

NSF 2012 in Kansai

JNSA 西日本支部 企画運営 WG

齋藤 聖悟

JNSA 西日本支部では西日本地域のセキュリティレベルの向上を目的として NSF 2012 in Kansai を下記の要領で開催しました。

日 時：2012年10月24日(水) 13時00分～17時45分

会 場：新梅田研修センター

主 催：NPO 日本ネットワークセキュリティ協会 西日本支部

定 員：200名

概 要：BYOD で持ち込まれた機器をどうすれば安全に利活用できるかについて考える

料 金：無料



スマートフォンの普及が進む環境においてクローズアップされてきたBYOD (Bring Your Own Device、個人所有デバイスの会社への持ち込み) ですが、どのような情報セキュリティ対策を講じるかについてはまだまだ手探りな状態であり、どの企業でも試行錯誤しているかと思われまます。そこで2012年度のNSF 2012 in Kansaiではテーマを「中小企業だからこそBYODを考えてみる」と題し、持込を単に禁止するのではなくどうやって有効活用すべきかを考えることを目的として開催しました。

■ 開会挨拶

近畿経済産業局地域経済部 情報政策課 山口洋課長が、ITは非常に有用なツールだが重要情報を不正に取得する標的型攻撃なども起きており、それら負の側面を回避しつつITの利点を有効活用することが重要であるとお話され、そのために近畿経済産業局としてはJNSAと協力し合って情報交換を行い、啓発活動を行っていきたいとお話を頂きました。

続いて西日本支部の井上支部長より本セミナーの位置づけとJNSAおよび西日本支部の活動状況の紹介がありました。



開会挨拶 山口洋氏

■ 基調講演

国立大学法人名古屋大学情報基盤センター 高倉弘喜教授より「凶悪化するサーバ攻撃の実態とその被害緩和手法」と題して、公開事例が少ない標的型攻撃の概要や被害を緩和するための対策設計について解説を頂きました。

冒頭では、マルウェアが2.5秒ごとに生成されるため、検体収集が追いつかず、解析も間に合わなくなっていることから、アンチウィルスの検知パターンが限界にきていること、APT対策を謳っているものの多くは境界制御の延長線上やコンプライアンス系であり、APT対策とマルウェア対策はまた違うものとの解説に加えて、それら現状の整理をされた後に実際の事例を踏まえた標的型攻撃の説明を頂きました。侵入された後の組織内部での活動状況や、そこから情報をどうやって送信するか、証拠の隠滅方法までと詳細な内容であり、IPv6やスマートフォンを悪用した事例や組み込み機器の脆弱性の解説から、攻撃手法も日々進化しているとの印象を強く受けました。

後半ではそれらの事例を踏まえて、新たなセキュリティ対策について触れ、これまでのような怪しいファイルを開かないなどの対策は現実的には難しく、侵入されても情報を持ち出されないようにするなど守り方を変える必要があると指摘を頂き、対策の見直しとしてログの取得方法についても言及がありました。ログは日々

増え続けかつ改ざんされる可能性があるため、VLANやSSIDの設定を適切に行い調査すべきログを減らし、早期発見に努める必要があるため、ログの定期検査を実施していくべきと提言していただきました。

最後にBYOD賛成だが製品のライフサイクルが短く、OSのサポートが追いつかないため、何処まで古い機器の利用を認めるかについて言及がありました。セキュリティを考慮しシステム購入時にライフサイクルをあらかじめ組み込んでおく必要性に触られました。中小企業でも使用期限や保守を考えてシステムを導入していく必要があるとまとめて頂きました。

■ パネルディスカッション

「ちゃんと」、BYODを考えてみるというテーマで、株式会社KDDI研究所 竹森敬祐氏、日本マイクロソフト株式会社 香山哲司氏、株式会社神戸デジタル・ラボ 近藤伸明氏をパネリストとして迎え、富士通関西中部ネットテック株式会社 嶋倉文裕氏にモデレータを務めて頂きました。

