TAG CYBER

SCHÄTZUNG DES SECURITY RETURN ON INVESTMENT (ROI) FÜR CLOUD MICROSHARDING

EDWARD AMOROSO, CHRISTOPHER R. WILDER
TAG CYBER

SHARDSECURE

TAG CYBER

SCHÄTZUNG DES SECURITY RETURN ON INVESTMENT (ROI) FÜR CLOUD MICROSHARDING

EDWARD AMOROSO, CHRISTOPHER R. WILDER

Es ist realistisch anzunehmen, dass Enterprise-Teams, die Microsharding für in der Cloud gehostete Daten einsetzen, eine geringere Wahrscheinlichkeit von Daten-Kompromittierung in Public Cloud- Umgebungen haben. Die damit verbundene Reduzierung der Reaktionskosten darauf ist nachweislich ausreichend, um den Kauf einer kommerziellen Plattform-Lizenz zu rechtfertigen. Dies bedeutet, dass Enterprise-Teams, die kritische Daten in der Cloud speichern in eine Microsharding-Lösung investieren sollten.

1. EINLEITUNG

Das Risiko, sensible Daten in einer Public Cloud-Umgebung zu hosten, verringert sich allmählich, da Betreiber Zugang zu neuen Tools, Plattformen, Diensten und Methoden zur Verbesserung der Sicherheit erhalten. Kommerzielle Anbieter bieten inzwischen hervorragende Lösungen für die Verwaltung von Cloud-Berechtigungen, die Zugriffskontrolle in der Cloud, die Verwaltung der Cloud-Sicherheit und die Verschlüsselung von Daten in der Cloud. Jede dieser Methoden konzentriert sich jedoch auf die Risiken des unbefugten Zugriffs auf Cloud-Daten durch Front-End-Zugriffskanäle. Man kann diese Lösungen so betrachten, als wären sie auf den Zugriff über die normale Benutzeroberfläche spezialisiert. Dies ist zwar wichtig und notwendig, allerdings entgegnen solche Lösungen in der Regel nicht dem Problem des Back-End-Zugriffs auf Daten durch Zugriff von Cloud-Administratoren mit Insider-Rechten.

Dieser Report gibt einen kurzen Überblick über Microsharding und verwendet dann eine Methode zur Abschätzung der Investitionsrendite (ROI) für den Einsatz dieser Technik in einer typischen Cloud-Umgebung. Die Analyse zeigt, dass der hohe präventive Nutzen von Microsharding ausreicht, um die Investition unter normalen Umständen zu rechtfertigen. Diese Behauptung wird durch eine Analyse der Auswirkungen von Microsharding auf die verschiedenen variablen Kosten für das Hosten von Daten in einer öffentlichen Cloud untermauert.

2. WIE CLOUD MICROSHARDING FUNKTIONIERT

Das Microsharding-Verfahren ist darauf ausgelegt, wichtige Daten in mehrere Komponenten aufzuteilen, die getrennt, verschleiert und in verschiedenen Cloud-Infrastrukturen gespeichert werden. Das Ergebnis ist, dass der Back-End-Zugriff auf die Daten durch Administratoren und andere Cloud-Hosting-Insider nicht zu einer Datenverletzung führen kann, da die Daten über mehrere Cloud-Speichereinheiten verteilt wurden (siehe Abbildung 1)..[1]

