CLOUDFLARE

リモートワーク、8つのセキュリティ対策

リモートワークは、様々な人たちがオンラインでつながって成り立っています。
そこでは正社員、契約社員、フリーランス、ベンダー、パートナーなどが同じツールを使って、一緒に働いています。そのような状況で、大切なデータにどんなセキュリティ対策をしていますか？
また、それらのツールがスムーズにアクセスできる環境ですか？
快適かつ安全なリモートワークを実現するために、8つの対策をご紹介します。

❶ VPN以外でアクセス保護

内部アプリケーションを保護するために、従来のVPNを使用しているかもしれませんが、多くの社員が遠距離から接続する環境は安全ではありません。
VPNは入ってくるもの全てを信頼してしまうという悪い面があります。VPNのフラストレーションやパフォーマンス低下を引き起こさず、デジタル的にデータのパケット全てに問い合わせを行うための最新ソリューションとして、ゼロトラストモデルがお勧めです。

❷ 脅威からチームを保護

SaaSアプリケーションを組み合わせて活用している場合、チームは潜在的にインターネットの未開の地に晒される可能性があります。これまで、企業はインターネットへのアウトバウンドトラフィックに脅威がないかスキャンするために本社にトラフィックをルーティングしていましたが、それでは時間がかかり規模によっては防御できません。チームの仕事を停止させることなく、最新の脅威を特定し、阻止する方法が必要です。

❸ 企業データを安全に管理

ビジネスにおいて、最も価値のあるデータはSaaSベンダー、内部アプリケーション、パブリッククラウドなど、様々な場所に保管されています。Cloudflareは機密データの保存をクラウド外とクラウドサービスの組み合わせでもサポートできるように設計。
保護を必要とするところにだけ、このデータが送信されるようにします。

リモートワーク、8つのセキュリティ対策

4 既存ツールの活用

セキュリティに対する取り組みが複雑な場合、社員はツールの使用が重荷に感じます。もしくはツールの使用を諦めてしまうかもしれません。それならすでに社員が使っているGoogleやOktaログインなど、チームにとっておなじみのシステムを使いましょう。

5 外部パートナーを迅速に追跡

今の時代、人員は流動的。契約社員やその他の外部パートナーのために、必要なものを揃えておくことは重要です。しかし一度プロジェクトが終わったら、彼らに与えていた権権限を全て取り消さなければいけません。最新の認証ソリューションで、契約社員や外部パートナーが使っていたサ ービスなどを追跡しましょう。

6 ツールを簡単に発見

優秀なリモートチームは、チームメンバーが必要なときに適切なツールを簡単に見つけられるようにします。launchpadは、アプリケーションを見やすく分かりやすいダッシュボードに集約。膨大な数のツールから必要なものを見つけやすくするよう設計されています。またlaunchpadにも多くの種類があります。あなたのlaunchpadは、きめ細かい権限をサポートしているか、従業員がアクセスする必要のあるツールだけを表示しているかを確認してください。

7 新しいソリューションを検討

レガシーアプリケーション（古いOSのアプリケーション）に不自由さを感じたら、SaaSソリューションに変更するチャンスです。SaaSアプリは高度な機能性と継続的な更新、そしてサブスクリプションモデルで提供してくれます。

8 もしものためにデータを保護

オフィスのダッシュボードが真っ暗になることがまれにありますが、情報が一緒に消えてなくなることがないようにしましょう。Security Information and Event Management (SIEM) プラットフォームにエクスポートする柔軟性を備え、広範囲なロギングと全てのリクエストの監査をサポートするソリューションを使っているか、確認してください。