netskope

クラウド活用した脅威の傾向

クラウドと脅威に関するレポート

提供:

netskope THREAT LABS

エグゼクティブサマリー

本レポートは、クラウドデータにおけるリスクと脅威に関する第5版のレポートとなります。リスクも脅威も今まで以上に高まっています。デジタルトランスフォーメーションが推進されるなか、クラウドを導入した企業の割合が2020年上半期では12%増だったのに対し、2021年同期では22%まで増加しました。しかし、会社で使用されているクラウドアプリケーションの97%が各部署や社員が個々で採用しているシャドーITであり、会社側で把握できていない現状があります。個人用アプリの使用は、退職する社員が個人用アプリのインスタンスに会社の機密データをアップロードするため、データセキュリティの課題を抱え続けることになります。また、会社の管理下にあるクラウドアプリであっても、サードパーティアプリのプラグインを許可していればデータセキュリティに対するリスクが潜んでいます。そしてクラウドワークロードがインターネット上に公開されているということは、攻撃者に侵入経路を教えていることと同じと言えます。攻撃者もまた、クラウドには前から目を付けていて、マルウェアをクラウド内で拡散させたり、ウイルスを仕込んだOffice文書を送り込んだりと、活動拠点を着々と広げています。

第5版となる本レポートでは、パンドラの箱ともいえる個人用アプリのインスタンスが、データ移動やデータ流出の温床となっているという現状について特筆しています。人気の高いSaaSの業務・個人インスタンス、シャドーIT、パブリッククラウドサービスをはじめとするアプリやクラウドサービスをインラインで復号化・分析できることが今回の調査結果における懸念を取り除く基礎となります。

Netskopeの脅威対策は　、幅広い可視性と膨大なメタデータに基づいて調査を行っています。セキュリティスタックも同様の可視性と制御のもとでデータ管理のリスクや脅威を軽減する必要があります。

ハイライト

- 離職まで30日を切った社員は、通常の3倍のデータを個人用アプリにアップロードする。アップロード先は個人のGoogleドライブやOneDriveが最も多い。
- Google Workspace ユーザーの97%が、1つ以上のサードパーティアプリに対して、業務用Googleアカウントへのアクセスを許可している。「Googleドライブ内のファイルの表示と管理」などにサードパーティアプリがアクセスして第三者にデータが流出する可能性がある。
- AWS、Azure、GCP内にあるワークロードの35%以上がインターネット上に公開されており、これらワークロードの8.3%がRDPサーバーが使用されハッカーにとって格好の侵入経路となっている。
- クラウドを標的としたマルウェアの増加率は過去最高の68%に達し、2020年初めの20%から増加している。クラウドストレージアプリは66.4%を占め、ウイルスの仕込まれたOffice文書は、ダウンロードによるマルウェア被害全体の43%を占めている。
- クラウドアプリの導入率は、2021年の上半期で22%増加し、従業員数500～2,000人規模の企業では、805種類のアプリやクラウドサービスが使用されている。これらのアプリの97%は会社の管理下にないシャドーITであり、各部署や社員が個々で採用している。
- 2021年6月末時点で、70%のユーザーが在宅勤務を継続している。2020年3月に発生した新型コロナウイルスの影響によるもので、オフィス勤務再開の目途は立っていない。

退職する社員が社内データの持ち出しにクラウドアプリを利用

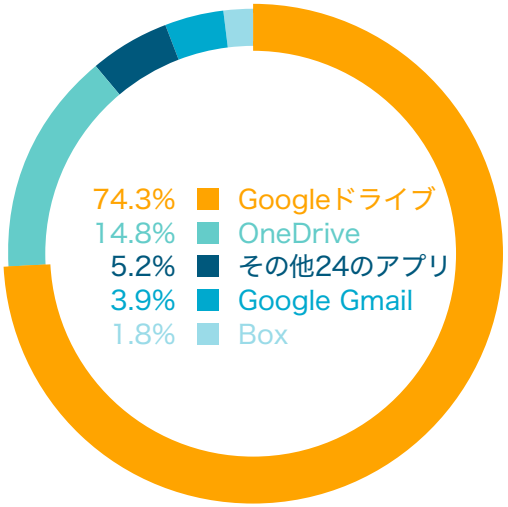
退職する社員がデータを持ち出すことによってデータセキュリティに脅威をもたらす場合があります。ユーザーが社内データを持ち出してしまうよくある例のひとつとして、個人用アプリのインスタンスにユーザーがデータをアップロードすることが挙げられます。退職まで残り30日をきった3分の1の社員においては、個人インスタンスへのデータのアップロード量が通常の3倍にまで増加します。主なアップロード先には、Googleドライブと OneDriveがあります。

