特集　サイバー攻撃の現状と防止策

“今”こそ見直すサイバー攻撃対策

株式会社日立ソリューションズ
ネットワークマーケティング部　浜村　憲

1．サイバー攻撃対策の考え方

2013年に入ってからもサイバー攻撃の被害に関するニュースが後を絶ちません。ニュースでよく報道されるのは官公庁や防衛産業、原子力関連の企業などですが、サイバー攻撃は政府や大企業のシステムを直接狙うのではなく、中小企業の社内システムや個人利用のPC、スマートデバイスを踏み台として侵入するケースもあります。つまり、インターネットを利用した通信やサービスを受けるすべての企業、学校、個人にサイバー攻撃対策が必要なのです。その攻撃手法は日々高度化していますので、対策がより一層困難になっています。要するに従来通りの定番のセキュリティ対策では不十分であり、今こそ見直しが必要な局面にきていると言えます。

サイバー攻撃とは、特定組織をターゲットに、メールや外部メディアなどで組織の端末に入り込み、そこからさらに組織の内部へ入り込んでいき、最終的に知的財産や個人情報などの組織にとって非常に重要な情報を組織に気が付かれることなく盗み出すというものです。

以下にサイバー攻撃の流れをご説明します。

●事前準備

サイバー攻撃では、標的の情報を盗む前の準備段階として、標的の組織に関係のある組織へ攻撃を行います。その組織に実在する個人名や組織間でやり取りしたメールなどの情報を収集します。

●初期潜入

準備段階で得られた情報を活用して組織内の特定のメールアドレスに対して関係者を装ったメールが送付されます。添付されているファイルがウイルス対策ソフトで検知できないとウイルスに感染してしまいます。

●バックドア通信確保

侵入したウイルスは、攻撃者と通信できるような環境を構築します。具体的には組織の業務で行っているHTTPの通信を模倣してやり取りを行い、攻撃者とウイルスが通信できるようにします。これがバックドア通信です。

●潜入調査

侵入したウイルスは数週間から数カ月に亘り組織のシステムに存在し、攻撃者とのやり取りを繰り返しながら重要な情報を探し出します。

●情報搾取

最後にバックドアを通じて重要な情報を攻撃者へ送付します。これで攻撃者の目的は達成ですが、さらに情報を窃取するために再攻撃を行うこともあります。

従来から組織内にウイルスを“入れない”ための対策として、ファイアウォールや侵入検知システム、ウイルス対策ソフトの導入、パッチ適用による脆弱性対策などが行われています。しかし、このような対策では十分とは言えなくなってきているのが現状です。すべてのソフトウェアの脆弱性対策を実施することは困難であり、すべての通信をシャットアウトするわけにもいきません。組織にとって最大の損失は重要な情報を搾取されることですので、万が一、ウイルスが組織内に侵入したとしても、ウイルスを“早く見つける”ようにすることと、攻撃者との通信をブロックして重要な情報を“出さない”ようにすることで、最悪の事態を回避するという考え方が必要になってきています。

２．キャンパスネットワークに求められる対策

サイバー攻撃は特定の大手企業や政府機関がターゲットになることが多いですが、決して大学や研究機関などが対象外ではありません。昨年10月には「ゴーストシェル」を名乗る国際的ハッカー集団によるサイバー攻撃を受けたとして、被害報告を出している大学が相次いでいます。この攻撃により、教職員や学生と見られる名前やメールアドレスなどの個人情報が流失してしまうという被害が出ています。

このような被害を未然に防ぐために、キャンパスネットワークのあるべき姿とはどのようなものでしょうか。ここ数年で多くの大学がPCを利用した授業を取り入れ、学生それぞれにPCを用意し、キャンパス内から有線・無線で自由にインターネットへアクセスできる環境を提供しています。さらにはTwitter、facebook、mixiなどのSNSアプリケーションやＷｅｂメール、Ｓｋｙｐｅ、Windows Live MessengerのようなP2P技術を利用したメッセージングアプリケーションが多様化し、多くの学生が利用しています。ところがサイバー攻撃においては、これらのアプリケーションが利用されているケースがあります。

そのような環境の中で大学のネットワークでは、「安全かつ利便性の高いネットワーク」の構築が求められています。安全なネットワークの構築には、次の三つのポイントがあると考えます。

○ウイルスを“入れない”対策
○侵入したウイルスを“早く見つける”対策
○重要な情報を“出さない”対策

この三つのポイントをまとめていきます。

（１）ウイルスを“入れない”対策

１）脅威

最近Twitter、facebook、mixi、などのSNSアプリケーションは就職活動中の学生にとって、人事担当者や先輩社員に直接コンタクトできるなどのメリットがあるので、利用している学生も多いかと思います。企業側も積極的にSNSを活用しているケースも多くなっているので、SNSを活用することが就職活動を成功させるカギになるとも言われています。しかし、これらのアプリケーションを利用することでウイルス感染を引き起こす可能性があり、大学側にとっては大きな脅威となります。

