

<http://www.computerworld.jp/topics/563/%25E3%2582%25BB%25E3%2582%25AD%25E3%2583%25A5%25E3%2583%25AA%25E3%2583%2586%25E3%2582%25A3%25E3%2583%25BB%25E3%2583%259E%25E3%2583%258D%25E3%2582%25B8%25E3%2583%25A1%25E3%2583%25B3%25E3%2583%2588/201117/%2B%25E3>

【NetEvents APACレポート】

「遮断」するべきか「許可」するべきか——それだけでは問題だ

ファイルやアプリ単位でアクセス権限を設定するネットワーク・セキュリティ対策
(2011年11月17日)

標的型攻撃から完全に逃げられる手だてはない——。多くの企業がネットワーク・セキュリティの確保に頭を抱えている中、ネットワーク・ベンダーらは「既存の対策では防御できない」と口を揃える。11月16日と17日にプーケットで開催中の「NetEvents Press Summit APAC」では、企業が直面しているネットワーク上の“脅威”について、多角的に紹介された。

Computerworld.jp



▲ Palo Alto NetworksのファウンダーでCTOを務めるニア・ズーク (Nir Zuk) 氏

一人のうっかりがデータセンターをダウンさせる

基調講演に登壇したのは、Palo Alto NetworksのファウンダーでCTOを務めるニア・ズーク (Nir Zuk) 氏。「最新のマルウェア攻撃に対する施策」をテーマに、マルウェアの現状について語った。

ズーク氏は、現在、特定の企業や団体を狙った攻撃（標的型攻撃）が増加していることを指摘。「こうした攻撃は、従来のセキュリティ対策では守れない」と強調した。

標的型攻撃は、ターゲットとなる企業の特定エンドユーザー（一社員）を狙い、そのユーザーに対してマルウェアを仕込んだドキュメントを送付して開封させ、バックドアを仕掛けるというものだ。「バックドアが仕掛けられて、そこから情報が流出してしまえば、従来のファイアウォールのような対策はまったく意味を持たない。1エンドユーザーのうっかりでデータセンターがダウンする可能性があることを理解すべき」（ズーク氏）という。

同氏は、「標的型攻撃は1つのソリューションで保護することできない。すべての“攻撃フェーズ”で適切なソリューションを組み合わせ、総合的な対策を施すしかない。企業はゼロデイアタックを心配するが、標的型攻撃のほとんどは、パッチが配布されている既知の脆弱性に対して行われている」と指摘する。

PDFをはじめとしたファイルは、あらゆるアプリケーション経由でダウンロードされる。これらすべてをISP（インターネット・サービス・プロバイダー）がスキャンできればよいのだが、マルウェアの“進化”のほうがはるかに速く、現実的ではない。さらに、すべてのネットワーク・トラフィックやダウンロードをリアルタイムで監視することも難しい。

こうした課題に対するソリューションとしてズーク氏は、「サンドボックスの利活用」と「シグニチャの自動生成」を挙げる。

疑わしいアプリケーションやファイルを保護された特定領域（サンドボックス）で実行すれば、振る舞いベースでマルウェアを検知できる。さらに、特定されたマルウェアに対するシグニチャを自動生成して配布すれば、ゼロデイ・アタックにも短時間で対応できるというのだ。

PaloAlto

Networksは先ごろ、標的型攻撃に対するソリューションとして「WildFire」をリリースした。同製品はクラウド上の仮想サンドボックスでのマルウェア検知や、シグニチャの自動生成機能も備える。

ズーク氏は、「今後こうしたソリューションは、すべての企業に必須となる。企業は“

遮断”か“許可”かの二者択一ではなく、ファイルやアプリケーション単位でセキュリティ・レベルを判断する必要がある」と強調した。

フィルタリングやネットワークにもインテリジェンスが必要



▲米国Blue

Coatでアジアパシフィックの製品／ソリューションマーケティングを担当するジョナサン・アンドレセン（Jonathan Andresen）氏

実際、多くのネットワーク・ベンダーは、「既存のファイアウォールやWebフィルタリングでは、現在企業が抱える問題は解決しない」と口を揃える。

その大きな要因は、Webアプリケーションとソーシャル・メディア・サービスの台頭だ。業務の一環としてfacebookやTwitterなどで情報を発信したり、Dropboxなどのクラウド・サービスを活用したりしているケースは多い。しかしネットワーク・セキュリティの観点からは、こうしたサービスをビジネスで利用することは歓迎されることではない。

では既存のセキュリティ・ポリシーに則って、こうしたサイトへのアクセスを遮断したり、データのアップデートを制限すれば問題は解決するのだろうか。米国Blue Coatでアジアパシフィックの製品／ソリューションマーケティングを担当するジョナサン・アンドレセン（Jonathan Andresen）氏は、「単に特定サイトへのアクセスを遮断するだけでは、何も問題解決しない」と語る。

「既存のWebフィルタリングは、URLでそのサイトへのアクセスを許可／拒否を判断する。しかし、ソーシャル・メディアではサイト内でさまざまな機能を提供している。こうしたサービスの利用をすべて禁止することは、生産性向上の観点から考えてもマイナスだ。今は『サイト』ではなく、『サイト内の

アプリケーション』をフィルタリングし、それぞれを制御できる機能を持ったソリューションが求められている」（アンドレセン氏）

同氏は、「facebookの最終形は“Webブラウザ”になること」だと指摘する。さまざまな機能をfacebook上に搭載し、その中でユーザーが行動すれば、ターゲティング広告も出しやすい。こうした動きは今後も加速していくという。

「白でも黒でもないグレーゾーンを、個別ユーザーに応じて判断する。フィルタリングにもネットワークにもこうしたインテリジェンスが求められている」（アンドレセン氏）