退職する社員のうち、個人用アプリのインスタンスにデータをアップロードする際に、会社の管理下にあるアプリインスタンスからデータを直接コピーしてファイルをアップロードしたり、会社のデータ管理規約に違反する行為をしたりする割合は、全体の15%に上ります。会社のデータを無許可でコピーする場合、OneDrive や Box からコピーをすることが多く、アップロード先は個人用 Googleドライブが最多です。会社のデータ管理規約に違反して持ち出されるファイルには、以下の4種類があります。

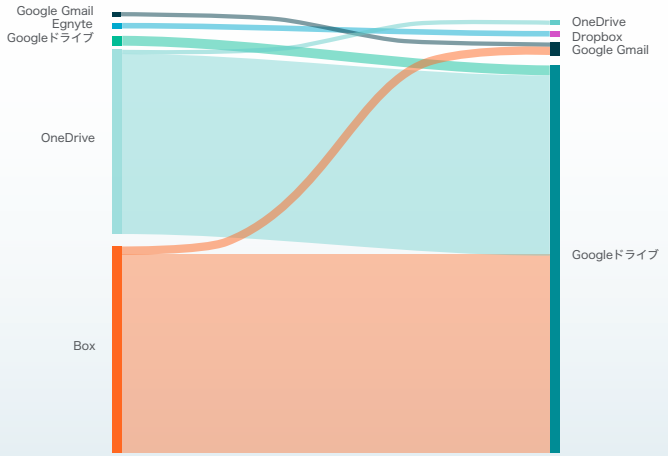
- 個人特定情報
- 社員の健康管理情報
- 知的財産
- ソースコード

退職時に個人用クラウドアプリを利用してデータを持ち出すことから、退職者が多くなるにつれ、セキュリティ上の重大なリスクにつながる可能性が高くなります。

アップロード先に使われている個人用アプリ



個人用アプリのインスタンスに移された社内データ



サードパーティアプリのプラグインによるデータリスク

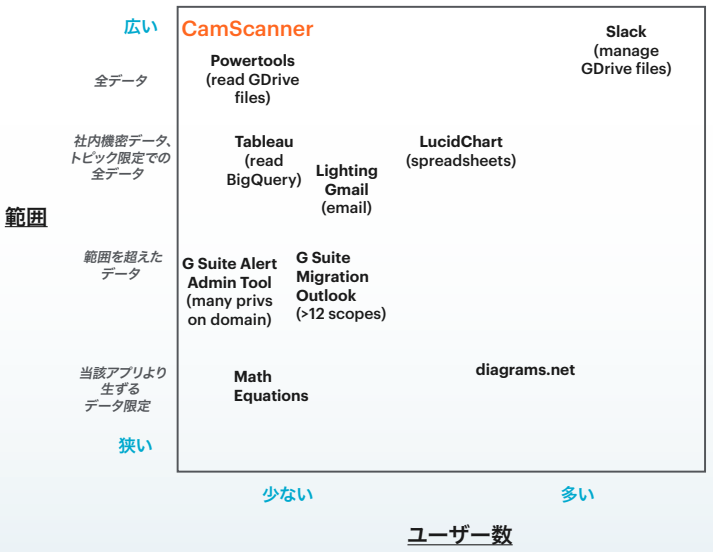
サードパーティアプリのプラグインを利用して、機密データへのアクセスを許可している場合、データセキュリティの脅威となります。例えば、Google Workspace ユーザーの97%が、ひとつ以上のサードパーティアプリに対して業務用Googleアカウントへのアクセスを許可しています。各サードパーティアプリが要求するアクセスの範囲は、Googleアカウントのプロフィールで一般公開されている「アカウントの基本情報」から、「Googleドライブにあるファイルの表示および管理」といったGoogleドライブに入っているすべてのデータまで様々です。「Googleドライブにあるファイルの表示および管理」などへのアクセスを要求するサードパーティアプリは、機密データをその他のサードパーティに公開する可能性があるため、データセキュリティの脅威となります。例えば「CamScanner」という画像スキャンアプリは、「Googleドライブにあるファイルの表示および管理」へのアクセス承認を要求してきますが、 2019年8月に、ロシアのカスペルスキー社がこのアプリにはマルウェアが仕込まれていたことを公表し、2020年6月にインド政府が、データセキュリティ問題を理由に同アプリの使用を禁止しました。