例えば、facebookで対象となる大学名で検索すれば、その大学に在籍する学生や職員、教授などが実名で把握することができます。攻撃者は実在する学生もしくは卒業生になりすましてアカウントを作成し、友達リクエストを送信するのです。攻撃者は巧妙なだましの手口を駆使しているので、偽物だと気が付かずに承認してしまうことがあるようです。SNSアプリケーション上で友達になると、ウイルスを仕掛けたサイトへ誘導したり、直接ファイルを送りつけたりするのです。友達から送られてきたファイルは警戒することなく開いてしまうケースが多いようです。

サイバー攻撃においては、こうしたソーシャルエンジニアリング(1)を巧みに利用した手法が多く利用されています。もし、このようなことが大学のネットワーク内で行われていたとすれば、ウイルス感染や、情報漏えいといった事故を招いてしまう可能性があります。

２）対策

ネットワーク上を流れるアプリケーションの把握が可能なファイアウォールの導入が有効な対策となります。大学のセキュリティポリシーに従ったルールを適用し、不正なアプリケーションの使用を制限することが重要です。完全に禁止してしまうと利便性を損なうので、例えばTwitterであれば“閲覧”は許可して“つぶやき”は禁止するなどの柔軟な対策をとることで、安全性と利便性の両立ができます。

また、サイバー攻撃で攻撃者が送りつけるウイルスは、従来通りのシグネチャーベースのパターンマッチングでは検出・駆除できない可能性が高いです。攻撃者は主要なウイルス対策ソフトでは検知されないことを確認した上で、ウイルスを送りつけていると考えられます。このような未知のウイルスへの対策においては、クラウド型のウイルス検知サービスが有効です。これはファイアウォールが任意のアプリケーションから送られてきた未知の「.EXE」や「.DLL」

ファイルを検出すると、そのファイルをクラウド上にある仮想サンドボックス環境で一旦実行し、挙動を明らかにすることにより、未知のウイルスであっても検知するサービスです。検知後は迅速にシグネチャを自動生成するため、継続する攻撃に備えることができます。

（2）侵入したウイルスを“早く見つける”対策

1）脅威

サイバー攻撃により、学内のネットワークへの侵入に成功したウイルスは、攻撃者のサーバ（C&Cサーバ）と通信ができるような経路を開設します。この通信経路であるバックドアは職員もしくは学生のPCからインターネットにアクセスするのと同じHTTP通信です。そのため、既存の対策で検知し、通信を遮断することは困難であると言えます。このバックドアを使って拡張機能がダウンロードされ、さらに学内の深部へと侵入してきます。これ以降、攻撃者はシステム内容を調査、情報搾取のために執拗に侵入し続け、目的の情報に辿り着くまで調査範囲を広げます。

2）対策

ウイルスに感染したPCを早期に発見し、バックドア通信を遮断することが重要となります。そのためには、ファイアウォールのログ分析が有効な対策となります。ログ分析で特徴的な通信の“振る舞い”からHTTP通信を偽装したバックドア通信を見分けることができるのです。

バックドア通信を確保する際には特徴的な動きがあります。具体的には、HTTP通信であってもIPアドレスベースのURLやDNSドメインのURL、登録されたばかりのドメインのURLに定期的に、頻繁にアクセスするのが特徴です。例えば1日に数十回以上、このような特徴的なURLにアクセスするような端末は、ウイルスに感染している疑いがあります。

ウイルスもすぐに重要な情報に辿りつけるものではなく、数週間から数カ月に亘り長い期間で、攻撃者とのやり取りを繰り返しながら重要な情報を探し出します。ですから定期的にログを分析し、早期に感染した疑いのあるPCを割り出すことで、最悪の事態（知的財産や個人情報などの情報漏えい）を未然に防ぐことができます。

（3）重要な情報を“出さない”対策

1）脅威

攻撃者は重要な情報を、バックドアを通して攻撃者のサーバ（C&Cサーバ）に送信します。これで攻撃者にとっては目標を達成したことになりますが、入手した情報にはシステム管理者のログインパスワードなども含まれますので、これらの情報をもとに再度攻撃を仕掛けてくる場合もあります。このように一度、学内のネットワークに攻撃基盤を構築してしまえば何度も侵入を繰り返して、さらに情報搾取されてしまうので、被害が拡大してしまいます。

