報道関係者各位
プレスリリース

2011 年 12 月 15 日
グローバルセキュリティエキスパート株式会社

新サイバー攻撃「APT 攻撃」で企業内部の情報漏えいが拡大中。GSX、対策に必要な“システムの免疫力”を把握する『APT 攻撃耐性評価』を 12 月 15 日より提供開始

グローバルセキュリティエキスパート株式会社(本社：東京都港区、代表取締役社長：松本 松仁、以下 GSX)は、企業の脆弱性を突き侵入してくる APT 攻撃を想定した脆弱性評価手法『APT 攻撃耐性評価』を確立し、2011 年 12 月 15 日より提供を開始します。

APT 攻撃では、不正プログラムを潜り込ませ、増殖させることでターゲットを奪取します。GSX が確立した『APT 攻撃耐性評価』は、これらの攻撃に対してどの程度の免疫強度があるのか、APT 攻撃に対する企業の免疫力を測り、その評価結果によって現状を把握することで、講じるべき対策を浮き彫りにします。

また今後 GSX では、「APT 攻撃対策セキュリティスイート」として、当サービスだけでなく実際の対策ソリューションも充実してまいります。詳しくは、コーポレートサイトにて発表していく予定です。
URL： http://www.gsx.co.jp/service/J1_15.html

【『APT 攻撃耐性評価』の必要性】

■被害企業が拡大する APT 攻撃。システムの脆弱性を突いて増殖・拡散中

これまで企業は、内外の脅威に対してさまざまなセキュリティ対策を実施してきましたが、新たなサイバー攻撃(APT 攻撃)への対応が遅れており被害が出始めています。
APT 攻撃は、攻撃者に狙われた場合、その企業に APT 攻撃に対する有効な手段が無ければ、ほぼ確実に内部情報が盗まれます。これまで外部からの脅威に対しては、ファイアウォールや侵入検知など、外部からの不正侵入を防ぐ対策(入口対策)を中心に進められてきたのが現状です。
しかし APT 攻撃は、これまでの入口対策をすり抜けて不正プログラムを内部に送り込み、情報システム環境が抱える脆弱性を突いて成長・拡散してきます。さらに、攻撃者とウィルスが http プロトコルを使用して互いに指示と応答を繰り返すため、既存の対策だけではその存在を検知できないケースがほとんどです。
この結果、企業が知らない間に、社内のシステム情報や重要情報が攻撃者によって不正に持ち出されたり、社内システムが踏み台にされて攻撃者の片棒を担ぐはめに陥ったりなど、被害の拡大に繋がります。

