「セキュリティマネジメントセミナー2010」に参加して

若松　進
工学系技術支援室 情報通信技術系

はじめに

本セミナーは、2010 年 3 月 9 日(火)にベルサール神田(東京都)において、ソフトバンククリエイティブ株式会社、ソフトバンクビジネス+IT 編集部の主催で、一般企業向けに開催されているセミナーであり、不正アクセスの現状報告と企業向けに不正アクセスから情報漏えいを防ぐための方法についての紹介であった。

1. 講演題目と講演内容について

本セミナーにおいて 4 つの講演があり、講演題目と講演内容の概要は、以下のとおりである。

1) 「最小の投資で最大の効果を上げる Web セキュリティ」、
上野 宣（株式会社トライコーダ）

当講演では、セキュリティ対策に必要な事柄についての報告がされた。

① 対策について、セキュリティ対策に終わりはないので、必要なセキュリティ対策を行えば良いのでは？

② 狙われる Web サイトとして、以前は有名企業・官公庁であったが、最近では金銭目的(個人情報・クレジットカード情報当)の改ざん等が主流であり、動機として技術力、政治的、金銭的なことが挙げられる。セキュリティ上に問題のあるサーバを利用し、偽装サイトの構築をされたり、マルウェアを自動的にダウンロードする細工を仕込まれたるする。被害例として、「価格比較サイト」や「楽器販売サイト」の被害状況が報告されている。

③ 安全な Web サイトを構築・運用するには、要件定義と設計が重要であり、脆弱性の 60%は要件定義・設計で決まる。

④ Web アプリケーションのセキュリティ要件として、明確に定義しておく。要求使用項目として、認証、アクセス制御、セッション管理、パラメータ、文字列処理等が挙げられる。

⑤ Web アプリケーションの脆弱性診断については、テスト方法、判断基準等が分からないため自社でのテストが実施されていない状況であり、専門業者に依頼する事が主である。

なお、本講演の中で引用された有用なサイト情報を以下に紹介する。

① LASDEC ウェブ健康診断
http://www.lasdec.nippon-net.ne.jp/cms/resources/content/1284/H20_web_kenko_shindan.pdf

② IPA 安全な Web サイトの作り方 改訂第 4 版
http://www.ipa.go.jp/security/vuln/websecurity.html

③ 発注者のための Web システム／Web アプリケーションセキュリティ要件書
www.tricorder.jp/security_requirement.html

2) 「安心なサービス提供を実現する Web サーバのセキュリティ対策のあり方」、
石山 明浩（日本電気株式会社）

本講演では、今主流となっている Gumblar 攻撃の特徴(リサイクル攻撃、アプリケーション脆弱性への攻撃、頻繁な攻撃パターンの変更)、Gumblar 攻撃の防御が困難な理由(正規サーバが改ざん、クライアント PC を攻撃、攻撃の検出が困難)についての解説があった。

次に、Gumblar の定義(2009 年前半から、正規 Web サイトを改ざんする事で感染拡大する「攻撃手法」ならびにその攻撃に使用されるマルウェアの総称)、Gumblar の攻撃方法、時系列による Gumblar の活動概要の説明の後、Gumblar の特徴(亜種が出回るスピードが速い、難読性が高く検知されにくい等)とその対策留意点(ftp プロトコルをインターネット側に接続しない、Web サイトの改ざんチェックツールの導入等)を踏まえ、Web サーバ更新の安全なやり方についての紹介があった。

最後に、NEC の新しいリモートアクセスソリューション(端末認証、PC 検疫との連携が可能等)、PC 検疫ソリューション、情報セキュリティ整備計画策定サービス、脆弱性の検査等の紹介があった。

3) 「マルウェアの脅威と安全対策 ～新たな攻撃、ウェブ改ざんに備える～」、
中田 太(株式会社セキュアブレイン)

本講演では、Gumblar 事件簿(今迄の Web 改ざん例の紹介)、攻撃手法(仕掛け、誘導、不正取得、感染拡大)、攻撃の進化(改ざんが複雑化→改ざん内容が難読化)等についての説明があった。

その後、自社開発した Gumblar 調査用のソフトウェア(gred)についての特徴と利用方法についての紹介があった。

有用な情報として、Gred セキュリティサービス(http://www.gred.jp)にアクセスし、Web サイトを入力することで、Gumblar 調査が可能である（無料）。例として、技術部についてチェックしたところ、安全であることが確認された。

4) 「Web アクセスから始まる脅威 ～ユーザ PC を介在とする攻撃の増加とその対策～」、
花壇 明伸（ゼットスケーラー株式会社）

前 2 つの講演と同様、Gumblar の動作メカニズム、ユーザ PC の保護等の説明の後、自社製品(Zscaler Page Risk Index)についての紹介、セキュリティに対する判定例、導入効果等の解説があった。

また、APT(Advanced Persistent Thread：新しい攻撃手段)についての流れ、この ATP 対策の検討についての説明がなされ、APT の特徴と対処(階層化された多角的な防御手段の必要性)について紹介された。その後、Web アプリケーションの制御に特化し多角的な対策を提供、SWG(Secure Web Gateway)に求められる機能(セキュリティ機能とその他の機能)、アプライアンスによる対策の限界についての解説、最後にクラウドから提供する SaaS 型モデルを利用した Zscaler のサービス構成(ウィルス対策・スパイウェア対策、新種の脅威への対策、ブラウザコントロール、URL フィルタ、Web2.0 アプリケーションコントロール、帯域最適化、情報漏洩対策、レポート・ログ解析)についての解説があった。

2. まとめ

本セミナーを受講して、最新のウィルス事情に関する状況とその対策方法を知ることができ有意義な時を過ごす事が出来た。また、企業向けのセミナーであるため、紹介された多くのウィルス対策には費用が掛かるため、本セミナーで紹介された機器やツール等を導入する事が困難である。しかし、一部無償で利用できるソフトウェアの紹介等もあり、これらを有効に利用する事でいままで以上のセキュリティ対策を進めていく事が可能となった。