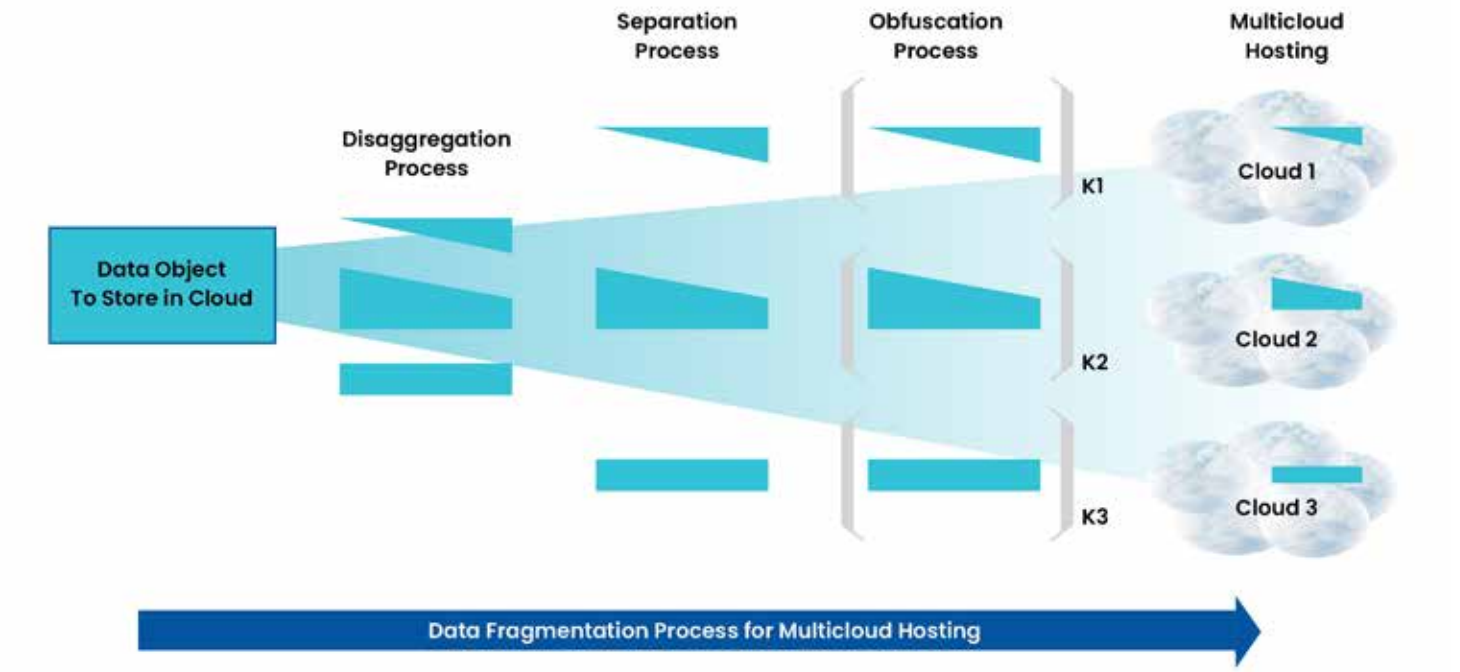

Figure 1. Microsharding Process

Die Komponenten des Microsharding-Prozesses sind in einer Pipeline angeordnet, die zum Schutz der Cloud-Daten führt. Jede dieser Verarbeitungskomponenten trägt zum Gesamtsicherheitssystem bei. Im Folgenden werden Einblicke in die algorithmische Strategie für diese Prozesse gegeben:

- **Disaggregation** – Die Zerlegung der in der Cloud zu speichernden Daten in einzelne Bestandteile ist ein wichtiger Aspekt des Microsharding-Prozesses. Durch eine solche Zerlegung wird die Gefahr eines direkten Backend-Zugriffs durch einen Insider oder einen Eindringling stark reduziert.
- **Trennung** – Die Trennung der disaggregierten Komponenten ist eine damit verbundene Aufgabe, die das Risiko eines unbefugten Zugriffs über Backend-Kanäle mit administrativem Zugriff weiter verringert.
- **Verschleierung** – Verschleierung bezieht sich auf den Prozess der Unkenntlichmachung der einzelnen disaggregierten Datenschnipsel bei der Überprüfung. Dies kann durch Verschlüsselung, Verblendungsalgorithmen und andere praktische Mittel geschehen.