Googleのプラグインとして利用される人気アプリ上位５種

1	Google Chrome	Chromeブラウザ	463,286	91.0%
2	iOS Account Manager	iOSアプリケーション	183,730	36.1%
3	Zoom	ビデオ通話	135,361	26.6%
4	Android device	OSレベル、モバイル	117,927	23.2%
5	Slack	メッセージ	95,848	18.8%

社内データをサードパーティに晒してしまう危険性のほかに、攻撃者は不正なアプリを作成しこのプラグインに対しユーザの環境へのアクセス圏を付与するために「不正な同意許可攻撃」と呼ばれる巧妙な手口でユーザーの環境にアクセスを試みます。このようなサードパーティアプリであるかを特定する方法は、前述のアクセス承認要求の範囲が多岐にわたっているか、そのアプリのユーザー数が比較的少ないことに着目することです。

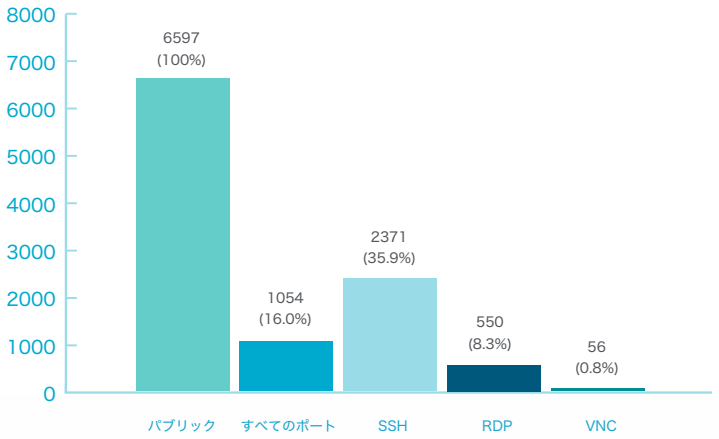
アプリが求めるアクセス範囲



クラウド環境へのパブリックアクセスが攻撃者に与える機会

ワークロードをインターネットに公開すると、攻撃者による侵入のリスクが高くなります。AWS、Azure、GCPといったクラウドサービスにある社内文書やデータの35%が、インターネットに公開されています。これは文書やデータすべてにパブリックIPアドレスが割り振られ、インターネットのどこからでもアクセス可能であることを意味します。公開されているワークロードの8.3%がRDP（Remote Desktop Protocol：リモートデスクトッププロトコル）を使用しています。こうしたRDPは、攻撃者にとっては格好の侵入経路となっています。ソフォス社が実施した調査報告によると、サイバー攻撃の30%が、インターネットに接続されたRDPサーバーを悪用した攻撃であったことが分かりました。最近公表された一例として、2020年9月に発生したエクイニクス社に対するサイバー攻撃があります。同社は社内のRDPサーバー74台をインターネットに接続していたことでサイバー攻撃の被害に遭いました。その他のRDPとして、SSHとVNCがあります。クラウドのワークロードを介した侵入リスクの多くは、VPN（Virtual Private Network：仮想プライベートネットワーク）やZTNA（Zero Trust Network Access：ゼロトラストネットワークアクセス）を使用することで軽減することができます。

