LABORATORIO 13 CYBERSEGURIDAD

CASO 1: Robo de credenciales por phishing en una entidad educativa

Escenario:

Un estudiante recibe un correo aparentemente institucional con un enlace a una supuesta plataforma de calificaciones. Al ingresar sus credenciales, estas son capturadas por un tercero. Al día siguiente, se detecta que alguien accedió con esas credenciales a los registros de notas y los modificó.

Detalles clave:

- Plataforma afectada: sistema académico web.
- No existe segundo factor de autenticación (2FA).
- No hay filtros de spam o análisis de enlaces en los correos entrantes.
- Usuarios no han recibido capacitación en ciberseguridad.

Activos:

Notas de los estudiantes

Información personal de los estudiantes CC, Nombre, etc.

Amenazas:

Phishing: El correo que se envió al estudiante

Acceso no autorizado: El atacante al ingresar con las credenciales del estudiante

Vulnerabilidades

- No existe un segundo factor de autenticación
- No hay filtros de spam
- Los usuarios no han recibido la capacitación de ciberseguridad

Impactos

El atacante pudo ingresar con las credenciales del estudiante y por ende cambio las notas de los estudiantes

Probabilidad

Alta ya que, si una persona detecta que puede ingresar a esta plataforma de esa forma, podría hacer lo mismo que hizo el atacante

Nivel de Riesgo

Alto ya que la plataforma tiene muchas vulnerabilidades de las cuales el atacante puede aprovechar y acceder a ella.

Medidas de tratamiento

1. Solucionar la autentificación doble factor
2. Hacer un filtrado y análisis del spam del correo afectado
3. Darles clases de ciberseguridad básica a los estudiantes

CASO 2: Ransomware en una clínica odontológica

Escenario:

Un empleado abre un archivo adjunto en un correo que aparenta ser una factura.
Inmediatamente, el sistema muestra un mensaje de que todos los archivos han sido cifrados.
Piden un rescate en criptomonedas. La clínica no cuenta con respaldos automáticos actualizados.

Detalles clave:

- Archivos clínicos, administrativos y financieros cifrados.
- Software antivirus caducado.
- Sin políticas de copia de seguridad.
- Sin segmentación de red.
- El ransomware se propaga a todas las estaciones de trabajo.

Activos:

Archivos clínicos, administrativos y financieros

Amenazas:

Phishing: El correo que le enviaron al empleado sobre la factura.

Rasomware: Cuando el sistema pide las criptomodenas para recuperar los datos.

Vulnerabilidades

- Software antivirus caducado
- Sin políticas de copia de seguridad
- Sin segmentación en la red

Impactos

El atacante pudo ingresar a los archivos de la clínica y gracias a eso está pidiendo dinero a cambio de recuperarla, y esto afecta no solo a los trabajadores de la clínica sino también a las personas que necesitan de este servicio

Probabilidad

Muy Alta Debido a que las clínicas es un punto donde ingresa muchas personas y alguna de estas puede conocer el sistema y atacarlo para aplicar el rasomware y a si afectar a la clínica

Nivel de Riesgo

Muy Alto ya que el sistema está muy débil por muchos lados lo que significa que cualquiera con conocimientos previos puede atacar cuando quiera y cuando pueda

Medidas de tratamiento

1. Actualizar el antivirus a la última versión.
2. Hacer siempre un respaldo para los datos mediante la copia de seguridad
3. Segmentar la red para todos los sistemas que conectan directamente con el computador principal

CASO 3: Acceso no autorizado a cámara IP de una empresa

Escenario:

Una empresa de seguridad privada instala cámaras IP para monitoreo remoto. Sin embargo, no cambian las contraseñas por defecto ni actualizan el firmware. Un atacante logra visualizar transmisiones en vivo desde una interfaz web abierta al público.

Detalles clave:

- Acceso remoto habilitado vía HTTP sin autenticación segura.
- Firmware desactualizado con vulnerabilidades conocidas.
- Contraseñas por defecto ("admin/admin").
- El sistema no genera alertas ni logs de acceso.

Activos:

Datos de la empresa de seguridad privada

Amenazas:

Ataque de fuerza bruta: Ya que el atacante puede adivinar las contraseñas de las cámaras de seguridad.