Der einzigartigste Aspekt des Microsharding-Prozesses ist, dass er die Vielzahl von Cloud-Sicherheitslösungen ergänzt, die sich mit dem Front-End-Risiko befassen. Das heißt, bei der bestehenden Cloud-Sicherheit geht es vor allem darum, sicherzustellen, dass der offene Weg zu den gehosteten Daten durch Identitäts-, Zugriffs-, Verschlüsselungs- und andere Mechanismen zur Durchsetzung von Richtlinien kontrolliert wird. Microsharding bietet Schutz für den Back-End-Zugriff auf die Daten durch Administratoren und anderem Cloud-Hosting-Personal.

3. MICROSHARDING-ROI-ANALYSE

Um den ROI für Cloud-Microsharding zu messen, müssen die Anwendungsfälle definiert werden, die in der Analyse berücksichtigt werden. Es gibt zwei Situationen, in denen Microsharding wichtig wird: Ein Unternehmen könnte kritische Daten aus seiner bestehenden lokalen Umgebung in die Cloud verlagern oder ein Unternehmen, das bereits kritische Daten in einer oder mehreren öffentlichen Clouds hostet, könnte Microsharding in Betracht ziehen, um die Sicherheit zu verbessern.

Beide Situationen sind wichtig, aber wir konzentrieren uns auf den letzteren Fall, in dem Microsharding für bestehende, in der Cloud gehostete Daten eingeführt wird. Dieser Fall ist für die ROI-Schätzung attraktiv, weil er eine einfache Berechnung der Vorher-Nachher-Kosten ermöglicht. Indem wir die relevanten Kostenvariablen für die Verwaltung und Sicherheit des Cloud-Hostings ermitteln, können wir die Unterschiede bei den Gesamtkosten abschätzen, wenn Microsharding verwendet wird oder nicht.

Die Leser sollten jedoch bedenken, dass die Verwendung von Microsharding im ersten Fall - wenn ein Unternehmen seine kritischen Daten von On-Premise in die Cloud verlagert - zu ROI-Einsparungen gegenüber dem Verzicht auf diesen Schritt führt. Das Hauptproblem besteht darin, dass die Reaktionskosten für Vorfälle in der Public Cloud, die möglicherweise einen von Insidern initiierten Verstoß gegen den Provider beinhalten, so hoch sein können, dass eine Vermeidung aus rein finanzieller Sicht zwingend erforderlich ist. Durch Microsharding der in der Public Cloud gespeicherten Daten wird der direkte Zugriff von Administratoren mit privilegiertem Zugang keine nützlichen Informationen ergeben.

3.1 ROI-Methodik

Daher beginnen wir unsere Analyse, indem wir zunächst die bestehenden Kosten eines Unternehmens für das Hosting kritischer Daten in einer Public Cloud ohne Microsharding und anschließend die gleichen Kosten mit Microsharding untersuchen. Die Analyse sollte auf alle Arten von kritischen Unternehmensdaten anwendbar sein, unabhängig vom Bereich (z. B. Finanzen, Gesundheitswesen, Behörden). Die Kosten und Vorteile, die im Zusammenhang mit Microsharding wichtiger Daten in der Cloud stehen, werden als *klein, mittel* oder groß kategorisiert.[2]

3.2 Basis-Kosten-Gleichung

Wir führen die ROI-Analyse anhand eines fiktiven mittelständischen Unternehmens namens ACME durch, das eine kritische Geschäftsanwendung namens AppX in der öffentlichen Amazon Web Services (AWS)-Infrastruktur hostet. Die mit AppX verbundenen kritischen Daten werden als S3-Objekte in Amazon S3 Storage Buckets gespeichert. Die übergeordnete Kostengleichung von ACME für diese von AWS gehosteten Daten kann wie folgt dargestellt werden:

Kosten(AppX) = DevOps-Kosten(AppX)[3] + Verwaltungskosten(AppX)[4] + Lizenzkosten(AppX)[5] + Sicherheitskosten(AppX)[6]

Der Umfang der DevOps- und Verwaltungskosten hängt von der lokalen Umgebung und dem Stand des Reifegrads ab. Unternehmen, die über mehr Erfahrung und Fachwissen in diesen Bereichen verfügen, werden niedrigere Kosten haben als Unternehmen, die gerade erst anfangen. Wir gehen davon aus, dass es keine besonderen Lizenzierungssituationen gibt und dass ACME branchenübliche Lizenzgebühren für alle mit dem Datenhosting verbundenen Dienste zahlt..

