テレワークのセキュリティ対策
ベストプラクティス集

ゾーホージャパン株式会社 | ManageEngine

目次

はじめに

10 年前、テレワークはまだ普及しておらず、在宅勤務はごく一部でしか認められていませんでした。しかし、働き方や情勢の変化に伴い、現在では国を挙げてテレワークの普及促進が行われるまでになっています。このような潮流の中で、優秀な人材を確保し同時に運用コストを削減するために、多くの企業がテレワークの体制構築を始めています。2018 年のグローバル調査によると、16%の企業で完全なテレワーク体制を実施しており、また 40%の企業でハイブリットワーク体制（テレワークとオフィスワークの両立）を実施しています。

テレワーカーはハッカーやサイバー攻撃者から標的にされやすいため、セキュリティ対策はテレワークにおける最大の課題と言えます。社員にテレワークを許可する際には、IT 管理者とリモートワーカーの両方に、それぞれのガイドラインを設ける必要があります。以下で、テレワークを実施する企業とその社員をセキュリティリスクから守るためのベストプラクティスを紹介します。

IT 管理者へ

1. VPN サービスを計画・導入し、適切にパッチ管理を行い、脆弱性がないことを確認する

テレワーク体制を整えるためには、計画的な VPN 戦略が必要です。戦略にはセキュリティ管理およびネットワーク帯域のキャパシティプラニングも含めて考えましょう。VPN のセキュリティ対策の一環として、VPN サービスに最新のパッチを適用しているか確認することが重要です。特に、古いバージョンには脆弱性が存在する可能性があり、ハッカーに悪用される恐れがあります。また、VPN が適切に暗号化されていることを確認することも重要です。

2. ファイアウォールをリアルタイムで監視する

ネットワークセキュリティにおいて「監視」は重要な役割を果たします。社員の大半が自宅で勤務するようになると、社員と会社間のネットワークは攻撃を受けやすい状態になります。このような状況でサイバー攻撃を早期に発見するための唯一の方法は、攻撃をリアルタイムに監視することです。会社のファイアウォールのログを監視することで、以下のことを特定できます。

・ネットワークを標的とする攻撃の種類
・攻撃の発信源
・どの IP アドレスを標的としているか

ファイアウォールの監視とは別に、ネットワーク動作の異常検知（NBAD）システムを導入することも重要です。NBAD システムは単なる監視だけではなく、ゼロデイ攻撃、未知のワーム（マルウェアの一種）、内部の脅威など、さまざまな攻撃や脅威の検知を行うことができます。ファイアウォール監視と NBAD を組み合わせることで、IT 管理者は攻撃をリアルタイムに検知・可視化し、攻撃から自社のネットワークを守ることができます。

3. ユーザーの行動を追跡し、トラフィックやセキュリティの異常に迅速に対応する

ネットワークやインフラの監視は非常に重要ですが、ネットワークユーザー（社員）の監視も同じくらい重要です。PwC が実施した調査では、回答者の 3 分の 1 近くが、セキュリティインシデントの原因を内部的なものと考えています。ネットワーク内のすべてのユーザーを監視し、アカウント権限は上司の承認を経て、必要な社員のみに付与される必要があります。また、セキュリティ管理者がユーザーの異常動作をすぐに検知・特定し、ネットワークの脆弱性を迅速に修正できるように、異常を通知する仕組みを実装することも大切です。

4. テレワークセキュリティコンプライアンス要件の見直しをする

多くの会社は、業種毎にセキュリティに関する様々なコンプライアンスを順守しているかと思います（PCI DSS、ISO 27001、NIST、SANS、NERC-CIP、Cisco IOS、SOX、HIPAA など）。テレワーク導入によるセキュリティ上の脅威の増加に伴い、このようなコンプライアンスを遵守することがより重要になってきています。しかし、それは以下のような理由で困難になり得ます。

・セキュリティの厳格化のために軽微な変更が発生し、コンプライアンス要件が変更される
・コンプライアンスが機能しているか確認するための内部監査を行う際に、運用上の問題が多数存在する

新しい変更を試験的に導入するだけではなく、テレワークに既存のコンプライアンス基準をどのように適用するかについて、計画する必要があります。適切な計画は、テレワークにおけるネットワークのセキュリティ対策とコンプライアンスの順守に役立ちます。

5. サイバー攻撃に関する最新情報を入手し、復旧手順についてマニュアル化する

ネットワークのセキュリティ対策には難しい側面もあるかもしれません。しかし、攻撃者が新しい手法を開発し続けているため、サイバー攻撃は急速に変化しています。セキュリティ管理者は、サイバー攻撃について常に最新情報を入手し、それぞれの攻撃に対する復旧計画を考えておく必要があります。このような事前の対策は、攻撃への迅速な対応を可能にするだけではなく、攻撃を受けても重要なサービスを提供し続けるために非常に重要です。

