不正侵入の徹底分析

ハッカーの侵入手口と防衛策

サイバー攻撃は企業に膨大な損失をもたらします。不正侵入を防ぐのはもちろん、攻撃された場合の被害を最小限に食い止め、すみやかに復旧するための計画は万全でしょうか。

Microsoft

目次

03 **はじめに:**
不正侵入の 4 つの段階

04 **第 1 段階:**
足掛かりを作る

05 **業界別事例:**
医療関連

07 **第 2 段階:**
より強力な権限を獲得する

08 **業界別事例:**
エンターテイメント & メディア

10 **業界別事例:**
食品製造

12 **第 3 段階:**
ネットワークへ侵入する

13 **業界別事例:**
政府機関

15 **第 4 段階:**
長期的な攻撃態勢を整える

16 **業界別事例:**
ハイテク製造業

18 **業界別事例:**
オンライン ショップ

20 **まとめ:**
防御、検知、対処

不正侵入の4つの段階

不正侵入の 4 つの段階

ますます巧妙化するサイバー攻撃。企業の収益にも、信頼性にも、気付かぬうちに深刻な影響を与え、その被害額は何百万ドルにも及びます。ご自身の会社にどのような脅威が潜んでいるか、ご存じでしょうか。不正侵入には 4 つの段階があります。各段階での攻撃を防ぐと同時に、攻撃された場合の被害を最小限に食い止め、すみやかに復旧するための計画は万全でしょうか。

このドキュメントでは、各段階の侵入手口を詳しく説明すると共に、実際の被害事例をご紹介します。また、"不正侵入を前提とする" 防衛策を立て、ご自身と会社を保護する方法も取り上げます。

第 1 段階:
足掛かりを作る

第 2 段階:
より強力な権限を獲得する
(ローカルでの権限昇格)

第 3 段階:
ネットワークへ侵入する
(Active Directory での権限昇格)

第 4 段階:
長期的な攻撃態勢を整える

第 1 段階: 足掛かりを作る

攻撃者は、ほんの小さな "穴" をついて組織へ侵入してきます。ワークステーションをウイルスに感染させる、修正プログラムを適用せずにインターネットへ接続しているサーバーを狙う、構成が不適切なサードパーティのデバイスを標的にするなど、あらゆる手段を講じて企業の防御をかいくぐり、ネットワークに侵入しようとします。システムに入り込んだ攻撃者は、内部を偵察して機密情報や重要なリソースを探し出し、標的を定めます。

主な用語:

フィッシング: ユーザーをだまして、内部へ不正アクセスするための個人情報、財務情報、企業情報を入手する行為。偽の Web サイトを表示したり、信頼できる送信元 (同じ会社の社員やサードパーティ ベンダーなど) を装って電子メールを送りつけ、感染ポイントの Web リンクや文書をクリックするよう仕向けます。

Watering Hole: 攻撃者が特定の組織や個人を狙う際、標的が頻繁に利用すると見なした Web サイト。そのサイトに悪質なリンクを設定し、マルウェアへ誘導して標的のコンピューターを感染させます。

マルウェア: malicious software (悪質なソフトウェア) の略。情報を盗み出す、身代金を支払うまで PC をロックする、PC を利用してスパムを送信するなど、PC 上で不正な操作を実行します。ウイルス、ワーム、トロイの木馬はすべてマルウェアに含まれます (このドキュメントでは、特定の業界や組織を狙う "標的型マルウェア" に焦点をあてます)。

エクスプロイト: ソフトウェアの脆弱性を悪用して PC 上の情報にアクセスしたり、マルウェアをインストールしたりするコード。

ゼロデイ: ソフトウェア ベンダーがまだ公表していない、あるいは修正プログラムを提供していないソフトウェア エクスプロイト。

業界別事例：医療関連

この数十年、医療業界は病院の合併による大規模な統合を繰り返してきました。こうした統合を通じて確かに医療は向上しましたが、多くの場合、病院の合併には技術的な課題が伴います。たとえば、いくつかの病院を統合した後、全体的な IT 投資を削減するため、複数の IT サービスを 1 つの部署に一元化するケースもあります。