3.3 Kosten für die Sicherheit

Die Schutzkosten für in der Cloud gehostete Anwendungen können in Präventionskosten und Erkennungs-/Reaktionskosten unterteilt werden. Die Präventionskosten dienen der Vermeidung von Cyber-Bedrohungen (oft als Shifting Left bezeichnet), während die Erkennungs-/Reaktionskosten für die Bewältigung laufender Angriffe bestimmt sind (als Shifting Right bezeichnet). Wir können daher die Kostengleichung von ACME für AppX um die folgenden Variablen erweitern:

Kosten(AppX)= DevOps-Kosten(AppX) + Verwaltungskosten(AppX) + Lizenzkosten(AppX)+ Präventionskosten(AppX) + Erkennungs-/Reaktionskosten(Appx)

Cybersicherheitsexperten sind sich einig, dass die Erkennung/Reaktion die höchsten Sicherheitskosten verursacht. Sie sind sich auch einig, dass Investitionen in die Vorbeugung, wann immer dies möglich ist, die Kosten für die Erkennung und Reaktion am Ende des Tages verringern. Dieses Konzept ist nicht umstritten, aber es funktioniert nur, wenn die Prävention wirksam ist. Fragwürdig wird diese Gleichung dann, wenn die Prävention keine Wirkung zeigt (z. B. bei frühen Generationen von Antiviren-Software).

3.4 Schätzung der Kostenwerte

Wir können damit beginnen, hohe, mittlere und niedrige Werte mit der Kostengleichung für ACME zu assoziieren. Vor der Einführung von Microsharding können wir in allen Fällen von mittleren Kosten ausgehen, um den allgemeinen, industriekonformen Aspekt der Nutzung widerzuspiegeln. Daraus ergibt sich die Kostengleichung für das ACME-Cloud-Datenhosting wie folgt aus:

Kosten(AppX)= DevOps-Kosten(AppX) + Verwaltungskosten(AppX) + Lizenzkosten(AppX)+ Präventionskosten(AppX) + Reaktionskosten(Appx)

DevOps-Kosten(AppX)= Mittel, Verwaltungskosten(AppX)= Mittel, Lizenzkosten (AppX)=Mittel, Präventionskosten(AppX)= Mittel, Reaktionskosten(AppX)= Mittel

Kosten(Appx)= Mittel + Mittel + Mittel + Mittel + Mittel

Wir können nun einfache numerische Kostenwerte (1, 2, 3, 4, 5) in einer Ordinalskala (bei der die jeweiligen Werte geordnet, aber nicht mit einer Arithmetik verbunden sind) mit *(sehr niedrigen, niedrigen, mittleren, hohen, sehr hohen)* Kostenschätzungskategorien verknüpfen. Obwohl Ordinalwerte nicht für detaillierte Berechnungen verwendet werden sollten, können sie helfen, vergleichende aggregierte Kostenschätzungen zu veranschaulichen.

Kosten (Appx) = 3 + 3 + 3 + 3 + 3 = 15

Die Verwendung von Ordinalwerten in der obigen Kostengleichung bietet natürlich nur eine einfache Vergleichsgrundlage, da den einzelnen Werten außer ihrer jeweiligen Reihenfolge (z. B. 15 ist größer als 3) keine absolute Bedeutung zugeordnet werden kann. Was wir jedoch tun können, ist zu zeigen, wie Veränderungen in verschiedenen Kostenvariablen zu entsprechenden Veränderungen in anderen Kostenvariablen hinzukommen oder diese ausgleichen können.

