¿Qué son los ataques internos?: ¿Qué tan preparado estás?

mexis aggity

Los ataques internos a menudo toman a las organizaciones por sorpresa porque son difíciles de detectar.

Apostar por soluciones reactivas como software antivirus o una solución de administración de parches para evitar tales ataques no es prudente.

Comprender qué contribuye al creciente número de amenazas internas y abordar estos factores es la única forma de proteger su empresa contra tales ataques.

Un ataque interno a menudo se define como un exploit por intrusos maliciosos dentro de una organización.

Este tipo de ataque generalmente se dirige a datos inseguros. Las amenazas internas pueden acechar dentro de cualquier empresa; En algunas industrias, pueden representar más del 70% de los ataques cibernéticos.

La mayoría de las veces, los ataques internos se descuidan. Tal vez por eso han estado en constante aumento.

Una encuesta realizada por CA Technologies en 2018 encontró que alrededor del 90% de las organizaciones se sienten vulnerables a los ataques internos.

Las organizaciones también sienten que los datos más vulnerables a los ataques internos son la información personal confidencial (49%), la propiedad intelectual (32%), los datos de los empleados (31%) y la información de cuentas privilegiadas (52%).

Muchos ataques internos están asociados con privilegios de acceso excesivos. Si bien puede ser desagradable o inconveniente no confiar en los empleados, las organizaciones deben estar atentas.

Clasificación de tres tipos de amenazas internas

Usuarios malintencionados: usan intencionalmente su acceso a datos confidenciales para dañar a la empresa.

Usuarios descuidados: representan una amenaza no intencional debido a un error humano o violaciones de la política de seguridad.

Usuarios comprometidos: Usuarios cuyas cuentas están comprometidas y son utilizadas por ciberdelincuentes.

Esto se puede lograr mediante el monitoreo de posibles fuentes de ataques cibernéticos. Un gran problema es que muchas empresas desconocen cómo identificar y combatir las amenazas internas.

Entonces surgen preguntas: ¿Dónde puede encontrar las mejores herramientas de seguridad de red para obtener más conocimientos sobre la lucha contra los ataques internos? ¿Qué estándares de seguridad debe seguir para mantenerse dentro de los requisitos de cumplimiento de seguridad de su industria y proteger mejor sus activos digitales? ¿Cómo se diferencia entre una información privilegiada maliciosa y una no maliciosa?

Advertencias de amenazas internas que debe tener en cuenta

Aquí hay algunas señales reveladoras que puede monitorear para evitar un ataque interno. Esté atento a cualquier persona que:

Descarga grandes cantidades de datos en dispositivos portátiles personales o intenta acceder a datos que normalmente no utilizan para su trabajo diario.

Solicita acceso a la red o a los datos a recursos no necesarios para su trabajo, o busca e intenta acceder a datos confidenciales.

Envía por correo electrónico información confidencial a una cuenta de correo electrónico personal o a personas ajenas a su organización.

Accede a la red y a los datos corporativos fuera del horario laboral habitual.

Exhibe actitudes o comportamientos negativos, por ejemplo, un empleado descontento que abandona la organización.

Ignora las mejores prácticas de concienciación sobre seguridad, como bloquear pantallas, no usar USB o unidades externas, no compartir contraseñas y cuentas de usuario, o no tomar en serio las amenazas cibernéticas.

Una vez que haya comenzado a monitorear, puede implementar medidas de seguridad para evitar que ocurran ataques. Hemos reunido una breve lista de soluciones para frenar las amenazas internas.

1. Confianza cero

Zero Trust, una nueva palabra de moda en ciberseguridad, es un enfoque holístico para reforzar la seguridad de la red mediante la identificación y concesión de acceso, o "confianza".

No hay ninguna herramienta o software específico asociado con este enfoque, pero las organizaciones deben seguir ciertos principios para mantenerse seguras.

Más usuarios, aplicaciones y servidores y la adopción de varios dispositivos IoT amplía el perímetro de su red.

¿Cómo ejerces control y reduces tu superficie de ataque general en tales casos?

¿Cómo puede asegurarse de que se concede el acceso correcto a cada usuario?

La seguridad de TI en algunas organizaciones refleja la antigua mentalidad de defensa de castillo y foso de que todo lo que está dentro del perímetro de una organización debe ser confiable, mientras que todo lo que está fuera no debería.

Este concepto se centra demasiado en la confianza y tiende a olvidar que podríamos saber poco sobre las intenciones de aquellos que consideramos "iniciados".

El remedio es Zero Trust, que revoca los privilegios de acceso excesivos de usuarios y dispositivos sin la autenticación de identidad adecuada.

