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5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。
4月は、メールアドレスを窃取するインシデントが多数発生しました。他にもスマートフォンや制御システムの脆弱性が報じられました。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4月の注目のサイバーインシデント(事件・事故)

- 2018年4月4日　[脅威情報] 政府機関メールアドレス流出報道で官房長官がコメント、他7件
- 2018年4月16日　[脅威情報] Android端末へのパッチ配布、一部で適用見送りも 研究者指摘、他1件
- 2018年4月19日　[脆弱性情報] HMI/SCADAシステム製品InduSoft Web Studio等に深刻な脆弱性、他1件

注目インシデントの解説と提言

脅威情報 政府機関メールアドレス流出報道で官房長官がコメント、他7件

4月は人事異動や転職、新規事業の開始などで人の動きが激しい時期です。そのタイミングで、メールアドレスを不正に取得しようとするインシデントが多く発生しました。クラウドなどのWebサービスではIDとしてメールアドレスを使うことが多くあるため、メールアドレスは攻撃者が欲しがる情報のひとつです。もしメールアドレスが盗み取られ、パスワードが推測されると、クラウドやシステムに侵入し、重要な情報を盗み取るようなインシデントの発生が想定されます。

提言

年度の変わり目には、個人情報を取得しようとする攻撃に対する警戒が必要です。メールアドレスを盗み取る行為の背景には、クラウドの利用が急増していることがあげられます。異なるクラウドサービスでも同じメールアドレスとパスワードを使い回していることが多いため、ひとつのメールアドレスの流出によって、複数のクラウドを乗っ取られる可能性が考えられます。メールアドレスの流出を防ぐのはもちろんですが、利用するサービスの重要度ごとに異なるパスワードを利用するような指示を徹底させるなど、これまで以上に留意した情報漏えいを防ぐ取り組みを進めてください。

脅威情報 Android端末へのパッチ配布、一部で適用見送りも 研究者指摘、他1件

スマートフォンやタブレットの脆弱性やパッチに関する報道が流れました。このAndroid端末の記事のほかに、4/25に「AppleがiOS等の脆弱性を修正」と報じられています。携帯電話の販売が、旧式のものからスマートフォンに変わり、これまで個人利用が主だったスマートフォンやタブレットを業務で利用するケースが増えています。スマートフォンやタブレットの旧機種へのパッチの配布を見送るメーカーも出ており、メーカーや機種によってセキュリティへの取り組みにばらつきが発生しています。パッチが未適応だと脆弱性が残ったままになり、そこからシステムに侵入される危険性があることを認識する必要があります。またPCとは違って、スマートフォンやタブレットは電源を落とすことも少なく、利用者が寝ている間にもネットワークにつながっているので、不正プログラムに感染していると、気が付かないうちにデータが流出することもありえます。業務利用のデバイスには価値のある企業の重要なデータや個人情報などが蓄積されているので、その情報を攻撃者は狙ってきます。

提言

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す。利用者が気付かずに悪意のあるアプリをインストールしてしまい、そこから業務システムへの攻撃や社内の重要システムへの侵入を許してしまうことも考えられます。業務で利用している端末のセキュリティは、より徹底した管理が必要です。

脆弱性情報 HMI/SCADAシステム製品InduSoft Web Studio等に深刻な脆弱性、他1件

4/20にも「Schneider ElectricのTriconex Triconに深刻な脆弱性、「HatMan」が悪用」（脆弱性情報）、という情報が報じられました。OT（Operational Technology）などの運用・制御システムは、ITシステムがベースとなっている部分も多くなってきており、ITシステムに搭載されているソフトウェアと同じ脆弱性が存在します。そのため、脆弱な部分を狙ったサイバー攻撃を受ける可能性が考えられるのです。

提言

OTシステムは専用システムでネットワークに接続されていないので「サイバー攻撃を受けないから安全」と考えている人が多いようです。最近は通信ネットワーク経由でITシステムと接続されているものもあります。そのため、OTシステムに存在した脆弱性が悪用されたインシデントは、これまでいくつも発生しています。もしサイバー攻撃でOTシステムにインシデントが発生すると、生産ラインの停止や不良品の発生など、莫大な経営損失が発生しかねません。OTシステムへのサイバー攻撃は、大きなビジネスリスクになることを認識し、強い警戒心を持って、適切なセキュリティ対策を講じなければなりません。

名和 利男の知見から読み解く、サイバー攻撃の着眼点

年度初めは人の動きが多くなる時期でもあり、そのタイミングでメールアドレスなどの情報を取得するサイバー攻撃が増加します。メールアドレスをIDとして利用するサービスもあるため、メールアドレスの流出には気を付けるべきです。人の動きが活発になる時期だからこそ、セキュリティの重要性を再認識する必要があります。

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