MobileIron

クラウドのベストプラクティス：エンドポイントセキュリティの監査チェックリスト

この10項目のチェックリストでは、エンドポイントでクラウドデータを保護するセキュリティアーキテクチャ設計のベストプラクティスを紹介します。企業のコンピューティングアーキテクチャは、過去10年間で大きく変化しました。従業員はモバイルアプリを通じて多くのビジネスクラウドサービスを利用するようになりました。ネットワーク周辺の保護とエンドポイントのロックダウンという従来のセキュリティ対策は、アプリとクラウドを多用する現代の職場に適切ではありません。

一般にクラウドサービスプロバイダーは、包括的なプログラムでデータセンターのセキュリティを確保し、データ漏洩のリスクを緩和しています。しかし、サービスプロバイダーの手を離れ、エンドユーザーのモバイルデバイスに保存されたデータは、適切なセキュリティ対策がない限り、たやすく侵害され、漏洩します。

多くの企業は、社内または社外のセキュリティ監査を受け、クラウド内とエンドポイントの両方で、ビジネスデータがどれだけ保護されているかをテストしています。NIST（米国国立標準技術研究所）のサイバーセキュリティフレームワーク（www.nist.gov/cyberframework）と欧州連合（EU）の一般データ保護規則（GDPR - www.eugdpr.org）は、監査の基準に影響を与える2つのフレームワークです。

このチェックリストは、綿密な監査を目的としたものではなく、出発点です。各企業では、これに加えて独自の分析を行い、制御対策を決定する必要があります。しかし、現状とこのチェックリストに格差がある場合は、リスクレベルが高い可能性があります。

MobileIron

japan@mobileiron.com

www.mobileiron.com

セキュリティ監査チェックリスト

1. デバイスの暗号化およびパスワード保護

モバイルデバイスの紛失はよくあります。デバイスの暗号化とパスワードは、デバイスが所有者の手を離れた際にデータに簡単にアクセスされるのを防ぎます。暗号化は、米国の医療保険の相互運用性と説明責任に関する法律（HIPAA）でもGDPRでも（リスクに対して適切であれば）要求されています。デバイスが対応していれば、バイオメトリクス、指紋、顔認証も不正アクセス防止に役立ちます。

2. ビジネスアプリと個人アプリのデータ共有を防止

モバイルオペレーティングシステムはデバイス上のアプリ間のデータ共有を許可します。たとえばエンドユーザーは、ビジネスメールに添付された文書を受信し、その文書をPDFリーダーやエディターで開くことができます。アプリは文書を開いた後、IT部門の管理外に文書を保存したり、送信したりできます。これは情報漏洩の一般的なパターンです。デバイス上のビジネスアプリから個人アプリへのデータエクスポートを許可すべきではありません。

3. 侵害を受けたデバイスから自動的にビジネスデータを削除

デバイスは、ジェイルブレイク（脱獄）、ルート化、マルウェア、旧いファームウェアなどのセキュリティ問題によってコンプライアンス違反となることがあります。防御対策は、IT担当者の介入なしで自動的に実行される必要があります。コンプライアンス問題が深刻な場合は、デバイスからビジネスデータを自動的に削除すべきです。コンプライアンスに応じた検知から修正までの一連のアクションは、リスク緩和に必須です。侵害されたデバイスがビジネスデータを保持する時間が長いほど、漏洩のリスクは大きくなります。プライバシーを保護するには、IT部門が、個人データに触れることなく、ビジネスデータを削除できなければなりません。

4. 個人トラフィックを分離し、ビジネストラフィックのみトンネリング

チェックリスト3がデバイス上のビジネスデータと個人データの分離を要するのと同様、この項目でもネットワーク上で同様の分離が必要です。デバイス全体のVPNは、ビジネスアプリと個人アプリの両方からデータを企業ネットワークに送ります。一方、Per-App VPNは、ビジネスアプリからのトラフィックのみ企業ネットワークに送信するよう構成することで、そのトラフィックを保護するとともに、エンドユーザーのソーシャルメディアフィード、その他の個人的な通信のプライバシーを維持することが可能です。