ネットワーク、インフラストラクチャ、ソフトウェアの統合は、一歩間違うと不正侵入につながります。攻撃者はまず、セキュリティが最も弱いネットワークを狙います。それに成功したら、内部のセキュリティ上の弱点を利用して、さらに他のネットワークに侵入します。事実、攻撃者が 1 つのネットワークにアクセスした後、ソーシャル ネットワーキングと電子メールを利用し、さらに別の院内ネットワークに侵入したケースがありました。サーバーをアップグレードしたとき安定性に問題が生じたことから、病院側は "何かおかしいい" と気付きます。調査したところ、ネットワークに不正アクセスするためのマルウェアがずっと以前から仕込まれていたことがわかりました。

この不正侵入にはいくつもの原因がありました。1 つは、病院側がネットワークと他の組織を分離していなかったため、セキュリティ対策の弱いネットワークへの侵入を許す結果となったことです。さらに、ネットワーク全体で同じ資格情報を使用していたため、ネットワークに侵入した攻撃者は、さまざまなエリアへ容易にアクセスすることができました。社内開発したレガシー アプリケーションの権限管理が甘かったことも大きな要因でした。その後、この病院では、ネットワークの再設計と再構築、および院内文化の立て直しに数年を要しました。

足掛かりさえ作ってしまえば、その後の攻撃は容易です。いずれかの手段でネットワークにアクセスした攻撃者は、より強力な資格情報を入手し、さらに重要な別のネットワーク エリアへ侵入していきます。

予防が大切…

スタッフのトレーニングを実施する、適切なテクノロジー ソリューションを導入するなど、セキュリティ対策を強化することで、院内ネットワークの安全性を高めることができます。

マイクロソフトが推奨するセキュリティ対策:

業界のセキュリティ基準を満たす堅牢な基盤を整える: ネットワークを分離し、強力なパスワード要件を設けます。さらに、"最小権限" を適用し、ネットワークごと、またはアクセス エリアごとに異なるパスワードを設定します。中でも、修正プログラムを適用できず、攻撃を受けやすいレガシー デバイスは、こうした対策が特に重要となります。

ネットワークをアップグレードする: ネットワーク インフラストラクチャを頻繁にアップグレードし、常に最新のセキュリティを適用してください。

規制準拠を考慮したソリューションを使用する: 医療保険の相互運用性と説明責任に関する法令 (HIPAA) (1996 年) が米国内のすべての医療会社に適用され、該当する医療会社は、個人の特定につながる医療情報の使用、開示、保護に関する要件を順守する必要があります。Microsoft のクラウド サービスは HIPAA に準拠しています。Windows 10 および Office 365 に備わっている Advanced Threat Protection 機能は、着信メールに添付されているファイルとリンクをすべて自動的にチェックし、潜在的な脅威を検知します。疑わしいメールはエンド ユーザーに配信されないので、ソーシャル エンジニアリングを利用したネットワークへの不正侵入が減少します。

第 2 段階: より強力な権限を獲得する

組織への侵入に成功した攻撃者が次に行うのは、ローカルでの権限昇格です。多くの攻撃者は、この時点で、ローカル システムのより強力な権限を得る方法を探ります。管理権限を得やすい、あるいは有益なデータを入手できる可能性が高い別のシステムを探す場合もあります。目的は、システム管理者のユーザー アカウントを突き止め、そのアカウントになりすましてシステム リソースにアクセスし、管理、更新することです。そしてさらに、標準ツールやダウンロードしたツールを利用して、攻撃に役立つシステムやネットワーク リソースを見つけ出し、ユーザー名とパスワードを入手しようとします。通常、標準ユーザーではこれらの操作を実行できません。

主な用語:

