Introducción a la Ciberseguridad

Ciberseguridad – FPUNA

Modelos de control de acceso

Modelos de Control de Acceso

- Un modelo de control de acceso es un conjunto definido de criterios que un administrador del sistema utiliza para definir derechos/permisos de los usuarios del/al sistema.
- Hay tres modelos principales de control de acceso:
  - Control de Acceso Obligatorio (Mandatory Access Control - MAC),
  - Control de Acceso Discrecional (Discretionary Access Control - DAC), y
  - Controles de Acceso Basado en Roles (Rule Based Access Control - RBAC).
- Además, una regla de control de acceso basado en roles (RBAC) es útil para la gestión de permisos a través de sistemas múltiples.

Control de Acceso Obligatorio

- En el modelo de control de acceso obligatorio se asignan las funciones de los usuarios estrictamente de acuerdo a indicado por el administrador del sistema. Este es el método de control de acceso más restrictivo, porque el usuario final no puede establecer controles de acceso en los archivos. El Control de acceso obligatorio es muy popular en ambientes/instalaciones altamente secretas, como la industria de defensa donde los archivos «perdidos» pueden afectar a su seguridad nacional.

Control de Acceso Discrecional

- El control discrecional de acceso esta en el otro extremo del espectro de acceso, diferente del modelo de acceso obligatorio, ya que es el menos restrictivo de los tres modelos. En el marco del modelo de acceso discrecional el usuario final tiene total libertad para asignar los derechos a los objetos que desea.
- Este nivel de control completo sobre los archivos puede ser peligroso porque si un atacante o algún Malware compromete la cuenta a continuación, el usuario malicioso o código tendrá un control completo también.

Controles de Acceso Basado en Roles

- La Función de control de acceso basado en permisos o Roles crea la asignación de derechos/permisos de acceso a funciones o trabajos específicos dentro de la empresa; RBAC a continuación, asigna funciones a los usuarios, con lo que le concede privilegios.
- Este modelo de control de acceso a las funciones de manera efectiva en las organizaciones reales es, debido a que a los archivos y los recursos se le asignan los permisos de acuerdo a las funciones que lo requieran. Por ejemplo, un administrador del sistema puede crear una función de acceso para los gerentes solamente. Así, un usuario se le tendría que ser asignado el papel de un gerente para utilizar esos recursos.

Confidencialidad, integridad, disponibilidad, acceso, autenticación, autorización, no repudio, privacidad

Confidencialidad

(Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Integridad

(Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

Disponibilidad

(Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Acceso y Control de Acceso

El control de acceso es una forma de limitar el acceso a un sistema o a recursos físicos o virtuales. En informática, el control de acceso es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios a los sistemas, recursos o información.

En los sistemas de control de acceso, los usuarios deben presentar credenciales antes de que se les otorgue acceso. Dentro de los sistemas físicos, estas credenciales pueden tener muchas formas, pero las credenciales que no se pueden transferir brindan la mayor seguridad.

Control de Acceso

Para la seguridad informática, el control de acceso incluye la **autorización**, **autenticación** y **auditoría** de la entidad que intenta obtener acceso. Los modelos de control de acceso tienen un sujeto y un objeto. El sujeto, el usuario humano, es el que intenta obtener acceso al objeto, generalmente el software.

Una lista de control de acceso contiene una lista de permisos y los usuarios a quienes se aplican estos permisos.

Funcionamiento Control de Acceso

Las fases por las que se debe pasar en un sistema de control de acceso son las siguientes:

1. **Autenticación**
2. **Autorización**
3. **Acceso**
4. **Administración del Control de Acceso**
5. **Auditoría**

Autenticación

(Inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

En primer lugar, se autentica una credencial. Después de que un usuario presenta una credencial (credencial móvil o tarjeta) en un lector, los datos de esa credencial se envían a la Unidad de Control de Acceso (ACU), y esta determina si el sistema conoce y reconoce esta credencial.

Autorización

A continuación, la ACU determina si el usuario al que pertenece esta credencial válida está autorizado para acceder.

¿Tiene acceso el usuario a esta entrada en particular? ¿Están utilizando el tipo correcto de credencial y tipo de disparador para esta entrada? ¿Están intentando desbloquear la entrada dentro de los horarios aplicables?

Para ser autorizado, un usuario debe:

1. Tener acceso a la entrada que intentan desbloquear
2. Utilizar uno de los tipos de credenciales permitidos predefinidos
3. Usar uno de los tipos de activadores permitidos predefinidos
4. Realizar la solicitud de desbloqueo dentro de los horarios definidos en la entrada o asignados al usuario o su grupo

Acceso

Una vez autenticada y autorizada, la ACU envía un comando al hardware de bloqueo de la puerta para desbloquear la entrada.

