WHITE PAPER

最も強固なデータの安全性を紐解く

SCALE TO WIN

INFINIDAT

直面する課題

2017年は世のCIO/CISOにとって大変な年でしたが、2018年になっても事態が好転する兆しは見えません。昨年は、Equifax、Uber、Yahooと1年の間にデータ漏えい事件がいくつも発生しており、世界的に規制が強化される中で企業の社会的責任を果たすべく、CIO/CISOにはデータセキュリティに対するアプローチの見直しが迫られています。

コンプライアンスは別にしても、企業には顧客や株主に対して責任があり、データを保護し、外部からの攻撃のみならず従業員への開示も最小限にとどめるよう努力する必要があります。2017年に多く見られたデータ漏えいの手口は、社内の従業員から送信されたフィッシングによるものでした（2018年データ漏えい調査報告書参照）（2017年版　データ漏洩/侵害調査報告書参照）。このように従業員は知らず知らずのうちにデータ漏えいに加担することになっているのです。成功したサイバー攻撃の80%以上で決定的な役割を果たしたのは人的要素です。ITに詳しくない普通の従業員が親しい友人から受け取った電子メールの添付ファイルを開いたり、危険なウェブサイトにアクセスしたりして、セキュリティ防御に穴をあけているのです。100%の防御などできないとはいえ、リスクを低減するためにはいくつか常識的なルールがあります。

ハッカーからデータを守ることについて考える時 、常に頭に入れておくべきことが2つあります。

> **「ソフトウェア環境の攻撃サーフェスは、不正ユーザー（“攻撃者”）がデータに侵入したり、データを引き出したりすることのできる異なるポイント（“攻撃のベクトル”）の総和である。攻撃サーフェスをできるだけ小さくすることがセキュリティ対策の基本である」**（Wikipedia）

もし企業が保有するデータをビジネスにおける優位性を生み出す源として扱い、それが顧客にとってどれほど秘密にしておくべきものであるかが分かっているなら、攻撃サーフェスをどのように最少化すべきでしょうか?また、オールフラッシュアレイ（AFA）はそれをどのように妨げているのでしょうか?

組織の体制がセキュリティ手法を決定づける

コンウェイの法則は、組織の構造が往々にして結果に影響を及ぼすことをずっと前から教えてくれています。これは何よりも設計に当てはまります。セキュリティに当てはめるなら、至ってシンプルなことです。もしCISOとストレージ責任者とが良好な関係にあれば、データはストレージレイヤーに暗号化されて格納される可能性が高く、“暗号”の入ったボックスはきちんとチェックされるはずです。

ストレージアレイはパフォーマンスを落とすことなくその場で暗号化でき、ストレージも “抵抗の最も少ないパス”になります。

しかし、ストレージレベルでの暗号化が攻撃サーフェスを狭める役に立つでしょうか？　少しは役に立つでしょう。しかし、ユーザーからアプリケーションやインフラストラクチャに至るまで、それ以外のすべてのレイヤーが暗号化されないままであれば、データの移動に伴ってネットワークを無防備な状態にしてしまいます。

どこでデータを暗号化するべきか

こんな風に考えてみてください。上位になればなるほど個人データや機密データが暗号化され、より多くのレイヤーが守られます。下の表の縦の項目は暗号化可能なレイヤー、横の項目は攻撃サーフェス（攻撃対象）を示しています。

ストレージレベルの暗号化が実際にはほとんどデータ保護に役立っていないことにお気づきですか？
それにもかかわらず、これがデータセキュリティの手法として幅広く用いられており、かつ唯一のセキュリティになっているというケースがよくあります。