キーロガー: ユーザーが押したキーを記録するマルウェア。"キーストローク ロギング" とも呼ばれます。攻撃者は、このマルウェアを利用してキー入力を記録し、標的組織のネットワークにログインするためのユーザー名とパスワードを収集します。

Pass-the-Hash (PtH): パスワード自体ではなく、そのハッシュ (コード) を利用して標的ユーザーになりすます攻撃手法。ユーザーの実際の資格情報がわからなくても、リモート サーバやサービスにアクセスできます。

ネットワーク スキャン: 攻撃者はこの方法でネットワークを偵察し、現在アクセス可能なシステム (ネットワークに接続されているホスト マシン、サービス、リソースなど) を特定します。その後、新たに入手した管理者権限でアクセスできるシステムの標的リストを作成します。

業界別事例: エンターテイメント & メディア

エンターテイメント & メディアは注目が集まりやすい業界です。特に、世間で話題のコンテンツはハクティビストの標的となります。メディア会社やエンターテイメント会社への攻撃は、多くの場合、情報入手もさることながら、"声明文を出す" ことが大きな原動力となっています。これまでハクティビストたちは、企業の機密情報を公表したり、組織の Web サイトを乗っ取るなど、さまざまな混乱を引き起こしてきました。

ある会社が不正侵入され、機能が停止しただけでなく、社員、顧客、知的財産に関する機密データが流出してしまった事件がありました。このハッキング事件の発生経緯は明らかになっていませんが、ソーシャル エンジニアリング、修正プログラムが未適用の脆弱性、単純な設定ミスなど、よくある攻撃経路から同様の事件がいくつも発生しています。

メディア会社が攻撃を受けると、そのダメージは広範囲に及びます。この会社の場合、不正侵入の規模とその影響は、財政的にも、地政的にも、前例のないものでした。攻撃を突き止め、侵入を阻止するための実質的なコストはもちろん、それ以上に問題なのは会社としての信頼性の低下です。本来であれば新規プロジェクトの開発にあてる時間と資金を信頼回復に費やさなければなりません。

有効なネットワーク ソリューション

攻撃による壊滅的な被害を防ぐには強力なセキュリティ戦略が必要であり、その中心となるのは総合的なリスク管理です。つまり、所有している資産、それらに対する潜在的リスク、それらが流出した場合のコストを明らかにし、自社の資産を保護するための対策を立てなければなりません。さらに、問題の発生をすみやかに検知し、それ以上の攻撃を阻止すると同時に、適切に対処することも不可欠です。これらのアプローチを、組織内でのセキュリティ ライフサイクルの一環として実施する必要があります。大切なのは、リスクを継続的に評価し、そこから得た教訓をシステムに反映させることです。

マイクロソフトが推奨するセキュリティ対策:

防御、検知、対処: セキュリティ システムの枠組みを構築する際に役立ちます。リスクを把握し、攻撃にすみやかに対処、是正して、その教訓を活かすため、マイクロソフトやその他の企業が採用しているアプローチの 1 つでもあります。

"最小特権" アクセス: 個々の仕事スタイルではなく、役割に基づいてネットワークのアクセス制御を定義し、割り当てられた職務や任務の遂行に必要な最小限のアクセス権を付与します。どの社員にも、任務の遂行に不要なネットワークやリソースへのアクセス権を付与しないでください。これは、不正侵入を阻止するための一般的な方法です。

セキュリティ開発ライフサイクル (Security Development Lifecycle): より安全なソフトウェアを開発するためのプロセス。セキュリティ コンプライアンス要件に準拠しつつ、開発コストを削減できます。

セキュリティの強化に役立つツール:

Local Administrator Password Solutions (LAPS): このソリューションでは、ドメイン内の各コンピューターにそれぞれ異なるランダムなパスワードを設定できます。ドメイン コントローラーはこれに基づいて、パスワードの読み取りを許可されているユーザー (ヘルプデスク管理者など) を特定します。