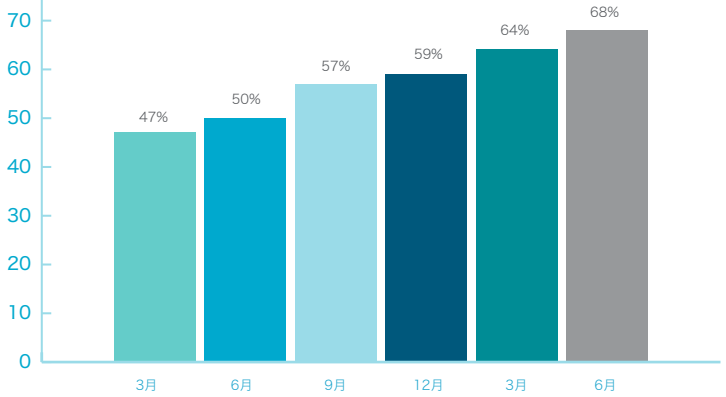
AWSのパブリックコンピュートインスタンス：リモートアクセス



クラウドアプリを悪用して検出を回避

攻撃者は以前にも増して、ユーザーの多い人気クラウドアプリを悪用してマルウェアを拡散したり、ブロックリストを回避しています。2021年の第2四半期では、マルウェアの68%が、クラウドアプリからダウンロードされたものでした。また、クラウドに拡散されたマルウェアの66.4%がクラウドストレージアプリによるものでした。続いて、コラボレーションアプリや開発ツールが多く、これは人気の高いチャットアプリやコードリポジトリを悪用した攻撃を仕掛けることが要因となっています。Netskopeは、2021年上半期に290の異なるクラウドアプリからマルウェアのダウンロードを検出し、ブロックしました。

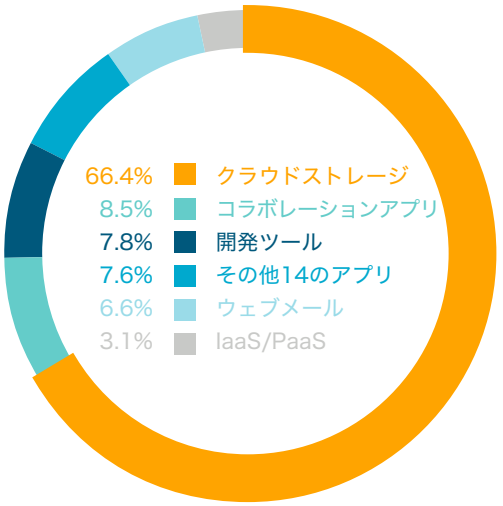
クラウドを標的としたマルウェアの増加率



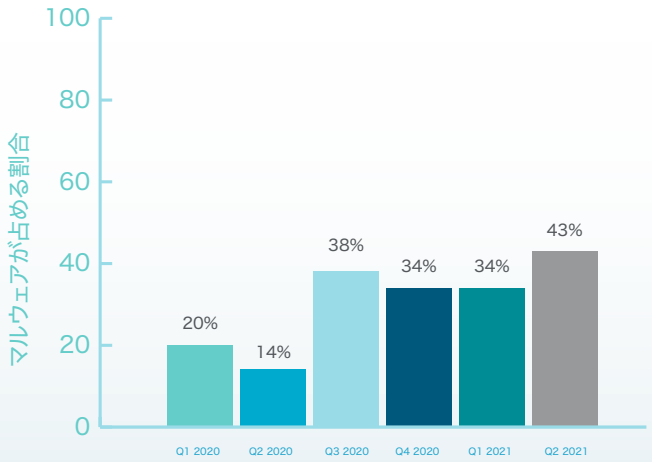
攻撃者がクラウドアプリを使ってマルウェアの拡散をする主な理由は、ブロックリストを回避できるほか、アプリ固有のユーザー承認リストを悪用するからです。被害報告を受けたクラウドサービスプロバイダーは不正コンテンツを削除してしまうため、クラウドからの攻撃は短命に終わりますが、攻撃者はそんな短い時間でも攻撃を仕掛けることが可能です。

