名和利男が説く「最新サイバーセキュリティ動向と日本企業への提言」

脅威・脆弱性情報マンスリーレポート～2018年2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。経営層は事故発生時に、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等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・脆弱性情報を経営層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。

1月は、開催間近である大規模な国際イベントへのサイバー攻撃やインシデントが発生しました。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。

2018年1月の注目のサイバーインシデント（事件・事故）

- 2018年1月9日　[脅威情報]　韓国開催の国際イベントに乗じたスピアフィッシング、実在の施策に乗じる
- 2018年1月18日　[関連情報]　国家によるサイバー攻撃の脅威、多様化も高水準続く
- 2018年1月22日　[脆弱性情報]　ネットワーク製品のファームウェアに脆弱性

注目インシデントの解説と提言

脅威情報　韓国開催の国際イベントに乗じたスピアフィッシング、実在の施策に乗じる

米セキュリティ企業McAfeeによると、特定のターゲットから重要なデータや個人情報を奪うサイバー攻撃、「スピアフィッシング（フィッシング詐欺）」が発生しました。今回は、韓国で開催される国際イベントの関係者が狙われました。韓国のテロリズム対策機関を騙るメールに不正なWordファイルが添付されており、起動した端末上で任意のコマンドが実行されます。過去、大規模な国際イベントや国際会議などでは、政治的な背景でサイバー攻撃が行われ、イベント運営に関係する組織のみならず、スポンサー企業なども標的とされています。

日本企業への提言

この攻撃は、韓国開催の国際イベントという時宜的な話題に乗じ、テロ対策を偽る形で受信者を欺く手法が用いられています。サイバー攻撃の被害を受けた組織が糾弾される風潮の中、大規模イベントに関連した攻撃の標的となった組織は、世界的な報道も相まって、ブランド価値の毀損など甚大なダメージを受けかねません。事前の対策や迅速な復旧が不可欠となりますが、単一のインシデントだけを近視眼的にとらえると、その背後にある動機や攻撃者を把握できず、的外れな対応に終始する可能性すらあります。今回のケースは、大規模な国際イベントに乗じた単なるスピアフィッシングとしてとらえるのではなく、遡及的な分析により攻撃の背景を理解することで、自社への影響を判断し適切な指示を下す必要があります。そのためには、経営層がサイバーセキュリティの動向に目を光らせる環境整備が重要です。

関連情報 国家によるサイバー攻撃の脅威、多様化も高水準続く

一昨年から大国を狙った国家規模のサイバー攻撃が報じられましたが、従来とは異なる国家の仕掛ける攻撃が増えている様子がうかがえます。地政学的要因により、昔から対立が激しい国家間に加え、近年の国際情勢下で新たな対立が顕在化した国家同士が、実際の紛争だけではなくサイバー空間でも衝突を繰り返しているためです。サイバー攻撃の対象は、国や政府が利用しているITインフラであり、そのシステム構築・運用に多くの民間企業が関与しています。つまり、国家間のサイバー攻撃を関係ないものとして傍観することはできず、民間企業も国家レベルの高度かつ大規模な攻撃を受ける可能性が高まっています。

日本企業への提言

国家レベルのサイバー攻撃を受けた場合、一企業での対処は困難を極めます。とはいえ対策の難易度に関わらず、ひとたび損失が生じれば企業は非難を浴び、責任を追及される傾向にあります。国家間のサイバー攻撃にも巻き込まれる可能性を想定し、独自の対策強化にとどまることなく、企業間の情報共有を活発化し、さらには行政機関や国を守る機関との連携強化を推進する必要があります。

脆弱性情報 ネットワーク機器のファームウェアに脆弱性

ネットワーク機器の集積回路に組み込まれたプログラム「ファームウェア」において、管理者権限を奪取できる脆弱性が報告されました。最近では、CPUの最適化処理の脆弱性を突きメモリ領域を読み取れる問題も報告されており、ハードウェアレベルでのリスクが顕在化しつつあります。ある国では、政府機関で導入する電子機器は、特定の国で製造されたものを採用しないと発表しています。今後は、電子製品の調達にも、事前にサイバーセキュリティ上の不具合がある製品ではないかに注意を払わなくてはいけないことを意味します。

日本企業への提言

製造業に強みを持つ日本にとって、影響が大きいニュースです。従来、情報セキュリティ対策は、情報資産やアプリケーションを中心に重要性が唱えられていました。IoT機器が拡大する現在、電子機器もセキュリティ対策の一環として考慮されるべきであり、安全性を見極めた上で調達することが求められます。この問題の大きさは、政府が進める次世代サプライチェーンのリスクマネジメントや、調達におけるセキュリティ確保・安全性の確保、総務省のIoTのサイバーセキュリティ戦略などにおいて、その取り組みが進められていることからも確認できます。

名和 利男の知見から読み解く、サイバー攻撃の着眼点

国家レベルのサイバー攻撃は、何らかの意思を持って行われています。大規模なイベントの開催とともに、国家レベルでのサイバー攻撃などに関する話題が増えてきた印象です。2020年には日本でも国際イベントを控えており、海外の事例を他山の石として、サイバー攻撃に対する警戒レベルを上げる必要があります。攻撃者は、ハードウェアの脆弱性を悪用するなど、常に新しい攻撃の糸口を探っています。対策する側も、俯瞰的にその動向を追い続け、柔軟な判断を下すことが必要とされています。

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