

発行

株式会社 エスクリエイト

名古屋市中区錦一丁目4番16号 日銀前KDビル4階

TEL: 052-222-3600 FAX: 052-222-3699

 URL: <http://www.screate-soft.co.jp/>

担当: コンサルタント 石垣 智博

tomohiro.ishigaki@screate-soft.co.jp

相次ぐサイバー攻撃の発覚！

ソニー米子会社、三菱重工、衆院議員そして在外公館までもがサイバー攻撃にあい、個人情報や機密情報が流出するに至りました(※在外公館は10/27現在ではウイルス感染のみ)。サイバー攻撃は以前よりありましたが、セキュリティ対策は万全だろうと考えられる組織からの流出だったので、驚きました。今後どのような対応・対策がなされるのか注目されます。(本当に対策が万全だったかどうかどうかも注目です。)

サイバー攻撃の手口がますます巧妙化しているなかで、経営資源(お金、知識)が潤沢ではない中小企業では、どのような対策が必要になるのか?を考えてみたいと思います。

◆どのようなサイバー攻撃があるのかを知っておく

孫子の言葉に『彼を知り己を知れば、百戦して殆(あや)うからず』というのがあります。何を行うにも、まずは敵(彼)を知ることから対策が始まります。

以下に情報セキュリティの情報を得ることができるWebサイトを紹介します。常に新しいセキュリティ情報を仕入れることが肝要です。まずは、敵を知りましょう。

- ① IPA(独立行政法人 情報処理推進機構) 情報セキュリティのWebサイト
<http://www.ipa.go.jp/security/index.html>
- ② IBM 2011年上半期 東京SOCレポート
<http://www-06.ibm.com/jp/press/2011/08/0301.html>

PC・スマートフォン・タブレットPC(以下、情報端末)は使っているけど、ITと聞くとアレルギー反応を起こしてしまう、ITに関するセキュリティはさっぱり分からない、という方もいるでしょう。

しかし、今後はそうも言っていられないでしょう。個人レベルでも最低限の知識は必要になってきます。最近のサイバ

ー攻撃に関する漏洩でも分かる通り、個人が使用している情報端末を介してウイルスが蔓延していくケースが多いということからもそう言えます。

◆標的型メール攻撃とは?

前述Webサイトでも指摘されていますが、膨大な個人情報を扱う会社、軍事産業関連企業そして国家機関など特定の組織を狙った「標的型メールによる攻撃」が増加しています。三菱重工や衆院議員の情報流出事件も「標的型メール攻撃」によるものだ。と言われています。

「標的型メールによる攻撃」とは、特定な組織の担当者にウイルス付きメールを送付するというものです。添付ファイル(例:実行形式ファイル(.exe)、圧縮ファイル、pdfファイル・Excelなどドキュメントファイルなど)を開くことがウイルスの起爆装置となります。そして、こっそり乗っ取られるということです。

昔からある手法じゃないか?怪しい添付ファイルは開かないのが鉄則では?と感じている方もいると思います。では、「経営者」「社員」「取引先」など知っている方からメール受信したら、添付ファイルを開けてしまいませんか?開けますよね。そこが犯人の狙い目なのです。

さらに、ウイルス蔓延の基になった方(ターゲットにされた方)のメールアドレスもウイルスなどの原因でメールアドレス含む個人情報がどこかで漏洩しているということも忘れてはいけません。

◆ウイルスセキュリティソフトをインストールしておけば安心か?

では、ますます手口が高度化するウイルスに対して、現状では100%安心できる対応策は無いというのが実情です。ウイルスソフトをインストールしていても、ソフトのウイルス定義ファイルの更新の方がウイルス発覚後になるからです。勿論ウイルスソフトをインストールし、常に最新に保っておくことは必要です。既出のウイルスに感染しない為には、