En el caso de las cerraduras electromagnéticas, la energía se interrumpe temporalmente cuando se desbloquea, mientras que con los golpes de la puerta se aplica energía temporalmente para desbloquear la puerta (también conocida como seguridad a prueba de fallos).

Administración del Control de Acceso

Administrar un sistema de control de acceso incluye agregar o eliminar entradas, usuarios, credenciales, cronogramas y alertas utilizando un software administrativo que se sincroniza automáticamente con las ACU conectadas a Internet.

Los sistemas de control de acceso basados en la nube más nuevos se integran con servicios de directorio como Google G Suite y Azure Active Directory, agilizando el proceso de administración. También proporcionan la mayor flexibilidad para mejoras de servicio en comparación con los sistemas heredados que se basan en el cliente-servidor.

Auditoría

- Los administradores pueden auditar los sistemas de control de acceso mediante la generación de informes para registros de acceso, incluida la actividad del usuario y la actividad de entrada.
- Esto es útil para revisiones generales del sistema; asegurando que el sistema funcione como se espera y que no haya problemas para acceder a las entradas.
- Los informes también son útiles para cumplir con los estándares de cumplimiento que requieren un cierto nivel de control de acceso físico. Los sistemas de control de acceso que se integran con los Sistemas de gestión de visitantes, Sistemas de gestión de vídeo y otras plataformas de tipo de seguridad proporcionan capacidades de auditoría adicionales.

No Repudio

Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen.

Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Privacidad

- Las medidas de ciberseguridad existen para proteger la información en el entorno digital y entre esa información a proteger está también la información personal o de carácter confidencial que manejan organizaciones privadas, organismos públicos y también los propios particulares.
- Sin esas medidas de ciberseguridad, sería imposible poder garantizar tanto la seguridad en Internet como la **privacidad** digital. Y, aunque es cierto que no podemos hablar de medidas de seguridad cien por cien infalibles (el riesgo cero nunca existe), sí podemos afirmar que la adopción e implantación de medidas técnicas y organizativas de ciberseguridad contribuyen a mantener privada y confidencial la información (sea esta personal, empresarial, comercial, gubernamental, etc.).

Aspectos legales

Aspectos legales

- Las medidas legales, es decir, leyes, normas y reglamentos que obligan a todo tipo de organizaciones a tener en marcha medios y mecanismos que garanticen **la ciberseguridad, la seguridad de la información y la privacidad**, es decir, recurrir a herramientas y soluciones que protejan la información personal de las personas.
- Las medidas de ciberseguridad se convierten en el muro a franquear por los cibercriminales (y otros posibles actores interesados) para poder acceder a la información confidencial que protege, información que puede, en ocasiones, convertirse en la escalera que permita superar ese muro de seguridad.

Ética asociada a la ciberseguridad

Ética

- La ética es una estructura de estándares y prácticas que influyen en cómo las personas llevan sus vidas. No se implementa estrictamente para seguir esta ética, pero es básicamente para el beneficio de todo lo que hacemos.
- La ética es diferente a las leyes que ordenan legalmente lo que está bien o mal. La ética ilustra los puntos de vista de la sociedad sobre lo que está bien y lo que está mal.

Ética informática

La ética informática es un conjunto de normas morales que rigen el uso de las computadoras. Son las opiniones de la sociedad sobre el uso de las computadoras, tanto de hardware como de software. Las preocupaciones sobre la privacidad, los derechos de propiedad intelectual y los efectos en la sociedad son algunos de los problemas comunes de la ética informática.

¿Por qué es necesaria la ciberética?

En la actualidad, con un mundo hiperconectado, la ciberética es necesaria para luchar contra las siguientes amenazas:

1. Aumento del delito cibernético
2. Aumento del comportamiento poco ético
3. Espionaje
4. Amenaza a la privacidad
5. Fraudes
6. Propiedad
7. Derechos de propiedad intelectual
8. Gestión de derechos digitales (DRM)
9. Accesibilidad, censura y filtrado
10. Libertad de información
11. Brecha digital

¿Quién debería preocuparse por la ética cibernética?

- Desde un usuario novato que recién comienza a navegar en una computadora e internet hasta cualquier profesional cuyo trabajo requiere el uso necesario de internet, todos deben estar familiarizados con el término ciberética.
- Así como cada cultura enseña a su conjunto cultural de personas a mantener un comportamiento ético en las organizaciones, los negocios y la gobernanza, de manera similar, a los usuarios en línea/digitales se les debe enseñar la importancia de la ciberética y cómo emplearla en su vida diaria y cumplir con sus términos.