SHARDSECURE

INFOPAPER

CLEVERES CLOUD-MANAGEMENT:

Wie Sie am Beispiel zweier Business Use Cases beim komplexen Thema Cloud-Security Kosten einsparen.

- Pascal Cronauer

Die Cloud-Technologie ist ein wichtiger Faktor für das digitale Business der Zukunft. Das Outsourcing seiner IT-Infrastruktur kann viele positive Effekte in Bezug auf die geschäftliche Agilität mit sich bringen. Sie ermöglicht hohe Geschwindigkeit, Flexibilität und Agilität bei der Anwendungsentwicklung und -modernisierung. Unternehmen haben einen schnellen Zugang zu einer Vielzahl von Tools, Prozessen und Dev-Ops-Abläufen. Die Herausforderung ist jedoch, die zunehmende Komplexität und das Management von Cloud-Umgebungen – vor allem was die Absicherung angeht.

Unternehmen, die in die Cloud migriert sind, stehen nunmehr vor der Herausforderung, ihre Sicherheit zu stärken und ihre Kosten innerhalb ihres bestehenden Cloud-Speichers zu minimieren.

Eine effiziente Möglichkeit zur Kostensenkung liegt bei der Datenspeicherung. Vor allem halbstrukturierte und unstrukturierte Datensätze wachsen exponentiell an, was zu höheren monatlichen Kosten für Cloud-Abonnements und einem massiven Ressourcenverbrauch führt. Unstrukturierte Daten wachsen derzeit viermal schneller als strukturierte Daten. Mit einem jährlichen Wachstum von 55 % bis 65 % machen sie mittlerweile mindestens 80 % aller Unternehmensdaten aus. Eine Cloud-Ressourcenoptimierung ist also notwendig, ebenso wie die Fähigkeit, die Cyberresilienz in der Cloud zu stärken.

ShardSecure bietet Kunden sowohl bei der Cloud-Optimierung als auch der Sicherheit - durch die transparente Integration mit Cloud-, Cloud-nahen und hybriden Speicherinfrastrukturen:

- Reduzierte Speicherkosten
- Verbesserte Datensicherheit im Ruhezustand
- Verbesserte Widerstandsfähigkeit
- Höhere Betriebszeit

Nachfolgend werden zwei unterschiedliche Einsatzmöglichkeiten der ShardSecure-Funktionalitäten vorgestellt. Der erste Business Use Case umschreibt Kosteneinsparungen mittels der eingesetzten Technologie. Der zweite Business Use Case beschreibt eine Lösung, wie die IT-Abteilung dem Fachkräftemangel entgegen wirken kann.

BUSINESS USE CASE #1

Kosteneinsparungen am Beispiel Amazon Web Services (AWS)

Als weltweit größter Cloud-Service-Provider bietet AWS viele verschiedene Lösungen, um den unterschiedlichen Speicherbedürfnissen für unstrukturierte Daten gerecht zu werden. Mit der richtigen Lösung können Unternehmen Kosten senken, ihre Agilität erhöhen, Time-to-Market reduzieren oder die Wartung der Infrastruktur optimieren.

Es gibt mehrere Haupttypen von Datenspeicherung bei AWS:

Amazon Elastic Block Store (EBS):
Ein Hochleistungs-Block-Speicherdienst, der für transaktionsintensive Workloads in jedem Maßstab konzipiert ist. EBS wird in Form einer virtuellen Festplatte bereitgestellt, die an Amazon Elastic Computer Cloud (EC2)-Instanzen angeschlossen wird, ähnlich wie die lokale Festplatte auf einer physischen Maschine.

Amazon Elastic File System (EFS):
Ein hochelastisches, skalierbares „Set-and-Forget"-Dateisystem, das Benutzern ermöglicht, Dateidaten ohne Bereitstellung oder Verwaltung von Speicherplatz zu teilen. Es kann mit sowohl Cloud- als auch On-Premises-Daten verwendet werden, wodurch Organisationen ihre Dateisysteme automatisch vergrößern und verkleinern können, wenn sie Dateien hinzufügen oder entfernen.