Windows 10 Credential Guard: Windows 10 Enterprise に導入されたこの仮想化ベースのセキュリティは、機密情報を分離し、権限を与えられたシステム ソフトウェアのみが機密情報にアクセスできるようにします。

Microsoft Advanced Threat Analytics (ATA): 行動分析に基づいて PtH 侵害や脅威を特定。開発コストを削減しつつ、ソフトウェアの安全性向上とセキュリティ要件への準拠を実現できます。

業界別事例: 食品製造

ある大手飲料メーカーは、ネットワーク セキュリティの強化と IT コスト削減の必要に迫られていたものの、どこから手を付ければよいかわかりませんでした。そこで、IT 業務をアウトソーシング (外部委託) し、社内では清涼飲料水の製造に専念することにしました。ところが、IT ベンダーに IT 業務を委託する際、社内データの安全性を考慮しなかったため、この飲料メーカーは多大な損失を被る結果となってしまいました。原因の 1 つは、顧客の重要なアカウントを保護するにあたり、デュー デリジェンス プロセスに従っていなかったことです。顧客の重要なアカウントを厳重に保護していなかったことも大きな原因です。これらのアカウントが流出すれば、機密情報が保存されたサーバーへのアクセスを許すことになってしまいます。

この事例では、IT ベンダーが自社の通常の活動と飲料メーカーのアカウントを分離していなかったため、飲料メーカーのアカウントが外部からの攻撃にさらされてしまいました。社員宛ての電メールや Web サーフィンを利用したソーシャル エンジニアリングなど、ごく一般的な攻撃です。飲料メーカーのアカウントを入手した攻撃者は、IT ベンダーを装って同社をリモートから管理し始めます。さらに悪いことに、既にこの飲料メーカーは、顧客のバックボーン システムをローカルで管理していなかったため、IT ベンダーを通じてやり取りしなければなりませんでした。これが原因で、修復チームがこれら重要なアカウントの制御を取り戻すまでは、調査や修復をスムーズに進めることができませんでした。

この飲料メーカーの場合、一部の重要なワークロードを外部委託するとしても、データやバックボーン システムへアクセスするための "鍵" は社内に保持するべきでした。また、オンサイトの電子メール システムをホスト型マネージド ソリューション (Office 365) に切り替えるなど、一部のビジネス システムをクラウドへ移行すれば、IT 業務を外部委託する必要がなく、本来の製造業務に専念すると同時にコスト削減も実現できます。ホスト型ソリューションには、社員の作業負荷が軽減される、毎月の必要コストを予測できる、ビジネスを制御できる、サービス プロバイダーの専門知識を利用できるなどのメリットがあります。

社内にキャパシティが飽和状態のシステムが多数存在する場合は、信頼できるクラウド サービスへの移行をお勧めします。プラットフォーム、インフラストラクチャ、およびサービスをクラウド経由で利用すれば、これらのシステムやデータセンターをセットアップしたり、管理したりする必要が一切ありません。また、オペレーティング システムやハードウェアに自分たちで修正プログラムを適用する必要もありません。

IT ベンダーに委託するか、クラウド サービス プロバイダーを利用するかにかかわらず、データのセキュリティ、プライバシーと制御、コンプライアンス、および透明性に関する規範とポリシーを必ず質問し、確認することが大切です。この飲料メーカーの事例でも、事前にこれらを質問し、情報を収集していれば、委託先 IT ベンダーのセキュリティに問題があると気付いたはずです。

成功の秘訣

IT 業務の外部委託 (アウトソーシング) は、オーバーヘッドの削減という点では魅力的な解決策です。ただし、自社のデータや知的財産を保護するうえで IT アウトソーシングが最善かどうかを必ず検討し、信頼に値するポリシーと規範を設けているベンダー (またはサービス プロバイダー) を選定する必要があります。上記の飲料メーカーの例からわかるように、アウトソーシングのメリットと、データ セキュリティを他社に委ねることのリスクを十分に比較検討しなければなりません。

ベンダーを探す前の確認事項:

- **外部委託 (アウトソーシング) するサービスの種類**
- **外部委託 (アウトソーシング) するアクセス レベル**
- **(サードパーティに委託する代わりに) クラウドを利用した場合、IT コストをどの程度削減できるか**

現状を確認したうえで、社外ベンダーに委託するか、クラウド サービス プロバイダーを利用するかを決定しましょう。プロバイダー候補を入念に調査し、検討してください。さまざまな質問をし、災害に備えて万全の対策がなされているかを見極めることが大切です。

ベンダー候補への質問事項:

- **Enhanced Security Administrative Environment (ESAE) の規範に従っていますか。**
- **ドメイン管理者 (DA) アカウントおよびエンタープライズ管理者 (EA) アカウントについて、ログオン可能なリソースを制限していますか。**
- **Azure Active Directory で Privileged Identity Management (特権 ID 管理) を使用していますか。**

第 3 段階: ネットワークへ侵入する

第 3 段階では、1 台のワークステーションまたはサーバーに侵入した攻撃者が他のシステムへ次々に移動し、ネットワークの侵入範囲を拡大していきます。その後、繰り返し侵入できるようにするための仕組み (バックドア) を設置する場合もあります。

攻撃者はさまざまなツールを利用します。マルウェア (インプラント) もその 1 つです。ネットワークへの再侵入だけでなく、環境内に隠れてさまざまなリソースにアクセスできるようにするため、偽のアカウントを作成する、リモート アクセスを獲得するなど、一見合法的な手段を使用する攻撃者もいます。一般に、インプラントやボットを手段とする攻撃者は、中央 "指令" コンソールを使用してすべてのリソースを制御します。さらに、ネットワークへの侵入拠点が適切に機能しているかどうかを確認する場合も、この "指令" コンソールを使用します。制御下にあるいずれかのアクセスが意図的にオフラインにされた場合、誰かが攻撃に気付いたと判断し、見つからないように身を隠すことができます。

主な用語:

ボット: 攻撃者によって PC 上にひそかにインストールされる小さいプログラム。

ボットネット: ボットをコピーして多数の PC にインストールする悪質なシステム。悪意のあるハッカーがボットネットを利用し、より大規模な攻撃を企てます。

指令 (C&C): ボットネットなど、中央から指令を出して多数のコンピューターを制御するときに使用するサーバーおよびインフラストラクチャ。ボットネットに指令を出すブラック ハット ハッカーを "ボットネット コントローラー" または "ボットマスター" といいます。

業界別事例: 政府機関

この政府機関は、ソフトウェアに修正プログラムをすみやかに適用する、管理者権限を与えるエンド ユーザーの数を制限する、セキュリティ チェック (レビュー) を定期的に実施するなど、考えられるほぼすべてのセキュリティ対策を講じていました。さらに、ドメイン管理者 (DA) およびエンタープライズ管理者 (EA) は専用の管理ワークステーションを使用しています (DA と EA は、組織内のその他すべてのアカウントを制御します。このレベルのアクセス権は、エンタープライズ内のごく限られたユーザーにのみ付与し、DA と EA の資格情報を割り当てる際は注意深く監視する必要があります)。

この機関の致命的なミスは、エンタープライズ全体 (人事、経理、および重要な IT 管理コンピューター) で同じローカル管理者パスワードを使用していたことです。セキュリティに敏感なはずの政府機関で、なぜこのようなミスが発生したのでしょうか。

ローカル管理パスワードの共有は、リスクを認識していない多く組織で行われている方法です。アカウントの権限が制限されていると、システムの初期セットアップに支障をきたす場合があります。この問題を解決するため、管理者は、アプリケーションのセットアップが完了するまでアカウントに多くの権限を与えます。ところが、問題が解決した後も、追加した権限をそのままにしておく管理者が少なくありません。また、緊急時にローカル アカウントを使用した後、将来に備えてそのままにしておくケースも考えられます。いずれの場合も、システムが攻撃にさらされることになってしまいます。IT 部門のこうした行動は、セキュリティを "ローカル" でのみ考えていることの表れです。インターネットに常時接続されている今日の環境では、システムを脅威から守ることができません。