Acceso no autorizado: El atacante visualiza el contenido de las cámaras sin permiso

Vulnerabilidades

- Utilización de HTTP
- Firmware desactualizado
- Contraseña insegura
- El sistema no genera alertas ni logs de acceso

Impactos

El atacante puede visualizar el contenido de las cámaras de seguridad y este puede realizar un ataque mayor en un futuro.

Probabilidad

Alta ya que, si alguna persona con conocimientos llega a detectar esta vulnerabilidad, puede afectar seriamente a la empresa privada.

Nivel de Riesgo

Muy alto, debido a que si se llega a saber lo que hay dentro de la empresa el atacante puede hacer un gran daño a la empresa gracias a estos videos.

Medidas de tratamiento

1. Utilizar HTTPS para mejorar la seguridad
2. Actualizar el firmware para hacer uno más robusto
3. Tener una contraseña menos predecible de por lo menos 12 caracteres
4. Administrar el sistema para que genere alertas en caso de ingresos

CASO 4: Uso indebido de información personal en una alcaldía

Escenario:

Un contratista accede a bases de datos con información personal de ciudadanos para “validar datos”. Después se descubre que vendía esta información a una empresa de marketing. La alcaldía no tenía controles para registrar el acceso a datos sensibles.

Detalles clave:

- No existen registros de logs ni auditoría.
- Acceso a bases de datos sin niveles de privilegio.
- Sin política de clasificación de la información.
- No se realizaron acuerdos de confidencialidad con el contratista.

Activos:

Información de datos personales de los ciudadanos

Amenazas:

Interna: El contratista que trabaja en la alcaldía.

Acceso no autorizado: El contratista ingresa a los datos de los ciudadanos, cuando este no puede hacer esto.

Vulnerabilidades

- No hay alertas de ingreso ni auditorias
- No ha niveles de privilegios en la base de datos
- No hay políticas de clasificación de la información
- No hubo ningún acuerdo con el contratista sobre la confidencialidad.

Impactos

El contratista divulga la información de los empleados a la empresa marketing con el fin de obtener ganancias con base a los gustos de los ciudadanos

Probabilidad

Muy Alta debido a que las amenazas más peligrosas siempre son las internas, y cualquier persona que acceda a la base de datos, puede obtener mucha información valiosa de esta.

Nivel de Riesgo

Muy Alto, todo esto porque las bases de datos no tienen seguridad y cualquiera puede acceder a ella sin ningún problema.

Medidas de tratamiento

1. Programar al sistema para que de alertas en caso de que haya ingreso.
2. Dar privilegios en la base de datos
3. Hacer políticas de clasificación de la información
4. Darle a entender al contratista sobre sus privilegios y lo único que puede hacer en el sistema

CASO 5: Corte de servicio por ataque DoS a sitio web institucional

Escenario:

El sitio web de una universidad sufre una caída durante el proceso de inscripciones. El análisis revela un ataque de denegación de servicio (DoS) lanzado desde múltiples IPs, provocando la caída del servidor durante 8 horas.

Detalles clave:

- No existían medidas de mitigación como WAF o protección DoS.
- El servidor web estaba sobrecargado y sin alta disponibilidad.
- No había monitoreo en tiempo real.
- No se informó al área de sistemas hasta pasadas 3 horas.

Activos:

La plataforma de la universidad, los servidores de la página.

Amenazas:

DOS: El ataque de varios dispositivos a la plataforma, que sobrecargaron el sistema y provocaron el colapso de este.

Vulnerabilidades

- No hay medidas de mitigación como WAF o Protección DOS
- Servidor web muy sobrecargado
- No hay monitoreo en tiempo real
- Se demoraron mucho en notificar el colapso de la plataforma

Impactos

Se colapsó toda la plataforma, lo que provoco que causo que muchos estudiantes o profesores de la universidad, no pudieron acceder al sitio web

Probabilidad

Media pues muy pocos atacantes van a hacer este tipo de ataque, pero si hay posibilidad de que ocurra en dado caso se dan cuenta de este detalle.

Nivel de Riesgo

Alto pues si la plataforma se afecta con este ataque, colapsara provocando que muchas personas no puedan acceder a este durante un buen tiempo.

Medidas de tratamiento

1. Usar un buen WAF para contrarrestar este ataque
2. Monitorear en tiempo real las peticiones y detectar el pico en caso de que ocurra el ataque.
3. Una vez detectado el ataque se debe notificar a los estudiantes lo ocurrido, para que ellos se enteren y comprendan lo que está sucediendo