DOCUMENTO TÉCNICO

Comprender el impacto de la **seguridad integral de datos**

SCALE TO WIN

INFINIDAT

Los retos

2017 no fue un año fácil para los CIO/CISO, y 2018 tampoco da muestras de serlo. Con tantas brechas en los datos acaecidas tan solo en 2017 y capaces de acabar con la carrera de cualquiera, (Equifax, Uber, Yahoo son algunos ejemplos), y los requisitos normativos reforzados a nivel mundial, los CIO/ CISO tienen la responsabilidad corporativa de replantearse su enfoque sobre la seguridad de los datos.

Dejando a un lado el cumplimiento de las regulaciones, las organizaciones tienen la responsabilidad ante sus clientes y accionistas de proteger los datos y minimizar su exposición, no solo ante ataques externos, sino también de los propios empleados. El método más común de filtración de datos en 2017 fue la suplantación de identidad (phising) recibida por empleados corporativos. (Véase 2017 Data Breach Investigation Report). Esto convierte a los empleados en cómplices involuntarios de la filtración de datos: más del 80% de los ciberataques se produjeron a partir de un fallo humano crucial: el profesional no tecnológico que recibe un correo de su mejor amigo ya infectado, o el empleado que accede a un sitio web comprometido y crea un agujero en el perímetro de seguridad. Si bien no existe la protección al 100 %, sí hay ciertas reglas de sentido común que disminuyen el riesgo.

Hay dos términos que debemos tener en mente a la hora de pensar cómo proteger los datos de los piratas informáticos:

> ***"La superficie de ataque de un entorno de software es la suma de los distintos puntos (los "vectores de ataque") donde un usuario no autorizado (el "atacante") puede intentar introducir o extraer datos de un entorno. Mantener el tamaño de la superficie de ataque al mínimo posible es una medida de seguridad básica."*** *(Wikipedia)*

Si una organización trata sus datos como fuente de su ventaja empresarial, y comprende lo delicados que son para sus clientes, ¿cómo puede minimizar la superfice de ataque, y cómo las AFA (cabinas all-flash) lo obstaculizan?

Cuando el organigrama dicta el método de seguridad

La ley de Conway nos ha enseñado que la estructura organizativa afecta a menudo a los resultados y al diseño más que cualquier otra cosa. En el contexto de la seguridad, es muy sencillo: si el CISO y el gestor del almacenamiento tienen una buena relación de mucho tiempo, es muy probable que los datos estén encriptados en la capa de almacenamiento, y la casilla de "encriptado" estará seleccionada.

El almacenamiento es también el "camino de menor resistencia" puesto que las cabinas de almacenamiento pueden habilitar instantáneamente el encriptado sin que ello repercuta en el rendimiento.

Pero, ¿ayuda el encriptado en el nivel del almacenamiento a su superficie de ataque? Un poco, sí. Aunque aún deja TODAS las otras capas entre el usuario, las aplicaciones y la infraestructura sin cifrar, y los datos surcan la red sin protección.

Entonces, ¿dónde deberíamos cifrar los datos?

Considérelo en estos términos: cuanto más arriba en la cadena se cifran estos datos personales o confidenciales, más capas se protegen. En la siguiente tabla, cada fila representa una posible capa que puede cifrarse, y cada columna representa una superficie de ataque.

¿Se da cuenta que lo poco que protege el encriptado en el nivel de almacenamiento?

Dónde se utiliza el encriptado	**✓ ¿Quién puede ver los datos?** **⚠ Quién puede causar por accidente una brecha en los datos?**						
	Admin App	Admin SO	Admin BD	Admin VM	Admin de red	Admin de almacenamient	Admin de Backup
Aplicación	⚠	✓	✓	✓	✓	✓	✓
SO de aplicación	⚠	⚠	✓	✓	✓	✓	✓
Base de datos	⚠	⚠	⚠	✓	✓	✓	✓
Encriptado de VM	⚠	⚠	⚠	⚠	✓	✓	✓
Entramado (datos en movimiento)	⚠	⚠	⚠	⚠	✓	⚠	⚠
Almacenamiento	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Backup	⚠	⚠	⚠	⚠	⚠	⚠	⚠

¿Cómo aumentan las cabinas all-flash su superficie de ataque?

