名和利男が説く「最新サイバーセキュリティ動向と経営者への提言」

脅威・脆弱性情報マンスリーレポート～2018年11月号～

pwc

世界中で発生しているサイバーインシデント（事件・事故）は、経営の根幹をゆるがす重大な脅威です。経営者は事故発生時に、組織横断的な観点で原因究明の指示や対応の判断が求められます。本レポートでは、サイバーセキュリティのスペシャリストである名和 利男が、世界中で起こるサイバーインシデント、犯罪傾向やプログラム不具合などのサイバー脅威を解説します。拡大するサイバー脅威に対し、事業継続に不可欠な脅威・脆弱性情報を経営者がどう読み解くべきか、サイバーインシデントへの備え方や対策方法を説明します。
10月は、サプライチェーンやICSネットワークを狙った攻撃など、ビジネスに悪影響を与えかねないサイバー攻撃による被害が目立ちました。以下、主なインシデントの解説とその対策方法を紹介します。

2018年10月の注目のサイバーインシデント（事件・事故）

- 2018年10月４日　［脅威情報］ NCCIC、APTキャンペーンでMSP（マネージド・サービス・プロバイダー）に注意喚起
- 2018年10月５日　［関連情報］ ハッカーが窃取した仮想通貨額は9億ドル以上 – 2018年3四半期合計
- 2018年10月23日　［関連情報］ 攻撃者にとってICSネットワークは恰好の餌食

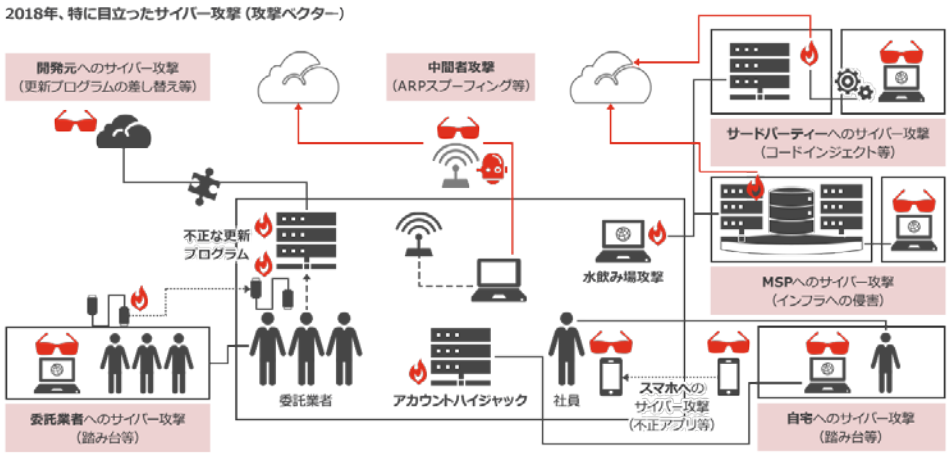
注目インシデントの解説と提言

脅威情報　NCCIC、APTキャンペーンでMSP（マネージド・サービス・プロバイダー）に注意喚起

米国のNCCIC（全米サイバーセキュリティ・通信統合センター）から、「MSP（マネージド・サービス・プロバイダー）に対するAPT攻撃（持続的標的型攻撃）が増加している」という注意喚起が出されました。MSPへの攻撃が増加している背景には、MSPを利用している企業の顧客情報や機密情報を一遍に窃取できるため、攻撃者にとって効率の良いターゲットとして狙われているという点があります。

提言

MSPを利用する企業にとって、自社のIT技術者を必要とせずにITシステムを運用・管理できるのは大きな利点です。しかし、インシデント発生時には、自社の技術者が直接対応に当たることができずにMSPの対応力に左右される事態となることも考えられます。1秒でも早い復旧に向けてあらゆる対応を講じている中で、MSPなどの外部要因による遅延は何としても回避する必要があります。そのためには自社だけにとどまらず、関連企業の対応も考慮したサイバーセキュリティ体制の構築、見直しが求められます。10月号でも「外部調達によるサプライチェーンに起因するリスクの検討が必要」と述べましたが、他社にサービス提供を受けている領域におけるリスクも考慮すべきです。