Amazon Simple Storage Service (S3):
Ein äußerst kostengünstiger Objektspeicher. S3 ist kosteneffizient, skalierbar und ideal für die Cloud-Speicherung. Es kann erhebliche Kosteneinsparungen im Vergleich nicht nur zu anderen AWS-Speichertypen, sondern auch zu traditionellem Speicher wie SSDs, NAS und SAN bieten.

Diese Arten von AWS-Speicher erfüllen unterschiedliche operative Bedürfnisse, ziehen aber auch ganz unterschiedliche Kosten nach sich. Zum Beispiel beträgt der Preis für S3 Infrequent Access US $ 0,013 pro GB pro Monat, während der Preis für EFS Standard US $ 0,3 pro GB pro Monat beträgt. Bei diesen Preisen würde eine Datenmenge von 250 TB pro Jahr US $ 38.400 in S3 und US $ 921.600 in EFS kosten - ein Faktor von 24 also.

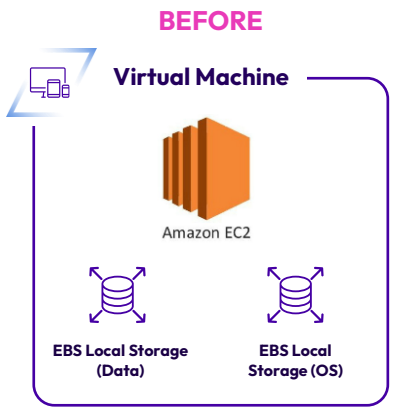
Kosten können nun wie folgt eingespart werden:

Einsatz der günstigeren Objektspeicherung (S3) anstelle teurer Speicher wie Elastic File System (EFS) und Elastic Block Storage (EBS).

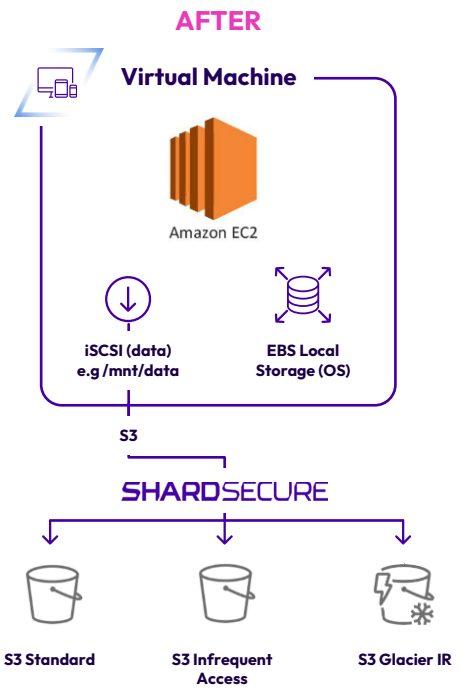
Verwenden Sie ShardSecure, um eine Zugriffsschicht bereitzustellen – somit können Legacy-Anwendungen Objektspeicherung umsetzen ohne Änderungen an der Applikation vornehmen zu müssen.

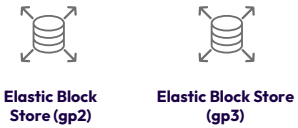
ShardSecure bietet darüber hinaus auch Datensicherheit, Widerstandsfähigkeit und Redundanz.

Kosten bei einem Umzug von EBS auf S3:



Relative List Cost of AWS Storage Options	
Storage Pricing	**PB/Month**
S3 Gracier Istant Retrieval	$ 4,194
S3 Infrequent Access	$ 13,107
S3 Standard	$ 22,020
EBS gp3	$ 83,886
EBS gp2	$ 131,072