6. 多要素認証を実装し、セキュリティインシデントの回避方法をリモートワーカーに教育する

テレワーク体制やデジタル社会の浸透とともにセキュリティ脅威は多くなっているため、社員の全員がセキュリティ対策における基本事項を正しく理解することが大切です。セキュリティ管理者は定期的に、セキュリティ対策においてよくある間違いや最新の攻撃について社員に共有する必要があります。また、組織内で多要素認証を実装していない場合は、すぐに実装する必要があります。

7. 暗号化されたメッセージングサービスを利用し、業務の協同作業がしやすい環境を構築する

社員同士のコミュニケーション促進のために、暗号化された安全なビジネス向けのコミュニケーションサービスを導入し、社員に利用を促す必要があります。一方、消費者向けのサービスは、セキュリティ面での脆弱性が高い可能性があるため、ビジネスにおけるコミュニケーションツールとしては適切ではありません。

企業のセキュリティ対策は IT 管理部門や社内のインフラだけでは成り立ちません。リモートワーカーも重要な役割を果たしています。したがって、IT 管理者は次項で紹介するポイントをすべてのリモートワーカーに伝える必要があります。

テレワーカーへ

1. 認証情報をメールやチャットなどで共有しない（IT 担当者とのやりとりも NG）

会社からテレワーカーに支給されるデバイスは、攻撃者の標的となり得ます。社員は特に、認証情報の取り扱いに注意する必要があります。IT 管理部門と社員のやりとりも含め、決して認証情報を誰かと共有しないようにしましょう。

2. 会社支給のデバイスをフリーWi-Fi に繋げて使用しない（個人契約の安全な Wi-Fi を使う）

会社のデバイスを自宅の Wi-Fi に接続する場合、Wi-Fi 設定の安全性を確認することが非常に重要です。社内ネットワークにアクセスする際に暗号化された VPN 接続を使用していたとしても、Wi-Fi ネットワークが攻撃を受けていれば、攻撃者は容易に社内ネットワークへ侵入してしまいます。Wi-Fi ネットワークを保護する方法を IT 管理者に尋ね、必要に応じて Wi-Fi 認証情報を再設定しましょう。また、フリーWi-Fi（公衆無線 LAN）は暗号化されていないことが多く、傍受やなりすましの危険性も高いため、仕事中は絶対に接続しないようにしましょう。

3. 怪しいメールは開かない、怪しいリンクや見慣れないリンクをクリックしない

金融機関や有名企業などを装うフィッシングメールや、人間の心理的な隙につけ込むソーシャルエンジニアリングは、テレワーカーから情報を盗み出すための常套手段です。メールを開封したり、メール内のリンクをクリックするなどの行動に移したりする前に、そのメールが信頼できる送信元であることを確認しましょう。

4. IT 管理部門で制定されているセキュリティガイドラインに従う

社員の 1 人 1 人が責任感を持って、会社の IT 管理部門で定められたセキュリティガイドラインに従いましょう。HDD やバックアップなどは必ず暗号化し、最新のセキュリティ情報や社内で発生したセキュリティインシデント情報はキャッチアップするようにしましょう。また、仕事を早く終わらせることに専念しすぎて、セキュリティに対する意識を蔑ろにしてしまうことにも注意しましょう。

最後に、セキュリティ対策は 1 人でできる一時的な取り組みではありません。継続してセキュリティ対策を行うためには、IT 管理者と社員の間で継続した連携が必要です。時には、セキュリティに関する規程を繰り返し変更する必要もあるでしょう。攻撃者はたとえ小さな脆弱性であっても攻撃を仕掛けようとしてくるので、社員はそうした変更をキャッチアップする必要があります。当 eBook で紹介したベストプラクティスが、テレワークを実施している企業様のセキュリティ対策において少しでもお役に立てるように願っております。

ManageEngine Firewall Analyzer について

ファイアウォールのポリシー(ルール)、コンフィグ、ログを継続的に監視、見直しすることは、テレワークのネットワークを保護する上で重要です。ManageEngine Firewall Analyzer は、ルール、コンフィグ、ログ管理のためのソフトウェアであり、セキュリティ管理者がセキュリティの脅威を迅速に検知し、ネットワークを保護するのに役立ちます。ManageEngine の Firewall Analyzer では、以下のことが可能です。

・VPN のユーザーセッションを追跡して、内部からの脅威を特定
・セキュリティログを分析して外部からの脅威を特定
・ファイアウォールログのフォレンジック分析を実行
・トラフィックとセキュリティの異常に対するアラート通知を設定
・ファイアウォールのポリシー(ルール)の記録、見直し、管理
・ファイアウォールのコンフィグ変更を監視
・コンプライアンスレポートの生成とセキュリティ監査の実行

ManageEngine Firewall Analyzer は、マルチベンダーのファイアウォールとオープンソースのセキュリティデバイスに対応しています。

ZJMR2020513267