【『APT 攻撃耐性評価』の概要】

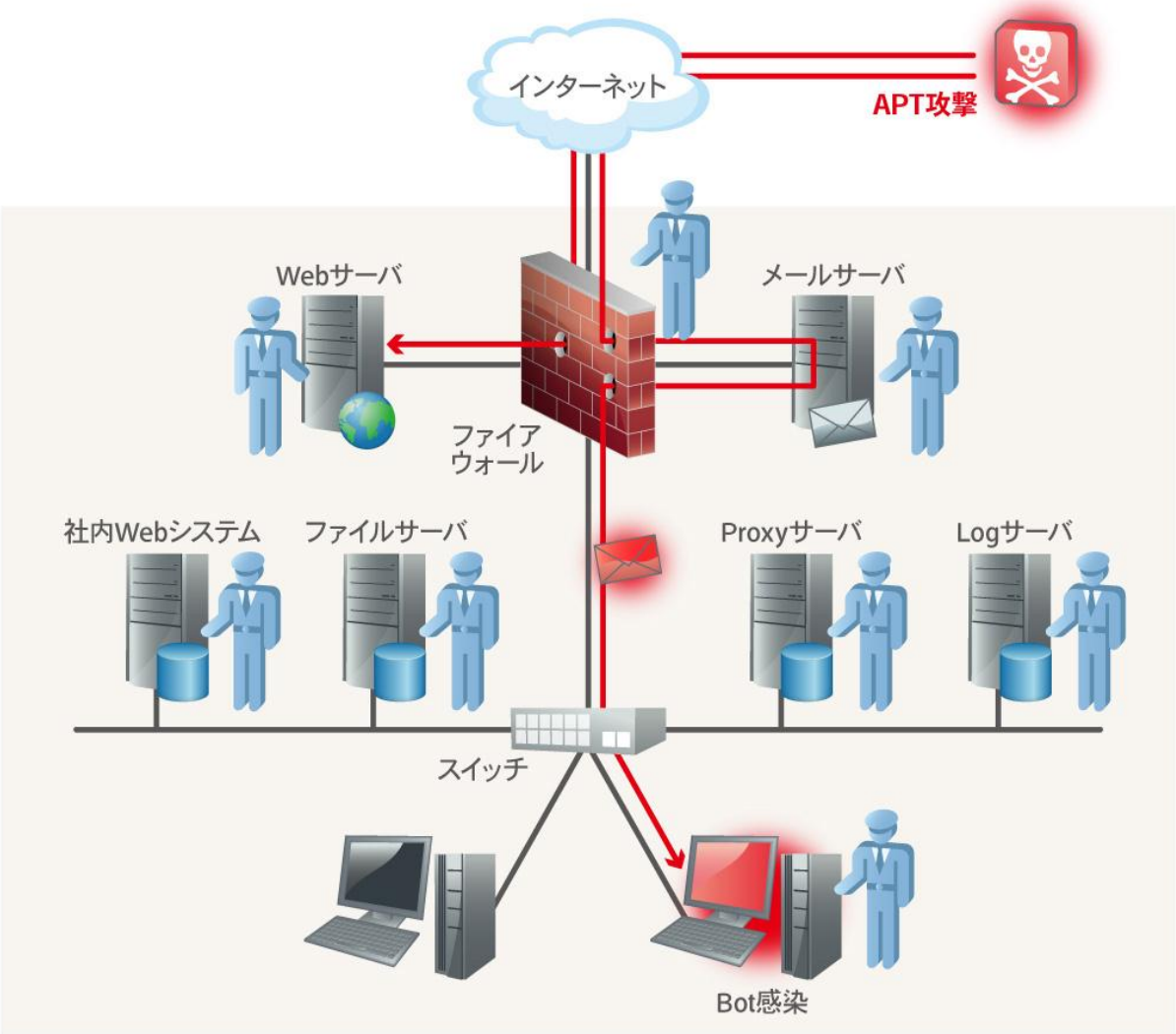
■APT 攻撃に対する免疫力を把握し、リスクを見積もる

APT 攻撃を迎え撃つには、これまでの様な侵入を入口で防ぐ考え方のみならず、社内への侵入を前提とした対策への取り組みも加えていく必要があります。つまり、既存の対策をすり抜ける APT 攻撃により、仮に不正プログラムが社内へ侵入しても、

◎不正プログラムを増殖させない
◎攻撃者と不正プログラムを会話させない

この 2 点を実現できれば、APT 攻撃によるリスクを相当数、取り除くことが可能となります。
それにはまず、APT 攻撃に対する免疫力が企業内にどの程度あるのかを把握しなければなりません。
しかしこれまでの様な健康診断的な評価手法では、APT 攻撃に対してどれだけ免疫力が備わっているのか把握できません。そこで GSX では APT 攻撃を想定した脆弱性評価手法を確立しました。
本サービスは、APT 攻撃によるリスクがどこにどの程度存在するのかを把握し、上記対策の足がかりを提供するサービスです。

【本サービスにおける GSX のコンサルティングの特色】
下記の耐性評価を実施し、実際の免疫力について耐性評価を実施します。



[APT 攻撃への耐性を総合的に評価]

●不正メールに対する耐性評価
APT 攻撃の侵入手段となる標的型攻撃を偽装テストし(不正メールの送付)、標的型攻撃に対して各従業員がどの程度回避できるのか評価します。

●Bot 感染 PC に対する耐性評価
GSX のコントロール下にある Bot 感染 PC を企業のネットワークに接続し、企業が的確に対応可能であるかを評価します。また、Bot 感染 PC からどの程度機密情報などにアクセス可能であるかを評価します。