ワクチンで例えると、新型インフルエンザにはかかる可能性があるが日本脳炎は予防するのだ。ということになります。

ウイルスセキュリティソフトをインストールし最新に保っていないと、間違いなくウイルスに侵されると思ってよいでしょう。

◆まずは、「手洗い」と「うがい」から



セキュリティ対策は、出来る事からスタートさせることだと思います。対策として、1つは個人のセキュリティ意識を向上させることが大事です。情報端末を使用しインターネットに繋がっているということが、常に脅威にさらされているという認識をもつことです。そして、セキュリティに関する教育を行います。前述のWebサイトの情報を印刷して社員に配るだけでも、教育になります。できる事から始めるべきです。不用意な行動が少なくなるからです。

次に、攻撃に対する対策の1つとして、「弱みを見せない」ことです。ウイルスはセキュリティ不備(セキュリティホール)を狙ってくるからです。「OS・ソフトウェアを最新にしておく」「ウイルスセキュリティソフトのエンジンと定義ファイルを最新にしておく」「定期的スキャンする」「ファイヤーウォールを設置する」「メール添付ファイルを開くときは送付元に電話などで確かめめる」「PCの電源は入れっ放しにしない」「安易にソフトウェアをインストールしない」「怪しいWebサイトは閲覧しない。クリックしない」「メールアドレスをむやみに教えない」「個人情報(クレジットカードNo.含む)をWebサイトで入力しない。又は、信頼できるWebサイト以外では個人情報を入力しない」など様々な心得を知りそして実践することです。自社対応が難しい場合は、セキュリティに強いITベンダーに相談しましょう。

簡単な事を「徹底して実践する」ことが鍵となります。
まずは、毎日の「手洗い」「うがい」の徹底です。

「本は考える為のサプリメント」(その7)

「本は考える為のサプリメント」です。考える為の知識を本から学び、日々のビジネス活動で活かそうという企画です。

今回は、ビジネスに関係した小説を紹介します。楽しむ小説も良いですが、楽しみながら学ぶ小説を読むのも良いのではないのでしょうか？

「会社蘇生」(高杉 良)

企業小説の著者として有名な高杉良氏の作品です。1988年に出版された作品ですが、今読んでも全く色あせない内容です。ストーリーは、ある老舗商社の破綻から再建への物語。主人公は破産管財人の弁護士です。破産管財人の苦悩・努力・胆力そして断固たる決意が伝わってきます。さらに、関係する人々(従業員、支社、取引先、銀行、その家族)が臨場感を創出しています。関係する人々が当事者としての葛藤、思い、考えが描かれており、とてもリアリティを感じます。さらに、裁判所に会社更生法を受理させるまでの展開は手に汗握ります。(注:現在の会社更生法は、小説当時の会社更生法から改正があり手続きが違います。)私は読んだ後で知りましたが、株式会社大沢商会グループの会社更生手続きがモデルだそうです。

1つのプロジェクトを導くためには「強烈でゆらぐ事のない決意」によって、熱意みなぎり、真剣に行動でき、関係者の理解・協力が得られるのだ。ということがわかりました。

この様な企業小説を読むのには抵抗が有るかもしれませんが(私もそうでした)。しかし、読んでみると面白く、そして得るものがあると思います。お薦めです。

編集後記

2011年9月14日に発表された「Windows8」開発者向けプレビュー版を試してみました。新しいモノに触るのはとてもワクワクします。

ユーザインターフェース(画面)は現行のWindowsとまったく違います。WindowsPhone(スマートフォン)に近い感じです。デスクトップPCやノートPCばかりでなくタブレットPCも意識したつくりとなっているかなと感じます。使い勝手は慣れの部分もあるので、慣れれば良いかなと思いました…。

驚いたことに、非常にOSの動きが軽快なことです。電源を入れたらあっという間に起動しました。評価PCのスペックはCPUがpentiumM(1.1)でメモリは512Mの7年前のノートPCです。今となっては使えないPCが蘇ったようでした。ただし、アプリケーションは試していませんので、古いPCで実用に耐えられるかは疑問がのこるところです。

評価開発段階なのでこの軽快さを保ってリリースさるのかわかりませんが、期待が持てそうです。

Windows8の発売は、噂ですがは2012年に予定されてるそうです。(プレビュー版が今でているのでその可能性は高いでしょう。)

Windows7が発売されて間もないので「えっ!もう次のOSが早すぎない!」と思いましたが・・・楽しみです。(石)

