Saul Hernandez Castilla

Laboratorio 13

Escenario 1

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.

Caso	Activos	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Niveles de Riesgo	Medidas de Tratamiento
Phishing a estudiante con acceso al sistema académico	• Credenciales del estudiante • Sistema académico • Registros de notas	Envío de correos de phishing para robo de credenciales	- Falta de 2FA - Falta de filtros de spam - Usuarios no capacitados en ciberseguridad	- Alteración de registros - Pérdida de confianza institucional - Daño a la integridad académica	Alta	Crítico	- Implementar 2FA en el sistema académico - Capacitación en ciberseguridad - Filtros anti-phishing y sandboxing en correos.

Saul Hernandez Castilla

Escenario 2

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.

Caso	Activos	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Niveles de Riesgo	Medidas de Tratamiento
Ransomware en la clínica por apertura de archivo malicioso	• Archivos clínicos, • Administrativos y financieros • Estaciones de trabajoRed interna de la clínica	Envío de ransomware vía correo con archivo malicioso	- Antivirus caducado - Falta de políticas de respaldo - Red sin segmentación - Usuarios no capacitados	- Pérdida total de datos Interrupción de operacion - Pérdida financiera y de confianza - Posible filtración de datos sensibles	Muy alta	Crítico	- Implementar respaldos automáticos y fuera de línea - Renovación de antivirus y software de seguridad - Segmentación de red- Políticas y simulaciones de phishing- Plan de respuesta a incidentes

Saul Hernandez Castilla

Escenario 3

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.

Caso	Activos	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Niveles de Riesgo	Medidas de Tratamiento
Acceso no autorizado a cámaras IP de seguridad privada	Cámaras IPPlataforma de monitoreoPrivacidad de clientes	Acceso no autorizado a transmisiones en vivo	- Contraseñas por defecto - Firmware desactualizado - Acceso HTTP sin seguridad - Sin logs ni alertas	- Violación de privacidad - Daño reputacional - Riesgo legal y de cumplimiento	Alta	Crítico	- Cambiar contraseñas por defecto - Actualización periódica de firmware- Habilitar HTTPS y autenticación fuerte- Configurar logs y alertas - Segmentación de red de dispositivos IoT

Saul Hernandez Castilla

Escenario 4:

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.

Caso	Activos	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Niveles de Riesgo	Medidas de Tratamiento
Uso indebido de datos personales por contratista	Bases de datos con información personal de ciudadanos	Uso indebido y venta de datos personales por personal interno o externo	- Sin logs ni auditoría - Sin control de accesos con privilegios - Sin clasificación de la información - Sin acuerdos de confidencialidad	- Pérdida de confianza ciudadana - Sanciones legales - Violación de normativas de protección de datos	Alta	Crítico	- Implementar controles de acceso y privilegios - Auditorías y logs de accesos- Política de clasificación de información - Firmar acuerdos de confidencialidad con contratistas

Saul Hernandez Castilla

Escenario 5

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.

Caso	Activos	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Niveles de Riesgo	Medidas de Tratamiento
Ataque de Denegación de Servicio (DoS) al sitio web universitario	Sitio web de inscripciones Infraestructura de servidores web	Ataque de Denegación de Servicio (DoS) desde múltiples IPs	- Sin protección DoS o WAF - Servidor sin alta disponibilidad - Sin monitoreo en tiempo real - Falta de protocolos de respuesta inmediata	- Caída del sitio por 8 horas- Pérdida de inscripciones y trámites- Daño reputacional	Alta	Crítico	- Implementar protección DoS y WAF - Mejorar la capacidad y alta disponibilidad de servidores - Implementar monitoreo en tiempo real