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7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。

6月に発生したサイバーインシデントを分析すると、これまで以上に多様な攻撃手法が使われていたことがわかりました。ネットワーク機器やウイルス対策ソフトの脆弱性をターゲットにした攻撃など、従来よりもシステムの深い部分を狙った攻撃が増加しており、これから留意すべき重要な事案になるかもしれません。以下に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6月の注目のサイバーインシデント（事件・事故）

- 2018年6月7日　［脅威情報］「VPNFilter」 が多数の製品を侵害、セキュリティ企業が詳報公開、他2件
- 2018年6月11日　［脆弱性情報］ ウイルス対策ソフトに複数の脆弱性、他1件
- 2018年6月26日　［脅威情報］ 米自治体収納代行サービスへの不正アクセス、他1件

注目インシデントの解説と提言

脅威情報　「VPNFilter」が多数の製品を侵害、セキュリティ企業が詳報公開、他2件

過去に発生したサイバー攻撃は、アプリケーションやデータをターゲットにした攻撃が主でした。今月はルータなどのネットワーク機器をターゲットとしたマルウェア「VPNFilter」が世界中で猛威を振るい、数十万台のネットワーク機器が感染したと報道されました。このマルウェアに感染するとネットワークの利用ができなくなり、サイバー攻撃の踏み台にされる可能性があります。日本でも感染する危険性が高まっています。

提言

今回の攻撃は、通信機能を階層構造にしたOSI参照モデルにおける、最上位のアプリケーション層より下位の層を狙った新たな手法が用いられています。これまでは構成図上の端末や機器を平面で捉えていましたが、階層構造を意識した立体的な視野からのセキュリティ対策を迫られることになります。日々サイバー脅威の動向に注意しつつ、既存の対策で守れないようなサイバー攻撃を見極め、CSIRTとも連携しながら今後のセキュリティ対策を講じることが重要です。

脆弱性情報　ウイルス対策ソフトに複数の脆弱性、他1件

「ウイルス対策ソフトなどのセキュリティ対策ソフトウェア利用したサイバー攻撃が常態化している」という調査レポートをセキュリティベンダーが公開しました。この攻撃を調べてみると、セキュリティ製品やログ解析ソフトウェアの脆弱性が狙われていたことが判明しました。本来、セキュリティ強化を目的として導入しているソフトウェアがサイバー攻撃にさらされるという、非常に深刻な事態に陥っています。

提言

どのようなソフトウェアであっても、新しい攻撃の対象になる脆弱性が発見されるなど、時間の経過とともに不安定になる可能性は否定できません。正規に販売されているソフトウェアだから安全だと断定することなく、サイバー攻撃の対象となっていないか警戒する仕組みを講じる必要があります。さらに、外部の事業者が作った業務ソフトウェアやサービスを導入する際は、調達先のセキュリティ対策を把握することが重要です。もしセキュリティ対策が自社の要求を満たさない場合、セキュリティ対策の改善あるいは調達先の変更を検討する必要があります。

脅威情報　米自治体収納代行サービスへの不正アクセス、他1件

不正アクセスによって海外で運営されるクラウドサービスから個人情報が漏洩するインシデントが複数件発生しました。当該サービスを利用していた日本企業は、被害状況確認などの対応に追われています。この事案は、サプライチェーンの一部から情報が流出したインシデントです。ほかにも、サプライチェーンを構成する業務委託先やサービス事業者などが狙われる事件が立て続けに発生しています。

提言

今回のインシデントは、サプライチェーンのリスクマネジメントについて、どのように取り組んでいくべきかを考えさせられる事案です。業務の委託などを行う際には、委託先からの情報漏洩も想定し、両社で連携したセキュリティ対策を取っていくことが求められます。委託先におけるセキュリティ強化は、追加の設備投資や人材確保が必要となり、コストも上昇します。日本では、委託先にセキュリティ強化を要求し、その対策コストの負担までも強いることが少なからずあるようです。サプライチェーン全体のセキュリティ強化を視野に入れ、コスト負担も含めた連携を検討する必要があります。

名和 利男の知見から読み解く、サイバー攻撃の着眼点

サイバー攻撃のトレンドが多岐にわたるようになってきたという印象を受けた6月でした。来月は、より多様な攻撃によるインシデントが発生するかもしれません。情報収集で事前に脅威の動向を察知し、新しいサイバー攻撃が登場しても慌てずに対応できる体制の構築を進めてください。

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