図：企業を取り巻くサイバー脅威の現状。さまざまな手法で企業システムへの攻撃が行われている。サプライチェーンなど、攻撃や侵入ルートが多様化しており、セキュリティ担当者にはより強固な防御策の検討が求められている。

関連情報 ハッカーが窃取した仮想通貨額は9億ドル以上 - 2018年3四半期合計

攻撃者は仮想通貨を恰好のターゲットとみなしており、不正な取引やマイニング（コンピュータの計算処理により仮想通貨を作り出す採掘作業）による仮想通貨の窃取が急増しています。その手段の一つとして、仮想通貨の不正アプリが挙げられます。不正アプリがインストールされている携帯端末において、盗んだ秘密鍵を悪用した不正送金や処理能力を不当に利用した採掘が発生しており、不正アプリ経由で企業のネットワークに侵入する攻撃も起きています。

提言

仮想通貨の窃取を目的としたサイバー攻撃の急増は、不正アプリの拡散を引き起こす可能性があります。仮想通貨に限らず、不正アプリが入っている端末が社内に持ち込まれ、社内ネットワークに侵入されると、情報漏洩やシステム停止などのインシデントが発生する危険性があります。トラブルやインシデントを引き起こさないためには、10月号でもお伝えしたとおり、業務における個人端末への対策強化が必要です。社内に持ち込まれる個人端末のセキュリティ対策や不正なアプリを利用させないためのコンプライアンス強化など、従業員に対してセキュリティを強化する取り組みや教育の推進が重要です。

関連情報 攻撃者にとってICSネットワークは恰好の餌食

ICSネットワーク（産業用制御ネットワーク：産業用機器やシステムを制御・連携するネットワーク）を狙った攻撃が増えています。ICSネットワークは製造業においてビジネスの骨幹となる重要なシステムです。障害が発生すると企業経営に大きな影響を及ぼすため、攻撃者のターゲットになりやすいといえます。インターネットや社内システムにつながっていない独自システムはサイバー攻撃の心配はない、という誤った認識のもと、十分なセキュリティ対策を取っていない企業も見受けられます。実際には、生産管理システムとの連携やUSBなどの外部端末との接続といった、外部からの侵入リスクが存在しています。対策を講じてないシステムが攻撃者から狙われ、ビジネスが停止するような重大な被害が発生する懸念があります。

提言

近い将来、日本政府が提唱するテクノロジーを活用した社会の仕組み「Society 5.0」が実現すると、人とモノがつながり、さまざまな知識や情報が共有される時代が到来します。そうなると、ICSネットワークは、社会を支える基盤として重要な役割を果たすことになります。また一方で、少子高齢化に伴う労働人口の減少や規制緩和に伴う競争の激化とコストダウン圧力に対する解決策として、ITの利活用を推進する必要があります。結果として、ITとICSネットワークの連携はさらに加速し、サイバー攻撃のターゲット範囲の拡大にもつながるため、情報システム同様にICSネットワークの万全な防御対策が必須となります。

名和 利男の知見から読み解く、サイバー攻撃の着眼点

10月に入り、報告される脅威情報の量が飛躍的に増えています。中でもMSPや業務委託・協力会社などのサプライチェーンを狙った攻撃が特に増加傾向にあります。たとえ自社の防御を強固にしても、自社ビジネスにつながるサプライチェーンがサイバー攻撃を受け、自社にまで被害や影響を及ぼすことがあり得るのです。経営者は、自社のシステムのみならず、サプライチェーンも含めたセキュリティ対策や、インシデント発生後に求められる対処プロセスの整備状況などを関係部署へ確認してください。もし不足があれば、速やかに対策するよう指示を出してください。

お問い合わせ

PwCサイバーサービス合同会社
〒100-0004　東京都千代田区大手町1-1-1　大手町パークビルディング
E-mail : JP_Cons_pcs.info@pwc.com