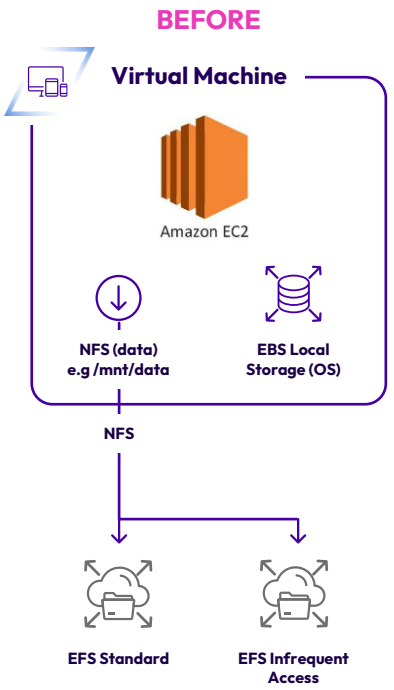




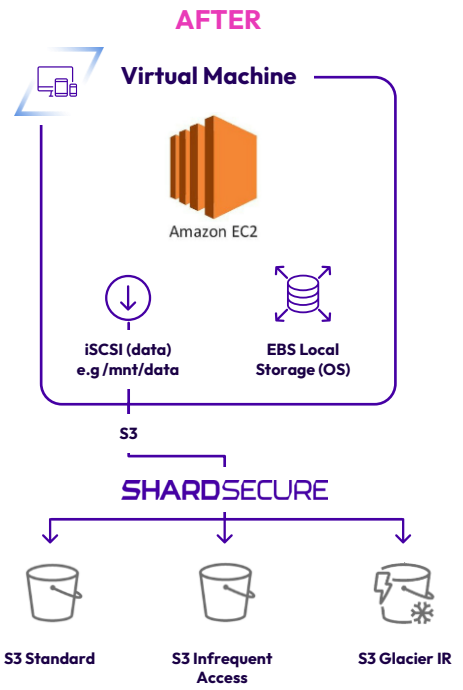
Storage Cost Multiplier	6x	4x	1x	0.6x	0.2x

ShardSecure kann Cloud-Nutzung zu optimieren und Daten in AWS schützen - einschließlich in Multi- und Hybrid-Cloud-Infrastrukturen - ohne Anwendungen neu zu schreiben, Datenflüsse neu zu gestalten oder das Benutzererlebnis zu verändern. Mit der transparenten Plug-and-Play-Technologie von ShardSecure können Unternehmen einfach Objektspeicher wie AWS S3 nutzen und von erheblich verbesserter Datensicherheit und Widerstandsfähigkeit profitieren.

Kosten beim Umzug von EFS auf S3:



Relative List Cost of AWS Storage Options	
Storage Pricing	**PB/Month**
S3 Gracier Istant Retrieval	$ 4,194
S3 Infrequent Access	$ 13,107
S3 Standard	$ 22,020
EFS Infrequent Access	$ 26,214
EFS Standard	$ 314,573



Storage Cost Multiplier	14x	1.2x	1x	0.6x	0.2x

Die ShardSecure-Lösung nutzt iSCSI, ein traditionelles SAN-Protokoll, um EBS- oder EFS-Speicher für den Server zu simulieren. Die Transparenz der Technologie bedeutet, dass Daten auf der Backend-Seite auf S3 verschoben werden können, um maximale Kosteneinsparungen mit praktisch keinen Änderungen an den Anwendungen des Unternehmens zu erzielen. Die Lösung eignet sich ideal für Unternehmen mit großen Datenmengen - das heißt, 250 TB oder mehr an EFS-Speicher. Die Leistung von ShardSecure ist der von EFS sehr ähnlich, so dass der Datenzugriff für die Benutzer schnell und einfach bleibt.

Cloud Security – mehr Resilienz von Nöten!

Eines der größten Risiken ist eine schwache Sicherheitskette. Cloud-Security umfasst Regeln, Prozesse und technische Vorgaben, um die Einhaltung gesetzlicher Vorschriften, den Schutz der Cloud-Infrastruktur und Anwendungen sowie die sichere Verarbeitung und Speicherung von Daten zu gewährleisten.

Starke Daten-Resilienz bedeutet, dass Organisationen in der Lage sind, ihren Regelbetrieb bei unerwarteten Ereignissen wie Cyberangriffen, Netzwerkausfällen, Datendiebstahl und mehr aufrechtzuerhalten. Ausfälle können auch dazu führen, dass Unternehmen gegen ihre Service-Level-Vereinbarungen verstoßen, die eine bestimmte Verfügbarkeit der IT-Systeme versprechen. Während Datensicherheitslösungen in der Regel die Privatsphäre und Vertraulichkeit schützen, garantieren sie nicht immer, dass kritische Daten bei einem Ausfall auch wieder verfügbar sein werden. Tatsächlich decken viele Werkzeuge zum Schutz von Daten im Ruhezustand - wie häufig verwendete Verschlüsselungs-, Authentifizierungs- und Anonymisierungsprodukte - Daten-Resilienz überhaupt nicht ab.