また、検出を回避できる画期的な新たな手法を発見したことで、Office文書を悪用した攻撃も増加しています。前年の初めにはわずか20%だったマルウェアのダウンロードが2021年第2四半期では全体の43%にまで増加しました。世界で脅威を振るったマルウェア「エモテット」が息の根を止められた後に増加しているため、攻撃者がエモテットの成功を研究し、その手法を応用したと考えられます。

マルウェアのダウンロードに使用される上位アプリ



Office文書を悪用したマルウェアの割合(%)

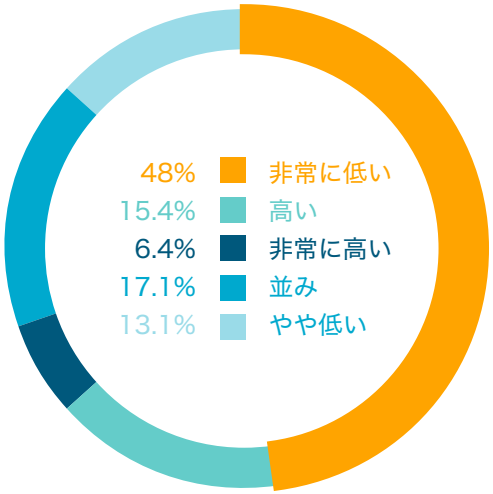


クラウドが複雑になるにつれデータと脅威に対するリスクも増大

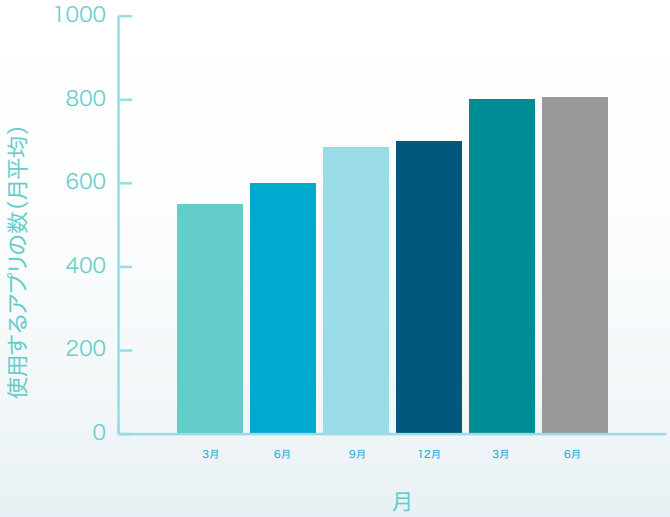
企業で使用されているクラウドアプリの数は増加しています。2020年上半期では12%増に対し、2021年上半期では22%増となりました。従業員数500人～2,000人規模の企業で使用されているクラウドアプリの種類は月平均805種類となります。そのうち97%が、社内の各部署や社員が個々で採用しているシャドーITアプリで、そのうち48%は、CCI（Cloud Confidence IndexTM）のリスク評価が「非常に低い」という結果となっています。企業はこのような安全性の低いアプリの使用を避け、より安全なアプリに切り替えるための措置を講じる必要があります。

クラウドアプリの導入が22%も増した最大の要因は、一般消費者向けアプリとコラボレーションアプリの需要が高まったことにあります。この傾向は、2020年初頭に新型コロナウイルスが世界的に流行した時期から見え始め、在宅勤務に切り替わったユーザーが、チームとつながるためにコラボレーションアプリを利用するようになったからと言えます。オフィス勤務と在宅勤務の境界線が曖昧になったことで一般消費者向けアプリの使用が増加し、この傾向は2020年末から2021年に向けてさらに加速しました。

