SHARDSECURE

White Paper:

Die Minderung der Auswirkungen von Ransomware-Angriffen mit ShardSecure

Die stetig wachsende Bedrohung von Ransomware

Die Gefahr von Ransomware-Angriffen hat sich in den letzten Jahren kontinuierlich erhöht. Cybersecurity Ventures merkt an, dass alle 11 Sekunden ein Unternehmen Opfer eines Ransomware-Angriffs wird, während der Verizon Data Breach Investigations Report einen Anstieg von 13% im vergangenen Jahr schätzt. Bis 2031 wird prognostiziert, dass alle 2 Sekunden ein Ransomware-Angriff stattfinden wird.

Auch die Kosten von Ransomware-Angriffen steigen signifikant. Die durchschnittliche Lösegeldzahlung liegt mit über 1,5 Millionen US-Dollar pro Vorfall auf einem Allzeithoch. Wenn zusätzliche Kosten wie Dienstleistungen zur Schadensbehebung durch Dritte, regulatorische Geldstrafen, Ausfallzeiten und entgangene Einnahmen berücksichtigt werden, ist es nicht verwunderlich, dass die Wiederherstellung nach einem Angriff Unternehmen durchschnittlich 3,32 Millionen US-Dollar pro Vorfall kostet. Forschungen zeigen zudem, dass der Unternehmenswechsel zur Cloud neue Bedrohungsvektoren mit sich bringt und Angriffe, die sich ausschließlich auf die Datenextraktion konzentrieren, zunehmen.

Dieses Whitepaper untersucht die komplexen Herausforderungen, die durch Ransomware entstehen. Es erläutert auch, wie die ShardSecure-Plattform die verschiedenen Auswirkungen eines Ransomware-Angriffs, einschließlich Datenverschlüsselung und Datenextraktionsangriffe, durch Funktionen wie Selbstheilung und robuste Datenresilienz abmildert.

Die vielschichtige Bedrohung von Ransomware

Die potenziellen Folgen eines Ransomware-Angriffs sind schwerwiegend. Organisationen sehen sich nicht nur mit der unmittelbaren Störung ihrer Betriebsabläufe konfrontiert, sondern auch mit langfristigen Auswirkungen wie Rufschädigung, finanziellen Verlusten und rechtlichen Konsequenzen.

Verlust von Daten und Datenzugang

Die bekannteste Konsequenz eines Ransomware-Angriffs ist sein zentrales Merkmal: die Verhinderung des Zugangs zu geschäftskritischen Daten. Durch die Verschlüsselung von Daten können Angreifer ganze Unternehmen, Systeme und Dienste offline nehmen.

Es ist wichtig zu beachten, dass nur sehr wenige Organisationen in der Lage sind, nach einem Angriff all ihre Daten wiederzugewinnen, selbst wenn sie mit den Angreifern zusammenarbeiten. Laut einem Bericht von Sophos aus dem Jahr 2022 haben Organisationen, die Lösegelder zahlten, nur 61% ihrer Daten wiedererlangt, und nur 4% der Organisationen haben alle ihre Daten wiederhergestellt. Selbst wenn ein Unternehmen seine Systeme ohne Datenverlust wiederherstellen kann, sind die Ausfallzeiten wahrscheinlich kostspielig. Für Fortune-

1000-Unternehmen kann eine einzige Stunde Ausfallzeit bis zu 1 Million US-Dollar kosten.

Wenn Ransomware unentdeckt bleibt

Das Problem von Ransomware wird durch Varianten verschärft, die sich der Erkennung entziehen. Diese fortschrittlicheren Formen von Ransomware können Netzwerke infiltrieren, ohne von herkömmlichen Sicherheitsmaßnahmen entdeckt zu werden, was Angreifern ermöglicht, größeren Schaden anzurichten, höhere Lösegelder zu fordern und Datenbackups zu infizieren. Einige Ransomware zielt auch gezielt auf Backups ab. So verfügt eine Variante beispielsweise über die Fähigkeit, cloudbasierte Backups zu sperren, wenn Systeme kontinuierlich in Echtzeit sichern (z. B. während einer anhaltenden Synchronisation).

Doppelte Erpressung und Datenextraktion

Bei der Ransomware mit doppelter Erpressung exfiltrieren Cyberkriminelle sensible Daten von ihren Opfern, um sie als Druckmittel zu verwenden. Die Angreifer drohen dann, die gestohlenen Daten im Internet zu veröffentlichen – oft durch Verkauf oder Veröffentlichung im Darknet –, wenn das Lösegeld nicht gezahlt wird. Die Datenextraktion ist zu einem immer häufigeren Element von Ransomware-Angriffen geworden, da sie Cyberkriminellen mehr Einfluss verschafft und die Wahrscheinlichkeit erhöht, dass sie Zahlungen erhalten.

