サイバーセキュリティ2014夏セミナー

独自分析レポートが示すセキュリティ攻防最前線
――組織に問われる対応力、サイバー攻撃から組織を守れ!

主催：NRIセキュアテクノロジーズ　　開催日：2014年7月17日・8月6日（東京）、9月3日（大阪）

■急増する企業へのサイバー攻撃

NRIセキュアテクノロジーズ（以下、NRIセキュア）では、毎年「サイバーセキュリティ傾向分析レポート」（以下、分析レポート）を発行している。これは、NRIセキュアが提供するセキュリティ診断やマネージドセキュリティサービス等から収集したデータをもとに、企業の情報システムに対するインターネットからの攻撃状況を分析し、その対策をまとめたもので、2014年で10年目を迎えた。関連して例年開催しているセミナーは、今回、申込受付直後に満席となり、急きょ追加したセミナーも好評であった。標的型攻撃に代表される企業へのサイバー攻撃が急増し、企業の危機意識が高まっていることがうかがえる。

■脆弱性発表の翌日から攻撃

セミナーではまず、2014年４月に大きな話題となったOpenSSLの脆弱性「Heartbleed」について、デモンストレーションを交えて解説した。「疑似ハッキング」によってセキュリティ診断を行うコンサルタントが、疑似環境でユーザーが入力したID・パスワードがサーバーのメモリー上で詐取できる様子を再現した。Heartbleedを悪用した攻撃は容易で、多くの企業の情報システムに影響が及ぶ可能性があることから、参加者の関心は極めて高かった。

さらに、「近年は脆弱性の公表から攻撃されるまでの時間が極端に短くなっており、本脆弱性も、公表翌日には相当数の攻撃が検知された」と説明したうえで、即時対応の難しさと対策の重要性、確認すべきポイントについて提言した。

■企業が一元的に存在を把握している自社ウェブサイトは約５割

このような攻撃に迅速に対応するには、自社の管理するウェブサイトの現状を正しく把握しておくことが重要である。それには管理対象のサイトを常にアップデートする必要がある。しかし、分析レポートでは「企業が一元的に存在を把握している自社ウェブサイトは約５割」というデータが出ている。これは、海外M&A（企業合併・買収）の増加やグループ会社の事業拡大などもあって、企業がすべてのウェブサイトを管理することが困難であるためと見られる。ウェブサイトが一元的に管理されていなければ、脆弱性が公表されたとしても何の対策も講じられないまま放置される危険性がある。こうした課題解決のため、企業に関連するウェブサイトを洗い出して棚卸しする、NRIセキュアの「Webサイト群探索棚卸しサービス GR360」という独自サービスも紹介した。

■組織に求められるインシデント対応力

サイバー攻撃は止むことなく、また100％防御することも難しい。特にパッチマネジメントが求められる運用過程では、常時、適切に対応し続けることは想像以上に負荷がかかる。このような環境で組織に求められるのは、「脆弱性の公表という有事に備え、対応すべき対象を洗い出し、対策指示と対策状況を追跡できる体制、および運用スキームの構築」である。

NRIセキュアでは、Webサイト群探索棚卸しサービス GR360のほか、企業のインシデント対策のサービスも提供しており、企業のサイバーセキュリティ対策を今後も支援していく。

本セミナーについてのお問い合わせは下記へ
NRIセキュアテクノロジーズ
テクニカルコンサルティング部　大久保
電話：03−6706−0569
電子メール：okubo@nri-secure.co.jp