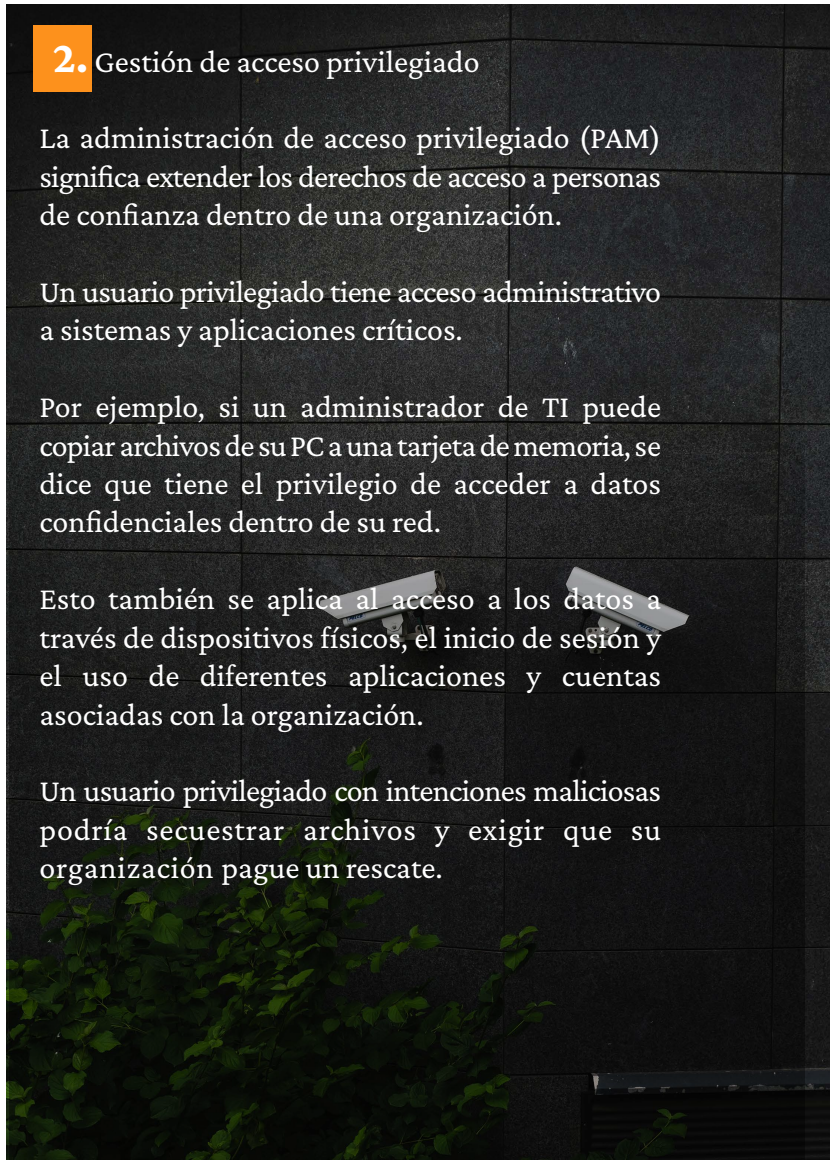
Al implementar Zero Trust, puede:

Comprenda las necesidades de acceso de su organización.

Disminuya el riesgo mediante la supervisión del tráfico de dispositivos y usuarios.

Reduzca el potencial de una violación.

Aumente profundamente la agilidad de su negocio.



2. Gestión de acceso privilegiado

La administración de acceso privilegiado (PAM) significa extender los derechos de acceso a personas de confianza dentro de una organización.

Un usuario privilegiado tiene acceso administrativo a sistemas y aplicaciones críticos.

Por ejemplo, si un administrador de TI puede copiar archivos de su PC a una tarjeta de memoria, se dice que tiene el privilegio de acceder a datos confidenciales dentro de su red.

Esto también se aplica al acceso a los datos a través de dispositivos físicos, el inicio de sesión y el uso de diferentes aplicaciones y cuentas asociadas con la organización.

Un usuario privilegiado con intenciones maliciosas podría secuestrar archivos y exigir que su organización pague un rescate.

Al implementar PAM, puede:

Haga que tratar con dispositivos y usuarios de terceros sea más seguro y accesible.

Proteja su contraseña y otras credenciales confidenciales para que no caigan en las manos equivocadas.

Elimine el exceso de dispositivos y usuarios con acceso a datos confidenciales.

Administre el acceso de emergencia cuando sea necesario.

3. Capacitación obligatoria en seguridad para empleados existentes y nuevos

No todos los ataques internos son intencionales; Algunos ocurren debido a negligencia o falta de conciencia.

Las organizaciones deben hacer obligatorio que todos sus empleados se sometan regularmente a sesiones básicas de capacitación sobre seguridad y conciencia de privacidad.

Los empleados también pueden ser interrogados sobre estas sesiones para que la capacitación sea más efectiva.

Asegurarse de que los empleados estén familiarizados con las consecuencias de costos que la negligencia puede causar a la organización puede ayudar a prevenir significativamente las amenazas internas no intencionales.

Con tanto que perder, es una maravilla que más empresas no estén tomando medidas para reducir sus posibilidades de sufrir un ataque interno.

Como se mencionó anteriormente, ningún software o herramienta en particular está detrás de los enfoques de seguridad mencionados anteriormente.

Más bien, su organización debe abordar estos aspectos mientras desarrolla una solución de seguridad propia o utiliza un servicio o producto similar de un proveedor.

Al hacerlo, puede proteger a su organización de malos actores dentro o fuera de su organización.

Sin embargo, para abordar específicamente la amenaza planteada por los iniciados que regularmente hacen un mal uso de sus credenciales de acceso o hacen funcionar dispositivos plug-and-play maliciosos, recomendamos buscar otros protocolos de seguridad, como la gestión de identidad y acceso y el análisis del comportamiento del usuario, para evitar contratiempos de seguridad interna.

Fuente de información: gbhackers.com