Eine blühende Branche: RaaS, KI und Angriffe auf Lieferketten

Die Prognose für Cloud-Ransomware bleibt düster. Der Aufstieg des Ransomware-as-a-Service (RaaS)-Modells hat zu einer Zunahme von Angriffen geführt, und neue Tools wie Künstliche Intelligenz haben dazu beigetragen, dass Ransomware immer raffinierter wird.

Geförderte, effektivere Phishing-Angriffe haben die Einstiegshürden für Cyberkriminelle gesenkt, was selbst solchen mit begrenzter technischer Expertise ermöglicht, bedeutende Angriffe durchzuführen. Gleichzeitig sind organisierte Ransomware-Banden in ihren Taktiken, Techniken und Verfahren (TTP) immer raffinierter geworden, indem sie tiefgehende Kenntnisse über Cybersicherheitslücken erlangen und technische Schwächen ausnutzen, um Systeme zu infiltrieren.

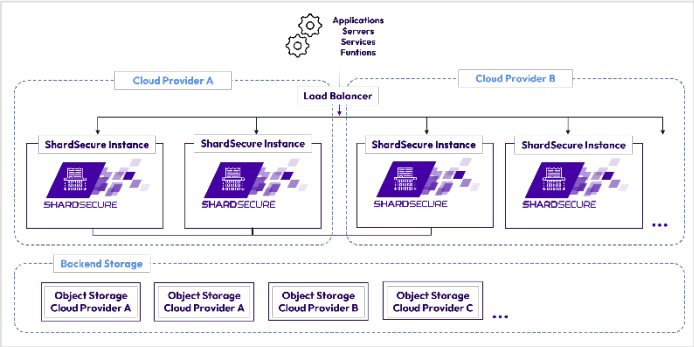
Ohne absehbares Ende herrscht Konsens darüber, dass Ransomware nicht mehr eine Frage des "ob", sondern des "wann" ist. Organisationen müssen einen proaktiven Ansatz in ihrer Cybersicherheit verfolgen und robuste Lösungen zur Datensicherung implementieren, um ihre sensiblen Daten vor Ransomware zu schützen.

Ransomware-Angriffe mit ShardSecure mindern

Die Funktionen für Datenintegritätsprüfungen, hohe Verfügbarkeit und Selbstheilung der ShardSecure-Plattform mindern die Auswirkungen von Ransomware-Angriffen. Die Plattform bietet Schutz überall dort, wo Daten gespeichert sind: lokal, in der Cloud oder in hybriden oder Multi-Cloud-Architekturen. Im Folgenden erklären wir, wie die ShardSecure-Plattform Ransomware-Angriffe mindert und Organisationen dabei hilft, ihre Geschäftskontinuität aufrechtzuerhalten.

Robuste Datenresilienz zur Aufrechterhaltung des Datenzugriffs während eines Angriffs

Die ShardSecure-Plattform bietet robuste Datenresilienz, einschließlich hoher Verfügbarkeit und Datenintegrität, um Unternehmen dabei zu helfen, den Datenzugriff während eines Ransomware-Angriffs aufrechtzuerhalten.



Um hohe Verfügbarkeit zu erreichen, ist jede Instanz von ShardSecure ein virtuelles Cluster, das lokal, in der Cloud oder in hybriden Cloud-Architekturen betrieben werden kann. Kunden können zwei oder mehr virtuelle Cluster für Failover konfigurieren, was eine hohe Verfügbarkeit über mehrere Clouds hinweg ermöglicht sowie in hybriden Cloud-Umgebungen, die eine Mischung aus lokalen, privaten Cloud- und Drittanbieter-Cloud-Providern wie AWS, Azure und GCP verwenden.

Automatische Datenmigration zur Verhinderung wiederholter Angriffe.

