見直されるセキュリティの常識

セキュリティポリシーの見直しが必要

・定期的なパスワード変更は必要？

パスワードの変更が多すぎて覚えられない
分かり易い規則性のあるものにしていないか
フィッシングサイトへ誘導されてパスワードが盗まれないか？

・パスワードを別メールで添付ファイルは暗号化が必須なの？

ウイルスチェックが充分にできず犯罪を助長する
宛先、発信元が同じで別メールする意味があるのか？
モバイル機器での使用などで、うまく中身が見れなず面倒

IT セキュリティの常識は、時代とともに変化しています。
以前は当たり前のように使用していた USB ストレージは、異なった PC のファイルの移動やコピーの重宝していましたが、今では、会社から許可された USB デバイス以外は、マルウェア等の侵入を恐れ、多くの会社のセキュリティポリシーにより使用することさえ禁止しています。
パスワードについても、以前は定期的な変更をするのが当たり前で、セキュリティポリシーで、1 ヵ月に 1 回変更することを強制していたりしましたが、それにより、パスワードを忘れロックされてしまい、管理者に方にも迷惑をかけることこもよく見受けられました。今では、忘れないようにするために、分かり易く規則性のあるパスワードを使うことによって推測されるリスクの方が高いため、定期的な変更は必要がないと言われています。
ところが、システムによっては、そのリスクのどちらが高いかはユーザに判断させるよう、定期的にパスワードの変更をするのか、同じパスワードを使い続けるかをログインした直後に確認しないと目的の処理をさせてくれない銀行系のアプリなどもあります。アプリ提供側は、自分たちは定期的に警告しており万が一情報漏洩した場合に、パスワードを毎回変更しなかったせいだとユーザに責任を押し付けたいのでしょうが、金融系のサイトは特にフィッシング攻撃により頻繁に狙われ、まったく同じイメージの偽サイトのページに誘導される恐れもあるため、このパスワードを入れさせる行為は、ユーザにとってはとてもリスクが高いと言わざるおえません。
また、最近では、メールで添付するファイルを必ず暗号化して、その解読パスワードは必ず別メールで送るというセキュリティポリシーを実行している企業が多い中、これでは、添付ファイルにウイルスが埋め込まれているかどうかのチェックが不十分でかえって危険だという意見も高まってきました。実際、既に zip 圧縮済みのファイルも含んで全体にパスワード付き zip ファイルにしてメール添付で送ろうとすると、Gmail は、ウイルスチェックができないため送れません。こうしたパスワード付き暗号化の添付は、ISMS やプライバシーマークなどを取得するためにやっていただけで、同じメール宛先に同じ発信元からパスワードを送って意味があるのかと思われていた人も多いと思われます。それでなくても、テレワークなどモバイル機器でメールを見る機会が多くなっているのに、送る方も受ける方も面倒で仕方ありません。
企業も新しい仕事のスタイルに合わせ、セキュリティポリシーの見直しは常に必要だと痛感させられます。