WHITE PAPER

Verständnis der Auswirkungen **umfassender Datensicherheit**

SCALE TO WIN

INFINIDAT

Die herausforderungen

2017 war kein einfaches Jahr für einen CIO / CISO, und auch 2018 gibt es derzeit keine Anzeichen dafür, dass es einfacher wird. Bei so vielen Datenverstößen, die sogar Karrieren beendeten, allein im Jahr 2017 (Equifax, Uber, Yahoo, um nur einige zu nennen) und mit weltweit verschärften regulatorischen Anforderungen haben CIOs / CISOs die unternehmerische Verantwortung, ihren Ansatz zur Datensicherheit zu überdenken.

Abgesehen von der Einhaltung gesetzlicher Vorschriften sind Unternehmen gegenüber ihren Kunden und Aktionären verpflichtet, Daten zu schützen und ihre Gefährdung nicht nur gegenüber externen Angreifern, sondern auch gegenüber Mitarbeitern zu minimieren. Die im Jahr 2017 am häufigsten genutzte Methode für Datendiebstahl war das Phishing, welches sich an interne Mitarbeiter von Unternehmen richtete (siehe Report zur Untersuchung von Datenverstößen im Jahr 2017). Damit wurden diese Mitarbeiter unwissentlich mitschuldig an der Datenverletzung: Über 80% der erfolgreichen Cyber-Angriffe erfolgten über den menschlichen Faktor als kritische Schwachstelle. Der Nicht-IT-Profi, der eine E-Mail von seinem kompromittierten besten Freund erhielt und einen Anhang öffnete, der Mitarbeiter, der auf eine gefährdete Website zugriff und so eine Lücke im Sicherheitswall seines Unternehmens erzeugte. Obwohl es keinen 100%igen Schutz gibt, lässt sich das Risiko durch vernünftige Regeln verringern.

Es gibt zwei Begriffe, die wir beachten müssen, wenn wir uns mit dem Schutz von Daten vor Hackern beschäftigen:

> ***„Die Angriffsfläche einer Softwareumgebung ist die Summe der verschiedenen Punkte (der „Angriffsvektoren“), an denen ein nicht autorisierter Benutzer (der „Angreifer“) versuchen kann, Daten in eine Umgebung einzugeben oder aus ihr zu extrahieren. Die Angriffsfläche so klein wie möglich zu halten, ist eine grundlegende Sicherheitsmaßnahme.”*** *(Wikipedia)*

Wenn ein Unternehmen seine Daten als Quelle seines Wettbewerbsvorteils betrachtet und versteht, wie sensibel dieser Bereich für seine Kunden ist, wie kann es also seine Angriffsfläche minimieren, und wie wird dies durch AFAs (All Flash Arrays) erschwert?

Wenn das organigramm die sicherheitsmethode vorschreibt

Conways Gesetz hat uns längst gelehrt, dass die Organisationsstruktur oft mehr als alles andere die Ergebnisse / das Design beeinflusst. Im Zusammenhang mit der Sicherheit ist das ziemlich einfach: Haben CISO und Storage-Manager eine gute Beziehung, werden die Daten höchstwahrscheinlich auf der Speicherebene verschlüsselt, und das Kästchen „Verschlüsselung" wird aktiviert.

Storage ist auch der „Weg des geringsten Widerstands", da Storage-Arrays sofort eine Verschlüsselung ohne Leistungseinbußen ermöglichen können.

Aber hilft die Verschlüsselung auf Speicherebene auch dabei, Ihre Angriffsfläche zu minimieren? Ein bisschen, ja. Allerdings bleiben ALLE anderen Schichten zwischen Nutzer durch Anwendung und Infrastruktur noch unverschlüsselt, und die Daten durchlaufen das Netzwerk ungeschützt.

Wo sollen wir die daten also verschlüsseln?

Stellen Sie es sich so vor - je höher in der Prozesskette persönliche oder sensible Daten verschlüsselt werden, desto mehr Ebenen werden geschützt. In der folgenden Tabelle stellt jede Zeile eine mögliche Verschlüsselungsebene und jede Spalte eine Angriffsfläche dar.

Sehe Sie, wie wenig die Verschlüsselung auf Speicherebene tatsächlich schützt? Und doch ist dies eine weit verbreitete Datensicherheitsmaßnahme (und oft sogar die Einzige).

Wo wird die Verschlüsselung verwendet?	**✓ Wer kann die Daten sehen?** / **⚠ Wer kann versehentlich eine Datenschutzverletzung verursachen?**						
	App Admin	OSf Admin	DBA	VM Admin	Netzwerk Admin	Storage Admin	Backup Admin
Applikation	⚠	✓	✓	✓	✓	✓	✓
Applikation OSf	⚠	⚠	✓	✓	✓	✓	✓
Datenbank	⚠	⚠	⚠	✓	✓	✓	✓
VM-Verschlüsselung	⚠	⚠	⚠	⚠	✓	✓	✓
Struktur (Daten in der Übertragung)	⚠	⚠	⚠	⚠	✓	⚠	⚠
Speicherung	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Backup	⚠	⚠	⚠	⚠	⚠	⚠	⚠

Wie vergrössern All-flash-arrays ihre Angriffsfläche?