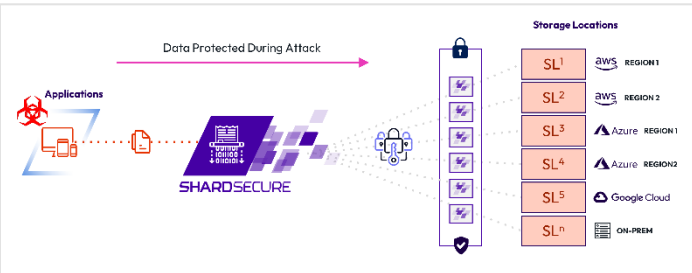
Die automatische Datenmigrationsfunktion der ShardSecure-Plattform ermöglicht es Kunden, alternative Speicherorte zu konfigurieren. Benutzerkonfigurierbare Schwellenwerte können so eingestellt werden, dass bei X Anzahl von Datenintegritätsprüfungen, die in einem Zeitraum von Y fehlschlagen, alle Daten im Tier-1-Speicher automatisch zu Tier-2 migriert werden. Diese Migration erfolgt im Hintergrund ohne Ausfallzeiten und gewährleistet einen nahtlosen Übergang zum sicheren alternativen Ort.

Automatische Selbstheilung zur Rekonstruktion verlorener oder kompromittierter Daten.

Wenn ein Speicherort eine Datenintegritäts-Health-Check wegen eines Ransomware-Angriffs oder anderer Formen der Datenmanipulation nicht besteht, rekonstruiert die Selbstheilungsfunktion der ShardSecure-Plattform automatisch die betroffenen Daten. Die Funktion arbeitet transparent und ohne Benutzer oder Datenflüsse zu stören, sodass Organisationen ihre Geschäftskontinuität während eines Angriffs aufrechterhalten können. Die Selbstheilungsfunktion arbeitet auch daran, Daten zu rekonstruieren, die von Ransomware-Angreifern gelöscht wurden, die manchmal Daten löschen, wenn sie diese nicht für profitabel halten.

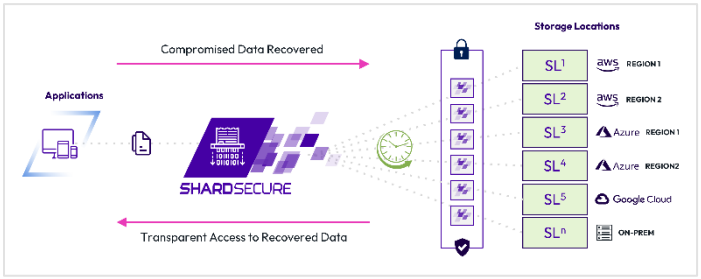
Unveränderliche Speicherschnittstelle und Rollback für schnelle Ransomware-Wiederherstellung.

Credential Missbrauch tritt auf, wenn Ransomware-Angreifer gestohlene Anmeldedaten verwenden, um unbefugten Zugriff auf kritische Daten zu erhalten und diese zu verschlüsseln. Um das Risiko und den potenziellen Schaden durch Credential-basierte Ransomware-Angriffe zu mindern, bietet ShardSecure Funktionen wie Objektsperren und eine unveränderliche Speicherschnittstelle, um sicherzustellen, dass wertvolle Daten verfügbar, genau und sicher bleiben.



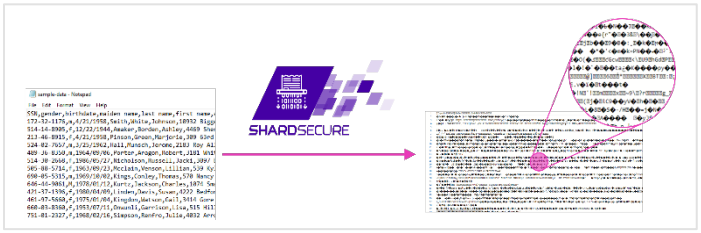
Im Falle eines Credential-basierten Ransomware-Angriffs können Daten zurückgesetzt und auf einen Zeitpunkt vor dem Angriff wiederhergestellt werden, um schnelle Wiederherstellungsbemühungen zu unterstützen. Diese Fähigkeiten reduzieren erheblich die Abhängigkeit von traditionellen Wiederherstellungstechniken von zeitaufwendigen und arbeitsintensiven letzten Ausweg-Backup-Lösungen.

Automatische Benachrichtigungen an das Security Operations Center (SOC) im Falle eines Angriffs. Wenn ein Speicherort bei einer Datenintegritätsprüfung durchfällt, sendet die ShardSecure-Plattform automatisch eine Benachrichtigung an das SOC-Team. Diese Funktion dient als Frühwarnsystem für Sicherheitsteams, um eine schnellere Erkennung, Untersuchung und Behebung zu ermöglichen und somit die Wahrscheinlichkeit zu verringern, dass die Ransomware unentdeckt bleibt.



