クラウドファーストの浸透とサイバーレジリエンス

EYアドバイザリー・アンド・コンサルティング(株)　松下 直

▸ Naoshi Matsushita

2000年より大手SIerにて、サイバーセキュリティ事業のリーダーとしてマネージドセキュリティサービスの立ち上げ、国内外の先端的セキュリティベンダーとのアライアンス、海外でのセキュリティアセスメントなどを担当。18年より現職にて、国内外で日系企業に対してサイバーセキュリティにおける教育、現状調査、改善計画立案と対策推進を包括的に支援するコンサルテーションを担当。EYアドバイザリー・アンド・コンサルティング(株) Cybersecurity Co-Leader。

Ⅰ　クラウドファーストの浸透

新たなシステムを導入する際に、クラウドを第一の候補とする「クラウドファースト」という考え方が出てきて久しいですが、ようやく日本企業でもクラウドの活用が本格化してきています。メール、ドキュメント作成、顧客管理、ファイル共有、ウェブ会議などのSaaS（Software as a Service）の活用が進み、さらにオンプレミスで開発・維持管理してきたシステムのPaaS（Platform as a Service）／IaaS（Infrastructure as a Service）への移行が進んでいます。日本政府においても、今年から数年のうちにシステムを順次クラウドへ移行する方針が打ち出され、官民でクラウドの利用が加速しています。今後新たに導入されるシステムについては、クラウドの利用をデフォルトとする流れができつつあります。

Ⅱ　クラウド利用時のサイバーセキュリティ

クラウドの利用が活発になってくると、社内ドキュメント、顧客情報、メールといった機微な情報が、クラウドに格納されることになります。加えてラップトップPCやスマホといったモバイルデバイスを活用した在宅や社外でのリモート勤務の普及により、社外のネットワークからクラウドに格納された情報へのアクセスが増加します。企業のネットワークとインターネットとの境界をFirewallなどのセキュリティ機器で防御する従来のセキュリティ対策は、モバイルデバイスからクラウドへのアクセスにおいては機能しません。クラウド上のデータを守るためには、IaaS／PaaSの場合はクラウドベンダーの提供するセキュリティオプションからセキュリティ対策を実装する必要があります。一方、SaaSを利用する場合は、クラウド側のセキュリティ対策については、クラウドベンダー側で行われることが期待できます。（＜図1＞参照）

また、モバイルデバイス自身は設定の堅固化や、デバイスにインストールするセキュリティ製品である程度守ることができますが、クラウド利用時に怖いのが、アカウントの乗っ取りです。

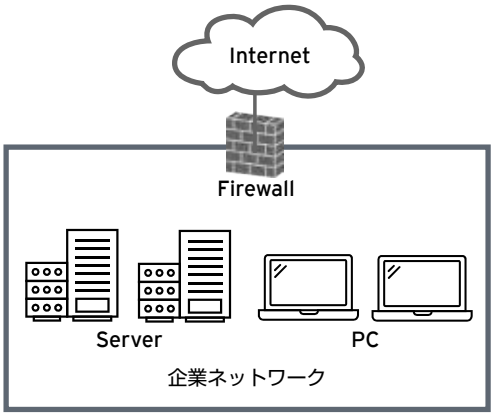
Ⅲ　新たな脅威

ユーザーを偽のログインサイトに誘導し、パスワードなどの認証情報を詐取してアカウントを乗っ取る攻撃は、情報漏えい、不正送金など甚大な被害をもたらしています。また、メールアカウントやSNSのアカウント乗っ取りは、攻撃者が正規のユーザーになりすますことで、さらなる被害に発展する恐れがあります。ユーザーの啓発や偽サイトの検出とTake Downなどの対策が講じられていますが、次々に新たな手口が出てきており、最近では攻撃者がパスワードを盗まずにアカウントを乗っ取る手口が、米国PHISHLABS社から報告されています※1。

