TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2-UNIDAD 3

Universidad Tecnológica de Pereira | faceIT

Seguridad de la autorización

Cuando un usuario se ha autenticado, se debe decidir qué puede ver y modificar y a qué sitios e información puede tener acceso. Este proceso es la autorización.

Existen varias técnicas de seguridad para administrar la autorización

Acceso condicional: Consiste en regular el acceso a un usuario basado en condiciones. Por ejemplo, si el usuario es un coordinador sí puede tener acceso a los registros de horarios de todo el personal a su cargo, pero si es un agente, solo debería tener acceso a los horarios de trabajo propios.

También se pueden establecer condiciones como el uso de equipos seguros. Por ejemplo, solamente se pueden acceder a los registros de nómina si se ingresa con un equipo autorizado en la sede central de la empresa y se es un usuario que trabaja en contabilidad. En caso de intentar ingresar con otro equipo o desde fuera de la cede, se niega el acceso.

Acceso con privilegios mínimos: Al dar acceso a los usuarios se debe validar cual es la mínima cantidad de información y de permisos que requiere. Por ejemplo, una persona que se sube a un avión solamente tiene acceso a la zona de la cabina que le permita llegar a su puesto. En ningún caso tendrá acceso a la cabina del piloto. Así mismo, al entrar a un concierto, el tiquete que porte un usuario solo le permite dirigirse a ciertas áreas dependiendo de los privilegios que ese tiquete incluyan. En seguridad informática es preferible conceder accesos restringidos y pocos privilegios ya que, si un usuario requiere de más acceso siempre avisará al administrador que necesita más permisos. Sin embargo, si un usuario tiene permisos para acceder a lugares o documentos que no debería, en muy raras ocasiones lo reportará a sus administradores. Si un usuario tiene privilegios restringidos, un atacante que logre hacerse con su cuenta y contraseña tendrá limitado el acceso para causar daños.

Desplazamiento lateral

Un atacante que accede a un sistema tiende a emplear la cuenta por la que pudo acceder para recopilar más información. De esta forma puede infiltrarse e ir

recopilando datos de otros sistemas, e incluso de usuarios con accesos más elevados. Así las cosas, un atacante puede hacerse con una cuenta que pueda instalar software, desplegar malware y atacar un sistema. Esta situación hace difícil encontrar la cuenta por medio de la cual el atacante accedió en primer lugar y permite que el atacante siga buscando nuevos puntos de acceso al interior de la red. Es similar a una persona que logra pasar el control de seguridad en la entrada de un edificio y se puede mover con libertad al interior de este.

Para mitigar los riesgos de desplazamiento lateral se suelen agregar capas de seguridad para el acceso a datos restringidos. En el ejemplo del atacante que ingresa físicamente al edificio, las capas de seguridad adicional pueden verse como puertas de acceso a sectores en los que se necesita una credencial que se debe escanear, o sistemas en los que se requiere una contraseña y una medición biométrica de la huella para que la puerta se abra limitando el acceso tanto a empleados no autorizados como a atacantes.

En seguridad informática estas capas extra de protección se implementan como más controles de acceso en donde se pide al usuario autenticación para poder acceder a pesar de que ya esté autorizado a ver otros recursos. Es decir, se pide de nuevo autenticación y se otorgan nuevos niveles de autorización.

Confianza cero

Es un modelo que permite a las organizaciones otorgar accesos seguros a los recursos. Como el nombre lo indica, nunca se confía y siempre se hacen comprobaciones antes de generar una autorización. Este modelo se basa en tres conceptos:

1. Comprobar explícitamente: Siempre que se quiera acceder a un recurso, se debe autenticar y autorizar por completo a un usuario. Se suele usar autenticación de múltiples factores y se garantiza el acceso condicional al recurso.

2. Se concede acceso de privilegios mínimos: Al autorizar un usuario para un recurso, solo se garantiza el mínimo de privilegios sobre el recurso. Con esto se limitan los daños de potenciales atacantes y se reduce el desplazamiento lateral.

3. Asumir vulneraciones: Se suele asumir que existen vulneraciones o que se pueden producir. De esta forma se suelen reestructurar los accesos y las medidas de seguridad que eviten a un atacante propagarse en una red interna.