Schutz vor Datenexfiltration Die ShardSecure-Plattform mindert doppelte

Erpressungsangriffe, indem sie Daten für unbefugte Benutzer unleserlich macht. Wenn ein Angreifer direkt auf die Speicherorte einer Organisation zugreifen kann, um Daten zu exfiltrieren, bleiben diese Daten unlesbar und nicht nutzbar. Sie können von unbefugten Benutzern nicht rekonstruiert werden, sodass selbst die sensibelsten Informationen weder veröffentlicht noch für Erpressungszwecke verwendet werden können. Unser innovativer Ansatz zur Dateiverschlüsselung bietet fortschrittlichen Datenschutz für sensible Daten, unabhängig von deren Speicherort.



Vereinheitlichte, plattformübergreifende Plattform über mehrere Clouds

Die ShardSecure-Plattform bietet eine einfache, agentenlose Integration und Verwaltung ohne den Overhead und die Komplexität traditioneller Datensicherheitslösungen und ohne Änderungen an Anwendungsverhalten oder Datenflüssen vornehmen zu müssen. Die Plattform ist infrastruktur- und anbieteragnostisch und vollständig transparent für bestehende Dienste und Anwendungen. Jede Instanz der ShardSecure-Plattform ist ein virtueller Cluster, der vor Ort oder in der Cloud bereitgestellt werden kann. Die S3-kompatible API, SMB/NFS- und iSCSI-Schnittstellen ermöglichen es Anwendungen, zu ShardSecure zu migrieren, mit minimalen bis keinen Konfigurationsänderungen. Daher hat ShardSecure nur minimale Auswirkungen auf Entwicklungsteams und Betriebsabläufe. Die ShardSecure-Plattform arbeitet im

Hintergrund als transparentes, ausfallsicheres Ereignis, und der Datenschutz wird ohne die Notwendigkeit erheblicher Ressourcen für die Pflege komplexer Systeme erreicht.

Fazit Mit zunehmender Vernetzung der digitalen Landschaft wächst der Schaden durch Ransomware-Angriffe weiter an. Die Anzahl und die Kosten der Angriffe steigen, und die Herausforderungen für Organisationen sind zahlreich und komplex. Die ShardSecure-Plattform mindert Ransomware durch robuste Datenresilienz, automatische Selbstheilung, SOC-Benachrichtigungen und Schutz vor Datenexfiltration. Ihre Funktionen helfen Organisationen, sensible Informationen zu schützen und die finanziellen Verluste sowie den Rufschaden von Ransomware-Angriffen zu vermeiden. Für weitere Informationen darüber, wie ShardSecure Organisationen in den Bereichen Finanzdienstleistungen, Gesundheitswesen, Fertigung und Biotechnologie bei der Stärkung ihrer Datensicherheit unterstützt, besuchen Sie uns online oder vereinbaren Sie eine Demo.

Fazit

Mit zunehmender Vernetzung der digitalen Landschaft nimmt der durch Ransomware verursachte Schaden weiter zu. Die Anzahl und die Kosten von Angriffen steigen, und die Herausforderungen für Organisationen sind zahlreich und komplex. Die ShardSecure-Plattform begegnet Ransomware mit robuster Datenresilienz, automatischer Selbstheilung, SOC-Benachrichtigungen und Schutz vor Datenabfluss. Ihre Funktionen unterstützen Organisationen dabei, sensible Informationen zu schützen und die finanziellen Verluste sowie den Rufschaden durch Ransomware-Angriffe zu vermeiden. Für weitere Informationen darüber, wie ShardSecure Organisationen im Finanzdienstleistungssektor, im Gesundheitswesen, in der Fertigung und Biotechnologie dabei hilft, ihre Datensicherheit zu stärken, besuchen Sie uns online oder vereinbaren Sie eine Demo.

https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
https://www.scmagazine.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023
https://www.sans.org/blog/ransomware-in-the-cloud/
https://www.csoonline.com/article/575307/insured-companies-more-likely-to-be-ransomware-victims-sometimes-more-than-once.html
https://www.atlassian.com/incident-management/kpis/cost-of-downtime
https://www.cisecurity.org/insights/blog/ransomware-facts-threats-and-countermeasures
https://www.trendmicro.com/en_us/ciso/22/i/prevent-ransomware-as-a-service-raas-attacks.html
https://www.forbes.com/sites/forbestechcouncil/2021/09/27/ransomware-gangs-who-are-they-and-how-to-stop-them
https://technative.io/2023-the-year-ransomware-is-no-longer-an-if-but-a-when/

@ShardSecure
@ShardSecure
@ShardSecure

ShardSecure GmbH
Mühldorfstr. 8
81671 München

info@shardsecure.com