●ファイアウォールの耐性評価
現在のファイアウォール設定が、APT 攻撃に対する対策として有効であるかを評価し、改善案を提示します。

●クライアント PC の耐性評価
APT 攻撃に利用されがちな社内のクライアント PC に内在する脆弱性を見つけ出し、改善案を提示します。

●社内サーバの耐性評価
APT 攻撃に利用されがちな社内サーバに内在する脆弱性を見つけ出し、改善案を提示致します。

●ファイルサーバ内の個人情報の点検
ファイルサーバにある守るべき個人情報などの重要情報がどこにどの程度存在しているのかを明確にします。

●ファイルパスワードに対する耐性評価
マイクロソフトの Office をはじめとする社内の電子文書に付けられたパスワードの強度や傾向を評価し、改善案を提示します。

●持込み PC に対する耐性評価
不正な持込み PC によるネットワーク接続などの脆弱性を評価し、改善案を提示します。

【『APT 攻撃耐性評価』導入のメリット】
●新たなサイバーテロ攻撃に対する備え
内部から外部へ繋がる出口対策の実施状況、被害の拡大に繋がる社内システム環境の脆弱性や個人情報の管理状況を評価し、対策を適用することで、新たなサイバーテロ攻撃による被害を最小限に抑えることができます。

●標的型攻撃に対する備え
APT 攻撃で使用される不正メールを偽装テストし、ユーザへ教育・啓蒙を推進することで、実際の攻撃に対する『APT 攻撃侵入リスク』を最小限に抑えることができます。また、セキュリティ担当者および管理者が攻撃を疑似体験することで、実際の攻撃を受けた時に迅速かつ適切な対応が可能となります。

【『APT 攻撃耐性評価』スケジュール】
1)プレヒアリング
対象部門・対象システムなどの実施対象の選定・実施要領の説明・スケジュール調整

2)実施計画策定
実施要領の明文化、対象部門に対するアナウンス・調整

3)評価実施
APT 攻撃を想定した評価の実施

4)結果・改善案のまとめ
評価結果の整理、改善案の策定、報告書のまとめ作業

5)中間報告
評価の結果、緊急性の高い問題点やリスクを発見した場合は、速やかに第一報を入れ、初動対応の支援を実施

6)最終報告
組織のキーマン(上層部向け、現場向け)に対して、評価結果を分かり易く説明し、今後の改善提案を実施

7)フォローアップ
評価結果・改善提案の不明点、および具体的な改善計画立案に向けたアドバイザリー支援

【『APT 攻撃耐性評価』価格】
1,000,000 円(税抜)から
※なお、対象規模と実施内容に応じたお見積となります。

【グローバルセキュリティエキスパート株式会社(GSX)について】
国内初の情報セキュリティ専門コンサルティング会社として 2000 年に設立され、セキュリティポリシーの導入、リスクマネジメント、各種コンサルテーション、システム実装、アウトソーシングにいたる広範な情報セキュリティサービスを提供しています。また、情報セキュリティポリシーの国際標準基準となった英国規格協会(BSI)の BS7799 を日本に初めて紹介し、同協会より高品質な情報セキュリティコンサルティングを行う「アソシエイツコンサルタント会社」として認知されています。2005 年 12 月には情報セキュリティコンサルティング会社として国内最初の ISO27001 を取得しました。
さらに、高い技術を有し、システムの脆弱性の発見のために侵入検査など様々な検査を行う「タイガーチームサービス(Tiger Team Service)」を組織しており、その手法が国内においてスタンダードとなっています。
GSX に関するさらに詳しい情報は、以下の URL をご参照ください。

社名　：グローバルセキュリティエキスパート株式会社
本社　：東京都港区南麻布 2-12-3 BBS ビル 6F
代表　：代表取締役社長　松本 松仁
設立　：2000 年 4 月
資本金：2 億 7,000 万円
URL　：http://www.gsx.co.jp

【本サービスの報道に関するお問合せ先】
グローバルセキュリティエキスパート株式会社
事業開発部　マーケティング　担当：菅田
電話：03-3457-1900
E-mail：mktg@gsx.co.jp