5. 不正デバイスによるビジネスクラウドサービスへのアクセスを阻止

多くの企業は複数のベンダーのビジネスクラウドサービス、たとえばMicrosoftの生産性向上スイートとSalesforceのCRMソリューションを利用しています。不正デバイスがいずれかのサービスにアクセスすれば、そのサービスからデバイスにデータをダウンロードでき、データはIT部門の管理外になります。これは、エンドユーザーがビジネスアプリを利便性目的で個人デバイスにダウンロードしたときによく起こります。IT部門がデバイス上のアプリを削除したり、データ共有を制御したりできる場合を除き、ビジネスデータをデバイス上に保存すべきではありません。IT部門は、ベンダーを問わず、利用しているすべてのビジネスクラウドサービスにセキュリティ制御を適用する必要があります。Office 365のセキュリティだけを確保したのでは不十分です。このような管理は、不正デバイスがビジネスデータにアクセスするのを防止する点で、GDPRおよびNISTのサイバーセキュリティフレームワークのカテゴリーDE.CM-7（「不正な人物、接続、デバイス、ソフトウェアの監視を実行する」）に関連します。

6. 不正アプリによるビジネスクラウドサービスへのアクセスを阻止

IT部門は、データを保護するため、クラウドサービスにアクセスするデバイスとアプリの両方のセキュリティを確保する必要があります。デバイスがセキュアでもアプリがセキュアでなければ、データは漏洩します。たとえばエンドユーザーが、企業向けアプリストアではなく、AppleのApp StoreやGoogle Playなどのコンシューマーサービスから直接ビジネスアプリを直接ダウンロードすることがあります。エンドユーザーには同じアプリに見え、実行するデバイスはセキュアですが、IT部門はアプリを削除することもデータ共有を制限することもできません。IT部門は、不正アプリによるビジネスクラウドサービス（Office 365だけでなく）へのアクセスを阻止する必要があります。このような管理は、不正ソフトウェア（アプリ）がビジネスデータにアクセスするのを防止する点で、GDPRおよびNISTのDE.CM-7に関連します。

7. ゼロデイ攻撃の検出と防御

事前の対策はデータ漏洩のリスクを緩和します。しかし、悪者は常に新しいハードウェア、ソフトウェア、挙動の脆弱性を見つけ、悪用しようとします。デバイス、アプリ、ネットワークに対する脅威を継続的に機械学習で分析し、エンドポイントで防御できれば、IT部門は新しい脅威に迅速に対応できます。

8. Android、iOS、macOS、Windows 10に対応する高度なセキュリティ制御機能

もはやWindowsだけの世界ではありません。ほとんどの企業はさまざまなオペレーティングシステムのエンドポイントをサポートしています。Windows 7のような古いオペレーティングシステムは、レガシーのセキュリティツールを使用していますが、Android、iOS、macOS、Windows 10などの現代のオペレーティングシステムは、エンドポイントアーキテクチャの進化により、統一されたクロスプラットフォームのセキュリティソリューションに対応しています。IT部門は、これらのオペレーティングシステムのネイティブのセキュリティフレームワークを最大限に活用する高度な制御機能を持ったソリューションを選択する必要があります。

9. デバイスセキュリティの認証（MDM対応のコモンクライテリアプロテクションプロファイル）

コモンクライテリアは、コンピューターセキュリティ認証の国際規格です。モバイルデバイス管理（MDM）向けのプロテクションプロファイルは、モバイルデバイスで企業データを処理し、企業ネットワークのリソースに接続するため、セキュリティポリシー適用に関する要件を定めています。コモンクライテリアは、多くの政府機関や高セキュリティ組織の要件にもなっています。IT部門は、この認証を持つセキュリティソリューションを選択する必要があります。

10. クラウドセキュリティの認証（SOC 2 Type 2とFedRAMP）

IT部門が採用するセキュリティソリューション自体がクラウドベースである場合は、業務とコンプライアンス制御に関する監査者のテストを詳細に説明したSOC（Service Organization Controls）2 Type 2の報告書が必要です。このテストが、プロバイダーのシステムのセキュリティ、可用性、処理の完全性、機密性、プライバシーに関する制御機能の有効性を確認します。FedRAMPの運用権限（ATO）は、プロバイダーが連邦のリスク管理プロセスに合格し、セキュリティ要件を満たすという米国の正式な証明書です。IT部門は、このような認証を持つセキュリティソリューションを選択する必要があります。

この10項目のチェックリストは、MobileIronのお客様に共通のベストプラクティスを集約したものです。これらをセキュリティ、コンプライアンス、法律的なポリシー決定の参考とし、各企業で、業種や地域、組織的なリスク耐性に最適なガイドラインを作成することをお勧めします。

