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6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。

5月に発生したサイバーインシデントのキーワードは、「パスワード」です。 パスワードの使い回しを悪用した不正侵入の可能性や、パスワード設定が不十分な機器が乗っ取られる可能性が報じられています。他にも大規模なイベントに乗じたサイバー攻撃や情報漏洩が発生しています。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5月の注目のサイバーインシデント（事件・事故）

- 2018年5月2日　［脅威情報］ 認証情報の漏えい発覚後はアカウント乗っ取り試行が3倍に、他4件
- 2018年5月7日　［脅威情報］ GDPR関連の連絡を装ったフィッシング、他6件
- 2018年5月25日　［関連情報］ パスワード使い回しは依然多数派との調査結果、他2件

注目インシデントの解説と提言

脅威情報　認証情報の漏えい発覚後はアカウント乗っ取り試行が3倍に、他4件

個人データだけではなく、クレジットカード情報の流出も発生しました。クレジットカード情報と個人データを組み合わせ、金銭の窃取を狙った攻撃が起きています。他にも個人データや認証情報の漏洩に関する報道が多くあることから、漏洩した情報を悪用した不正アクセスやアカウント乗っ取りの発生が推察されます。

提言

金融機関では情報流出を防ぐ対策が進んでいるものの、依然として重要な情報の流出が報じられています。サイバー攻撃が多様化していることもあり、最適なセキュリティ対策・改善がうまく進んでいない企業もあるようです。 あるいは、これまでとは異なる手法が使われ始めており、従来のセキュリティ対策では対処できていない可能性があります。自社から重要な情報を漏えいして被害者にならないために、脅威情報の動向を把握し、常に最善なセキュリティ対策を講じるほか、社員に向けたセキュリティ教育などを進めてください。

脅威情報　GDPR関連の連絡を装ったフィッシング、他6件

5月25日にGDPR（EU一般データ保護規則）という、企業の情報セキュリティ関係者に影響が及ぶ法律が施行され、世界中の企業が対応に追われました。それに乗じたスピアフィッシング（特定のターゲットから情報を奪おうとするサイバー攻撃）が発生しています。他にも5月にはイベントや事件に関するスピアフィッシングによるサイバーインシデントが起きており、国内外で注意喚起が出されています。イベントが開催されたり、何らかの事件が発生すると、そのことに関心が集まります。そのため、関連したタイトルの付けられた偽装メールなどによるサイバー攻撃の危険性が高まります。

提言

2019年から2020年にかけて、日本では国際的にも関心の高いイベントがいくつも開催されます。このようなイベントとの関係を装った、不正プログラムが添付されたメールや悪質なウェブサイトを利用したサイバー攻撃の発生が懸念されます。特に、自社の業務に関連づけられると、誤って添付ファイルを開封したりウェブサイトへアクセスしたりして、マルウェアに感染してしまう可能性があります。セキュリティ担当者は、イベントがある時期には関連するサイバー攻撃が発生するということについてさらなる注意を社内に促してください。

関連情報 パスワード使い回しは依然多数派との調査結果、他2件

バージニア工科大学が実施した調査では、複数のオンラインサービスに同一のパスワードを使用するユーザーが半数以上との調査結果が発表されました。サービスの性質による分類では、金融サービスやメールサービスなど、機微な情報を扱いうるアカウントにおいてパスワードの使いまわしが多くみられる傾向が見られました。
その他にも5月は「パスワード」に関係するニュースが報じられています。標的型ランサムウェア「SamSam」が企業ネットワーク内の脆弱性を悪用して拡散を進めていることがわかりました。具体的には、RDP（Remote Desktop Protocol）のパスワードを破るブルートフォース攻撃（暗号やパスワードを解読する攻撃手法の一つ。総当たり攻撃とも言う）やID盗難にあった認証情報の流用によりシステムの侵害を試み、感染先の拡大を図ります。
別のニュースでは、ある電機通信事業者が提供するWi-Fiギガビットルーターの設定に不備があり、インターネットで確認できるポートが開放状態の端末が多数存在すると指摘されています。ポートが開放状態になっており、さらにパスワードによるログインが無効化されていたため、「高度な設定」画面へアクセスできれば、第三者がルーター管理用の認証情報を設定することが可能となります。

提言

従業員が利用しているパスワードの管理が適切かどうかを確認してください。あわせて、パスワードの使い回しをさせないなど、パスワード管理を厳格にするための教育やツールの導入を図ることを検討すべきでしょう。パスワードの管理が不十分だと、不正ログインや機器の不正利用を受けて情報流失やシステムの乗っ取りなどの被害に遭う可能性があります。そこから事業継続を脅かすようなインシデントが発生しかねません。パスワード管理の厳格化と共に、不正ログインを防ぐための仕組みづくりを関係部署に提案してください。

名和 利男の知見から読み解く、サイバー攻撃の着眼点

海外では長期休暇シーズンを迎えることもあり、軽微な社内ルール違反を見逃すこともあるようです。しかし忙しいからといってルール違反を許してしまうと、そこが重大な情報漏洩やサイバー攻撃の原因になりかねません。忙しい時期だからこそ、サイバーセキュリティに関するルール運用を厳格に行うことの重要性を周知徹底してください。

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