この政府機関の場合、ネットワークに侵入された原因は、感染した文書にユーザーがアクセスしたこと、あるいは不正コードが埋め込まれた Web サイトへのリンクをクリックしたことと考えられています (正確な感染経路はわかっていません)。機関内の複数の部署で同じローカル管理者パスワードを使用していたため、攻撃者はネットワークを探索し、DA および EA の資格情報を手に入れることができました。これらの資格情報は "中枢へのパスポート" です。攻撃者はデータセンター、サーバー、Microsoft Exchange にコードを埋め込み、ネットワーク全体への侵入を成功させました。

システムの再構築、パスワードの再発行、データ窃盗とその "原因" の公開調査だけでも、その損失額は数百万ドルに及びます。さらに、この攻撃で失った信頼の代償は計り知れません。

包括的な防御策

この政府機関はさまざまな対策を講じていましたが、攻撃の阻止に必要なのは包括的なアプローチです。

マイクロソフトが推奨する防御策:

Microsoft Enhanced Mitigation Experience Toolkit (EMET): ソフトウェアの脆弱性が悪用されるのを防ぎます。

Microsoft Office 365: この製品スイートは、法的基準、規制基準、技術基準に即したデータの利用など、組織のセキュリティ ニーズを満たすように設計されています。

Enhanced Security Administrative Environment (ESAE): 最先端の技術と推奨規範を利用し、高度なセキュリティ保護を備えた管理環境とワークステーションを実現します。

Active Directory 向け Privileged Identity Management: 特権 ID を管理。Azure Active Directory やその他 Microsoft オンライン サービス (Office 365、Microsoft Intune など) のリソースへアクセスする特権 ID を制御、監視できます。

Microsoft Advanced Threat Analytics (ATA): 行動分析に基づいて、アカウントや資格情報の変則的な使用を監視します。

Operations Management Suite (OMS): クラウドベースの IT 管理ソリューション。攻撃者の監視、警告、追跡に役立ちます。

第 4 段階: 長期的な攻撃態勢を整える

第 4 段階は、長期的な攻撃拠点の設置です。できるだけ長い間潜伏し、脆弱性を利用するマルウェアを実行したり、データを監視して盗み出したりするための一連のプロセスを展開します。攻撃者は、自分自身のアカウントを作成してネットワークに潜入し、パスワードを変更して検知を逃れます。

第 3 段階と同様、攻撃者はインプラントやボットを利用し、環境内に潜入して繰り返し攻撃するための拠点を作成します。さらに、司令 (C&C) コンソールを操り、攻撃拠点からリソースを探索したり、ネットワーク内のチャネルにアクセスしたりします。見つかりそうになった場合に備え、すみやかに撤退して、再びアクセスするための手段とリソースも用意しています。

主な用語:

持続的標的型攻撃 (APT): 特定の対象を標的とする攻撃。攻撃対象のシステムに潜入し、一定期間にわたって情報を盗み出します。

Assume Breach (不正侵入を前提とする対策): ビジネスリーダーや CISO に求められる戦略的考え方。単なる予防型のセキュリティ対策ではなく、侵入の検知、対処、復旧という一連のセキュリティ プロセスに注目すること。

業界別事例: ハイテク製造業

相手は執拗に攻撃をしかけてきます。何百日のもの間、ネットワークに侵入されていることにまったく気付かない場合もあります。その間、攻撃者はシステムを改変し、ログを書き換え、ハッキング ツールを更新します。あるハイテク製造会社は、少なくとも 1 年半の間、"招かれざる客" がネットワークに侵入していることに気付きませんでした。その間、攻撃者は、顧客のホーム ドライブ サーバーに高度な標的型マルウェアを仕込んでいました。このサーバーには、顧客のほぼすべての知的財産 (IP) が格納されています。

