LABORATORIO TECH 13

JESUS DAVID DE LA HOZ PEÑA

UNIVERSIDAD POPULAR DEL CESAR

VALLEDUPAR

2025

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

Activo: Sistema académico web (Plataforma de calificaciones)

Amenazas: El correo que llega pareciendo legitimo

Vulnerabilidades: no presenta autenticación de segundo factor, no hay capitación y no hay filtro de spam a los correos entrantes

Impactos: Cambios en los datos de la plataforma de forma no autorizada

Probabilidad: 50%

Nivel de riesgo: 8

Medida de tratamiento: Aislar el pc afectado, bloquear la cuenta afectada, ver que no haya sido mas nada afectado, hacer una recuperación de seguridad y cambiar las credenciales del estudiante afectado

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.

Activo: Sistema de la clínica

Amenaza: El archivo adjunto al correo

Vulnerabilidades: No hay copia de seguridad, falta de capacitación para no abrir adjuntos desconocidos

Impactos: Cifrado de archivos importantes del sistema

Probabilidad: 80%

Nivel de riesgo: 9

Medida de tratamiento: Habria 2 opciones, pagar el rescate confiando en que devolverán los datos e implementar para futuros sucesos, actualizar el antivirus y capacitar

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.

Activo: Camaras

Amenaza: hacker de camara

Vulnerabilidades: No cambiar la contraseña

Impactos: Introduccion y poder ver las cámaras en vivo

Probabilidad: 60%

Nivel de riesgo: 6

Medida de tratamiento: Implementar autenticación segura y cambiar contraseña frecuentemente

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.

Activo: Base de datos de ciudadanos

Amenaza: Robo de informacion

Vulnerabilidades: No presentaba auditoria de lo que se hacia en la base ni acuerdos de confidencialidad

Impactos: Venta a otra empresa la información personal de los ciudadanos

Probabilidad: 90%

Nivel de riesgo: 9

Medida de tratamiento: Colocar logs y auditoria para ver que se hacen con los datos, ya sea editar, ingresar eliminar o descargar

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.

Activo: Sitio web de la universidad

Amenaza: Ataque DoS

Vulnerabilidades: No había monitore en tiempo real y no tener medidas de mitigacion

Impactos: Caida del servidor y no disponibilidad

Probabilidad: 95%

Nivel de riesgo: 9

Medida de tratamiento: Colocar medidas WAF y análisis en tiempo real