Si bien la mayoría de (si no todas) las AFA ofrecen encriptado en el nivel de disco, este es el único nivel de encriptado que permiten. Si los datos se cifran en cualquier otro sito, las AFA no pueden realizar la reducción de datos, lo que echa por tierra toda la rentabilidad de las AFA. Las AFA deben confiar en la reducción de datos (en una ratio de entre 3:1 y 6:1) para minimizar la prima de precio a un punto donde sea rentable.

Cuando lo “óptimo” choca con lo factible

ESTE ENFOQUE ÓPTIMO A LA SEGURIDAD DE DATOS A MENUDO SE VE LIMITADO POR HECHOS ANTERIORES:

- La aplicación con una antigüedad de diez años que no ofrece encriptado y ya carece de soporte.
- La aplicación crítica para el negocio cuyo mantenimiento lleva un año.
- El responsable de la aplicación que se niega a invertir el tiempo en cifrar los datos.

A la hora de la verdad, a menudo son necesarios compromisos para acelerar la adopción de la seguridad de los datos. Muchos optarán por cifrar los entornos en los niveles más bajos de la pila (DB/VM/OS) para cumplir con los requisitos corporativos y gubernamentales. Este enfoque es a menudo necesario para cumplir con las fechas de cumplimiento normativo, sin embargo, merece la pena limitar el número de enfoques independiente para evitar unos elevados costes generales administrativos. También es recomendable observar que todas estas alternativas tienen el mismo efecto: acaban con las posibilidades de reducción de datos de las AFA y aumentan el coste total de propiedad..

Otras ventajas de cifrar toda la pila

DISTRIBUCIÓN DE LA CARGA DE TRABAJO Y RENDIMIENTO

Con la excepción de las unidades autocifradas (SED), el encriptado requiere de una cierta cantidad de energía de la CPU. Una pila tecnológica tiene siempre más huéspedes que cabinas de almacenamiento; por lo que mover la tarea de encriptado de datos a un nivel superior en la pila tiene como resultado una mayor distribución de la carga de trabajo, reduciendo la carga de trabajo en los dispositivos individuales y mejorando así el rendimiento general.

GRANULARIDAD

Cuanto más alto se sitúa el nivel de encriptado en la pila, mejor es la granuralidad: una aplicación solo puede cifrar información personal identificable (PII) tal y como "entiende" el contexto/significado de los datos. Esto también reducirá los costes generales.

Si descendemos un nivel, el administrador de bases de datos (DBA) puede ofrecer espacios de tablas encriptados y no encriptados, y colocar los datos correctos en el lugar adecuado. Aunque es menos granular, es mejor que cifrar todo una VM o LUN.

PREPARADO PARA LA NUBE

Elevar el encriptado en la pila es un requisito para la migración a la nube si los datos necesitan mantener el mismo nivel de protección, incluso por cable (WAN). Los datos encriptados pueden moverse de forma segura o entrar en ráfaga hacia la nube sin la necesidad de mecanismos de seguridad adicional (como la gestión de encriptado en el nivel de la nube).

FÁCIL INTEGRACIÓN

Integrar los niveles de sistema operativo, base de datos o hipervisor tiene una ventaja: no son muy diferentes, y hay muchas aplicaciones en el entorno. Desde una perspectiva operativa, esto puede reducir la complejidad.

LLAMADA A LA ACCIÓN

- Planifique un enfoque integral a la política de protección de datos
- Establezca una fecha límite para empezar a diseñar las aplicaciones con cifrado de forma nativa
- Forme a sus desarrolladores en metodologías que incluyan la seguridad como parte del diseño de las aplicaciones
- Revise sus aplicaciones para encontrar la mejor manera de proteger sus datos mientras son transferidos
- Construya un plan de transición para cifrar sus aplicaciones legacy que manejen datos sensibles