Título: Informe Ejecutivo del Incidente de Seguridad
Subtítulo: Resumen, Acciones Tomadas y Recomendaciones Futuras
Empresa: 4Geeks Academy
Fecha:26/02/2025

- Introducción y Contexto
- Resumen del Incidente
- Acciones Inmediatas y Correctivas
- Impacto y Lecciones Aprendidas
- Recomendaciones Futuras
- Próximos Pasos
- Preguntas y Respuestas

Introducción y Contexto

- Breve descripción del incidente de seguridad detectado
- Importancia de los servicios críticos para la operatividad de la empresa
- Objetivo de la presentación: informar a la gerencia sobre lo ocurrido y planificar mejoras futuras

Resumen del Incidente

- Fecha y Hora de Detección: 24 de febrero de 2025, 09:00 hrs
- Vectores de Ataque:

1. Accesos no autorizados vía SSH mediante ataques de fuerza bruta
2. Explotación de configuración insegura en el servicio FTP
3. Exposición de archivos críticos (ej. wp-config.php)

- Modus Operandi del Atacante:

4. Uso de credenciales débiles
5. Creación de backdoors y manipulación de logs

Acciones Inmediatas y Correctivas

- Contención del Incidente:

1. Aislamiento de sistemas afectados
2. Bloqueo de cuentas comprometidas y cierre de puertos no esenciales

- Análisis Forense y Recuperación:

3. Recolección y revisión de logs (SSH, FTP, etc.)
4. Restauración de configuraciones seguras y actualización de credenciales

- Fortalecimiento de la Seguridad:

5. Implementación de autenticación basada en claves
6. Reconfiguración del servicio FTP y ajuste de permisos en archivos críticos
7. Monitoreo continuo con herramientas como Fail2ban, Wireshark, OpenVAS

Impacto y Lecciones Aprendidas

- Impacto en la Operación:

1. Riesgo de exposición de datos sensibles
2. Posible interrupción temporal de servicios críticos

- Lecciones Aprendidas:

3. Necesidad de configuraciones seguras y gestión adecuada de credenciales
4. Importancia del monitoreo en tiempo real y respuesta rápida ante anomalías
5. Valor de la documentación y análisis forense para mejorar procesos futuros

Recomendaciones Futuras

- Fortalecimiento de la Infraestructura:

1. Revisar y actualizar configuraciones de seguridad periódicamente
2. Implementar autenticación multifactor (MFA) y políticas de contraseñas robustas

- Mejoras en la Gestión de Incidentes:

3. Realizar simulacros y pruebas de penetración de forma regular
4. Actualizar el plan de respuesta a incidentes y el SGSI conforme a ISO 27001

- Monitoreo y Auditorías:

5. Invertir en herramientas de monitoreo avanzado y análisis continuo de logs
6. Establecer auditorías de seguridad periódicas para detectar vulnerabilidades

Próximos Pasos

- Programar una revisión completa de la infraestructura de seguridad
- Establecer un calendario de simulacros y capacitaciones para el equipo
- Coordinar con los equipos de TI y Seguridad para implementar las mejoras recomendadas
- Preparar informes periódicos de monitoreo y auditoría para la gerencia

Conclusión

- Resumen de los hechos y acciones tomadas
- Compromiso de la empresa con la seguridad y continuidad de los servicios críticos
- Agradecimiento a todos los equipos involucrados en la respuesta y recuperación