情報管理

セキュリティの確保

5つの要点

現代の情報管理では、データ漏洩が現実のものとして恒常化しているようです。事業運営に支障をきたし、企業や顧客のデータ流出につながっています。Gemalto　社の調査によると、2016年には13億件以上の記録がデータ侵害によって失われたと推定されています[1]。大手小売業者やサービスプロバイダーなど、注目度の高い数件の漏洩が報道で最も注目されましたが、それ以外にも、小規模であまり知られていない企業や組織での多くの漏洩が、この統計の元になっています。これは、「隠蔽によるセキュリティ」という考え方が、情報管理ではもはや有効な戦略とは言えないという事実を強調しています。保護されていない小規模な企業や組織は、ハッカーにとって格好の標的となり、こうした侵害が発見されず、報告されない可能性も高くなります。

驚異の状況は、この10年間で劇的に変化しました。洗練した高度に自動化されたハッキングツールが広く普及したことで、侵入の障壁が低くなり、ハッカーが急増しています。ハッカーに対するハリウッド映画的なイメージは捨ててください。今日、最も一般的な侵害行為は、産業スパイや国際スパイによるものではありません。ハッキングは、一般の人々の個人情報を盗むというありふれた目的をもった、いわば大型のビジネスとなり、その規模は拡大しています。

...2016年、13億件以上の記録がデータ侵害で喪失

個人を特定できる情報（PII）とは、Eメールアドレス、ウェブサイトのログオン情報、社会保障番号、銀行やクレジットカードの口座、健康保険の情報などです。大学や病院から銀行や保険会社まで、このような顧客情報は多くの業務運営の中核をなしていますが、十分に保護されていないことが多いのです。こうした情報が適切なセキュリティ対策なしに取得、使用、保管されると、組織とその顧客は、罰金、訴訟、顧客の喪失につながる過度のリスクにさらされることになります。

1.Gemalto.Findings from 2016 Breach Level Index.2017

情報管理のセキュリティ確保

情報管理ソリューションは、顧客導入、トランザクション処理、およびケース管理に不可欠なものです。これらのソリューションは、個人情報を収集し、必要な人、プロセス、システムに配信できるようにする基幹業務テクノロジーエンジンです。

今日の業務システムでは機密データが大量にやり取りされているため、最新の情報管理ソリューションには、**データセキュリティの面でに厳しい監視**にも対応できることが求められます。

以下の5つの要点は、新たなリスクや脆弱性を組織に提示する上で役立つではなく、貴重な業務データや顧客データの保護に役立つベンダーやソリューションの選択に役立ちます。

1 あらゆる状態のデータを保護

今日の情報主導型の組織では、データは通常、常に複数の状態で存在し、保護する必要があります。

保存データ

文書スキャニングソフトウェアとインポートソリューションは、文書を取り込んでファイルサーバーに保存します。これらの文書に財務や個人の機密情報が含まれている場合、情報管理ソリューションにこれらのファイルを暗号化する機能が必要です。フルディスク暗号化は、強固なセキュリティ防御のための優れたレイヤーですが、それはハードディスクの盗難の脅威からの保護に過ぎません。サーバーの電源を入れてディスクの暗号を解除すると、シャットダウンするまで再び暗号化されることはありません。ほとんどのファイルサーバーは、24時間365日オンラインで利用可能である必要があるため、それらのファイルは危険にさらされています。

ハイランドのOnBaseは、暗号化ディスクグループモジュールにより、フルディスク暗号化の限界を克服します。OnBaseでは、適切なセキュリティ権限を持つユーザーがアクセスするまで、ファイルを暗号化しておくことができる機能が提供されます。

保存データを保護する別の要点は、パスワード管理です。パスワードは機密情報へのアクセスを許可するものですから、ベンダーがデータベースにパスワードをどのように保存・管理しているかを必ず確認してください。OnBaseでは、デフォルトで中程度のセキュリティパスワードポリシーが事前に設定されています。業界で認められているPBKDF2パスワードハッシュアルゴリズムでパスワードを暗号化して保護します。また、事前に設定された高セキュリティのパスワードポリシーも利用できます。

転送中のデータ

業務プロセスでは、文書をスキャナからファイルサーバー、アプリケーションサーバ、ワークステーション、タブレット、プリンタ、携帯電話など、さまざまな場所に移動させる必要があります。情報があるシステムやデバイスから別のデバイスに移動する際、悪意のある個人やアプリケーションによって、知らないうちに情報が傍受され、取得される危険性があります。

情報があるシステムやデバイスから別のシステムやデバイスに移動する際、**情報が傍受され、取得される危険性があります**。

そのため、コンテンツを移動中に保護することは非常に重要です。ネットワーク上を移動するコンテンツをどのように保護しているのか、検討中のベンダーに確認してください。OnBaseでは、堅牢なトランスポート層セキュリティ(TLS)を活用して転送中のデータを暗号化し、攻撃者や権限のない個人に傍受されても使用できないようにしています。

使用中のデータ

ユーザーがアクセスしているときのデータを保護することも重要です。現代の組織では、多数の部門にわたって広範なデータを管理しています。承認されたユーザーのみが機密情報にアクセスできるようにすることは、簡単なことではありません。検討中のベンダーに、そのベンダーのソリューションが使用中のデータ保護にどのように役立つかを確認してください。

OnBase では、使用中のデータを複数のレベルで保護します。

- きめ細かにコントロールできる包括的なセキュリティポリシーにより、業界標準や規制に準拠したアクセスセキュリティを実現
- ダイナミックなデータマスキングや伏字により、文書転送中のセキュリティをさらに強化
- カスタマイズ可能なタイムアウト設定により、活動していないユーザーをログアウトさせることが可能