2）対策

「2.（1）ウイルスを“入れない”対策」でも書きましたが、ファイアフォールによってネットワークを流れるアプリケーションを正しく把握し、不正なアプリケーションの使用を制限することは、情報漏えいを未然に防ぐ対策としても有効です。

サイバー攻撃の被害事例を見てみると、攻撃者のサーバ（C&Cサーバ）は海外に設置してあることが多いです。侵入したウイルスは、指定されたC&Cサーバと通信してバックドアを確保しようと試みますので、サイバー攻撃でよく利用される特定国への通信を排除することができれば、バックドア通信を遮断する対策にもなります。国別のIPアドレスを保持しているデータベースを利用し、特定国との不要な通信を遮断する設定が可能なファイアウォールであれば、有効な対策ができます。仮にその国に姉妹校がある場合には、その姉妹校との通信だけは許可することも可能です。

3．遠隔操作ウイルスの対策

少し話は変わりますが、情報セキュリティの分野でサイバー攻撃と肩を並べるほどに注目されているのが、遠隔操作ウイルスによる事件です。これは不正プログラムを仕掛けた他人のPCを使って、インターネット上の掲示板（2ちゃんねる）に犯行予告の書き込みを行ったとされる事件で

す。この事件で犯人は「Tor」（トーア）を利用していると報道されています。「Tor」はThe Onion Routerの略であり、接続経路の匿名化を実現するためのアプリケーションで、タマネギの皮のように暗号化を積み重ねることが名前の由来と言われています。

この遠隔操作ウイルスの被害者にならないためにも、ファイアウォールは有効な対策となります。仮に、今回の事件と同様の手法で職員のPCが遠隔操作ウイルスに感染したとしても、「２ちゃんねる」への書き込みを禁止」という設定をしておくことで、未然に防ぐことができます。さらに「Torを禁止」という設定をしておくことで、キャンパスネットワークが犯罪の舞台として利用されるリスクを低減できます。

４．まとめ

サイバー攻撃への対策を考えるにあたっては、「外部からの攻撃は完全に防げないため、万が一ウイルスに感染しても、重要な情報の流出を未然に防ぐことで被害を最小限に抑える」という考え方が重要です。それを実現するためには、多層防御の考え方が必要です。つまり、何枚もの防衛壁を設置するように複数のセキュリティ保護対策を組み合わせて実施するということです。今回はサイバー攻撃の対策として“入れない”、“早く見つける”、“出さない”という三つの対策を紹介してきました。簡単にまとめると以下のようになります。

（１）ウイルスを“入れない”対策

ネットワークを流れるトラフィックをアプリケーションで識別し、不正な目的で利用されるSNSアプリケーションを制御する必要があります。仮に未知のウイルスが添付されたファイルを開いても、検知・駆除できる対策をしておくことも重要です。

（２）侵入したウイルスを“早く見つける”対策

ファイアウォールのログを解析することで、ウイルスに感染した疑いのある端末を早期に発見することが重要です。侵入したウイルスは、C&Cサーバとのバックドアを確保しようと試みますので、その振る舞いを検知できれば、ウイルスが拡大する前に対策を打つことができます。

（３）重要な情報を“出さない”対策

ネットワークを流れるアプリケーションを制限し、サイバー攻撃でよく利用される特定国への通信をシャットアウトすることで、バックドア通信を遮断できます。大学にとって最大の損失は、重要な情報の流出であることを再認識する必要があります。

安全なネットワークの構築には、利用されるアプリケーションの制御、利用できるユーザの制限に加えて、バックドア通信を遮断することが必要です。ここで誤解をしないでいただきたいのは、「アプリケーションの制御とは、SNSアプリケーションは危険なのですべて禁止にしてしまう」ということでありません。

先に述べました通り、就職活動中の学生にとっては活用すべきアプリケーションですので、利用方法と利用者を制限した上で許可する必要があります。このように大学のネットワーク構築には、安全性と利便性の両立を考えて、柔軟に対応できるようなセキュリティポリシー策定が求められています。

今回ご紹介した対策のように、ファイアウォールの導入は非常に大きな効果があります。ただし、ファイアウォールを導入すれば、対策は万全というわけではありません。導入したファイアウォールを大学内で定めたセキュリティポリシーに沿って運用することも重要です。さらには、サイバー攻撃の始まりがソーシャルエンジニアリングであることを考えれば、だましの手口に引っかからないために、学生や職員を対象にしたセキュリティ教育の実施も必要であることを忘れてはいけません。

注

(1)人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法のこと。

参考文献

[1]「新しいタイプの攻撃」の対策に向けた設計・運用ガイド改定2版. 独立行政法人情報処理推進機構セキュリティセンター.