MobileIronを クラウドセキュリティに活用

MobileIronは、行政グレードのクラウド/エンドポイントセキュリティプラットフォームです。ここでは、MobileIronテクノロジーを利用して上記のチェックリストに対応する例をご紹介します。

チェックリスト1、2、3、8

MobileIronにデバイスを登録：IT部門は、MobileIronを利用してデバイスに構成プロファイルをインストールし、ビジネスデータの保護に必要なセキュリティ対策を取ることができます。

セキュリティポリシーの設定：MobileIronで適切なパスワードと暗号化ポリシーを設定します。バイオメトリクス認証を利用できる場合もあります。デバイスがコンプライアンス違反となった場合には、自動的に検疫やセレクティブワイプが実行されます。従業員が組織を去る場合には、企業所有のデバイスにはフルワイプ、従業員所有のデバイスにはセレクティブワイプを実行します。

ビジネスアプリを管理：MobileIronを利用し、Apps@Work企業向けアプリストアまたはマネージドGoogle Playを通じてビジネスアプリを配布します。これらのアプリはインストール後、MobileIronに設定したポリシー制御機能で管理されます。つまりIT部門は、ビジネスアプリとコンシューマーアプリのデータ共有を防止し、必要に応じてリモートでアプリを削除できます。企業データをIT部門の制御下に置き、しかもデバイス上の個人データのプライバシーを侵害することがありません。

チェックリスト4

Per-App VPNの導入：MobileIronで構成したビジネスアプリは、MobileIron Tunnel Per-App VPNを通じてのみオンプレサービスに連携します。このようにビジネスアプリのトラフィックとコンシューマーアプリのトラフィックを分離することにより、過度に個人データが企業ネットワークに流れることはありません。

チェックリスト5、6

信頼できるデバイスとアプリにのみクラウドサービスへのアクセスを許可：MobileIron Accessでは、非マネージド、無許可、コンプライアンス違反のデバイスやアプリをOffice 365、Salesforce、ServiceNow、Workdayなどのクラウドサービスの認証からブロックします。MobileIron Accessは、マルチクラウド、マルチIDで、標準規格ベースのソリューションであり、企業内の多くのクラウドサービスとIDプロバイダーに対応します。

チェックリスト7

ゼロデイ攻撃に対する検出と防御：MobileIron Threat Defenseで疑いのあるデバイス、アプリ、ネットワーク活動を監視します。問題が発見された場合は、MobileIronのポリシーが適用され、ユーザーへの通知、デバイスの検疫、データワイプなどの適切な防御策を実行します。

チェックリスト9、10

セキュリティ認定を軽視しない：MobileIronは、MDM v2に対応するコモンクライテリア（CC）プロテクションプロファイルの認証を業界で初めて取得しました。MobileIronは、SOC 2 Type 2にも準拠し、FedRAMPの運用権限（ATO）を取得しています。

現代のセキュリティは進化を続け、Microsoft Intuneがこのチェックリストを完全に満たしているのかとITプロフェッショナルに尋ねられることがあります。当社は満たしていると考えません。特に3、4、5、6、7、8、9、10です。MobileIronは、現代の企業にクラス最高の技術を選択していただけるよう、マルチOS、マルチクラウド、マルチIDのセキュリティアーキテクチャを重視しています。

まとめ

多くの企業は、今後数年で、社内であれ社外であれ、何らかのセキュリティ監査に直面するでしょう。目標は同じ、すなわち悪意のある侵害と悪意のない漏洩の両方からデータを保護することです。しかし、従来のセキュリティアーキテクチャと現代のセキュリティアーキテクチャでは保護のメカニズムが大きく異なります。組織がクラウドサービスという革新をスピーディーかつセキュアに利用するには、明確な監査チェックリストを出発点として、人材、プロセス、技術に投資する必要があります。

どのようにクラウドを導入する場合でもエンドポイントセキュリティを最優先し、GDPR（一般データ保護規則）、NIST（米国国立標準技術研究所）のサイバーセキュリティフレームワーク、その他同様のコンプライアンスモデルに適合する必要があります。従業員は現代のエンドポイントと現代のアプリを通じてクラウドサービスを利用しますが、これらのエンドポイントとアプリがセキュアでなければデータは漏洩します。どれだけデータが漏洩するかは、Microsoft Office 365、Salesforce、ServiceNow、Workdayなどに移行する企業が、どれだけ早くMobileIronのようなエンドツーエンドのマルチクラウドセキュリティソリューションを実装するかにかかっています。