Während die meisten (wenn nicht alle) AFAs eine Verschlüsselung auf Festplattenebene anbieten, ist dies allerdings auch die einzige Verschlüsselungsstufe, die sie zulassen. Werden Daten irgendwo anders verschlüsselt, können AFAs keine Datenreduktion durchführen und dies verwirft die gesamte Wirtschaftlichkeit von AFAs. AFAs müssen sich auf Datenreduktion (im Verhältnis 3:1 bis 6:1) verlassen, um den Preisaufschlag so gering wie möglich zu halten.

Wenn “optimal” auf machbar trifft

DIESER OPTIMALE ANSATZ ZUR DATENSICHERHEIT WIRD OFT DURCH BEREITS VORHANDENE REALITÄTEN EINGESCHRÄNKT:

- die zehn Jahre alte Anwendung, die keine Verschlüsselung bietet und nicht mehr unterstützt wird.
- die geschäftskritische Anwendung, deren Wartung ein Jahr in Anspruch nimmt.
- der Anwendungsverantwortliche, der sich weigert, Zeit für die Verschlüsselung der Daten zu investieren.

Kommt es zur realen Umsetzung in der Praxis, sind oft Kompromisse nötig, um die Einführung der Datensicherheit zu beschleunigen. Viele werden sich dafür entscheiden, diese Umgebungen in niedrigeren Ebenen des Stacks (DB / VM / OS) zu verschlüsseln, um die Unternehmensanforderungen und die Anforderungen der Aufsichtsbehörden zu erfüllen. Auch wenn dieser Ansatz oft notwendig ist, um die Fristen einzuhalten, lohnt es sich aber doch, die Anzahl der einzelnen Ansätze zu begrenzen, um einen hohen Verwaltungsaufwand zu vermeiden. Es ist hierbei auch anzumerken, dass alle diese Alternativen den gleichen Effekt haben: die Datenreduktionsfähigkeiten der AFAs zu zerstören und ihre Gesamtbetriebskosten (Total Cost of Ownership – TCO) zu erhöhen.

Zusätzliche Vorteile der Verschlüsselung des Stacks

WORKLOAD-VERTEILUNG UND PERFORMANCE

Mit Ausnahme von Self Encrypting Drives (SED) benötigt die Verschlüsselung eine gewisse CPU-Leistung. Ein IT-Stack hat immer mehr Hosts als Speicher-Arrays; die Verlagerung der Aufgabe der Datenverschlüsselung auf eine höhere Ebene im Stack führt auch zu einer breiteren Workload-Verteilung, wodurch die Arbeitslast auf den einzelnen Geräten reduziert und somit die Gesamtleistung verbessert wird.

GRANULARITÄT

Je höher der Stack, den wir verschlüsseln, desto besser ist die Granularität: Eine Anwendung kann nur Personal Identifiable Information (PII) verschlüsseln, da sie den Kontext / die Bedeutung der Daten „versteht". Dies wird auch zu geringeren Betriebskosten führen. Gehen wir eine Ebene tiefer, kann der Datenbankadministrator (DBA) einen verschlüsselten und einen unverschlüsselten Tablespace bereitstellen und die richtigen Daten an den richtigen Ort bringen. Dies ist zwar weniger granular, aber immer noch besser als eine ganze VM oder LUN zu verschlüsseln.

EINSATZBEREITSCHAFT FÜR DIE CLOUD

Die Verschiebung der Verschlüsselung nach oben ist eine Voraussetzung für jede Cloud-Migration, wenn die Daten das gleiche Schutzniveau beibehalten sollen, auch über das WAN. Verschlüsselte Daten können ohne zusätzliche Sicherheitsmechanismen (wie z. B. Verschlüsselungsmanagement auf Cloud-Ebene) sicher in die Cloud verschoben oder im Burst-Modus übertragen werden.

EINFACHE INTEGRATION

Die Integration der OS-, DB- oder Hypervisor-Ebenen hat einen Vorteil: Von ihnen gibt es nur wenige Varianten, während es viele Anwendungen in der IT-Umgebung gibt. Aus operativer Sicht kann dies die Komplexität reduzieren.

AUFRUF ZUM HANDELN

- Planen Sie die ganzheitliche Datenschutzrichtlinie Ihres Unternehmens
- Legen Sie einen Stichtag für neue Anwendungen fest, die ab dem ersten Tag verschlüsselt werden sollen
- Schulen Sie interne Anwendungsentwickler in konzeptionsintegrierten Sicherheitsmethoden
- Überprüfen Sie vorhandene Anwendungen, für den richtigen Weg für Ihr Unternehmen, Daten während des Flugs zu schützen
- Erstellen Sie einen Übergangsplan, um ältere Anwendungen mit privaten oder vertraulichen Daten zu verschlüsseln