ランサムウェア防御のベストプラクティス

統計データが示すランサムウェアの勢いは
すさまじい。この状況を簡単に言うと、どんな企業でも
ランサムウェアの攻撃を受ける可能性が高い、ということだ。
おそらく、ランサムウェアで最も恐ろしいのは、連続して
攻撃を受けることだ。データを回復するために身代金を
払って、1時間後に別なランサムウェアの攻撃を受けた時の
絶望感を想像して欲しい。しかし、これは実際起こっている。
攻撃者は被害者に対して同情も憐れみも持たない。

このような攻撃がもたらす深刻な被害に鑑み、
企業はこの脅威を真剣に受け止め、攻撃を防ぐための
対策を講じなければならない。
バックアップはランサムウェアに対する最後の
防御線であって、最前線ではない。

過去において、企業はマルウェア予防についての
ユーザー教育の効果に絶大な期待を寄せていた。
ユーザーがフィッシング・メールの見分け方を教われば、
そのようなメールの悪意あるリンクをクリックすることは
ほとんどないだろう、と。
しかし、残念ながらどんな優れたユーザー教育によっても、
悪意あるリンクのクリックや悪意ある添付ファイルの
オープンは完全には防げない、ということが
実際に起こったことから明らかになった。

思い切ってユーザー教育は効果がない、
と仮定するのもこの問題を解決するため
には、良い方法だ。

そして、有効な戦略は、メールサーバーの側で
メッセージをスクリーニングすることだ。
そうすれば、フィッシング・メールは決してユーザーの
メールボックスに届かない。
同様に、万が一ランサムウェア攻撃が発生した際の
被害を最小化するために、ユーザー権限を制限して
おくことだ。

これを行うには、多種多様な方法がある。特に効果的
なのは、アプリケーション・ホワイトリストを使う方法だ。
これにより、ユーザーは許可されていないプロセスを
稼働できなくなる。さらに一般的な方法は、権限の監査を
行い、ユーザーがどうしても必要なところに対してのみ
書き込み権限を持つようにしておく事だ。これ自体が、
ランサムウェア感染を防ぐわけではないが、ランサムウェアは
ユーザー権限を利用するので、こうしておけばランサムウェア
はユーザー権限を超えたアクセスができない。
この方法により、被害は限定できる。
もうひとつの方法は、管理者特権を必要とする処理の実行
以外は、ITスタッフに非管理者アカウントを使用するよう要求
することだ。

フィッシング・メールが多様なランサムウェアの
中の、ほんの一形態であることを思いだすのは
重要だ。攻撃者が犠牲者のコンピューターに
ランサムウェアを 潜り込ませるために、偽の
技術サポートを名乗る、というのもよくある。

ユーザーがIT部門の本物の電話番号と
ニセモノを見分けられるように、ユーザーを
教育してもらいたい。
言うは易く、行うのは難しいことではあるが。