今日の焦点

これからのセキュリティ対策

セキュリティは、新しい価値を産み出すための手段である。例えば、電子マネーは、カードをかざすだけで支払いができ、大きな利便性を提供している。しかし、セキュリティは、一般には秘密を守るための防衛的な技術と見られている。余裕があったら、事故が起きたら、導入しようと考えられることが多い。IT投資として効果が見えにくいため、どうしても優先順位が低くなる傾向がある。

新たな攻撃から情報資産を守るには

システムを守るセキュリティについては、ここ数年で大きく状況が変わってきた。以前は、システムの内と外の間の壁、すなわちファイアーウォールを固めておけば、内は安全という考え方が一般的であった。ファイアーウォールは、システムの外から内に侵入しようとするクラッキング行為を監視し、不正なアクセスを検出・遮断することにより、システムを守っていた。最近は、特定の企業・組織を狙って機密情報を盗み取る標的型攻撃が多く見られるようになった。取引先などの実在する人の名を騙って業務を装ったメールを送り、不正プログラムを仕込んだ添付ファイルを開かせる。攻撃者は、不正プログラムにより端末を遠隔操作して企業情報を窃取する。このように攻撃が巧妙化するにつれて、「企業のシステムを壁で完全に守ることが不可能である」という考え方が一般的になってきた。その中で対策は大きく分けて、二つの方向性があるように思う。

ひとつは、通信をしっかり監視して怪しいものを見つけて、すぐに対策をとることによって、侵入されても大きな被害を出さないようにする考え方（システム管理の徹底）である。パソコンやサーバの既知の不正プログラムの対策としてパッチを当てていることは当然としても、ゼロディ攻撃（パッチ公開までの間に実行される攻撃）を受ける可能性が残る。異常が検知された場合、即座に隔離して被害を極小化する必要がある。

もうひとつは、暗号技術を使って大事な情報をカプセル化しておき、許可された人しか見られないようにすることで、情報が流出しても安全にする考え方（データ保護の徹底）である。最近は、ビジネスで多くの会社とコラボレーションすることが多い。秘密情報をパートナーに公開することは避けて通れない。パートナー企業内の監視まではできないことを考えると、データそのものを守る技術は必須である。

NTTソフトウェア株式会社
代表取締役社長
山田 伸一 氏

これらの２つの対策のどちらか一方だけでよいということではなく、脅威・リスクにあわせて、いろいろな方法をバランスよく組み合わせるしかないというのがコンセンサスだと思う。

利便性と安全性の両立を目指して

企業向けのクライアントといえば、パソコンだけ考えればよい時代は終わり、スマートフォン、タブレットなどモバイルデバイスの活用が必須になってきた。クラウド上のストレージサービスを利用して、複数のデバイスにまたがって情報を共有できるDropboxのような仕組みが企業でも必要とされている。しかし、米国では、Dropboxシンドローム（社員が勝手にDropboxに社内の重要な情報を持ち出してしまうこと）が問題となっており、クラウドやモバイルが提供する利便性を損なわずに安全性を確保することが求められている。こういった要求に答えられる仕組みとして、自社開発・市販製品などを検討した結果、WatchDox社と提携し、同社の製品を国内でお勧めすることにした。ファイル操作をコントロール（コピー、印刷、転送など）するとともに、その利用（いつ、どこで、誰が、何をしたのか）を追跡できる。ぜひ一度見てほしい。

【弊社ホームページ】
http://www.ntts.co.jp/products/watchdox/

どんなに技術が進歩しても、それを巧妙に回避する攻撃手法が次々と登場する。セキュリティはいたちごっこであり、これで十分ということはない。これからも新しい仕組みを常に探し続けたい。何かお困りのことがあれば、ご相談いただけるとありがたい。