UN DOCUMENTO TÉCNICO SOBRE SEGURIDAD

Seguridad de los servicios en la nube en PaperCut MF

Seguridad de datos en la nube desde cero

Proteger datos importantes es una búsqueda que se remonta a siglos.

En 1586, un noble inglés llamado Anthony Babington comenzó a enviar mensajes a la encarcelada María, reina de Escocia. El contenido de la correspondencia se centraba en un complot para asesinar a la reina Isabel e instalar a María en el trono de Inglaterra. Babington utilizó una serie de técnicas para mantener sus mensajes lo más secretos posible, ya que la traición estaba bastante mal vista.

En el mundo cibernético actual nos referiríamos a su enfoque como seguridad en capas. Primero, cifró los mensajes, luego los escondió en los corchos de barriles de cerveza y luego los hizo transportar a través de una red de cómplices de confianza. Desafortunadamente para Babington, utilizó un cifrado débil y su red también quedó comprometida. A los pocos meses, pagó el precio más alto por la falta de seguridad de sus datos.

En PaperCut prestamos especial atención a múltiples aspectos de la seguridad de los datos y está diseñado en todo lo que construimos. Quizás también desee leer el documento técnico Cómo proteger su sistema de impresión.

Negocio riesgoso

Proteger un activo valioso siempre conlleva algún riesgo inherente. Por lo general, el objetivo de la seguridad de los datos es reducir el riesgo al nivel más bajo aceptable y al mismo tiempo mantener los objetivos comerciales y contener el costo. Por eso siempre debemos tener en cuenta estos tres elementos: riesgo, objetivos y coste.

Podríamos crear un plan de seguridad de datos que tenga absolutamente cero riesgo al hacer que los datos sean inaccesibles para cualquiera, pero esto probablemente no cumpliría con los objetivos comerciales o tendría un costo exorbitante.

Los datos electrónicos introducen algunos riesgos adicionales a considerar. Antes, para robar un activo, los ladrones tenían que robarlo físicamente. Ahora, con los datos electrónicos, pueden simplemente hacer una copia y, en la mayoría de los casos, la copia es tan valiosa como el original. Y lo que es peor, a menudo hay poca evidencia de que la copia haya sido robada, por lo que ni siquiera sabes que te han robado.

En 1980 hubo una serie de robos de aviones comerciales en Estados Unidos. Por casualidad, el caso se resolvió el 14 de mayo en Atlanta, Georgia, cuando un baúl de carga se abrió durante la carga. La tripulación descubrió un polizón escondido dentro del maletero con algo de comida y un tanque de oxígeno. Resulta que salía del maletero en pleno vuelo, agarraba todos los objetos de valor que podía y luego se los llevaba de nuevo al maletero. Compare este robo físico de objetos de valor con el robo de datos electrónicos: llamaríamos a sus acciones un clásico ataque del Hombre en el Medio y robo de datos en tránsito.

Afortunadamente, el robo de artículos físicos hizo que el robo aéreo se hiciera evidente rápidamente, pero con los activos digitales, el robo suele pasar desapercibido durante un período de tiempo.

Identificar adecuadamente sus objetivos comerciales en materia de seguridad de datos puede llevar bastante tiempo. Los objetivos deben incluir requisitos legales (por ejemplo, GDPR, HIPAA), eficiencia operativa para aspectos como la planificación de la continuidad del negocio y la cadena de suministro, y elementos básicos como quién requiere acceso a los datos y con qué rapidez. Podríamos cubrir algunos de esos objetivos poniendo todos los datos de la empresa en un servidor web público, sin cifrar. Podría ser muy eficiente para los negocios, pero podría ser desastroso para la reputación, la confidencialidad y la integridad. Por lo tanto, sus objetivos comerciales también deben cubrirlos.

Los activos electrónicos como información médica protegida (PHI), información de identificación personal (PII), datos de tarjetas de crédito, propiedad intelectual y otros deben protegerse de manera que minimice el riesgo de pérdida, exposición o copia.

Localización

Un factor clave en su decisión de proteger los datos electrónicos es dónde ubicar los datos almacenados. Normalmente, esto significa elegir alojamiento local (es decir, local) o en la nube. Sin embargo, la decisión no es tan clara como solía ser, principalmente debido a los importantes avances en la seguridad de la nube.

