UNA UNIVERSIDAD NACIONAL COSTA RICA
DTIC Dirección de Tecnologías de Información y Comunicación

BOLETÍN DTIC

7 de julio de 2022
Boletín 5
dtic@una.cr

Noticias, comentarios y anuncios tecnológicos

En esta edición:

"Computadoras portátiles, tabletas y celulares como endpoints"

¿Qué es un endpoint?

Un endpoint, es un dispositivo informático que generalmente se refiere a los equipos electrónicos que utilizamos de forma diaria, a saber: computadores portátiles y de escritorio, dispositivos móviles tales como celulares, tabletas, entre otros.

Los endpoint o "puntos finales" poseen un sistema operativo que permite la interacción con la persona interesada. Estos sistemas operativos los conocemos con nombres como Windows, macOS, Android y Linux, para citar los más conocidos.

Los sistemas operativos son susceptibles a recibir ataques informáticos, o ser dañados por algún software de tipo malware. En este sentido, se hace indispensable la utilización de algún software de protección del sistema operativo, sus aplicaciones y datos almacenados en el endpoint.

¿Qué es un EDR?

Un Endpoint Detection and Response (EDR) o sistema de protección de equipos e infraestructuras, consiste en un software especializado para la protección de los equipos computacionales de actividades relacionadas al malware y otras amenazas informáticas.

Generalmente lo conocemos como un software antivirus, sin embargo, pueden poseer facilidades adicionales tales como antimalware en general, prevención de intrusos, prevención de pérdida de datos, firewall o muro de fuego, protección contra ransomware, cifrado de disco, entre otros.

Malware – Parte 2

Caballo de Troya

Un troyano es un tipo de malware que aparece en 1975, aparentando ser un software inofensivo o de uso cotidiano.

Generalmente se ocultan dentro de otro software que eventualmente llegamos a instalar y utilizar en algún momento.

Sin embargo, su misión es la de infectar un dispositivo informático, teniendo algunas consecuencias como las siguientes: espiar el contenido y la actividad de un computador; convertir el equipo en zombi, es decir, miembro de una red Botnet; crear puertas traseras o "backdoor" para permitir el ingreso no autorizado de un tercero desde una ubicación externa, entre otros.

Software Espía

Como indica su nombre, este tipo de malware recopila información de un dispositivo afectado y la transmite a un tercero sin el conocimiento de su dueño.

Generalmente funciona de forma permanente, y puede llegar a capturar "en vivo" las pantallas y datos que se teclean en un momento dado (incluyendo nombres de usuario, contraseñas y otra información confidencial).

No se replica como un virus, por lo que más bien se le considera un parásito.

En términos generales: evite la instalación de software desconocido, utilice herramientas antimalware, y ponga atención a cualquier comportamiento anómalo de su computador.

Firewall

Un firewall, muro de fuego o cortafuegos es una solución que existe tanto en hardware (equipos) como en software (programas de cómputo), destinado a proteger la infraestructura tecnológica (equipos de telecomunicaciones, servidores, servicios digitales y datos); de accesos no autorizados por parte de terceros, ya sea internos o externos a la organización.

En muchos casos, los accesos no autorizados son intentos de ataque que pretenden ingresar al recurso informático de forma anómala. Este recurso puede corresponder a servidores institucionales de correo electrónico, de páginas web, de sistemas de información y bases de datos, repositorios de contenido, etc. También, el objetivo del ataque puede ser el computador de uso diario de una persona en particular.

Las organizaciones en general deben implementar firewalls en sus infraestructuras tecnológicas como medida inicial de protección ante el tráfico de red no autorizado.

Los sistemas operativos Windows, macOS y Linux implementan como medidas de protección soluciones de firewall para la protección de los endpoint.