Mit *Microsharding* zu Cyberresilienz in der Cloud

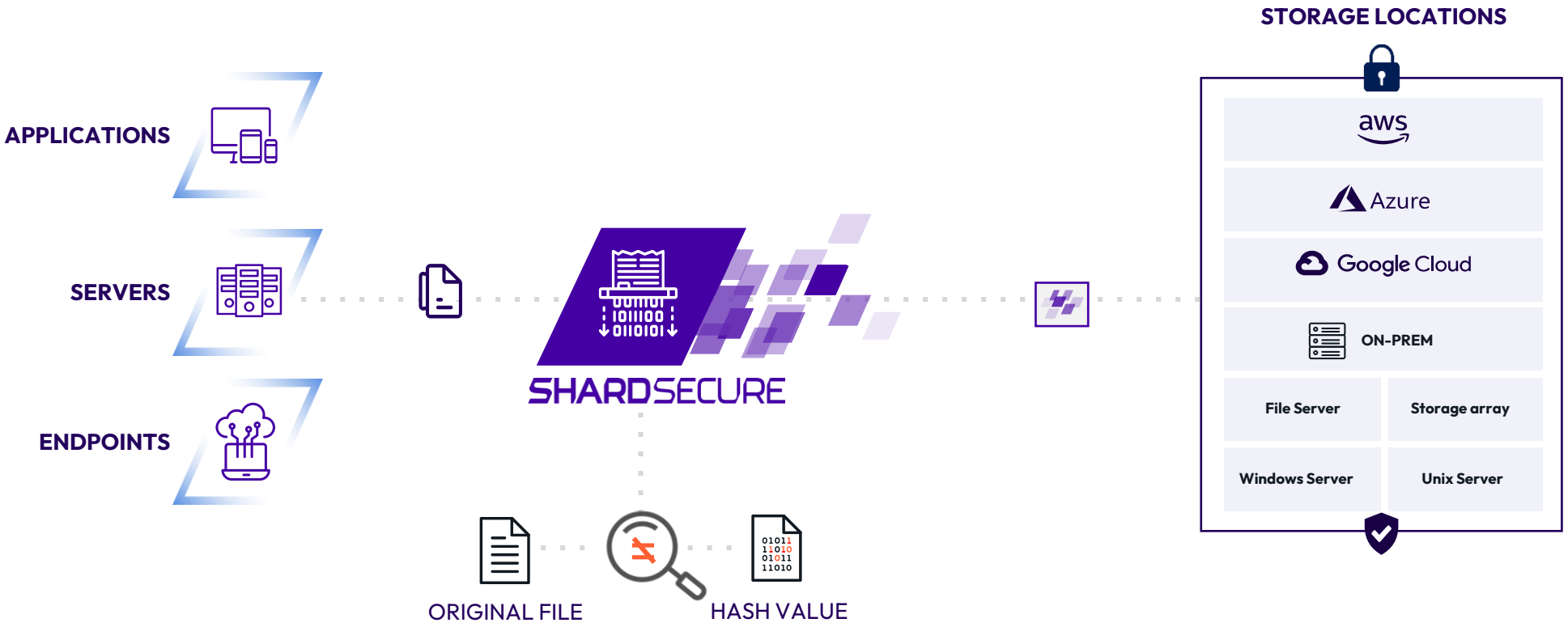
Eine vielversprechende Technik, um das Risiko einer Datenkompromittierung in einer Cloud-Hosting-Umgebung anzugehen, ist das Zerkleinern von Daten, auch Microsharding genannt. Diese Methode, die aus Algorithmen zur Datenverwaltung abgeleitet wurde, ist darauf ausgelegt, die Cyberrisiken bei dem Backend-Zugriff auf in der Cloud gehostete Daten zu eliminieren. Das Verfahren ist besonders gut geeignet für Multi-Cloud-Hosting, das in den meisten modernen Hybrid-Architekturen üblich geworden ist. Die Lösung arbeitet transparent und in Echtzeit, um Daten in Multi-Cloud- und Hybrid-Cloud-Konfigurationen zu verteilen und so die Resilienz zu verbessern.

