Microsoft Security

セキュリティ意識を高める

ビジネスを保護するためのベスト プラクティス

脅威が急速に変化している現在の状況では、組織の最初で最後の防衛線となるのはテクノロジではなく人間です。

各自がサイバーセキュリティの責任を負う必要があります。個々のチーム メンバーとセキュリティ担当者は全員、果たすべき重要な役割を持っています。オンラインで安全に行動するためのベスト プラクティスを理解することにより、全員が自分の役割を果たし、サイバー スマートになることができます。

サイバー スマートになる

サイバーセキュリティに関する以下のインフォグラフィックを使って、組織内の全ユーザーが自分自身と同僚をオンラインで安全に保つためにできることを理解できるようにしましょう。

デバイス
インフォグラフィックを見る ›

詐欺
インフォグラフィックを見る ›

フィッシング
インフォグラフィックを見る ›

パスワード
インフォグラフィックを見る ›

社員が直面している脅威

社員が直面している脅威は人間を標的としているため、攻撃者はソーシャル　エンジニアリングの戦術を利用してユーザーを騙し、アクセス資格情報を提供させたり、機密情報を開示させたりします。最もよく利用される戦術のいくつかを以下に示します。

フィッシング

詐欺師は会社の社員に対して、同僚、友人、信頼できる人や会社を装い、リンクや添付ファイルを含むメールを送信します。

スピア フィッシング

より高度な形のフィッシングであるスピア　フィッシングは、ランダムなターゲットではなく、特定の人 (貴重な情報やアクセス権を持っている可能性が最も高い人) を標的とします。

コンテンツ インジェクション

このタイプの攻撃では、普段から利用されている Web サイト (オンライン バンキング ポータルなど) に、機密情報を求めるセカンダリ Web サイトにユーザーを誘導する悪意のあるリンク、フォーム、またはポップアップが挿入されます。

リンクの操作

信頼できるソースのリンクを装った悪意あるリンクです。ユーザーを偽装 Web サイトに誘導し、そこでアカウント情報の入力を求めます。

中間者

サイバー犯罪者が 2 人の人をだまして、お互いに情報を送信させます。詐欺師が虚偽の要求を送信したり、各当事者が送受信しているデータを改ざんしたりします。

マルウェア

マルウェアには、コンピューター、タブレット、スマートフォン、その他のエンドポイント デバイスを破壊したり通常使用を妨害したりする、悪意のあるアプリケーションやコードが含まれます。

基本的なサイバーセキュリティにおける 5 つの側面

99% の攻撃から組織を保護する方法:

1 多要素認証 (MFA) を有効にする
2 ゼロ トラストの原則を適用する
3 最新のマルウェア対策を使用する
4 システムを常に最新の状態に保つ
5 データの保護

1 多要素認証 (MFA) を有効にする

MFA を有効にすると、アカウントへの攻撃の 99.9% を防止することができます。[1]

MFA のベスト プラクティス

簡単に使えるようにする

社員の手間を最小限に抑える MFA オプション (デバイスでの生体認証や、Feitan または Yubico セキュリティ キーなどの FIDO2 準拠要素を使用するなど) を最小限に抑えた を選択します。

慎重になる

MFA は、あらゆる操作に適用するのではなく、追加の認証が機密データやクリティカルなシステムの保護に役立つ場合に選択します。

エンドユーザーの手間が増えないようにする

条件付きアクセス　ポリシー、パススルー認証、シングル サインオン (SSO) を使用することにより、デバイスで最新のソフトウェア更新プログラムが適用されている場合、ユーザーが企業ネットワーク上のクリティカルでないファイル共有や予定表にアクセスする際にサインオン　シーケンスを複数回行わなくてもよいようにします。

2 ゼロ トラストの原則を適用する

ゼロ トラストは、組織への影響を軽減するレジリエンス計画の基礎です。

ゼロ トラストの原則

侵害を想定する

攻撃者はあらゆるもの (ID、ネットワーク、デバイス、アプリ、インフラなど) を攻撃する能力を持っており、実際にそうすると仮定し、それに応じて計画を立てます。これは、攻撃を受ける可能性がある環境を絶えず監視することを意味します。

明示的に検証する

リソースへのアクセスを許可する前に、ユーザーとデバイスの状態が良好であることを確認します。信頼とセキュリティに関するすべての決定が、関連する利用可能な情報とテレメトリを使用するという事実を明示的に検証することにより、資産を攻撃者の制御から保護します。

最小限の特権アクセスを使用する

ジャストインタイムと必要最小限のアクセス (JIT/JEA) と、適応型アクセス制御などのリスク ベースのポリシーにより、侵害されう可能性がある資産へのアクセスを制限します。リソースへのアクセスに必要な特権のみ許可し、それ以上は許可しません。

3 最新のマルウェア対策を使用する

拡張検出および応答マルウェア対策を使用します。攻撃を検出して自動的にブロックし、セキュリティ操作に関するインサイトを提供するソフトウェアを実装します。

4 最新の状態に保つ

修正プログラムが適用されていない古いシステムは、多くの組織が攻撃の被害を受けている主な理由になっています。ファームウェア、オペレーティング システム、アプリケーションなど、すべてのシステムが最新の状態に保たれていることを確認します。

3 つのベスト プラクティス

修正プログラムを適用する

修正プログラムの迅速な適用、既定のパスワードの変更、既定の SSH ポートの変更よって、デバイスの堅牢性を高めます。

減らす

不要なインターネット接続とオープン　ポートをなくし、ポートのブロック、リモート アクセスの拒否、VPN サービスの使用によりリモート アクセスを制限します。

セグメント化する

ネットワークをセグメント化し、攻撃者が最初の侵入後に侵入を拡大する可能性を減らします。IoT デバイスと OT ネットワークは、ファイアウォールを通じて、企業の IT ネットワークから分離する必要があります。

5 データの保護

重要なデータとそれ存在する場所、適切なシステムが実装されているかどうかを把握することは、適切な保護を実施するうえで非常に重要です。

上記のサイバー管理対策について詳しくは、「Basic cyber hygiene prevents 99% of attacks」をご覧ください 。

ネットワークを保護するために念頭に置くべきヒント トップ 10

1. メールとブラウジングの安全な使用に関するトレーニングを社員に提供する。
2. Microsoft Defender for Office 365 の攻撃シミュレーション トレーニングを提供する。
3. パスワードレスに移行して MFA を使用する。
4. 社内のすべてのデバイスで、最新バージョンの Windows とインターネット ブラウザーを使用する。
5. ファイル保存に関する社内規定を設ける。会社のデータをクラウド上に安全に保管し、暗号化する。
6. セキュアな接続に関して社員を教育する。ブラウザーに HTTPS Everywhere プラグインをインストールする。
7. Web サイトの証明書を確認して Web サイトの出所を確認するよう社員をトレーニングする。
8. 自動化のベスト プラクティスとデータ ガバナンス戦略について調べてセキュアな環境を確保する。
9. ポップアップ ブロッカーを既定で有効にする。
10. Microsoft Windows Defender などの、クラウドベースのウイルス対策ソリューションを使用する。

---

[1] https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

サイバーセキュリティの他のベスト プラクティスとスキルアップの機会については、https://aka.ms/cybersecurity-awareness をご覧ください。

Microsoft Security