ソフトウェア暗号化と規制遵守比較的に低コストで大半のセキュリティリスクに対応するソリューション

規制とコンプライアンスの要件

今までデータセキュリティは IT 部門に限定されていましたが、消費者データの漏洩が相次いだため、世界各国の政府は個人を特定できるデータをすべて暗号化して保護する義務を、さらに厳しく企業に課すようになっています。

医療分野の HIPAA から、EMEA の GDPR やカリフォルニアの CCPA まで、規制によってデータクラス保護のための暗号化が義務付けられています。それらの規制と関連する罰金や法的賠償リスクが著しく増加したため、コンプライアンス組織の数も過去３年あまりで急増しました。

このような変化を受けて、IT 部門はセキュリティの維持とコスト上昇の課題に直面しています。コロナ禍のため、データ暗号化に重点的に取り組むための費用は後回しにされ、予算はハードウェアの追加とファイアウォールへの投資に費やされています。

実際に Microsoft BitLocker® や、Symantec、McAfee などの会社のエンドポイント管理ソフトウェアを使用したソフトウェア暗号化が増加しています。一部の企業や消費者は、一部のベンダが提供するソフトウェア「Vault」ドライブ付きの標準的な USB ドライブも使用しています。

暗号化とデータ転送

従業員や消費者は、データを持ち運ぶ必要があります。使用できる選択肢には、次のものがあります。

1. クラウドサービス：長所は、インターネットに接続できれば、どんなデバイスからでもアクセスできることです。しかし、柔軟性には代償があります。クラウドにデータを保存すると、ユーザーや企業がデータを管理できなくなり、ご存知のようにサーバーのロックが解除されるか、アクセスされる潜在的リスクがあります。
2. 標準的な USB ドライブ：USB ドライブを携帯する方が安全に見えますが、ドライブを複製してデータ漏洩が起きるリスクは甚大です。たとえば、機密情報の入った USB ドライブを紛失した事例や、クリーニング店の引き出しに忘れ物の USB ドライブがたくさん入っている事例などがあります。
3. ハードウェア暗号化 USB ドライブ：これらの USB ドライブには、オンボード暗号化コントローラとアクセス制御を組み込んだカスタムアーキテクチャがあります。データは一般に、XTS モードで最強の AES-256 ビット暗号化機能によって暗号化され、その他にも物理攻撃およびファームウェア攻撃を軽減する保護機能が搭載されています。これらのドライブは、セキュリティデバイスの専門企業によって製造され、標準的な USB ドライブより高価で、データセキュリティに優れています。FIPS 197 または FIPS 140-2 レベル 3 ドライブは保護レベルが高く安心できます。
4. ソフトウェア暗号化を搭載した標準的な USB ドライブ：規制で要求されるセキュリティには、BitLocker などのツールを使ったソフトウェア暗号化を使用できます。比較的安価で、AES-256 XTS と同等の暗号化を利用できるため、妥当な選択肢です。

当然、企業や業界では多くの場合、４つ目の選択肢の「ソフトウェア暗号化を搭載した標準的な USB ドライブ」を使用しています。その主な理由は、BitLocker などのデータ保管ユーティリティが「無料」だからです。

ソフトウェア暗号化は規制に準拠していない

ビジネスセキュリティ専門家にとって、ソフトウェア暗号化は、高価なハードウェア暗号化 USB ドライブとまったく同じ暗号化機能を提供できます。しかしそれで大丈夫でしょうか？予算が限られているため、企業はコンプライアンス対応のためにソフトウェア暗号化に移行しつつありますが、ソフトウェア暗号化の短所を認識していません。

ソフトウェア暗号化 USB ドライブの問題とは何でしょうか？使用していないデータや転送中のデータが AES-256 XTS で暗号化されていますか？一般的には、暗号化されています。問題は、ソフトウェア暗号化が「除去可能な暗号化」と考えられていることです。

除去可能？つまりソフトウェア暗号化 USB ドライブは、ユーザーによって暗号化を無効にできるということでしょうか？

答えは「できる」です。ユーザーはソフトウェア暗号化機能を USB ドライブから除去できます。その理由は？ユーザーがパスワードを使用せずにファイルにアクセスしたいだけの場合や、パスワードを忘れても USB ドライブにアクセスする必要がある場合があるからです。

暗号化 USB ドライブからソフトウェア暗号化を除去する方法

データにアクセスするために、複雑なパスワードなどを入力するのが面倒なユーザーにとって、手順は簡単です。

1. ソフトウェア暗号化ドライブをコンピュータに挿入します
2. ドライブをフォーマットします
3. ドライブのフォーマット後、すべての暗号化が除去されます
4. そのドライブに機密情報の入ったファイルをコピーして、アクセスしやすくします

制限のかかっていないコンピュータを使用すれば、ユーザーとってこの操作は容易です。IT 部門は会社のコンピュータでのフォーマットコマンドの使用を制限できますが、会社以外のコンピュータで実行できてしまいます。

コンプライアンスの目的としては、データ暗号化の除去が容易だということは、会社の提供したドライブが暗号化されていない場合、上記の方法で暗号化が一旦除去されれば、ドライブ上で暗号化されたデータは永遠に失われたと見なされます（暗号化キーはデータと結び付けられています）。暗号化が除去された後でデバイスにコピーされたデータは、保護されておらず、コンプライアンスに対応していないと見なされ、HIPAA、GDPR、CCPA の他、多くの規制に違反するリスクがあります。

