ウォッチガード、「Motion Picture and Television Engineers Conference」でサイバーセキュリティについて講演

2015年5月26日（火）

ー企業向け統合型セキュリティソリューションのグローバルリーダであるWatchGuard（R）Technologiesの日本法人である、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、社長執行役員
根岸正人、以下ウォッチガード）は、同社のCTO（チーフテクノロジオフィサー）であるコリー・ナクライナー（Corey Nachreiner）が、Bits By The Bayカンファレンスにて放送業界が直面するサイバーセキュリティの脅威と脆弱性について講演を実施しました。本イベントはSociety of Motion Picture and Television Engineers（R）をスポンサーとし、現代の「ネットワーク時代」における長期的トレンドとビジョンについて放送業界のエンジニアを啓蒙することを目的としています。

ナクライナーは次のようにコメントしています。「インターネットは社会のコミュニケーション方法に多大な影響を与えたとともに、それを支えるネットワーク技術は世界中でのコンテンツの共有において大いなる可能性を解き放ちました。しかし一方では、この繋がった世界は日々117,000件以上のサイバー攻撃を受けており、膨大なリスクを生み出してしまいました。もはやハッカーから逃れられる業界はありません。」

放送業界が直面するサイバー脅威に対する理解を深め、脅威から身を守るための方法を伝授するために、ナクライナーは、サイバーセキュリティの暗部とデータを保護するための最善の防御体制の構築方法を概説しました。

・ もはや安全な業界は存在しない：
今日のセキュリティの脅威は世界中で劇的に増殖しています。事実、2013年から2014年にかけて企業により報告されたセキュリティインシデントは、2,890万件から4,280万件へと48%増加しました。ITと放送技術の融合が進むにつれ、脆弱性を突く高度なサイバー攻撃も増加しています。最近の被害例としてSony PicturesやTV5 Mondeが周知の事実として取り上げられています。

・ サイバーキルチェーンを理解する：
高度な攻撃を防ぐには、サイバーキルチェーン3.0で紹介されたように多層防御が必要であり、予備調査、配布、侵入／突破、感染／インストール、コマンド＆コントロール、感染活動、目的の実行／脱出といった攻撃者が辿るチェーン（連鎖）を断ち切る方法を理解し、業務に影響が及ぶ前にデータの安全を確保する方法を学ぶべきです。

・ ネットワークを可視化する：
今年は標的型攻撃（APT）元年と言われており、最先端の攻撃手法により、付加価値の高い企業情報が長い期間をかけて密かに搾取されています。このようなタイプの攻撃は、スピアフィッシング、ドライブバイダウンロード、ウォータリングホール、チェーンオブトラストといった一般的な攻撃方法と同様に、メディアや放送業界も標的にしています。一般的に、悪意のある攻撃を発見するには80日間かかり、除去するには120日を要すると言われています。企業側で気づいた時にはすでに被害を受けている事になります。このような事故の原因として、私たちのネットワークが膨大なデータに埋もれ、全体の可視性が欠如しているためにこうした事態に陥ってしまうことが挙げられます。

・ ビジネスを保護するには：
NGFW（次世代ファイアウォール）やUTM（統合脅威管理）アプライアンスを活用することが重要であり、特にAPT（標的型攻撃）対策機能を導入することが必要です。また、ネットワークやデータに対する可視性を高めることも必須です。しかしながら、技術だけですべてを解決することはできません。IT部門によるエンドユーザへの周知と教育も必要です。更にデバイスのファームウェアのパッチやアップデートも欠かせません。そして最後に、セキュリティの専門家はディザスタリカバリプランも考慮に入れないと、悲惨な結果を招いてしまう可能性があります。

ナクライナーは、16年にわたりサイバーセキュリティの前線に立ち、10年近く情報セキュリティの傾向について評価および的確な予測を立ててきました。また、ネットワークセキュリティの権威および国際的に著名なコメンテーターとして、Gartner、Infosec、RSAが主催するフォーラムでスピーカーを務め、その専門知識を生かして複雑なセキュリティのトピックについて解説してきた経験を持っています、さらにCNET、Dark Reading、eWeek、Help Net Security、Information Week、Infosecurityなどの著名なメディアに定期的に寄稿しており、Facebookにウォッチガードの「デイリーセキュリティバイト」のビデオも投稿しています。

以下のツイートもお待ちしています。
.@WatchGuard and @Secadept speak to sold out audience @SMPTEConnect at broadcast conference about #cyberkillchain.

【WatchGuard Technologiesについて】
WatchGuard (R)
Technologiesは、業界標準ハードウェア、ベストオブブリードセキュリティ、ポリシーベースの管理ツールを独自アーキテクチャにより統合したビジネスセキュリティソリューションを提供するグローバルリーダとして、全世界の企業にセキュリティソリューションを提供しています。ウォッチガード製品は、複数のセキュリティサービス、シングルコンソールによる導入と管理、インテリジェントに統一された脅威管理を統合し、すべての規模の企業に安全なビジネスの継続を支援し、先進的な独自のサポートプログラムLiveSecurity (R) により守られています。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジアパシフィック、ラテンアメリカに支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多くのパートナーを通じて、アプライアンス製品、セキュリティの「可視化」、セキュリティとネットワークの「管理」など拡大するニーズへのソリューションを提供しています。詳細は http://www.watchguard.co.jp をご覧下さい。

WatchGuardは、WatchGuard Technologies,
Inc.の登録商標です。その他の商標は各社に帰属します。

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041
東京都港区麻布台1-11-9 CR神谷町ビル5階
マーケティング担当：堀江
Tel： 03-5797-7205
Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： http://www.watchguard.co.jp

Generated by ぷれりりプレスリリース
https://www.prerele.com