このマルウェアを通じて、顧客の PowerPoint プレゼンテーション、各種文書、プロジェクトのスケジュール、および詳細な製造プロセスがすべて攻撃者の手に渡ってしまいます。侵入に気付いたときは、顧客のネットワークのさまざまなエリアから、調査や開発に関する膨大な情報が盗まれていました。

より強力なセキュリティ対策

この製造会社の顧客ネットワークに攻撃者がどのように侵入したのかはわかりませんが、攻撃手法から考えて、何らかの方法で入り込み、マルウェアを設置したのは間違いありません。

この種の不正侵入の防止に役立つツール:

Advanced Threat Protection: Office 365 のこの機能は、着信メールに添付されているファイルとリンクをすべて自動的にチェックし、潜在的な脅威を検知します。疑わしいメールはユーザーに配信されないので、ソーシャル エンジニアリングを利用したネットワークへの不正侵入が減少します。

多要素認証 (MFA): ユーザー名とパスワードだけでなく、さらに別の要素を使用してユーザーを認証する方法。たとえば、電話をかけたり、テキスト メッセージを送信して、本人であることを確認します。

Azure Rights Management (Azure RMS): この情報保護ソリューションは、暗号、ID、および承認のポリシーに基づいてファイルや電子メールを保護します。スマートフォン、タブレット、PC など、さまざまなデバイスで使用できます。

Microsoft OneDrive: このクラウド ストレージ ソリューションには、ファイルの安全性を高めるための機能が複数用意されています。OneDrive にアップロードしたファイルは、公開フォルダーに保存するか、自分で共有を選択しない限り、他のユーザーと一切共有されません。推測されにくいパスワードを作成し、既存の Microsoft アカウントのセキュリティを強化し (別の電子メール アドレスを使用する、セキュリティの質問を設定するなど)、2 段階認証を使用することで、セキュリティを一層強化できます。

Microsoft データセンター: 数十年にわたってエンタープライズ ソフトウェアを手掛け、グローバル オンライン サービスを運用してきたマイクロソフトは、その経験を活かして信頼されるセキュリティ テクノロジーを開発し、最善のセキュリティ対策を実施しています。Microsoft データセンターは物理的な建造物であり、フェンス、守衛、身元調査、生体認証 (アクセス制御) によって厳重に管理、監視されています。さらに、セキュリティ トレーニングを実施し、ハードディスク シュレッダーと同様の機器でサーバーを廃棄しています。どのデータセンターも 24 時間監視されており、多要素認証 (生体認証を含む) を採用し、内部ネットワークを公共のインターネットから分離しています。

業界別事例: オンライン ショップ

最後の被害事例はインターネット関連です。

犯罪目的でオンライン ショップの顧客データが狙われ、大きな注目を集めた事件がありました。多くのオンライン ショップは、ほとんど制限なく、主要ベンダー (クレジットカード サービスなど) へリモート ネットワーク アクセスできるようになっています (ほぼすべての従業員にアクセスが許可されている場合もあります)。これが第 1 の危険要因です。2 番目は、ネットワークが分離されていないこと。いったんネットワークに侵入してしまえば、標的組織のサーバー間を自由に移動することができます。

攻撃者が標的会社のサーバーへリモート アクセスする際、その会社のベンダー接続を利用したケースがいくつもあります。システムに入り込んだ攻撃者は、ベンダーになりすまして環境内を偵察し、財務データや (財務データにアクセスできる) アカウントが格納されている重要なシステムに侵入します。つまり、1 つの会社に侵入した後、その会社と取り引きしている別の会社にもアクセスしているのです。

この方法で攻撃された小売会社は、侵入発覚から 1 週間で株価が大幅に低下します。不正侵入された会社、特に (規制準拠が義務付けられている) 規制対象産業の企業には、数十億にも及ぶ高い罰金が科せられます。さらに、罰金や訴訟が発生すれば、世間から攻撃を受けやすい会社であると見なされてしまいます。不正侵入に対処するための保険に入っている会社もあります。