冒頭では神戸デジタル・ラボと日本マイクロソフトそれぞれの社内環境、業務環境での業務の進め方や持ち込み端末の使い方などについて事例を交え、解説頂きました。その中でも印象深かったのは、「ブラックリスト(使用させない機能)だとしても抜け道を考えてしまうためホワイトリスト(許可する機能)によって管理している」という香山氏のお話でした。

続いて竹森氏からは、BYOD端末としてスマートフォンを前提とした安全性に関する技術解説を頂きました。個人が所有する端末のOSや機種は多種多様であるため技術的対策は非常に難しく、初期状態で安全なOSに制限する視点はOKだが個人所有デバイスへのインストール制限はやりすぎであるとのお話がありました。そして、社内規程で個人端末でも実施可能な対策、例えばルート化の禁止、ジェイルブレイクの禁止、リモートロックの実施程度なら可能であり、その上で企業所有デバイスだけMDMで管理する、などの提言を頂きました。また実際にBYODを運用するうえでUSB

バックアップ機能は使用しない、企業ネットワークではテザリングを使用させないなど具体的な部分にも触れて頂きました。

最後に具体的な対策に向けて「リスクと向き合いバランスの取れた対策のポイントは？」というテーマでは、竹森氏からは勝手に設置されているAPを探し出して停止させることや、法人契約のMDMなど運用の話や社員へお願いするべきことなどの対策が紹介され、近藤氏と香山氏からはスマートフォンで使用できる社内システムはWebのみに制限している運用状況から、Webで使用できるシステムかどうかで線引きするのも有効との提言を頂きました。

■ JNSA 拡大勉強会

JNSA西日本支部では定期的に情報セキュリティ勉強会を開催しており、本セミナーではその拡大版となる新たな試みとしてスマートフォンの「セキュリティ」ではなくスマートフォンの「新しい使い方」を知ることを目的として企画しました。

これまで開催してきた勉強会ではある程度対策が成熟した情報セキュリティを取り上げてきましたが、スマートフォンは、使用方法が多様で技術進歩が早く、対策が追いつかなくなる現状にあります。そこで、「対策」部分の勉強会ではなく技術や使い方そのものを勉強して対策のきっかけを作ることを目的としました。

前半はNHN Japan株式会社 増村洋二氏に「スマートフォンアプリ提供事業者におけるBYOD制度」と題して講演頂きました。LINEに代表されるスマートフォンアプリを作成する企業として、社内にはスマートフォンの購入には補助があり、積極的に使用させている一方で社内規程ではセグメント別ポリシーを整備し、ビジネスの成長を止めないセキュリティ対策を実施しているとの紹介を頂きました。

後半はPayPal Pte. Ltd. 井尾慎之介氏より「PayPal Here (tm)、スマートフォンの新たな可能性」と題して講演頂きました。PayPalでは誰でも使用できる決済シ

ステムとしてiPhone向けにPayPal Hereをリリースしており、その解説とデモを実施して頂き、私物のスマートフォンでも決済データが残らず、安全に使えるとのことでした。また、デバイスやアプリケーションのセキュリティ面でポイントとなるのはアカウントの管理であると補足頂きました。

■ NSF 2012 in Kansai のまとめ

本セミナーの締めくくりとして、高倉氏と嶋倉氏と筆者にて振り返りを行いました。

■ NSF2012in Kansai を終えて

当日は昨年とほぼ同じ130人の方にご参加頂きました。

アンケートではセミナーに参加した感想として回答者の99%が「大変有益だった・有益だった」と回答しており、情報セキュリティセミナーとしては成功したと思います。各セッションでは基調講演とパネルディスカッションについては「大変有益だった・有益だった」が98%でした。拡大勉強会では「大変有益だった・有益だった」が約6割となっています。これはある程度予想していた結果ではありますが、セッションの位置づけをしっかりと解説するなど次年度以降改善の余地がある部分です。

今年度も昨年同様に企業ブースを併設し、相談コーナーも設けると共に、西日本支部メンバーによる「入社してから退社するまで」ソリューションマップを配布しました。

これからも多くの方に参加いただける機会を作りまた関西圏のセキュリティレベル向上のためJNSA西日本支部としてセミナー・勉強会を継続していきますのでご期待ください。