SHARDSECURE

White Paper

Mit der Microshard-Technologie haben Sie die Möglichkeit, die für die Bedürfnisse Ihres Unternehmens geeignete Kombination von Cloud-Datenschutz zu wählen.

Wann ist Microsharding, wann Verschlüsselung und wann beides sinnvoll?

Wir haben gerade die Nachricht von unserem unterzeichneten Series A Funding in Höhe von 11 Mio. USD erhalten und freuen uns, Ihnen mitteilen zu können, warum unsere Technologie das Vertrauen unserer Investoren gewonnen hat.

Es sollte nicht überraschen, dass unsere Microshard™-Technologie oft mit Verschlüsselung verglichen oder sogar als eine weitere Form der Verschlüsselung angesehen wird. Beides sind Lösungen für Datensicherheit und Datenschutz, und beide bieten Schutz für sensible Daten.

Aber ist Microsharding dasselbe wie Verschlüsselung? Können beide zusammen verwendet werden? Da diese Fragen häufig gestellt werden, fangen wir gleich damit an.

Die Grundlagen

Das Wichtigste zuerst: Die Microsharding-Technologie ist keine Verschlüsselung.

Wenn es um Daten im Ruhezustand geht, haben sowohl Microsharding als auch Verschlüsselung das gleiche Ziel des Datenschutzes im Auge. Wie die beiden Lösungen dieses Ziel erreichen, ist jedoch völlig unterschiedlich.

Schlüsselbasierte vs. schlüssellose Lösungen

Bei der gängigsten Art der Verschlüsselung ist der Schlüssel ein grundlegendes Konzept. Ich gehe davon aus, dass Sie mit den Abenteuern von Bob und Alice vertraut sind, daher werde ich Ihnen nicht erzählen, was Sie bereits wissen. Die wichtigste Erkenntnis ist, dass Schlüssel - und deren Verwaltung und Schutz - für die Verschlüsselung von zentraler Bedeutung sind.

Microsharding hat kein Konzept eines Schlüssels. Unser "Schreddern. Mischen. Verteilen"-Ansatz ist eine Form der Verschleierung. Es gibt keine Schlüsselrotation oder irgendetwas Ähnliches wie eine Schlüsselverwaltung - damit entfallen die Kosten und die Komplexität ebenso wie alle Bedenken hinsichtlich der Schlüsselverwaltung durch Dritte.

Wenn wir den Kundenspeicher nutzen, speichern wir keine Ihrer Daten. Wir fragmentieren Ihre Daten lediglich und setzen sie auf dem Weg zu und von Ihrem Speicherplatz wieder zusammen.

Vollständige vs. fragmentierte Daten

Verschlüsselte Daten werden als Ganzes gespeichert, Microshard-Daten nicht.

Das meine ich folgendermaßen: Wenn Sie eine verschlüsselte Datei speichern, speichern Sie die gesamte Datei an einem einzigen Ort. Ja, sie ist verschlüsselt, aber es ist immer noch die ganze Datei, die gelöscht, mit Ransomware wieder verschlüsselt oder exfiltriert werden könnte. Damit könnte ein gut ausgerüsteter Gegner versuchen, die Verschlüsselung im Laufe der Zeit zu knacken, oder einfach mit einem gestohlenen Schlüssel die Datei entschlüsseln.

Andererseits speichert die Microshard-Technologie aus Gründen der Parität einen 1/(x-1) gemischten Bruchteil des gesamten Datensatzes an mehreren Speicherorten des Kunden (wobei x = die Anzahl der Speicherorte minus eins). Wenn ein Speicherort kompromittiert und Ihre Daten gestohlen werden, erhält der Angreifer ein unsinniges Durcheinander von Zeichen, das nur einen Bruchteil des vollständigen Datensatzes darstellt.

Selbst mit der fortgeschrittenen Rechenleistung des Quantencomputers kann ein vollständiger Microshard-Datensatz nicht wieder zusammengesetzt werden, da der unbefugte Benutzer zunächst jeden Speicherort der Microshard-Daten kennen und dann jeden einzelnen Speicherort kompromittieren muss.