CCIによるアプリのリスク評価



従業員数500～2,000人規模の企業に勤務するユーザー

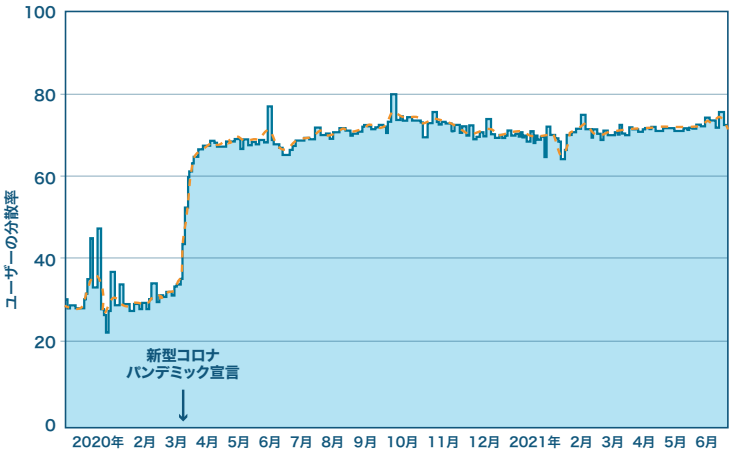


オフィス勤務再開にはまだ時間がかかる

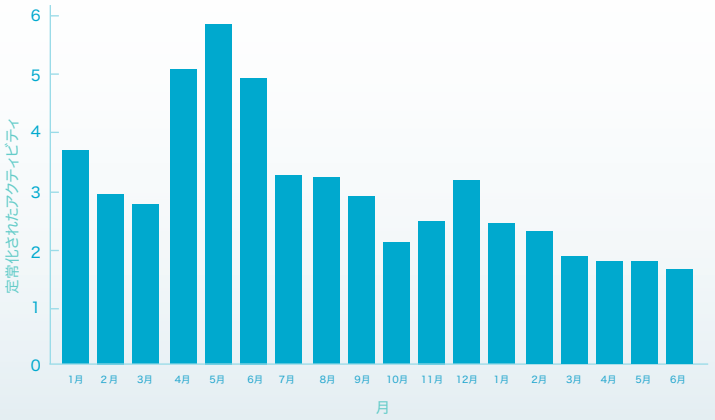
クラウドアプリの導入が22%も増した最大の要因は、一般消費者向けアプリとコラボレーションアプリの需要が高まったことにあります。この傾向は、2020年初頭に新型コロナウイルスが世界的に流行した時期から見え始め、在宅勤務に切り替わったユーザーが、チームとつながるためにコラボレーションアプリを利用するようになったからと言えます。オフィス勤務と在宅勤務の境界線が曖昧になったことで一般消費者向けアプリの使用が増加し、この傾向は2020年末から2021年に向けてさらに加速しました。

自宅で仕事をするようになったコロナ禍の初期段階では、アダルトコンテンツ、ファイル共有、海賊版サイトなど、危険なWebサイトを閲覧するユーザーが急増しました。しかし、ユーザーが在宅勤務に慣れてきたことや、ITチームがユーザーに利用規定の指導を行ったことで危険なWebサイトの閲覧は減少していきました。

在宅勤務の推移



リスクが高いユーザーによるWeb上アクティビティ



アプリ、データ、ユーザーを保護するクラウドセキュリティに関する10のベストプラクティス

1 会社の管理下にある／管理下にないアプリに対してクラウドサービスと連動した強力な個人認証システムとIDアクセス管理（SSO、MFAなど）を活用する。

2 ユーザー、アプリ、アプリの潜在リスク、インスタンス、デバイス、場所、データの機密性、送信先に基づいた適応型アクセス制御で、特定作業へのアクセスを選択的に許可したり、作業を開始する前にステップアップ認証を行う。

3 データセンターやパブリッククラウドサービスのプライベートアプリにZTNAを導入することで、アプリの公開を減らし、ネットワーク内でのデータ横移動を制限する。

4 パブリッククラウドサービスを継続的にセキュリティ評価することで、設定ミスや一般公開されているデータを検出する。さらに保存データをストレージスキャンすることでデータの保護と脅威を防御する。

5 会社の管理下にある／管理下にないクラウドアプリをインラインで分析し、データのコンテキストを把握するほか、ウェブトラフィックにセキュアなシングルパスのSASE（Secure Access Service Edge）アーキテクチャを取り入れることで、高速なユーザーエクスエクスペリエンスを提供しながらデータの保護と脅威からの防御を実現する。