3.5 Abschätzung des ROI für Microsharding

Die primären Kostenannahmen, die in Bezug auf die Nutzung von Microsharding in der Cloud gemacht werden, lassen sich wie folgt beschreiben: Bei der Einführung von Microsharding in einer zweiten Cloud (z. B. Microsoft Azure) sind die folgenden Kostenauswirkungen zu erwarten:

DevOps: Keine Veränderung (3)
Verwaltung: Keine Änderung (3)
Lizenz: Erhöhung für Microsharding-Tool plus zweite AWS-Cloud (3 bis 4)7
Prävention: Keine Änderung (3)
Reaktion: Verringerung, um die geringere Wahrscheinlichkeit eines Vorfalls widerzuspiegeln (3 zu 1)

Anhand dieser Schätzungen lässt sich ein einfacher Anwendungsfall für die Einführung von Microsharding in einer typischen Umgebung.

Vor-Microsharding:
Kosten (ca.) = 3 + 3 + 3 + 3 + 3 + 3 = 15
Nach-Microsharding:
Kosten (Appx) = 3 + 3 + 4 + 3 + 1 = 14

Auch hier gilt, dass Ordinalwerte nicht genau verglichen werden können, so dass die beiden Gleichungen dahingehend interpretiert werden sollten, dass mit steigenden Lizenzkosten die entsprechenden Reaktions-Kosten sinken. Im gezeigten Fall übersteigt der Rückgang der Reaktions-Kosten den Anstieg der Lizenzkosten, so dass der ROI positiv ist. Unsere Analyse bei TAG Cyber legt nahe, dass der positive Fall unter vernünftigen Annahmen wahrscheinlich ist (siehe unten).

3.6 Realistischere Schätzungen zur Berechnung des ROI

Wenn wir realistischere Kostenannahmen für ein typisches Unternehmen einführen, das Daten in einer Public Cloud hostet, dann können wir die oben vorgestellte ROI-Methode verwenden, um aussagekräftigere Beispielwerte zu veranschaulichen. Darin enthalten sind die spezifischen Kosten, die sich für ACME bei der Durchführung des Microsharding über AWS und Microsoft ändern, die Erhöhung der Lizenzkosten (für die zusätzliche Cloud und das Microsharding-Tool) und die entsprechend sinkenden Reaktionskosten:

Vor-Microsharding:
Lizenz: Angenommen 500 TB zu 120.000 $/Jahr für AWS
Reaktion: Angenommen, ein Team von 5 Vollzeitbeschäftigten zu 1 Mio. $/Jahr für Response-Arbeit
Lizenz + Reaktionskosten insgesamt: $1.12M

Nach-Microsharding:
Lizenz: Angenommen, 250 TB für 65.000 $/Jahr bei AWS und 250 TB für 65.000 $/Jahr bei MS
Lizenz (Microsharding): 100.000 $/Jahr (Schätzung auf der Grundlage der ShardSecure-Preise)
Reaktion: Reduzierung des Response-Teams um zwei Vollzeitkräfte mit einem Gehalt von je 200.000$, was zu drei Vollzeitkräften bei einem Gehalt von je 200.000 US-Dollar führt.
Gesamtkosten für das Response-Team = 600.000 US-Dollar/Jahr
Lizenz + Reaktion insgesamt: $830K

Aus der Analyse ergibt sich, dass ACME in diesem hypothetischen Beispielfall zwei Vollzeitmitarbeiter in seinem Incident-Response-Team einsparen kann, da die Zahl der angenommenen Datenkompromittierungen in der Public Cloud deutlich zurückgeht. Trotz eines geringfügigen Anstiegs der Public-Cloud-Lizenzen für AWS und der Lizenzkosten für ein Microsharding-Tool wie ShardSecure werden die Gesamtkosten für ACME aufgrund der Entscheidung, die Sicherheitskontrolle zu implementieren, sinken.

