Quest

90%

の組織がインサイダー脅威に対して脆弱であると感じています。[1]

インサイダー攻撃の検知、防御、およびインサイダー攻撃からの復旧

境界防御は万全に構築しました。しかし、ネットワーク内に既に存在する脅威への備えはできていますか?

課題

毎週のように新しいデータ漏洩がトップニュースとして報じられています。誰もがハッカーについて心配しているので、組織は歴史的に、境界防御に多額の投資を行ってきました。しかし、現実は、全データ漏洩のうちの半数以上が、ネットワーク内部の誰かによって引き起こされているのです。[2] 例えば、転職を成功させるためにIPを盗もうとする従業員や、タイプミスにより重大な設定エラーを起こす管理者などです。実際には、正規のアカウントを乗っ取った外部の攻撃者であることが多いです。Microsoft社の報告では、9500万のADアカウントが毎日サイバー攻撃の標的にされており、[3] 毎日1000万回のAzure ADログインの試行がサイバー攻撃であるとされています。[4]

このため、セキュリティの専門家は「侵入ありき」の心構えを持つように勧めています。つまり、何者かが重要をデータを破損させたり盗んだりしようと、遅かれ早かれネットワークをうろつくようになることを受け入れるのです。最高の境界防御であっても、そのような人を阻止することはできないので、強力なアクティブディレクトリのセキュリティとガバナンスを導入することが不可欠です。

皆様への影響

インサイダー脅威に効果的に対抗するためには、次のことが必要です。

- **新しい技術を実装することによって、業務のニーズを安全な方法でサポートする。**クラウドを高速化したり私物デバイスの業務利用を拡張したりすることは、ビジネス目標を推進する可能性がありますが、セキュリティリスクを最小限に抑える必要があります。
- **すべての機密データを保護する。**近年、データは急激に増加しており、その多くが、建物内のロックされたデータセンターの少数のデータベース内に格納されずに、SharePoint OnlineやOneDriveなどのクラウドリポジトリ内に非構造化データとして保存されています。その結果、どのようなデータがあるのか把握することすら困難になり、すべてを安全に保つことができなくなっています。
- **ますます厳しくなり、増え続けるデータプライバシー規制に従う。**少し前まで、規制が厳しかったのは一部の業界だけで、ISO認証があれば十分でした。しかし、今では、PCI、GDPR、CCPAなどの規制が、あらゆる業界に深く入り込んでいます。コンプライアンスを確立するだけでなく、新たな規制の出現や進化に合わせて継続的にそれを維持する必要があります。
- **監査に合格し、不名誉なニュースの見出しにならないようにする。**データ漏洩の損害額は壊滅的になものになる可能性があり、平均で386万ドルと言われています。[5] 監査に失敗すると、非常に高額な罰金が課され、組織が廃業に追い込まれる可能性さえあります。ビジネスを守れるかどうかは、あなた次第です。

これらの目標を達成するには、ユーザのアクセス権限を管理し、全員の行動に目を光らせる必要があります。しかし、ネイティブツールでは、これは簡単にはできません。実際、ユーザの62パーセントが、必要以上のアクセス権を持っていると認めています。[6] SIEMは、ユーザの活動に一定の可視性を与えますが、ライセンス料金が高額なうえ、設定や使用方法が複雑です。さらに、うまく機能させるためにはデータをフィードする必要があります。また、ネイティブログには大きなギャップがあって、重要な分野で正確性を欠きます。攻撃者が、検出されるまで平均101日という長い間密かに動き回っていられるのも不思議ではありません。[7]

1 Cybersecurity Insiders『Insider Threat 2018 Report（インサイダー脅威2018レポート）』

2 同書より

3 ZDNet、『Active Directory czar rallies industry for better security, identity（アクティブディレクトリの第一人者が、セキュリティと識別の向上のため業界に呼びかけ）』、2015年6月9日

4 Softpedia News『Microsoft Sees Over 10 Million Cyberattacks per Day on Its Online Infrastructure（オンラインインフラストラクチャで毎日1000万のサイバー攻撃を目の当たりにするMicrosoft）』、2016年5月6日