オンライン ショッピングの保護

リモート アクセスを利用したハッカーの攻撃を防ぐ最善の方法は、リモート アクセスを禁止することです。とはいえ、オンライン サービス会社やオンライン ショップなど、多くの企業にとっては現実的な対策とはいえません。

自社ネットワークへベンダーが安全にアクセスできるようにする方法:

Azure 経由で公開する: Web インターフェイス アクセスやバックエンド データベースなど、社内ワークロードの一部を信頼できるクラウド PaaS (サービスとしてのプラットフォーム) へ移動します。クラウド ワークロードを使用すれば、社内ネットワークの必要なデータにのみ最小限のアクセスレベルを保持できます。この方法であれば、顧客のネットワークへ直接アクセスするユーザーの数を制限できます。同時に、必要な PaaS リソースへのアクセスのみを許可することで、ネットワーク内でユーザーに与える権限を減らすことができます。

多要素認証 (MFA): ユーザー名とパスワードだけでなく、さらに別の要素を使用してユーザーを認証する方法。たとえば、電話をかけたり、テキスト メッセージを送信して、本人であることを確認します。

リモート デスクトップ接続 (RDP) サーバーを Azure の仮想マシン (VM) へ移行する: VM を使用することで、ネットワーク セグメントごとに異なるパスワードを設定し、情報へのアクセスを制御できます。

まとめ

防御、検知、対処

防御、検知、対処

エンタープライズ セキュリティを改善しましょう。マイクロソフトは総合的なアプローチを推奨します。標的型攻撃の一般的な手口を理解することが大切です。サイバー攻撃は決して対岸の火事ではありません。エンタープライズ システムへの長期にわたる不正侵入が繰り返し発生していることを考えると、不正侵入を能動的に検知し、リスク軽減対策を講じることが重要といえます。標的型攻撃に迅速かつ効果的に対処する方法をご確認ください。

マイクロソフトは不正侵入対策を 3 つのステップに分けました。

ステップ 1: 防御

リスク管理と最小特権アプローチが有効です。次の事項を確認してください。

- その担当者は、そのリソースへ本当にアクセスする必要がありますか。
- 自分のデータがどこにあるか知っていますか。
- そのデータに誰がアクセスできるか知っていますか。
- 必要な規制に準拠していますか。
- ソフトウェアは最新の状態にアップデートされていますか。

ステップ 2: 検知

いつ侵入されてもおかしくはありません。疑い深くなりましょう。
次の事項を確認してください。

- どのようなときに不正侵入されるかを理解していますか。
- 侵入検知に役立つツールが用意されていますか。
- 侵入分析に役立つツールが用意されていますか。

ステップ 3: 対処

侵入対処プロセスが用意されており、適切なタイミングで始動することを確認しておきましょう。次の事項を確認してください。

- 不正侵入にどのように対処しますか。
- 資産が損なわれたり、会社としての評判が失われたりした場合、どのように対処しますか。
- 顧客とのコミュニケーション計画が策定されていますか。
- この教訓を活かすにはどうすればよいでしょうか。

マイクロソフトは、お客様のデータおよびシステムの安全性と機密性を維持するため日々取り組んでいます。組織におけるサイバーセキュリティ、プライバシーと規制、およびコンプライアンスのベスト プラクティスについて詳しくは、www.microsoft.com/trustedcloud をご覧ください。

Trusted Cloud (信頼できるクラウド) チームは、この電子ブックを作成するにあたり、貴重な時間、知識、才能を捧げてくださった Bruce Cowper 氏、Kasia Kaplinska 氏、Matt Kemehar 氏、IB Terry 氏、Yvette Waters 氏に深く感謝いたします。

© 2016 Microsoft Corporation.All rights reserved.この文書は情報提供のみを目的としています。Microsoft は、この文書に記載した情報について、明示的か黙示的かにかかわらず、一切保証を行いません。