ManageEngine

7 principios de seguridad Zero Trust

Según el NIST Special Publication 800-207, cualquier arquitectura de Zero Trust necesita seguir siete principios:

1. Todas las fuentes de datos y servicios informáticos se consideran recursos.

Qué significa esto:
Ya sea un dispositivo IoT, un producto SaaS o un dispositivo personal, si está dentro de la red empresarial o puede acceder a los datos y servicios propiedad de la empresa, se debe considerar un recurso.

2. Toda comunicación está protegida, sin importar la ubicación de la red.

Qué significa esto:
Nunca confíe automáticamente en un usuario o dispositivo con base en la ubicación de su red. Ya sea que una solicitud de acceso proviene de la red empresarial o de una red no empresarial, debe cumplir los mismos requisitos de seguridad.

3. Se otorga el acceso a recursos empresariales individuales según la sesión.

Qué significa esto:
Evalúe en cada momento la confiabilidad de la solicitud antes de otorgar el acceso. Garantice que otorga los mínimos privilegios necesarios para completar sus tareas y que otorgar acceso a un recurso no suponga automáticamente el acceso a los otros.

4. El acceso a los recursos está determinado por políticas dinámicas.

Qué significa esto:
Defina su lista de recursos, los miembros de su organización y quién tiene qué nivel de acceso a cuáles recursos. Tenga en cuenta la información contextual como ubicación, estado del dispositivo, contexto de red, etc., y varíe los métodos de autenticación de acuerdo con la sensibilidad del recurso al que se accede; es decir, el rigor de la autenticación debe ser proporcional a la sensibilidad.

5. Monitoree y mida la integridad y postura de seguridad de todos los activos propios y asociados.

Qué significa esto:
Monitoree y evalúe la postura de seguridad de todos los dispositivos que acceden a su red, incluyendo las vulnerabilidades conocidas, estado de parche y otros riesgos de seguridad informática, antes de otorgarles acceso. Se debe tratar diferente a los dispositivo no gestionados, nuevos en la red o gestionados pero con vulnerabilidades conocidas con respecto a los dispositivos gestionados cuya seguridad se conoce.

6. Todas las autenticaciones y autorizaciones de los recursos son dinámicas y se aplican estrictamente antes de permitir el acceso.

Qué significa esto:
Garantice la verificación de amenazas de forma continua y reevalúe la confianza dada a los usuarios que acceden a sus recursos. Utilice soluciones para la gestión de accesos e identidades con el fin de controlar el acceso y aplique MFA para acceder a los recursos empresariales. Asegúrese de monitorear continuamente las actividades de los usuarios, volver a autenticarlos y autorizarlos cuando sea necesario.

7. Recopile tanta información como sea posible sobre el estado actual de los activos, infraestructura de la red y comunicaciones, y cómo se usan para mejorar la postura de seguridad.

Qué significa esto:
Recopile y analice datos sobre las posturas de seguridad de los dispositivos, el tráfico de la red, solicitudes de acceso, etc., para mejorar la postura de seguridad de su organización. Estos datos también pueden dar contexto adicional sobre los requisitos del principio 4.

Referencias

National Institute of Standards and Technology Special Publication 800-207, Zero Trust Architecture

Conozca más de Zero Trust en
manageengine.com/latam/seguridad-zero-trust/