Wichtige Daten werden also in mehrere Komponenten zerlegt, die dann voneinander getrennt, verschleiert und über unterschiedliche Cloud-Infrastrukturen gespeichert werden. Das Ergebnis: ein Backend-Zugriff auf die Daten durch Administratoren und andere privilegierten Zugänge führt nicht zu einem Datenbruch, da die Daten über mehrere Cloud-Speichereinheiten verteilt wurden.

Die Technologie bietet Funktionen, um die Daten-Resilienz bei Manipulationen, Löschungen, Ausfällen, Ransomware und anderen unerwarteten Ereignissen sicherzustellen. Daten können auch nach einer Attacke einfach wieder hergestellt werden.

ShardSecure: die innovative Alternative zur clientseitigen Verschlüsselung

Die clientseitige Verschlüsselung ist seit langem der Goldstandard für den Datenschutz. Sie verhindert, dass Drittanbieter Ihre sensiblen Daten einsehen können, und trägt dazu bei, dass persönliche Informationen bei Cyberangriffen nicht preisgegeben werden. ShardSecure erfüllt den gleichen Zweck wie die clientseitige Verschlüsselung und bietet starke Datenvertraulichkeit und -integrität. Aber es bietet auch Datenverfügbarkeit und hohe Widerstandsfähigkeit gegenüber Bedrohungen wie Cyberangriffen, und die Anforderungen an die Entwickler sind weitaus geringer.



Quelle: ShardSecure

Um den Datenschutz zu unterstützen, zerlegt ShardSecure in einem dreistufigem Prozess Dateien in Vier-Byte-große Einzelteile und verteilt diese “Datenschnipsel“ dann auf die unternehmenseigenen Speicherorte in Hybrid- und Multi-Cloud-Umgebungen. Eine Schlüsselrotation oder Neuverschlüsselung ist zu keinem Zeitpunkt erforderlich.

1. ZERKLEINERN

Zunächst werden die Daten in vier Byte große Einzelteile zerkleinert. Diese Datenschnipsel sind zu klein sind, um ein Geburtsdatum, eine ID-Nummer oder einen vollständigen sensiblen Datensatz zu enthalten. Durch die Demontage wird das Risiko eines direkten, Backend-basierten Zugriffs durch einen Insider oder Eindringling erheblich reduziert

2. MISCHEN

Anschließend werden toxische Daten hinzugefügt und die Einzeldaten werden in mehrere logische Container gemischt abgelegt. Identifizierende Informationen wie Dateierweiterungen, Dateinamen und andere Metadaten werden ebenfalls entfernt. Die Trennung der aufgeschlüsselten Bestandteile reduziert das Risiko eines unautorisierten Zugriffs.

3. VERTEILEN

Nach dem Mischen werden die Container in mehreren vom Kunden besessenen Speicher-Repositorys in Multi-Cloud- oder Hybrid-Cloud-Konfigurationen verteilt.

Das Verfahren der Datenzerkleinerung bietet darüber hinaus eine hohe Datensicherheit und trägt dazu bei, die Datenverfügbarkeit bei Ereignissen wie Providerausfällen und Ransomware-Angriffen aufrechtzuerhalten. Durch mehrfache Prüfungen der Datenintegrität und transparente Wiederzusammensetzung kompromittierter Speicherorte wird sichergestellt, dass Benutzer ohne Unterbrechung weiterarbeiten können.

