Seguridad y privacidad en redes - Practica 1

Franco Dalla Gasperina

Agosto 2025

1 ¿Cuál es la diferencia entre seguridad y privacidad?

Ambos terminos engloban distintos significados. Puede considerarse también que la privacidad es algo englobado dentro de la seguridad incluso. La seguridad entonces, podría considerarse como las distintas prácticas para mantener seguro algo(entorno, información, entre otras cosas), mientras que la privacidad consistiría en el estado o la practica para mantenerlas accesibles a los usuarios correspondientes.

1.1 Seguridad

Sobre la seguridad hay conceptos universales a tener en cuenta, estos son:

- Mínimo privilegio: Este principio consiste en que los permisos otorgados a un sujeto deben estar basados en las necesidades de los mismos.
- Valores por omisión seguros: A menos de que se le asigne un objeto a un individuo explícitamente. Este debe ser denegado en caso de ser solicitado.
- Economía de mecanismos: Los mecanismos de seguridad deben ser lo más simple posible.
- Mediación completa: Todos los accesos a objetos deben poder auditarse.

1.2 Privacidad

La privacidad de la información se refiere al derecho de los individuos y las organizaciones a controlar cómo se recopila, usa, almacena y comparte su información personal o confidencial.

2 Defina y relacione los conceptos de vulnerabilidad, amenaza e incidente.

- Confidencialidad: Garantiza que la información sólo sea accesible por las personas autorizadas.

- Integridad: Garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo
- Disponibilidad: Garantiza que los usuarios autorizados tienen acceso a la información y recursos relacionados cuando lo necesiten.

3 ¿A qué se hace referencia con el concepto de "seguridad en capas" y "zero trust"? ¿Considera que están relacionados?

3.1 seguridad en capas

La seguridad en capas consiste en organizar las practicas de seguridad para cada capa del modelo tradicional de internet. Un enfoque posible seria el siguiente:

- Seguridad a nivel de sistema: Las medidas de seguridad de sistema representan la última línea de defensa contra un problema de seguridad relacionado con Internet. Por lo tanto, el primer paso de una estrategia de seguridad en Internet completa debe ser configurar debidamente la seguridad básica del sistema.
- Seguridad a nivel de red: Las medidas de seguridad de red controlan el acceso sistemas de red. Cuando conecta la red a Internet, debe asegurarse de que tiene implantadas las debidas medidas de seguridad adecuadas a nivel de la red para proteger los recursos internos de la misma contra la intrusión y el acceso no autorizado. El medio más común para garantizar la seguridad de la red es un cortafuegos. El proveedor de servicios de Internet (ISP) puede proporcionar una parte importante del plan de seguridad de la red. El esquema de seguridad de la red debe indicar qué medidas de seguridad proporciona el ISP, como las reglas de filtrado de la conexión del direccionador del ISP y las medidas de precaución del sistema de nombres de dominio (DNS) público.
- Seguridad a nivel de aplicaciones: Las medidas de seguridad a nivel de aplicaciones controlan cómo pueden interactuar los usuarios con las aplicaciones. En general, tendrá que configurar valores de seguridad para cada una de las aplicaciones que utilice. Sin embargo, conviene que preste una atención especial al configurar la seguridad de las aplicaciones y los servicios que utilizará de Internet o que proporcionará a Internet. Estas aplicaciones y servicios son vulnerables al mal uso por parte de los usuarios no autorizados que buscan una manera de acceder a los sistemas de la red. Las medidas de seguridad que decida utilizar deberán incluir los riesgos del lado del servidor y del lado del cliente.
- Seguridad a nivel de transmisión: Las medidas de seguridad a nivel de transmisión protegen las comunicaciones de datos dentro de la red y entre

varias redes. Cuando se comunica en una red que no es de confianza como Internet, no puede controlar cómo fluye el tráfico desde el origen hasta el destino. El tráfico y los datos transportados fluyen a través de distintos sistemas que están fuera de su control. A menos que configure medidas de seguridad como, por ejemplo, la configuración de las aplicaciones para utilizar TLS (Transport Layer Security), los datos direccionados están disponibles para que cualquiera pueda verlos y utilizarlos. Las medidas de seguridad a nivel de transmisión protegen los datos mientras fluyen entre los límites de otros niveles de seguridad.

3.2 zero trust

Refiere a una estrategia de seguridad de red basada en la filosofía de que ninguna persona o dispositivo dentro o fuera de la red de una organización debe tener acceso para conectarse a sistemas hasta que se considere explícitamente necesario.

4 Busque noticias sobre algún incidente de seguridad de la información de público conocimiento. Identifique cuál fue el bien afectado, qué error permitió el problema y qué se podría haber realizado para evitar el mismo.