5 Ponemon Institute『2018 Cost of Data Breach Study（2018年のデータ漏洩による損害額調査）』

6 Ponemon Institute『Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations（企業データを保護するためのセキュリティギャップの解消: 米国およびヨーロッパの組織の研究）』

7 FireEye『M-Trends 2018レポート』

「以前は、管理グループに対する変更を管理することができませんでした。Change Auditorを導入してからは、メールのフォルダを見るだけで、こうした重要な変更を簡単に監視できます。」

— Region Halland社、ITシステム技術者、Dennis Persson氏

頼りになるセキュリティとコンプライアンスのソリューション

優れた選択肢

各ユーザが自分の仕事を行うために必要なアクセス権だけを持つようにすることで、ユーザ（またはそのユーザの資格情報を盗む人）による被害を抑えられるとしたらどうでしょうか。誰かが危険な行動を取ったとき、すぐに警告を受け取ることができるとしたらどうでしょう? 一人一人の正常な行動のベースラインを設定して、そこから外れた行動を直ちに検出できるとしたら? そして、脅威に対して迅速に調査し、対応できるとしたらどうでしょうか?

QUESTならではの実現可能な機能

Questは、あらゆるオンプレミスまたはハイブリッドのMicrosoft環境にセキュリティおよびコンプライアンスソリューションを提供する、頼りになるベンダーです。内部環境を境界と同じくらい厳重に保護し、継続的な法令遵守を保証する、完全なソリューションパッケージを提供します。

修正と軽減

インサイダー脅威に対する防御は、適切なガバナンスから始まります。Quest® ソリューションは、ユーザのプロビジョニングやプロビジョニング解除を含む管理タスクを自動化して、セキュリティホールを塞ぎ、リスクを低減します。承認ベースのワークフローにより、ガバナンスと制御の層が1枚厚くなります。

脆弱性のプロアクティブな識別

IT環境は動的なので、脆弱性を定期的に確認する必要もあります。Questのソリューションでは、オンプレミス、ハイブリッド、またはクラウドの環境全体にわたって、自動化され、統合されたレポート作成を可能にするので、誰が何に対してアクセス権を持ち、どのようにそのアクセス権を得たのか、簡単に判断できます。さらに、その レポートから、適切なアクセス権を設定することができます。また、最も機密性の高いデータがどこにあるのか検出できるので、データが保護されていることを確認したり、GPOを簡単にレビューしたり、重要なオブジェクトがそもそも変更されることを防ぐこともできます。

疑わしいアクティビティの検出と警告

Questのソリューションでは、ユーザおよび管理者のアクティビティに対してリアルタイムの監査を行い、権限の拡大、不適切な変更、その他の疑わしいアクティビティに対して警告を行うことで、アクティブな脅威により早く対応することが可能になります。詳細なユーザ行動分析は、個々のユーザの行動パターンをモデル化し、異常な行動を検出します。アクティビティのブロック、ユーザの無効化、変更の取り消しなど、対応を自動化することもできます。

攻撃の迅速な調査と回復

データ漏洩を食い止めるのには、平均で69日かかります。[8] Questは、一元管理されたデータコレクションやGoogle風の検索および科学調査エンジンを使用して、セキュリティインシデントを迅速かつ簡単に突き止めることを可能にします。さらに、ディザスタリカバリ計画用の仮想テストラボを構築して、長時間のネイティブADフォレストの回復プロセスをシンプルなGUI駆動プロセスに変えることができます。

法令遵守の維持と証明

これらの機能が組み合わさって、幅広い法規制に対するコンプライアンスを確立、維持、および実証することが可能になります。さらに、Questのソリューションは、スマートでスケーラブルなログ圧縮を提供するので、監査データを何年にもわたってコスト効率よく保管しながら、セキュリティ調査や監査チェックのためにいつでも利用することができます。

---

8 Ponemon Institute『2018 Cost of Data Breach Study（2018年のデータ漏洩による損害額調査）』

Quest
quest.com/jp
世界各地のオフィスの情報については、（quest.com/jp-ja/locations）をご覧ください

SolutionBrief-MPM_SecurityCompliance-US-JA-WL-38251