiables, Negocios seguros

Ransomware Prevention

ENJOY SAFER TECHNOLOGY™

Ransomware Prevention

Un **ransomware** es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Este ransomware se caracteriza por cifrar los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Los vectores más comunes de infección son:

1. Explotación de vulnerabilidades en servidores públicos.
2. Explotación de vulnerabilidades en servidores web públicos.
3. Ataques del tipo phishing a los usuarios de la organización.

Utilizando algunos (o todos) los vectores de ataque detallados arriba, los atacantes logran comprometer hoy en día el 100% de las organizaciones que se ponen como objetivo.

Sin embargo, existen formas de estar preparados y evitar así ser víctima de este tipo de ataque malicioso: realizar un **diagnóstico con nuestro servicio Ransomware Prevention.**

Network Penetration Test / Web Application Penetration Test:

Los servicios de test de intrusión (tanto de red como web) son técnicas utilizadas para evaluar la seguridad de los recursos y activos de la organización desde el punto de vista de la materia de seguridad a nivel servidores, redes y Web.

Estas técnicas no solo identifican las vulnerabilidades existentes en la infraestructura de red, sino que también lo hace en los sistemas, software instalado y en las aplicaciones web, sino que además ejecuta el análisis con mayor profundidad. Específicamente, se busca además de la identificación, la explotación de las vulnerabilidades y de esa manera se observa el impacto real sobre la organización.

Social Engineering Test:

Un Social Engineering Testing es una técnica utilizada para evaluar la seguridad de los recursos y activos de la organización desde el punto de vista de la materia de seguridad de las personas dentro de nuestra organización.

Esta técnica identifica las vulnerabilidades existentes a nivel de concientización y conocimiento sobre diferentes vectores de ataques orientado a las personas dentro de nuestra organización. Especialmente, se busca además de la identificación, la explotación de las vulnerabilidades referidas al engaño de personas y de esa manera se observa el impacto real sobre la organización por medio de esta.

Objetivos principales:

- Entender del estado de la seguridad que la organización en relación a los dispositivos de perímetro (o públicos) como servidores o servidores web expuestos a internet.
- Conocer el grado de concientización de los usuarios y comprender así si estos podrían introducir este tipo de amenazas a la red sin darse cuenta.

¿Qué incluye el servicio de Ransomware Prevention?

- Un External Network Penetration Test.
- Un External Web Application Penetration Test.
- Un Social Engineering Test.
- Capacitación a los usuarios en relación a los resultados del test de ingeniería social.
- Capacitación al personal técnico para conocer como remediar los problemas detectados en los servidores y en las aplicaciones web.
- Un Re-Test para conocer si tanto las medidas de entrenamiento como de mitigación de riesgos han sido efectivas.
- Ransomware Prevention Kit: este Kit elaborado por ESET que contiene todo tipo de guías para diferentes audiencias técnicas y no-técnicas, así como también licencias de prueba para varios productos de ESET.

Las etapas asociadas a este servicio son:

- Realización de los test de intrusión de red y web.
- Realización del test de ingeniería social.
- Entrega de resultados (reportes).
  Prestado de curso de seguridad basado en los resultados del test de ingeniería social.
- Entrenamiento al personal técnico para conocer como mitigar los problemas detectados.
- Ejecución de Re-test y armado de reportes de estado.
- Plan de acción basado en los últimos resultados.
- Entrega del Ransomware Prevention Kit.

Entregables

En este servicio se generan varios entregables o reportes que ayudan y guían al cliente en el proceso de remediación de los riesgos.

Los test de intrusión (o Network / Web Penetration Test) incluyen los siguientes entregables:

- El primero de ellos, el Informe Ejecutivo, describe el nivel de riesgo de la compañía sin entrar en detalles técnicos, evidenciando las problemáticas por medio de conceptos claros y gráficas.
- El segundo reporte, el informe técnico, apunta al área técnica de la empresa, ayudando al personal de TI a solucionar los problemas detectados. En este reporte se muestran todas las evidencias de los tests ejecutados de manera tal que todas las tareas sean repetibles y transparentes para el cliente.

Asimismo, el servicio de ingeniería social incluye el siguiente entregable:

- Reporte de estado del nivel de concientización y acciones necesarias para mejorar el mismo.