暗号化されていないドライブを紛失した結果

会社指定の USB ドライブが紛失後に発見された場合、当初は会社がそれに気付かず、後からソーシャルメディアを介して知らされたとしても、会社は特定の要件を課せられ、次のことを要求される可能性があります。

1. 紛失したデータを特定するためのフォレンジック調査の実施
2. 法務に相談し、法律違反が発生しているかを判断
3. 顧客に通知すべきかを判断

この点に、USB ドライブの紛失が非常に高く付く可能性があります。法務の料金は時間あたり何百ドル以上になる場合があり、このコンプライアンス手続きによって多額の出費が発生する可能性があります。また、データ流出によって罰金、顧客などからの訴訟、会社の評判の低下などのおそれもあります。

ソフトウェア暗号化を低コストな実装と見なしている場合、このようなリスクとその結果の多額の財政的損失が考慮されていません。

また、暗号化されていない USB ドライブを会社のネットワークで使用させてしまう危険もあります。これは通常「BadUSB」と呼ばれます。BadUSB は一種のマルウェアで、企業のファイアウォールを突破し、USB ストレージデバイスを介して企業のサイバー防御網の中にマルウェアを侵入させるために、攻撃側によって使用されます。

BadUSB

USB ドライブがコンピュータに挿入されると、ファームウェア経由でコンピュータのチップセットコントローラが USB ドライブとハンドシェイクを開始します。この交信は、Microsoft/macOS/Linux などのオペレーティングシステムが、USB ドライブの接続を認識する前に発生します。各 USB ドライブにはファームウェアがあり、ドライブを USB ポートに挿入した時に実行されます。

攻撃側は、このハンドシェイクの仕組みを通じてマルウェアを侵入させることができることを知りました。USBドライブ上で実行されるファームウェアを他の悪意あるファームウェアに置き換えれば、標的のコンピュータシステムが USB ドライブとの通信を開始する際に、その悪意あるファームウェアによってマルウェアを注入することができます。標準的な USB ドライブには、コントローラによって実行される内部ファームウェアに対するセキュリティがないため、BadUSB が生み出されましたが、良い USB ドライブにはファイアウォールの突破やサイバー防御網の侵害に対する武器があります。

多くの企業は、社内システムでの USB ドライブの使用を禁止しようとし、USB ポートを樹脂で埋めるところもありました。しかし、この種の従業員はデータを USB ドライブに入れて持ち運ぶ必要があることがわかりました。たとえば、企業幹部は作業するため、または社内クラウドを使用できない社外法律顧問や金融顧問に渡すためにデータを携帯したいと考え、企業の委託業者は社内データベースへのアクセスが制限されているために作業用データを必要とし、金融アナリストは月次報告書を急いで完成させるために自宅でスプレッドシートで作業する必要があります。

以前の分析で示されたとおり、この標準的な USB ドライブとソフトウェア暗号化ソリューションを使用することには、多大なリスクがあります。一見安上がりに見えるものには、非常に大きな潜在的危険があり、ずっと高くつく可能性があります。データ漏洩の可能性について、たった2〜3時間弁護士に相談する費用で、安価なソリューションを使って節約した金額は帳消しになります。

ハードウェア暗号化 USB ドライブは、規制遵守に最適なオプション

ハードウェア暗号化 USB ドライブが規制対応に最適な選択である理由：

1. ハードウェア暗号化 USB ドライブでは、暗号化が常に有効な状態：ユーザーによる暗号化の無効化、パスワード規則（最短の長さ、複雑さなど）のリセット、自動パスワード再試行の無効化は不可能。ソフトウェア暗号化では、ソフトウェア辞書攻撃による反復パスワード類推を防止しませんが、ハードウェア暗号化ではパスワードの試行回数を制限し、間違ったパスワードが 10 回（もっと少ない場合もあります）入力されるとデータをロックします。スーパーコンピュータの時代には、これは非常に安全です。
2. ハードウェア暗号化ドライブには、最高級の暗号化コントローラが使用され、多くのセキュリティ機能が組み込まれています。弊社ではすべてのセキュリティ対策を常に公開しているわけではありませんが、BadUSB に対する防御策もあります。工場で、ハードウェア暗号化ドライブのみにファームウェアをロードする際に、ファームウェアにデジタル署名をしてロードします。つまり、暗号化 USB が挿入されると、暗号化コントローラはまずデジタル署名によってファームウェアの完全性を確認し、検証をパスした場合のみロードします。ファームウェアを置き換えようとするとドライブは破損し、機能しなくなって攻撃を防ぎます。
3. ハードウェア暗号化 USB ドライブには、特定の企業用のカスタム製品 ID（PID）設定も可能です。これらのプレミアムドライブには、デジタル ID をプログラムできますので、ドライブが社内外のファイアウォールに接続されると、会社支給のドライブと判別できます。たとえば、従業員が会社のドライブを紛失して同じモデルを小売店で購入した場合、新規購入したドライブは社内ネットワークの検証を通りません。このカスタマイズによって、USB ドライブを使用する際のセキュリティが一層強化されます。
4. ハードウェア暗号化ドライブでは、短期間にコストを節約できます。リスクの軽減や解消によって、回収サイクルが短縮します。

Kingston は世界最大級の暗号化 USB ドライブメーカーで、さまざまな機能と価格帯のドライブファミリーを提供しています。企業役員、従業員、請負業者など向けの暗号化 USB ソリューションをコンプライアンス維持に役立てる方法については、Kingston までお問い合わせください。

 MKF-956JP