Dividamos la decisión de ubicación de datos en cinco objetivos.

Costo

Los centros de datos alojados localmente tienen costos iniciales y de funcionamiento significativamente más altos que los centros de datos en la nube privada (es decir, infraestructura como servicio*). Necesitará servidores, discos, licencias, equipos de red, energía eléctrica, sistemas de refrigeración y un excelente personal de TI para administrar, mantener y actualizar todo. Un centro de datos en la nube privada, por otro lado, tiene un costo de entrada muy bajo, pero pagará por casi cada kilobyte de disco y ciclo de procesador que utilice. También correrá con la mayor parte de los costos de licencia, administración y actualización de software. Sí, esto también puede acumularse con el tiempo, pero llega un punto de equilibrio (generalmente medido en años) en el que la nube privada tiene un costo total de propiedad más alto. Otros costos a considerar y equilibrar con los objetivos comerciales incluyen la escalabilidad, el cumplimiento legal y el flujo de caja.

Nota: Los servicios en la nube de PaperCut MF se incluyen como parte de su licencia cuando tiene mantenimiento y soporte activos.

Seguridad

Este solía ser un éxito para los centros de datos alojados localmente, pero eso fue hace "muchos años" (en australiano significa "bastantes años"). Un centro de datos alojado localmente le brinda control total sobre dónde y cómo proteger los datos. Para algunas organizaciones, este control es innegociable para ciertos datos que manejan. Un motivo es cumplir con las normas de protección de datos (por ejemplo, GDPR, HIPAA, FERPA). No siempre es posible comprobar el cumplimiento de la normativa por parte de terceros que tienen acceso a los datos en la nube pública.

Los datos alojados localmente solo van a donde usted los indique y solo pueden acceder a ellos las personas y los sistemas que usted autorice, a menos que los almacene en un disco o los coloque en una red. Porque si alguien puede acceder a los datos, puede robarlos. Considere algunas estadísticas sobre violaciones de datos:

- Más del 20 % de las infracciones en 2021 utilizan credenciales robadas (Verizon, 2022 Data Breach
- Informe de Investigaciones)
- El 93% del malware ingresa por correo electrónico'
- Los ataques a la cadena de suministro aumentaron más del 600% en 20213
- El 27% de las infracciones son resultado de errores humanos, el 25% de fallas del sistema y el 48% son ataques maliciosos (muchos de los cuales fueron "internos")

La mayoría de las organizaciones que alojan sus propios datos ya no pueden seguir el ritmo del aumento en la cantidad y la sofisticación de las amenazas. Muy pocos están preparados para defenderse de las vulnerabilidades de los chips de hardware, los exploits de día cero, los ataques multivectoriales o el malware polimórfico.
Estamos en el punto en el que la mayoría de los proveedores de nube dedicados ofrecen mayor seguridad que los autohospedados. Sin embargo, todavía existen preocupaciones importantes sobre la seguridad de los datos en la nube, y la mayoría de ellas entran en la categoría de cómo se utiliza la nube. Por ejemplo, millones de registros de datos han quedado expuestos en los últimos años debido a depósitos de Amazon S3 mal configurados. Alerta de spoiler: resulta que si no configuras la autenticación y el cifrado, otros pueden ver tus datos.
Un área más donde las infracciones se reportan como "acceso en línea" ocurre en la cadena de suministro. Estas infracciones pueden ocurrirle a terceros que desempeñan un papel en sus operaciones comerciales y que tienen acceso a sus datos. La mayoría de las organizaciones no cuentan con procedimientos adecuados de investigación de antecedentes por parte de terceros. Su responsabilidad en materia de protección de datos incluye aquellos con quienes comparte esos datos.

Una escuela que proporciona información de los estudiantes a un tercero que prepara sus comidas es tan vulnerable como el eslabón más débil de la cadena de suministro. Un hospital que comparte datos de pacientes con un cobrador de facturas médicas externo es vulnerable y responsable de las violaciones de PHI. Antes de confiar sus responsabilidades de protección de datos a un proveedor de la nube, asegúrese de que garantice la seguridad de todos los terceros.