Pràctica 1 - Parte 2
Políticas de Almacenamiento y Caract de Disposi

Pol de la Viuda

Contenido

Parte 3

Análisis completo de incidente de seguridad

Identifica todas las amenazas presentes

1. Phishing por correo electrónico
2. Malware tipo ransomware, que cifra los archivos del servidor
3. Fuga potencial de datos personales, al no estar las copias cifradas
4. Error humano, al no actualizar ni proteger el pendrive

Fallos de la política de almacenamiento

1. Las copias de seguridad no están automatizadas
2. Usan un solo pendrive como backup
3. Copias no cifradas
4. Las copias de seguridad están en el mismo edificio

Artículos RGPD

- Artículo 5: principios de integridad y confidencialidad
- Artículo 32: falta de medidas técnicas y organizativas adecuadas
- Artículo 25: no aplicar protección de datos desde el diseño
- Artículo 24: responsabilidad del responsable del tratamiento
- Artículo 33: posible obligación de notificar brecha de seguridad

¿Que medidas técnicas y organizativas deberían implementarse?

Medidas Técnicas

- Copias de seguridad automáticas
- Copias cifradas
- Antivirus en el servidor
- Control de acceso

Medidas Organizativas

- Formacion en ciberseguridad
- Auditorias de seguridad

¿Cómo habría cambiado el resultado si la empresa usara: Copias de Seguridad en la nube, un plan 3-2-1, ¿cifrado + autenticación multifactor?

Con las copias de seguridad en la nube, la recuperación habría sido mas rápida y no huibiesen perdido datos, con el plan 3-2-1, siempres hubese existido una copia válida y el ransomwarte no hubiese afectado a todas las copias y con el cifrado, tendrían mas priotecion de los datos personales y reducen el riesgo de brechas de datos

Diseño de arquitectura segura de almacenamiento

Usuario → Firewall → Servidor Principal → Copias de seguridad Diarias → Copias externas

La empresa cuenta con un servidor equipado con discos SSD en configuración RAID 10, lo que permite ofrecer un alto rendimiento y proteger los datos frente a posibles fallos de hardware.

Para asegurar la información, se realizan copias de seguridad incrementales todos los días en un NAS local, además de copias completas semanales que se almacenan en la nube. Estas copias conservan hasta 30 versiones, lo que facilita la recuperación de datos antiguos en caso de necesidad.

Toda la información está protegida mediante cifrado, tanto cuando se almacena como cuando se transmite, utilizando protocolos seguros como TLS y AES. Las copias externas se guardan en un proveedor de servicios en la nube ubicado en Europa, cumpliendo así con la normativa vigente.

Por último, la disponibilidad del sistema las 24 horas del día se garantiza gracias al uso de RAID, sistemas de monitorización y una infraestructura con redundancia eléctrica.

Análisis Coste-Beneficio

¿Qué opción es mejor a largo plazo?

La mejor opción a largo plazo es la opción B, porque reduce totalmente el riesgo, mejora la disponibilidad y cumple el RGPD

¿En que casos conviene la opción A?

En empresas muy pequeñas y con presupuesto muy limitado

¿Qué impacto tendría en disponibilidad, recuperación y cumplimiento del RGPD?

La opción A ofrece una disponibilidad limitada. Aunque el RAID 1 permite seguir trabajando si falla un disco, las copias de seguridad son semanales y solo locales, lo que hace que la recuperación ante un problema grave sea lenta y con riesgo de perder datos recientes. Además, al no usar cifrado ni copias externas, el cumplimiento del RGPD es bajo.

En cambio, la opción B garantiza una alta disponibilidad gracias al RAID 5, la monitorización y las copias diarias en la nube. Esto permite una recuperación rápida ante incidentes y asegura el cumplimiento del RGPD mediante el uso de cifrado y almacenamiento seguro en la nube.

Escenario de continuidad de negocio

Qué pasaría si la empresa solo usara RAID

Si la empresa solo usa RAID, un incendio destruiría los servidores y todos los datos. El RAID no protege frente a desastres físicos, por lo que no sería posible recuperar la información

Qué pasaría si la empresa usara copias locales pero no remotas

Aunque existan copias de seguridad, al estar en el mismo edificio se perderían con el incendio. La empresa sufriría una pérdida total de datos y una larga interrupción del negocio

Qué pasaría si aplicara el método 3-2-1 correctamente

Con el método 3-2-1, una copia estaría fuera del edificio. Los datos podrían recuperarse desde la copia externa y la empresa podría continuar su actividad

Tiempo estimado de recuperación en cada caso

Con solo RAID o copias locales, la recuperación sería imposible o tardaría semanas. Con 3-2-1, la recuperación podría realizarse en pocas horas o un día

Redacta un mini plan de recuperación

Tras el incidente, se activa el plan de emergencia, se habilita una infraestructura alternativa, se restauran los datos desde la copia externa, se verifica la información y se reanuda la actividad

Evaluación de dos escenarios de almacenamiento

Empresa 1

SSD NMVe + RAID 0

En la Empresa 1, que trabaja con vídeo en 4K y archivos muy grandes, la mejor opción es usar SSD NVMe con RAID 0 porque ofrece mucha velocidad. En este caso no importa tanto perder algún archivo, así que se prioriza el rendimiento para trabajar más rápido con los vídeos

Empresa 2

RAID 10 + nube cifrada

En la Empresa 2, que maneja datos financieros y personales, lo más importante es la seguridad y que los datos no se pierdan. Por eso es mejor usar RAID 10 junto con nube cifrada, ya que hay redundancia, buena disponibilidad y los datos están protegidos, cumpliendo con el RGPD