2 設定なしですぐに使えるセキュアなデフォルト設定

ベンダーによっては、セキュリティ機能を提供していますが、管理者オプションの中に隠れていることがあります。これは、ベンダーがすべてのセキュリティ機能の有効化と設定をお客様に委ねている、汎用的なソリューションで特によく見られます。これは、優れた柔軟性を備えているように見えますが、実際には、高度な設定を習得し、業界標準を満たすようにソリューションを設定するために、業務システム管理者に過度の負担を強いることになります。

基本的なセキュリティ機能を有効にして設定しなければ、**データやシステムが危険にさらされます。**

どのようなセキュリティ機能がソリューションで有効化され、事前に設定されているかを、検討中のベンダーに確認してください。

OnBaseソリューションでは、セキュリティ機能が有効になっており、業界のベストプラクティス、標準、規制に基づいたセキュリティモデルを提供しています。

3 セキュリティを犠牲にすることなく、ユーザーの利便性を向上

最先端の侵入検知や防御技術を導入しても、従業員がセキュリティインフラストラクチャの最大の脆弱性の一つであり続けます。組織のデータ志向が高まるにつれ、従業員はより多くのシステムやデータソースにアクセスしなければならなくなっています。しかし、規制やコンプライアンスの要件が拡大しつつある中、これらのデータへのアクセス方法や使用方法の管理を強化する必要があります。従業員は自分の仕事を効果的かつ効率的に行うために努力しますが、過剰なセキュリティポリシーや手順を課すことは、最終的に生産性を低下させ、コンプライアンス違反のリスクを高めることになります。

…従業員がセキュリティインフラストラクチャシステムの**最大の脆弱性の一つ**であり続けます

情報管理ソリューションは、アクセスコントロールをインテリジェントに管理し、セキュリティを犠牲にすることなく仕事を遂行するために必要な情報をユーザーに提供することで、このセキュリティのパズルを解く要点となるはずです。

OnBaseは、情報へのセキュアな役割ベースのアクセスという概念に基づいて構築されています。セキュリティコントロールは、ユーザーの権限を、業務を遂行する上で必要な最低限のものに制限するように設計されています。このアプローチは、「最小特権の原則」に従い、ユーザーの生産性を妨げることなく、意図的または非意図的な暴露のリスクを最小限に抑えます。

4 脆弱性対策

最近のソフトウェアは非常に複雑で、何十ものさまざまなソースからのモジュールが含まれていることがよくあります。ソリューション全体に潜在する脆弱性を追跡し、脆弱性が発見されたモジュールを積極的に更新または修正することは、ベンダーの責任です。Open Web Application Security Project (OWASP) のような組織は、複数のベンダーが自社のソフトウェアで使用している可能性のある一般的なソフトウェアパッケージの脆弱性データを追跡しています。OWASPは、最も重要なアプリケーションセキュリティリスクの上位10リストを発表しています。検討中のベンダーに、自社製品の脆弱性をどのように追跡し、テストしているか確認してください。

ハイランドのOnBaseとその他のソリューションでは、社内の開発や品質保証担当者がOWASPの上位10リストで注目されているものを含め、あらゆる潜在的な脆弱性や悪用を追跡し対処しています。さらにハイランドは、セキュアな開発手法、自動化されたセキュリティスキャン、手動による侵入テストを利用して、幅広い攻撃に対してソリューションを継続的にテストし、安全性を確保しています。

5 セキュリティは、うわべのものではない

責任あるソフトウェア開発会社は、セキュリティを後回しにするようなことはしません。セキュアな情報管理では、ソフトウェアの開発方法が最終製品と同様に重要です。ベンダーはデータ保護に真剣に取り組むため、開発、テスト、サポートなど、製品ライフサイクルの各段階で、セキュリティの原則とタスクを実施しなければなりません。検討中のベンダーには、製品ライフサイクルの各段階におけるセキュリティの役割を説明してもらうようにしてください。

セキュアな情報管理では、ソフトウェアの開発方法が最終製品と同様に重要です。

データとシステムを保護するために、ハイランドは厳格なセキュリティ開発ライフサイクル手法を採用しています。これにより、製品の開発、テスト、品質保証の各段階で、特定のセキュリティタスクが確実に実行されます。また、ハイランドでは、すべての開発や品質保証担当者に対して、ソフトウェアの脆弱性を防止・検出するために必要なスキルやツールのトレーニングを行っています。

セキュリティ強化の準備はどうですか？

適切な情報管理ソリューションは、新たなリスクや脆弱性を提示する上で役立つのではなく、リスクを低減し、コンプライアンスを向上させるものでなければなりません。

資料をダウンロード：Choose a Secure Information Management Solution

このワークシートをダウンロードして選択プロセスに役立ててください。

ハイランドのOnBaseについて

OnBaseは、コンテンツ、プロセス、ケースをオンプレミスまたはハイランドクラウドで管理する単一のエンタープライズ情報プラットフォームです。エンタープライズコンテンツ管理（ECM）ケース管理、ビジネスプロセス管理（BPM）、記録管理、キャプチャのすべてを単一のプラットフォーム上で提供する OnBaseは、世界中の企業をより行動力のある能率的かつ効率的な組織に変えています。OnBaseプラットフォーム用のエンタープライズクラウドベース共有は、ハイランドが補完的に提供する、ハイランドの ShareBase でご利用いただけます。

詳細は OnBase.com/Security»を参照ください。

OnBase by Hyland