Caso 2

Infraestructura computacional.

Tabla de contenido

[1. Análisis y entendimiento del problema 1](#_Toc448088869)

[1.1. Amenazas 1](#_Toc448088870)

[1.1.1. Un empleado autorizado hace cambio de la información de Time & Attendance 1](#_Toc448088871)

[1.1.2. Una aplicación móvil envía datos falsos 2](#_Toc448088872)

[1.1.3. Un atacante utiliza Time & Attendance para modificar el código fuente del servidor dos 2](#_Toc448088873)

[1.1.4. Ataque DoS al servicio Time & Attendance 2](#_Toc448088874)

[1.1.5. Se presenta un caso de spoofing 2](#_Toc448088875)

[1.2. Vulnerabilidades 2](#_Toc448088876)

[1.2.1. Supervisor de campo o agente no cambia la contraseña dada por defecto de su cuenta 2](#_Toc448088877)

[1.2.2. Un agente de campo recibe más privilegios de los necesarios 2](#_Toc448088878)

[1.2.3. Un supervisor recibe más privilegios de los necesarios 2](#_Toc448088879)

[1.2.4. Buffer Overflow 3](#_Toc448088880)

[1.2.5. Phishing 3](#_Toc448088881)

[2. Propuesta de Soluciones 3](#_Toc448088882)

[2.1. Un empleado autorizado hace cambio de la información de Time & Attendance 3](#_Toc448088883)

[2.2. Una aplicación móvil envía datos falsos 3](#_Toc448088884)

[2.3. Un supervisor recibe más privilegios de los necesarios 3](#_Toc448088885)

[2.4. Ataque DoS al servicio Time & Attendance 3](#_Toc448088886)

[2.5. Se presenta un caso de spoofing 3](#_Toc448088887)

# Análisis y entendimiento del problema

# Amenazas

# Un empleado autorizado hace cambio de la información de Time & Attendance

Si un usuario autorizado cambia los datos que se encuentran en el segundo servidor especialmente los de time & Attendance podría eventualmente modificar las horas y coordenadas de los trabajadores haciendo que algunos sean despedidos injustamente u otros pagados sin hacer nada. Si esta amenaza de consolida el servicio de información de Time & Attendance no ofrecería ni integridad, ni confidencialidad ni no repudio ni autenticación de fuente ni destino. Es decir la aplicación de time & Attendance no serviría.

# Una aplicación móvil envía datos falsos

Un atacante es capaz de cambiar el código fuente de su aplicación móvil para que esta modifique los datos antes de ingresarlos a memoria. Si esta amenaza se consolida sería catastrófico para todo el sistema puesto que no se tendría confiabilidad en los datos reportados en la aplicación Time & Attendance

# Un atacante utiliza Time & Attendance para modificar el código fuente del servidor dos

Un atacante es capaz de modificar el código fuente de la aplicación time & Attendance para acceder al sistema operativo del servidor dos. Si esta amenaza se consolida todos los servicios provistos por el servidor no serían confiables y la empresa tendría problemas puesto que no sabrían si sus agentes y supervisores de campo están haciendo su trabajo

# Ataque DoS al servicio Time & Attendance

Un atacante podría hacer ataques de negación de servicio bloqueado los servicios de Time & Attendance. Si esta amenaza se consolida los agentes y supervisores de campo no tendrán forma de reportarse, además eventualmente el procesamiento en el servidor dos seria solo de peticiones de Time & Attendance por lo cual el servicio de correo electrónico también podría verse negado.

# Se presenta un caso de spoofing

En el portal web, se puede presentar el caso de suplantación (spoofing) en este caso el empleado podría acceder a información a la cual no tiene acceso autorizado, así accediendo a la información de clientes y otros datos importantes para la empresa.

# Vulnerabilidades

# Supervisor de campo o agente no cambia la contraseña dada por defecto de su cuenta

Al recibir la aplicación móvil el agente o supervisor de campo no cambian su contraseña dada por defecto. Esto causa que

# Un agente de campo recibe más privilegios de los necesarios

Un agente de campo solo debe poder reportar su posición y no más. Si un agente de campo puede consultar las posiciones y horas de otros agentes y supervisores eventualmente podría hacer una negación de la consulta de estos servicios.

# Un supervisor recibe más privilegios de los necesarios

Un agente supervisor solo debe poder reportar la posición de sus subordinados y la propia. Si este puede consultar las posiciones y fechas de otros agentes y supervisores y modificarlos eventualmente podría hacer que la integridad del sistema se pierda además de poder hacer una negación de servicios.

# Buffer Overflow

Existe la posibilidad de que el buffer se desborde (Buffer Overflow) y así se pierda información del sistema, en este caso no sólo se pierde información importante si no que si se pierde, no se sabe qué información fue la que se perdió y esto puede afectar a cualquiera de las 3 aplicaciones que estamos evaluando ya que todas almacenan información importante.

# Phishing

No se puede tener certeza que un empleado o cliente esté accediendo a la legitima Pagina Web de la empresa, otra página web podría hacerse pasar por la nuestra y el cliente al acceder a está estaría revelando información personal de él a un tercero.

# Propuesta de Soluciones

# Un empleado autorizado hace cambio de la información de Time & Attendance

Manejo de responsabilidades (separación de privilegios/privilegios mínimos) y uso de contraseñas; todo tipo de usuario tendrá un rol y cada rol tendrá diferentes responsabilidades y autorizaciones, extra a esto, se manejaran registros de las tareas autorizadas, un log de todo lo que se hace de modo que si le logra la adulteración de información se sabrá quién o por lo menos de qué usuario y en qué momento sucedió.

# Una aplicación móvil envía datos falsos

Para esta amenaza implementaremos niveles de defensa tales como Firewalls, IDS y antispywares de modo que se restringirá el acceso de atacantes y más importante aún se cifraran los mensajes que se manejen con los servidores con llaves asimétricas de modo que se pueda saber si el mensaje enviado es o no por uno de los empleados de la empresa al hacer el descifrado con las llaves publicas correspondientes.

# Un supervisor recibe más privilegios de los necesarios

En este caso separaremos y minimizaremos los privilegios, de este modo un supervisor no podrá recibir más privilegios de los que son seguros que tenga.

# Ataque DoS al servicio Time & Attendance

Para esta amenaza implementaremos niveles de defensa tales como Firewalls, IDS y antispywares de modo que se restringirá el acceso de atacantes.

# Se presenta un caso de spoofing

Uso de llaves simétricas, todo mensaje almacenado estará cifrado con una llave asimétrica de modo que esta información no podrá ser leída por ningún empleado que no disponga de la autorización. Esta llave sólo la conoce quien o quienes sí estén autorizados a conocer dicha información