Daten vs. selbstheilende Daten

Wenn verschlüsselte Daten gelöscht werden, sind sie weg. Ende der Geschichte. Ähnlich verhält es sich mit verschlüsselten Daten, die neu verschlüsselt wurden.

Und wenn ein Speicherdienst mit verschlüsselten Daten offline geht, sind diese Daten ebenfalls unzugänglich. Auf der anderen Seite sind Microshard-Daten selbstheilende Daten. Denken Sie an RAID-5 für Daten in der Cloud.

Wenn Microshard-Daten in irgendeiner Weise manipuliert wurden, können wir dank der Selbstheilungsfunktion der Daten die betroffenen Microshard-Daten rekonstruieren, um sie in ihren ursprünglichen Zustand zurückzuversetzen.

Das Gleiche gilt für Microshard-Daten, die nicht verfügbar sind, wenn ein Speicheranbieter vorübergehend ausfällt. Dies trägt dazu bei, den ununterbrochenen Zugang für die Benutzer aufrechtzuerhalten.

Verschlüsseln? Microshard? Beides?

Ja.

Wir haben nichts gegen Verschlüsselung. Das ist ein starker, bewährter Ansatz.

Wir sind auch entschiedene Befürworter von Defense in Depth. Wir glauben, dass es eine gute Sache ist, komplementäre Sicherheitstechnologien angemessen zu kombinieren.

Einige Kunden verwenden Microsharding für ihre verschlüsselten Daten. Andere verschlüsseln ihre Daten nicht, sondern verschlüsseln sie mit Microsharding, und wieder andere verschlüsseln einige Daten und verschlüsseln andere Daten mit Microsharding.

Die richtige Mischung hängt davon ab, was Sie brauchen. Hier sind einige grobe Anhaltspunkte:

1. Unterliegen Sie irgendwelchen Gesetzen/Vorschriften, die eine Verschlüsselung vorschreiben? Wenn ja, dann ist es ziemlich klar, dass Sie verschlüsseln sollten, um die Vorschriften einzuhalten. Ziehen Sie den Einsatz der Microshard-Technologie für alle sensiblen Daten in Betracht, die nicht in den Geltungsbereich der Vorschriften fallen. Und denken Sie daran, dass Sie verschlüsselte Daten für zusätzliche Sicherheit auch mit Microsharding sichern können.

2. Verwalten Sie Ihre eigenen Verschlüsselungsschlüssel? Wenn ja, sollten Sie den Einsatz von Microsharding anstelle von Verschlüsselung in Erwägung ziehen, um die Kosten und den Verwaltungsaufwand, die mit der Schlüsselverwaltung verbunden sein können, erheblich zu reduzieren. Microsharding kann auch dazu beitragen, die durch die Verschlüsselung verursachten Leistungseinbußen abzumildern.

3. Verwenden Sie eine serverseitige Verschlüsselung, die von Ihrem Cloud-Anbieter verwaltet wird, und fühlen Sie sich unwohl, wenn ein Dritter Ihre Schlüssel verwaltet? Mit Microsharding behalten Sie die Kontrolle über Ihre sensiblen Daten, auch darüber, wo sie gespeichert sind und wer Zugriff darauf hat. Wir glauben zwar, dass Cloud-Anbieter vertrauenswürdig sind, aber Ausfälle und Benutzerfehler kommen trotzdem vor, und eine Fehlkonfiguration kann leicht dazu führen, dass sensible Daten im gesamten Internet zugänglich sind. Diese Sorge hören wir vor allem von Kunden in Europa, für die strenge Datenschutzbestimmungen gelten.

Die Verschlüsselung ist eine bewährte Sicherheitstechnologie mit einer langen Geschichte. Aber sie war auch die einzige Möglichkeit, Ihre Daten im Ruhezustand zu sichern - bis jetzt.

Blog

https://shardsecure.com/blog/microshard-encrypt-both?utm_campaign=2022%20Blog%3A%20Jan-Dec%20Website&utm_content=210714515&utm_medium=social&utm_source=linkedin&hss_channel=lcp-35584883

@ShardSecure
@ShardSecure
@ShardSecure

101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

info@shardsecure.com