暗号化技術が使われる場所	✓ データを見ることができるのは誰か？ ⚠ 漏えいの原因を作る可能性があるのは誰か？						
	アプリケーション管理者	OS 管理者	DBA（データベース管理者）	VM 管理者	ネットワーク管理者	ストレージ管理者	バックアップ管理者
アプリケーション	⚠	✓	✓	✓	✓	✓	✓
アプリケーション O	⚠	⚠	✓	✓	✓	✓	✓
データベース	⚠	⚠	⚠	✓	✓	✓	✓
VM 暗号化	⚠	⚠	⚠	⚠	✓	✓	✓
ファブリック（移動中のデータ）	⚠	⚠	⚠	⚠	✓	⚠	⚠
ストレージ	⚠	⚠	⚠	⚠	⚠	⚠	⚠
バックアップ	⚠	⚠	⚠	⚠	⚠	⚠	⚠

オールフラッシュアレイが攻撃サーフェス(攻撃対象領域)を拡大

すべてとは言わないまでも、ほとんどのオールフラッシュアレイ(AFA)はディスクレベルで暗号化を行い、これが暗号化できる唯一のレベルとなっています。データがそれ以外のどこかで暗号化されるとAFAではデータを処理できず、AFA経済全体が破たんしてしまいます。AFAの場合、追加料金を最小限に抑えて手ごろな料金まで価格を引き下げるには、データを整理して処理(3:1〜6:1の割合で削減)できなければならないのです。

"最適"と実現可能性の両立

このようなデータセキュリティのための"最適な"アプローチは、既に存在している事柄によってしばしば制約を受けます。

- 暗号化機能を持たず、サポートも終了した10年来使用しているアプリケーション
- 保守管理に1年かかる基幹業務アプリケーション
- データ暗号化に時間をかけることを拒否するアプリケーション所有者

実際にスタートする段階になると、データセキュリティの導入を加速するためにさまざまな妥協が必要になることもよくあります。多くの場合、企業や規制当局の要件を順守するために、こうした環境でスタックのより低いレベル(DB / VM / OS)での暗号化を行う道を選択することになるでしょう。このアプローチではしばしばコンプライアンス適用開始時期に合わせる必要があるものの、管理経費の上昇を避けるためにアプローチの数を限定する意味はあります。また、どの選択肢を選んでも効果は同じであることに気が付くという点でも価値があります。AFAのデータ整理機能が破壊されると総所有コスト(TCO)が上昇するということです。

スタック上位の暗号化のその他の利点

ワークロードの分散とパフォーマンス

自己暗号化ドライブ(SED)を除き、暗号化には何らかのCPUパワーが必要です。ITスタックには常にストレージアレイよりも多くのホストがあり、データ暗号化タスクをスタックの上位レベルに移動することでワークロードをより分散させ、デバイスごとの負荷を低減して全体のパフォーマンスを向上できます。

粒度

スタックの上位を暗号化すればするほど、より粒度を上げることができます 。

アプリケーションは文脈やデータの意味を“理解”して初めて個人を特定できる情報(PII)を暗号化できます。これはオーバーヘッドの低減にもつながります。その1つ下にレベルを下げれば、データベース管理者(DBA)の表の欄は暗号化、非暗号化とすることができ、適切なデータを適切な場所に収めることができます。粒度は下がるものの、VMやLUN全体を暗号化するよりは良い結果になります。

クラウドへの対応

WANを含め、あらゆるクラウドへの移行でデータの保護レベルを維持する必要がある場合には、スタックの中で暗号化のレベルを上げることが必須条件になります。暗号化することでデータはクラウド内で安全に移動したり分散させたりすることができ、別のセキュリティメカニズム(クラウドレベルの暗号化管理など)を追加する必要はなくなります。

容易な統合

OS、DBあるいはハイパーバイザーレベルを統合することには利点があります。それぞれにいくつかのフレーバーがあり、この環境には多くのアプリケーションがあります。これによってオペレーション面での複雑さを低減することができます。

アクション確認事項

- ▶ 組織の全体的なデータ保護ポリシーを計画する
- ▶ 新規構築のアプリケーションには最初から暗号化を計画する
- ▶ 社内で開発するアプリケーションの開発者にセキュリティデザイン手法についてトレーニングし重要性を認識させる
- ▶ 既存のアプリケーションを調査し、データの送受信のデータを保護する方法を確立する
- ▶ 個人情報や機密データを保護するためにレガシーアプリケーション暗号化の移行プランを立案する