4. AKTIONSPLAN FÜR UNTERNEHMEN

Ein Aktionsplan für Unternehmen, der auf dieser ROI-Bewertung basiert, sollte die folgenden Managementschritte beinhalten, um den oben dargestellten Vorteil des Microshardings voll auszuschöpfen:

- **Schritt 1: Bestandsaufnahme.** Das Unternehmensteam sollte eine Bestandsaufnahme aller kritischen Daten vornehmen, die entweder bereits gehostet werden oder für das Hosting in einem Public Cloud-Dienst vorgesehen sind.

- **Schritt 2: ROI-Instanzierung.** Das Unternehmensteam sollte die oben dargestellte beispielhafte generische ROI-Analyse als Grundlage für eine realistischere Analyse unter Verwendung der tatsächlich anfallenden Kosten verwenden.

- **Schritt 3: Überprüfung der Plattform.** Das Unternehmensteam sollte die kommerzielle Landschaft nach geeigneten Microsharding-Tools durchforsten, die geprüft und getestet werden sollten (z. B. ShardSecure, auf das in diesem Bericht verwiesen wird).

- **Schritt 4: Implementierungsplan.** Unter der Voraussetzung, dass die ROI- und Anbieterprüfungen erfolgreich verlaufen, sollte das Unternehmensteam einen Implementierungsplan zur Integration von Microsharding in die Datenhosting Infrastruktur zu integrieren.

---

[1] The analysis of microsharding benefited from cooperation with the ShardSecure team which offers a commercial platform supporting this technique. The analysis was completed with their expert assistance to ensure that no technical assumptions were made that were either incorrect or unrealistic. The final ROI conclusion was developed independently by the TAG Cyber team, however, and was not pre-determined by ShardSecure or any other commercial participant in this industry.

[2] Unternehmensteams, die diesen ROI-Bericht verwenden, können und sollten diese allgemeinen Gruppierungen in spezifischere quantitative Werte umwandeln. Außerdem werden alle Kostensenkungen, die ohne entsprechende negative Auswirkungen auf das Cyberrisiko erzielt werden können, als Kostenvorteile interpretiert.

[3] Bei den DevOps-Kosten wird davon ausgegangen, dass sie alle Entwicklungs-, Test-, Bereitstellungs-, Aktualisierungs- und Fehlerbehebungskosten umfassen.

[4] Verwaltungskosten umfassen die tägliche Pflege, Wartung, Überwachung und Unterstützung.

[5] Als Lizenzkosten gelten alle an Dritte gezahlten Gebühren für Software, Hosting oder andere Dienstleistungen.

[6] Zu den Sicherheitskosten zählen alle Aufgaben im Zusammenhang mit der Vorbeugung, Erkennung und Reaktion auf Cyber-Bedrohungen.

[7] Dies ist eine aggressive Schätzung, die von einem Kostenanstieg ausgeht. Tatsächliche Verhandlungen könnten zu einem besseren Ergebnis führen.

ÜBER TAG CYBER

TAG Cyber ist ein vertrauenswürdiges Analystenunternehmen für Cybersicherheit, das unvoreingenommene Brancheneinblicke und Empfehlungen für Anbieter von Sicherheitslösungen und Fortune-100-Unternehmen bereitstellt. Das 2016 von Dr. Edward Amoroso, dem ehemaligen SVP/CSO von AT&T, gegründete Unternehmen widersetzt sich dem Trend der kostenpflichtigen Forschung, indem es eingehende Forschung, Marktanalysen, Beratung und personalisierte Inhalte anbietet, die auf Hunderten von Einsätzen mit Kunden und Nicht-Kunden gleichermaßen basieren - alles aus der Perspektive eines ehemaligen Praktikers.