Während sich einige Lösungen zur Daten-Resilienz nur auf die Datenverfügbarkeit konzentrieren, bietet ShardSecure gleich mehrere Überprüfungen in Bezug auf die Datenintegrität. Mit einer automatisierten Kontrolle wird innerhalb des Prüfungsprozesses auf die Datenintegrität unautorisierter Änderungen reagiert und die Daten werden in ihren früheren Zustand „zurückgebaut“. Wenn ein Container während des Zusammenbau-Prozesses eine Integritätsprüfung nicht besteht, wird das Sicherheitsteam informiert und der betroffene Container neu aufgebaut. Dies hilft sicherzustellen, dass verfügbare Daten auch korrekte und unveränderte Daten sind.

BUSINESS USE CASE #2

Der Einsatz von Microsharding macht in zwei Bereichen Sinn: Ein Unternehmen verschiebt wichtige Daten aus seiner bestehenden On-Premises-Umgebung in die Cloud oder ein Unternehmen, das bereits wichtige Daten in einer oder mehreren öffentlichen Clouds hostet, möchte sein Sicherheitsniveau verbessern.

Beispiel:

Wir führen die Kostenanalyse in einem fiktiven, mittelgroßen Unternehmen namens MÜLLER GmbH durch. Die MÜLLER GmbH hostet eine kritische Geschäftsanwendung namens AppX in der öffentlichen Amazon Web Services (AWS) Infrastruktur. Die kritischen Daten, die mit AppX verbunden sind, werden als S3-Objekte in Amazon S3 Storage Buckets gespeichert.

Die Kostengleichung für diese bei AWS gehosteten Daten der MÜLLER GmbH lassen sich wie folgt darstellen:

Basis-Kosten (AppX) = DevOps-Kosten (AppX) + Admin-Kosten (AppX) + Lizenzkosten (AppX) + Sicherheitskosten (AppX):

DevOps-Kosten beinhalten alle Entwicklungs-, Test-, Bereitstellungs-, Update- und Fehlerbehebungskosten. *Administrations-Kosten* umfassen die tägliche Pflege, Wartung, Überwachung und Unterstützung. *Lizenzkosten* beziehen sich auf Gebühren, die an Dritte für Software, Hosting oder andere Dienstleistungen gezahlt werden. *Sicherheitskosten* umfassen alle Maßnahmen zur Vorbeugung, Erkennung und Reaktion auf Cyberbedrohungen.

Die Größe der DevOps- und Admin-Kosten hängt von der lokalen Umgebung und ihrem Reifungszyklus ab. Organisationen, die über mehr Erfahrung und Expertise in diesen Bereichen verfügen, werden geringere Kosten haben. Wir gehen davon aus, dass keine besonderen Lizenzsituationen vorliegen und dass die MÜLLER GmbH branchenübliche Lizenzgebühren für alle datenbezogenen Hosting-Dienste zahlt.

Die Sicherheitskosten:

Die Kosten für den Schutz der Cloud gehosteten Anwendungen können zum einen in Präventionskosten und zum anderen in Erkennungs-/Reaktionskosten unterteilt werden. Präventionskosten sollen Cybersicherheitsbedrohungen vermeiden (oft als Verschiebung nach links bezeichnet), während Erkennungs-/Reaktionskosten zur Bewältigung laufender Angriffe (Verschiebung nach rechts) bestimmt sind.

Wir können daher die Kostengleichung der MÜLLER GmbH für AppX anpassen, um die folgenden Variablen zu berücksichtigen:

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

Cybersicherheitsexperten sind sich einig, dass die Erkennungs-/Reaktion die höchsten Sicherheitskosten darstellen.

Investitionskosten für die Lösung:

Die wichtigsten Kostenannahmen bei der Verwendung von Microsharding in der Cloud lassen sich wie folgt zusammenfassen: Wenn die Lösung mit einer zweiten Cloud (z.B. Microsoft Azure) eingeführt wird, sollten die folgenden Kosteneinflüsse erwartet werden:

DevOps: Keine Veränderung (3)
Admin: Keine Veränderung (3)
Lizenz: Erhöhung für Microsharding-Tool plus zweite AWS-Cloud (3 bis 4)
Prävention: Keine Veränderung (3)
Reaktion: Reduzierung aufgrund verringerter Vorfallwahrscheinlichkeit (3 bis 1)

Mit diesen Schätzungen lässt sich eine einfache Use-Case-Darstellung der Einführung des Verfahrens in eine typische Umgebung erstellen.

