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1月号～

pwc

経営判断を行うために、なぜ脅威・脆弱性情報が必要なのか。サイバー脅威インテリジェンスのスペシャリストとして活躍する名和 利男が、サイバー脅威の動向や注目すべき情報の読み解き方を解説。事業継続に不可欠なサイバー攻撃に備えた対策方法や、今後のサイバーインシデントの動向を説明します。

2017年12月の注目のサイバーインシデント(事件・事故)

- 2017年12月 4日　[関連情報] ランサムウェア被害の英NHS、セキュリティ機能強化に約30億円
- 2017年12月13日　[脅威情報] 96時間以内の支払いを求めるランサムウェア「Spider」欧州で拡散
- 2017年12月19日　[脅威情報] 「TelegramRAT」不正プログラムの不可視化進む
- 2017年12月26日　[関連情報] 「Fancy Bear」がジャーナリスト200名にサイバー攻撃

名和利男による、最新サイバーセキュリティ動向の解説と、日本企業への提言

各国と日本のサイバーセキュリティ対策の違いを象徴するインシデントがありました。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。

関連情報　ランサムウェア被害の英NHS、セキュリティ機能強化に約30億円

イギリスの国民保健サービス(NHS)が、セキュリティ対策に日本円でおよそ30億円相当の投資を行ったことが報じられました。この報道から、欧米各国のサイバーセキュリティに対する姿勢を読み解くことができます。PwCが毎年世界中の経営層を対象に実施しているグローバル情報セキュリティ調査2017によると、情報セキュリティ予算の平均額がグローバルで5百万ドルを計上しているのに対して、日本はその3分の2にあたる3.4百万ドルとなっています。日本のサイバーセキュリティへの投資が依然として消極的であることがわかります。

日本企業への提言

NHSが投資した30億円を、非常に大きな金額だと捉えた方も多いでしょう。しかし、過去に国内で発生した情報セキュリティインシデントによる個人情報漏洩事件では、NHSの投資額以上の事故対応費用が必要となったケースもあります。事故発生後に多額の費用が発生するケースも鑑み、事前対策として投資することを積極的に検討すべきでしょう。

脅威情報　96時間以内の支払いを求めるランサムウェア「Spider」、欧州で拡散

「Spider」はボスニアをターゲットとしたものです。件名や添付文書がターゲットの地域文化に合うように改修した「ご当地型」ランサムウェアが活発になっています。昨年、日本をターゲットとした標的型攻撃を行う「ONI」というランサムウェアも日本国内で発見されています。

日本企業への提言

海外で発生している「ご当地型」のサイバー攻撃が始まっている状況を把握し、自社の対応を行う必要があります。海外で発生したサイバー攻撃を「関係ない」と切り捨てるのではなく、国内での展開を想定してセキュリティ対策に取り組むことが重要です。あわせて、新種のマルウェア攻撃にも対応可能なサービスやプロダクトの導入も検討すべきです。

脅威情報 「TelegramRAT」不正プログラムの不可視化進む

Telegramは、海外の企業がサービス提供をしているインスタントメッセージシステムです。Telegramは通信内容が暗号化されているため、サイバー攻撃に利用されることがあります。2015年12月下旬に発生したウクライナの電力供給会社に対するサイバー攻撃ではTelegramが攻撃サーバへの指示ツールとして使われました。Telegramは送ったメッセージを送信者側から消去できるため、攻撃指示の記録を抹消することができます。

日本企業への提言

日本でも、通信内容の暗号化や、送信後にメッセージ消去可能な機能を持ったSNSやメッセージアプリがあります。遠くない将来、それらのアプリを使って、「TelegramRAT」のような不正プログラムが作られる危険性を認識する必要があります。サイバー攻撃により管理者権限を取られると、遠隔操作ツールにより、すべての組織は丸裸にされたのと同様となり、情報漏洩被害や事業継続へのマイナスの影響が発生することが懸念されます。

関連情報 「Fancy Bear」がジャーナリスト200名にサイバー攻撃

国際的なイベントやサミットなどの大規模イベントは、サイバー攻撃の対象として狙われる傾向にあります。まもなく韓国で国際的なイベントが開催されます。「『Fancy Bear』がジャーナリスト200名にサイバー攻撃」というニュースは、イベントと関係するサイバー攻撃だと推測されます。ジャーナリストに不確かな情報を発信することで、真実と違う報道が広がり、誤った情報により世論が動かされることも懸念されます。「Fancy Bear」は、サイバー攻撃を行う集団です。彼らは、主催者がドーピングを実施したとされる国を排除したことに対するリベンジを行ったと見ています。

日本企業への提言

日本で開催する国際イベントの広報活動を行う企業は、サイバー攻撃に対して最大の関心を払う必要があります。海外の紛争に起因するサイバー攻撃の情報を把握し、同様の被害にあわないためにセキュリティ対策を講じるとともに、被害を未然に防ぐ準備が必要です。

名和 利男の知見から読み解く、サイバー攻撃の着眼点

経営層の皆さんにおいては、サイバー攻撃対策は情報システム部門や事故対策チームへお願いする仕事という認識ではありませんか。事業基盤をITが支えている現在では、サイバー事故への備えや有事の対応は経営責任です。システム部門への舵取りは船長である経営層と、現場との連携が必要な時代になったのです。インターネットで地球が物理的に小さくなった現在、海外で発生したサイバー攻撃は対岸の火事ではありません。従来は日本語という言語の壁があり、英語圏でのサイバー攻撃が日本で見つかるまで時間がかかりましたが、現在はその時間差も無くなりました。海外で大きな影響を与えているご当地型ランサムウェアやメッセージ消去可能なSNSが、日本国内でサイバー攻撃を展開することを想定し、事前にセキュリティ対策を講じることが重要です。

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