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9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。

8月は不正アクセスやサーバー設定ミスによる大規模な漏洩、個人情報の取得を目的とした攻撃などが発生しました。漏洩する情報は1件あたりのデータ流出数も多くなっており、被害発生時に企業が受けるダメージは深刻です。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8月の注目のサイバーインシデント（事件・事故）

- 2018年8月8日　［脅威情報］ 教育機関へのスピアフィッシングメールで認証情報収集
- 2018年8月10日　［脅威情報］ クラウドの設定情報等が誤公開　AWS S3の誤設定で
- 2018年8月13日　［脅威情報］ モバイルPOS端末に決済額改ざんなど可能となる問題

注目インシデントの解説と提言

脅威情報　教育機関へのスピアフィッシングメールで認証情報収集

大学などの教育機関を狙ったサイバー攻撃が増加しています。その背景として、産学連携が活性化し、教育機関側が企業の情報を保有しているためと考えられます。攻撃者は、これらの情報を窃取するために、企業ほどセキュリティ対策が強固ではない教育機関への攻撃を意図したものだと推測されます。さらには、教育機関が保有している在校生・卒業生・教職員などの個人情報が狙われています。窃取した個人情報には組織の重要人物あるいはその同級生などが含まれており、プライベート情報を外部に晒すことで行動・能力・機能を低下させる「Doxing（ドクシング）」という攻撃で直接あるいは間接的に悪用される懸念があります。

提言

ビジネスパートナーを含む、多くの関係者がサプライチェーンでつながる状況下において、自社だけセキュリティを強化しても十分ではありません。協力先や子会社・関連企業から情報が洩れる可能性を考慮し、サプライチェーン全体においてセキュリティ強化を図る必要があります。同様に、教育機関と共同で研究やビジネスを行う際には、サプライチェーンにおいて要求するセキュリティ体制と同レベルのものを教育機関と構築するなど、情報流出を防ぎ、早期発見する取り組みが重要となります。

脅威情報　クラウドのサーバー設定情報等が誤公開　AWS S3の誤設定で

クラウドサービス提供者側の誤設定により、サーバー設定情報が第三者でもアクセスできる状態になっていました。そのため、サーバーに保管されていたデータが外部に多数流出するインシデントが発生しました。流出した情報の中には、サービス契約者情報や宿泊客情報、会員のメールアドレス情報など、重要な情報が多数含まれていました。一件あたりの情報流出規模も増加しており、データ流出の防止策を進めることが急務です。

提言

攻撃手法がますます巧妙化し、データ流出経路も多様化したことから、サイバー攻撃を受けるリスクは増加しています。自社のセキュリティ体制が万全でも、委託先の管理・運用時のミスで情報流出が発生することを考慮した対策が求められます。委託先が原因となる情報流出を防止するためのリスクアセスメントを進め、委託先と協力した万全なセキュリティ対策を講じる必要があります。

脅威情報 モバイルPOS端末に決済額改ざんなど可能となる問題

近年、高額な専用POSシステムに代わり、市販のモバイル端末に専用アプリをインストールしたPOSシステムの導入が進んでいます。個人用や業務用のスマートフォンやタブレットが普及するにつれ、モバイル端末へのサイバー攻撃やセキュリティ問題が多数発生しています。たとえば、不正アプリのインストールなど、不備のある端末が重要な施設内に持ち込まれた際に、盗聴や録画で重要な情報が盗み出される危険があります。業務端末のセキュリティ対策は当然ながら、社内に持ち込まれる個人所有のモバイル端末に対する管理・対策も急務になっています。

提言

会社から貸与しているモバイル端末だけではなく、個人の所有物を社内に持ち込んでいるケースが多数あります。管理外のモバイル端末が社内に存在することで、そこから情報が洩れる危険性があることを認識する必要があります。5月号でも「業務で利用しているスマートフォンやタブレットは、PCと同等のセキュリティ管理を行うことが重要」であることをご紹介しています。これまでのセキュリティ対策は、主に社内PCやサーバーからの情報漏洩を抑止するものが中心でした。今後は、持ち込まれるモバイル端末に対するセキュリティ管理も、情報流出を防ぐ取り組みのひとつとして推進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

8月のサイバー攻撃の傾向を見ると、データ流出・漏洩が増加しています。流出原因はPCやサーバーへの攻撃だけではなく、モバイル端末やクラウドサービスへの攻撃など多様化しています。自社だけで外部からの攻撃を防ぐだけではなく、あらゆるところにリスクが存在していることを認識し、対策を進めることが重要です。

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