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3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。
2月は、韓国で開催された国際的なイベントに便乗したサイバー攻撃やインシデントにくわえ、金融をターゲットにした攻撃が発生しました。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2月の注目のサイバーインシデント(事件・事故)

- 2018年2月9日　[脅威情報] 電子カルテのサーバに仮想通貨採掘プログラム 米テネシー州
- 2018年2月14日　[脅威情報] 産業技術総合研究所で不正アクセス被害
- 2018年2月20日　[脅威情報] SWIFTシステムへサイバー攻撃 インドの金融機関で
- 2018年2月26日　[脅威情報] 国際イベント関連サイトとの誤認もくろむドメイン名多数

注目インシデントの解説と提言

脅威情報 電子カルテのサーバに仮想通貨採掘プログラム 米テネシー州

仮想通貨の採掘(マイニング)プログラムを動作させるために、米国の電子カルテを保存するクラウドサーバへの不正アクセスが起きました。攻撃者にとって、対象となるサーバがどこに設置されているかは問題ではなく、攻撃可能かどうかが重要となります。今回は、セキュリティ対策が十分でないクラウドサーバが狙われました。

提言

クラウドサービス利用の抵抗感が薄れて急激に普及が進む中、攻撃者の目がクラウドサービスへも向けられています。サイバー攻撃で情報が流出すると、本来被害者であるにもかかわらず、企業は管理責任を問われます。企業の利用環境が社内だけではなくクラウドへも分散するにつれて、責任範囲が拡張されることになります。総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」、経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン改訂版」、「クラウドセキュリティガイドライン活用ガイドブック」などを指針とし、クラウドも含めて広い視野でセキュリティ強化を実施することが求められています。

脅威情報 産業技術総合研究所で不正アクセス被害

日本は「知的財産が豊富」と言われています。知的財産を巡って、国や企業は熾烈な開発競争を繰り広げており、時にはその情報を盗み取ろうとする行為も発生しています。サイバー攻撃の目的は、直接的な金銭窃取だけにとどまらず、企業の知的財産や機密情報などの売買や盗用にまでおよんでいるのです。

提言

企業の知的財産や産業情報を狙った攻撃の増加にともない、現場担当者は大小さまざまなサイバー事件・事故の処理や対応に忙殺されます。現場担当者が攻撃検知や対応時に知りえたサイバー攻撃の狙いや手法は、今後の対応や対策検討に有用ですが、経営者が求める内容ではないため報告されることは稀です。そもそも経営者はすべての詳細情報を把握する必要はありません。経営者には有事の際に適切な経営判断を下すための材料として、サイバー攻撃の動向を把握しておくことが重要なのです。

脅威情報 SWIFTシステムへサイバー攻撃　インドの金融機関で

SWIFT（金融メッセージ通信サービス）は、全世界で利用されている金融取引システムです。銀行間の安全な国際取引を支えるために、非常に強固なセキュリティを備えていると言われています。それにもかかわらず、スピアフィッシング（フィッシング詐欺）により、SWIFT操作端末側で不正操作された事件が発生したのです。これまでも同じ手法で攻撃された被害が発生していますが、今回の攻撃では過去の教訓が生かされませんでした。

提言

堅牢なセキュリティを実装したシステムであっても、攻撃者は脆弱な点を探し出し攻撃を仕掛けてきます。例えば、その脆弱な点が運用する“人“であったとしてもです。サイバーセキュリティ態勢を講じるには、人、技術、プロセスすべてを網羅的に整備する必要があります。経営者はセキュリティ投資を進める際、セキュリティ製品やサービスの導入と並行して、運用する人に対するセキュリティ啓発や教育など、意識向上のプログラムや制度を充実させてください。

脅威情報 国際イベント関連サイトとの誤認もくろむドメイン名多数

ホモグラフ攻撃という、見た目が類似した文字列（例えば数字の0（ゼロ）と英小文字のo（オー））を用いた偽装サイトへ誘導する攻撃が多数発生しました。大規模な国際イベントの時期には、関係する名称を偽装したドメインへ誘導するホモグラフ攻撃が多く発生します。偽装サイトにアクセスすると、個人情報の漏えいやマルウェアに感染するといった、サイバー被害に遭う懸念があるので注意が必要です。

提言

アクセスしたサイトが正しく安全なものか、「デジタル証明書（サイトの身元を保証する証明データ）」により確認できます。ウェブブラウザでアクセスすると、画面に鍵のマークや「保護された通信」といったメッセージが表示されます。米国では、ほとんどの役所や大手企業がデジタル証明書を利用しています。しかし日本では、デジタル証明書を利用していない、政府機関や省庁のサイトが数多くあります。来年以降、G20首脳会議をはじめ国際的なイベントが、日本で多数開催されます。この時期は日本の企業も世界から注目されます。経営者は、自社のサイトがデジタル証明書を利用していない場合はデジタル証明書を取得するよう指示してください。

名和 利男の知見から読み解く、サイバー攻撃の着眼点

2月は、米国で源泉徴収票データ等を要求するフィッシングメールを使ったサイバー攻撃が発生しました。3月は年度末の企業も多く、決算や確定申告などの経理的な処理が多い時期です。この時に気を付けてほしいのが、不正振り込みを誘導するビジネスメール詐欺です。日本語では怪しいとわかっても、英語だとわからずに処理してしまう可能性もあります。攻撃者は業務内容を把握し、攻撃が成功しやすい文章を使って攻撃してきます。金銭目的のサイバー事例が発生していることを念頭において、多忙な時期だからこそセキュリティに対する意識を高めてください。

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