Recientemente ocurrio un leak bastante grande a una empresa desarrolladora de videojuegos llamada Gamefreak. Esta empresa es conocida por ser la desarrolladora de los videojuegos de Pokemón. Entre todo el material filtrado se encontraba: Arte conceptual, prototipos de videojuegos, herramientas de desarrollo, repositorios utilizados por la empresa; información sobre futuros juegos, etc. mediante esta filtración en especifico también se conoció sobre los planes de Nintendo (empresa con la que están muy relacionados) sobre el plan de crear una nueva consola de videojuegos que reemplace a la Nintendo Switch. Este ejemplo funciona para relacionarlo con el concepto de confidencialidad ya que se divulgo mucho material que no se planeaba fuera público y que podría afectar a la empresa en imagen o economicamente. Se teoriza que la filtración se dio por un acceso no permitido a un servidor de archivos del que hacía uso la empresa. El acceso al mismo se dio por haber descubierto un gitlab privado en el que se publicaron accidentalmente credenciales de acceso para el servidor. Una forma de haber evitado esto podría haber sido agregar más seguridad (o seguridad por capas, podría pensarse) para el servidor de archivos, como filtros de direcciones IP, hacer uso de VPN, entre otras. También tener herramientas para detección de filtrado de credenciales en el gitlab.

5 Analice los riesgos introducidos en una organización por el uso de redes sociales y mensajería instantánea. Relacione con ingeniería social y ciberinteligencia. Dé al menos un ejemplo que se haya judicializado.

Los riesgos introducidos a causa de estas aplicaciones son muchos. Es común las malas practicas en organizaciones en relación a información que debería ser privada y el uso de estas. Por ejemplo, empleados enviando credenciales mediante WhatsApp. En caso de que se roben las cookies de una sesión de WhatsApp web, un atacante podría ver la información compartida. También, el uso de este medio para la transmisión de información confidencial es una muy mala práctica. Podría causar que empleados caigan más fácilmente en estafas basadas en ingeniería social o ataques de phishing o spear phishing.

6 Gestión de accesos y privilegios. Definir y describir brevemente los siguientes conceptos:

- IAM(Identity and access management): Gestion de identidad y acceso. Herramientas y prácticas de este tipo ayudan a garantizar que las personas adecuadas puedan acceder a los recursos adecuados por las razones correctas en el momento adecuado (DIOS, QUIEN ESCRIBIO ESTO KJJJJ) Segun el sitio de cloudfare: Es un modo de administrar un conjunto dado de identidades digitales de los usuarios y los privilegios asociados a cada identidad.
- PAM(Privileged Access Management): Gestión de acceso privilegiado. Esta práctica consiste en el control de los usuarios con acceso privilegiado para controlar que hagan el uso debido de sus funciones.
- PIM(Privileged Identity Management): Gestión de identidad privilegiada. Esta práctica esta enfocada en controlar a los usuarios con permisos elevados de que cambien configuraciones y modifiquen los accesos deseados al sistema. Generalmente soluciones a esto son monitoreo o distribuir las permisiones en distintos roles para evitar tener roles administrador con mucho poder en un sistema.
- IGA(Identity Governance and Administration): Gobernanza y administración de identidades. Esta permite a administradores de seguridad manejar de manera eficiente identidades de los usuarios y su acceso en todo un sistema. Aparte de permitir la posibilidad de implementar los controles necesarios para evitar accesos inapropiados o riesgosos.

- BYOI(Bring Your Own Identity): Pone tu propia identidad. Esta práctica consiste en delegar la tarea de autenticación a un tercero. Un claro ejemplo de esto es Oauth para autenticarse con google en distintos sitios.
- Password Less: Literalmente falta de contraseña. Es la práctica de realizar autenticación en un sistema sin hacer uso de contraseñas. Ejemplos de esto son el uso de datos biométricos, tarjetas de acceso, entre otros.
- Factores de autenticación: Distintas formas de autenticarse, tales como por biometría(información biológica única de cada ser humano), número de teléfono o la posesión de un dispositivo.
- MFA(Multi Factor Autentication): Autenticación multi factor. Consiste en dividir la autenticación en etapas o pasos. Requiriendo que se realice la totalidad, o un porcentaje aceptable de las mismas para lograr autenticarse en un sistema.
- SSO(Single Sign-On): Inicio de sesión único. Práctica que consiste en brindar acceso a un usuario a multiples aplicaciones, herramientas y sistemas mediante un único set de credenciales. Centralizando este proceso. Teoricamente, esta práctica seria favorable al evitar multiples cuentas en otros sistemas (menos seguros) en las que el usuario podría repetir las credenciales que podrian verse expuestas ante vulnerabilidades o filtraciones.
- OTP(One-Time Password): Contraseña de un solo uso / de una sola vez. Consiste en la generación de contraseñas mediante aleatoriedad que solo sean funcionales para autenticarse una vez. Tras hacer uso de la misma, esta sería inhabilitada.
- Framework AAA(Authentication, Authorization, Accounting): Marco de trabajo cuyo objetivo es proveer estas tres características a un sistema.