

Informe Ejecutivo del Incidente de Seguridad

Guillermo Garcia Arranz



Índice

01. Introducción
02. Resumen del Incidente
03. Acciones Inmediatas y Correctivas
04. Impacto y Lecciones Aprendidas
05. Recomendaciones Futuras
06. Proximos Pasos

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: SSH, FTP, exposición de archivos críticos.
- Modus Operandi del Atacante: uso de credenciales débiles, backdoors y manipulación de logs.



Acciones Inmediatas y Correctivas

- Contención Inmediata: Aislamiento de sistemas, bloqueo de cuentas y cierre de puertos.
- Recuperación y Reconfiguración: Restauración de configuraciones seguras, actualización de credenciales, implementación de autenticación basada en claves.
- Monitoreo Continuo: Uso de herramientas como Fail2ban, Wireshark y OpenVAS.

Impacto y Lecciones Aprendidas

- Impacto: Riesgo de exposición de datos y posible interrupción temporal de servicios críticos.
- Lecciones Aprendidas: Importancia de configuraciones seguras, monitoreo en tiempo real y análisis forense detallado.



Recomendaciones Futuras

- Fortalecimiento de la Infraestructura: Revisión periódica de configuraciones, autenticación multifactor y políticas de contraseñas robustas.
- Gestión de Incidentes: Simulacros y pruebas de penetración regulares, actualización continua del plan de respuesta a incidentes y SGSI.
- Monitoreo y Auditorías: Inversión en herramientas avanzadas y auditorías de seguridad periódicas.

Próximos Pasos

- Revisión completa de la infraestructura de seguridad.
- Calendario de simulacros y capacitaciones.
- Coordinación con equipos de TI y Seguridad para implementar mejoras.
- Informes periódicos de monitoreo y auditoría.



Conclusión

- Resumen de los hechos y acciones tomadas.
- Compromiso con la seguridad y continuidad de los servicios críticos.