6 アプリの包括的なリスク評価に基づく安全性の高いクラウドアプリを選択する。ユーザーに対するリアルタイムの指導や「続行／中止」アラートによるより安全な代替アプリの推奨機能を活用する。

7 アプリや企業・個人インスタンス、シャドーIT、ユーザー、Webサイト、デバイス、ロケーションなどを条件とした粒度の細かいポリシー制御でデータを保護する。

8 機密データを保護するクラウド型DLP（Data Loss Prevention：情報漏洩対策）を使用してWeb、メール、SaaS、シャドーIT、パブリッククラウドサービスへの内部／外部からの脅威を防ぐ。

9 振る舞い分析でデータの動きに対する異常、ログイン失敗、不自然なアクティビティを検出する。また、ユーザーの信頼度指数と実際の行動との相関関係を時系列で評価し、振る舞いの変化を可視化する。

10 高度な分析を行うことで、アプリやデータの動きに対するリスク、脅威アクティビティ、データ保護の違反、主要セキュリティ指標、調査結果を詳細に可視化する。

終わりに

この1年の間で、組織はビジネスを持続させる新たな方法を模索してきました。予想外の外的要因によってビジネス環境が大きく変わり、それに対応するためのアプリやビジネスプラクティスが迅速に導入されました。一方、データセキュリティチームは、企業ネットワークの外部に置かれたユーザー、アプリ、データの保護に対する理解を深めてきました。従来のネットワーク境界内での制御が通用しなくなった現在、企業が情報を保護し、リスクを最小限に抑えるセキュリティ原則の適用方法に大きな関心が寄せられています。

今年の調査では、在宅勤務が継続されているなかで危険なWebサイトの閲覧が前年より減少していることなど、現状について肯定的にとらえることができる要因が示されています。しかし、会社の管理下に置かれているクラウドアプリへのアクセスには、CCIで「非常に低い」と評価されたアプリのリスクを軽減する対策やデータ移動の制限を強化することが不可欠となるため、依然として大きな課題が残っています。

脅威の進化は止まることを知らず、今年の調査では、マルウェアが仕込まれたOffice文書の危険性がこれまで以上に高まっていることが判明しました。Office文書に仕込まれたマルウェアはエンドポイントでのシグネチャスキャンや持ち運び可能な実行ファイルのサンドボックスでの検知を回避することができます。文書の送信者になりすましユーザーの警戒心を解かせ攻撃を仕掛けることを考えると驚くべき調査結果ではありません。

組織の多くが基本的なアプリの可視化に取り組んでいる現状では、クラウドの構成（リモートアクセスの設定ミス、サードパーティアプリのエコシステムに潜むデータ共有におけるバックドアなど）は、頭の痛い課題となっています。組織内のアプリを把握している場合でも、セキュリティチームはアプリの動作を今まで以上に精査することで設定ミスの有無、下流でのデータ共有の可能性などを確認する必要があります。

オフィス勤務が本格的に再開する兆しは未だ見られませんが、ユーザーの振る舞いや、クラウドとWebサイトの利用における適切な制御に関する教訓は、オフィス勤務、在宅勤務、ハイブリッド勤務など、勤務形態に関わらず応用することができます。この1年の間に、組織はユーザーからアプリへのアクセスポリシーの適用にはネットワーク境界の保護だけでは不十分であるということを学びました。これは今に始まったことではありませんが、セキュリティのあり方が変わった現在、セキュリティモデルはネットワークの物理トポロジーに依存できません。今後は、Webやクラウド上にアップロードされた機密データの保護には、ゼロトラストの考え方に基づいた多層防御へと移行していくでしょう。

詳しくはこちら

クラウド脅威や、Netskopeの脅威対策に関する最新レポートの詳細は、
こちらをご覧ください。

NETSKOPE.COM/NETSKOPE-THREAT-LABS

リスク軽減に関する対策の詳細は、こちらにお問い合わせください。

WWW.NETSKOPE.COM/REQUEST-DEMO

提供:

netskope
THREAT LABS