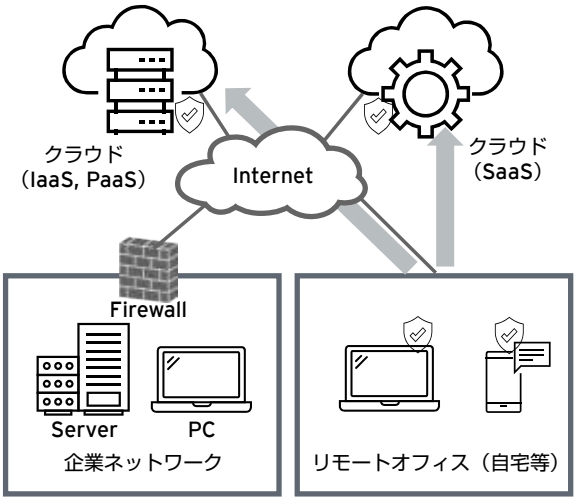
従来の手法では基本的に偽のログインページが表示

※1　info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset

▶図1　オンプレミス環境とクラウド・モバイル活用におけるセキュリティ対策



オンプレミス環境でのセキュリティ対策



クラウド・モバイルの活用時のセキュリティ対策

されますが、この手口では表示されるのは本物のログインページであり、認証に使われるAPIを悪用してアプリをインストールさせ、クラウドのアカウントへのアクセス権を詐取します。この攻撃の被害に遭うと、その後パスワードを変更したとしても攻撃者はアクセスを継続できるため、不正アクセスが長期化する恐れがあります。企業への攻撃を想定した場合、従業員がアクセス権の許可のダイアログボックスが不自然であることに気付けば被害を避けられますが、いかに従業員教育を徹底しても、このような新たな手法を用いた攻撃に遭う従業員をゼロにすることは無理でしょう。企業ではこのようなインシデントの発生確率を下げる従業員教育を継続する一方で、インシデントを少しでも早く検知し、被害を最小限に食い止めるための準備が求められます。

Ⅳ　SOCトランスフォーメーションによるサイバーレジリエンスの実現

インシデントを検知する監視体制であるSOC（Security Operation Center）は、企業に広く導入されています。自前の24時間稼働のSOCを有する日系企業はさほど多くはありませんが、多くの企業がベンダーとのコソースやアウトソースによりSOCを構築しています。EYが2019年に実施したグローバル情報セキュリティサーベイ※2によると、企業で過去一年間に発生したセキュリティ侵害のうち、SOCが検知した割合は26%と低い水準にとどまっています。この調査結果は、新しい攻撃手法に対して従来のSOCでは対応できていないことを示唆しており、前述のクラウドのアカウントの乗っ取りは、現段階ではSOCの監視対象にすらなっていない可能性があります。このケースでは、インシデントを発見するための方法の一つは、クラウドのアクセスパターンのアノマリ（通常と異なるアクセス）検知です。ユーザーのクラウドへのアクセス元の情報や利用時間帯、アクセスパターンなどを示すシステムログを解析することにより不自然なアクセスを検知する方法が考えられます。また、検知後一定の時間アクセスをブロックし、その間に本人に確認を求めることができれば被害を最低限に食い止めることができます。クラウドファーストが浸透し、企業の機密情報の保存場所が社内ネットワークからクラウドへと移っていく中、クラウドにおけるアカウントの乗っ取りは、企業における大きなリスクの一例です。このような深刻なインシデントの発生を想定し、早期発見・影響の極小化・早期復旧の手だてを事前に準備するサイバーレジリエンスの実現が、企業には求められています。クラウド活用という企業の攻めの戦略の一環として、SOCの対象を広げ、人手に依存していたインシデント分析を自動化し、またインシデント発生時の対応を機械化する次世代のSOCへのトランスフォーメーションを今こそ行うべきです。

※2　www.ey.com/ja_jp/giss