Vor der Einführung:

Kosten (Ungefähr) = 3 + 3 + 3 + 3 + 3 = 15

Nach der Einführung:

Kosten (Ungefähr) = 3 + 3 + 4 + 3 + 1 = 14

Beide Gleichungen sind so zu interpretieren, dass bei einer Erhöhung der Lizenzkosten entsprechende Reaktionskosten sinken. Im gezeigten Fall übersteigt die Reduzierung der Reaktionskosten die Erhöhung der Lizenzkosten, so dass ein positiver ROI vorliegt.

Wenn wir die Gleichungen nun in monetäre Investitionen übertragen ergibt dich folgendes Bild:
Durch die Einführung der Lösung ergibt sich eine Kostenveränderungen für die MÜLLER GmbH in Bezug auf AWS- und Microsoft-Lizenzen, dem Erwerb der Microsharding-Lizenz sowie die entsprechende Reduzierung der Reaktionskosten:

Vor der Einführung:

Lizenzkosten: Angenommen werden 500 TB bei 120 TEUR/Jahr für AWS
Reaktion: Angenommen werden 5 festangestellte Mitarbeiter: Lohnkosten ca. 500TEUR pro Jahr
Summe Lizenz- und Reaktionskosten: 620 TEUR jährlich

Nach der Einführung:

Lizenz: Angenommen werden 250 TB bei 65 TEUR pro Jahr bei AWS und 250 TB bei 65 TEUR pro Jahr bei
Lizenzkosten ca. 100.000 US-Dollar pro Jahr
Reaktion:
Einsparung: 2 festangestellte Mitarbeiter. Lohnkosten: 200TEUR pro Jahr
Gesamte Lizenz- und Reaktionskosten: 430.000 US-Dollar

Kostenersparnis: ca. 200 TEUR

Die Auswirkungen dieser Analyse zeigt, dass die MÜLLER GmbH in diesem hypothetischen Beispiel zwei Vollzeitstellen in seinem Incident-Response-Team abbauen kann, aufgrund einer erheblichen Reduktion der angenommenen kritischen Vorfälle in der Cloud. Trotz geringer Erhöhungen der Lizenzkosten für die öffentliche Cloud bei AWS und den Lizenzkosten für eine Lösung wie die von ShardSecure, werden die Gesamtkosten für die MÜLLER GmbH aufgrund der Entscheidung, die Sicherheitskonfiguration durch Microsharding zu verbessern, um fast 200 TEUR sinken.

Fazit

Innovation ist in jedem Bereich der Informationsverarbeitung Treiber und Katalysator, bestehende Modelle zu überdenken und zu verbessern. Insbesondere Cybersecurity ist nicht mehr denkbar, ohne dass bewährte Sicherheitslösungen um neue Technologien erweitert werden. Die mittlerweile vor uns liegenden Schwierigkeiten in der IT-Sicherheit können nur durch Innovation gelöst werden. Die SIEMs beispielsweise erreichen langsam ihre Leistungsgrenzen. Die Flut von Sicherheitsereignissen überfordern die Analysten auf lange Sicht. Mehr Analysten anzustellen, kann nicht die Lösung sein. Denn erstens sind sie nicht leicht zu finden und zweitens würden die Kosten ins Unermessliche steigen.
Doch für all die neuen vernetzten Funktionalitäten sind auch neue Sicherheitslösungen gefragt. Der einzige Ausweg aus dieser Misere ist, dass Sicherheit in Zukunft ein integraler Bestandteil von neuen digitalen Lösungen sein muss. Mancher Hersteller muss hierbei bestehende Businessmodelle überdenken und sich überlegen, wie er Sicherheit in seinen Produkten auch monetär zu einem Erfolgsfaktor macht. Nur wenn sich Sicherheit für alle Parteien auszahlt, wird eine substanzielle Sicherheit geschaffen, die wir in Zukunft dringend brauchen werden.

Source:
https://mitsloan.mit.edu/ideas-made-to-matter/tapping-power-unstructured-data

SHARDSECURE


@ShardSecure


@ShardSecure


@ShardSecure


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


info@shardsecure.com