Managed secure IT | no matter what

IMPORTANCIA DE LA SEGURIDAD EN LOS ENDPOINTS

Como su nombre lo indica, los Endpoints son una especie de “aduana” que protege a un país digital de la entrada de agentes maliciosos que puedan poner en riesgo su seguridad interior.

Entender la importancia de la seguridad de los Endpoints para una empresa es comenzar a apreciar lo necesario que es protegerlos bajo los más estrictos estándares de blindaje.

Cloud

Al ser la primera capa de seguridad, los Endpoints son los primeros puntos en los que se detectan y enfrentan los ataques y amenazas cibernéticas. Además, su ubicación permite dar la alarma al resto del sistema para que se active un protocolo de defensa que proteja la información que contiene.

En pocas palabras: los Endpoints son componentes fundamentales en un sistema de seguridad, ya que además de ser la primera línea de defensa ante un ciberataque, permiten controlar cualquier tipo de intrusión que busque filtrar información contenida en la Nube.

Endpoints también permiten conocer el origen del ataque y su naturaleza, lo que ayuda a un equipo de TI a reaccionar con tiempo para contener la amenaza antes de que sea demasiado tarde.

Los Endpoints “viven” en cada equipo conectado a una red corporativa. Son dispositivos móviles, impresoras, cajeros automáticos, laptops, equipos de punto de venta y PC’s. En fin, la plataforma que usa un usuario o empleado para acceder a una base de datos o servicio.

Para evitar pérdidas de datos valiosos o convertirse en víctima del ransomware, hace falta proteger estos equipos con el mayor nivel de seguridad pues no importa si la información más valiosa para un negocio vive en la Nube; cuando un equipo Endpoint se infecta, toda la red puede colapsar.

Por ello, una compañía que no atienda la protección de sus Endpoints y la subestime, podría ser la próxima en convertirse en una víctima más de los cibercriminales.

Un estudio reciente de McAfee Labs indicó que en 2018 los riesgos de los Endpoints se incrementarán respecto al año anterior. Esta predicción alarma aún más si tomamos en cuenta que ya en 2016, la misma empresa había vaticinado que ese año, los ataques se doblarían respecto a los registrados en 2015.

La tendencia de los cibercriminales es atacar empresas y hacerlas perder millones de dólares infectando sus redes a través de sus Endpoints, por lo que su protección debe ser fundamental para no acabar convirtiéndose en una víctima más de sus ataques.

Actualmente existen cercos integrales de protección que protegen los datos de una empresa desde los Endpoints hasta el último kylobyte contenido en una Nube protegida y alejada de las ciberamenazas. Lo único que hace falta es consultar a un equipo de expertos para recibir orientación sobre qué herramientas y plataformas son las mejores para cada negocio.

Para proteger bien los Endpoints hacen falta varias cosas: una estructura de seguridad escalable y adaptable a las nuevas amenazas, recursos para la detección de amenazas, rutinas diarias de

protección, comunicación con otras redes respecto a posibles amenazas y consolidación de agentes y procesos para saber cómo reaccionar ante un ataque.

Recuerda que una organización que no protege sus Endpoints, podría colapsar debido al robo de su información más importante o perder miles de millones de dólares por el secuestro de sus bases de datos y sistemas críticos de trabajo.

No te arriesgues y busca orientación con nuestros especialistas Mexis de cómo proteger mejor cada aspecto de tu negocio, sin importar escala o giro, al navegar en la web, el peligro de ser víctima de un cibercriminal está latente.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.