休暇明けのセキュリティー対策について

日常的に怪しいメールは開かない、修正プログラムの適用や定義ファイルの更新などを徹底していても、休暇明けなどのタイミングでは社内の気の緩みが生じやすく、セキュリティー事故が発生しやすくなります。

例えば休暇明けは、受信メールのチェックが忙しくなるため、誤操作や対応の遅れなどが発生しやすくなりがちです。こうした状況を踏まえ今一度見直していただきたいセキュリティー対策をご紹介いたします。

■ マルウェアやウィルス感染は対岸の火事ではありません

IT Expert Servicesご契約中のお客様においても、直近ではサービスデスクへの問い合わせの **5.7%** はマルウェアやウイルス感染関連のお問合せとなっており、**PC445台に1台**がマルウェアやウイルス感染する恐れがあります。問い合わせいただいたお客様は企業規模/業種/業態も多様です。

サービスデスクへお問合せいただく感染事例の多くは、トロイの木馬ウイルスによるものです。

「Emotet」は、トロイの木馬と呼ばれる高度なウイルスで、メールの添付ファイルやリンクをクリックさせる手口により感染します。

「Emotet」に感染してしまうと社内のデータが大量に流出したり、なりすましメールが取引先等に送られるなど、重大な被害を引き起こします。

<代表的なトロイの木馬>

種類	概要
バックドア型	通信用のポートを開き遠隔操作する
ダウンローダー型	ファイルをダウンロードする機能を持つ
キーロガー型	ユーザーのキーボード操作を記録し、記録したログをサイバー攻撃者に送信する
クリッカー型	Webブラウザの設定変更、特定の場所を強制的にクリックするなど、設定を変更しようとする機能を持つ
パスワード窃盗型	PCの内部を探索しパスワード情報や設定情報を探し盗み出す
プロキシ型	感染したPCのIPアドレス変更を行う
ボット型	ユーザーに気づかれないようPCに侵入し、様々な操作を行う

IT Expert Servicesのお客様のうち・・・

POINT

✓お問合せの **5.7%**はマルウェアやウイルスに関するもの

✓ **445台に1台** がマルウェアやウイルスに感染する恐れ

■ 休暇明けはメール増でチェックがおろそかに

サイバー攻撃者は休みなく皆さまを狙っており、標的型メールやフィッシングメールは常に発信されています。特に、多くのメールが溜まる休暇明けは、防衛心理が手薄になるタイミングとして攻撃対象になりやすくなっています。

休暇明けは、溜まった大量のメールを一度にチェックすることになり、油断や対応漏れが起きやすい状態です。また、未対応案件が多くなることで焦りも生じ、ミス発生のリスクが高まります。

■ 休暇明けの対策

1.定義ファイルの更新

休暇中に電源を切っていたPCは、セキュリティソフトの定義ファイルが古い状態のままになっています。**電子メールの送受信やWebサイトの閲覧等を行う前に**セキュリティソフトの定義ファイルを更新し、最新の状態になっていることを確認しましょう。

2.修正プログラムの適用

休暇中にOSや各種ソフトウェアの修正プログラムが公開されている場合があります。担当者にも確認しながら、必要な修正プログラムを適用してください。

3.持ち出しPCや外部記憶媒体のウイルスチェック

休暇中にPCや、データを保存していたUSBメモリ等の外部記憶媒体を自宅や外出先に持ち出していた場合、ウイルスが混入していないか、**組織内でPCや外部記憶媒体を利用する前にセキュリティソフトでウイルススキャン**を行ってください。

4.不審なメールはURLと添付ファイルを開かない

実在の企業や人物を騙った不審なメールが届き、被害にあうケースが個人、企業においても多数発生しています。

こういった**メールの添付ファイルを開いたり、本文中のURLにアクセスしたりすることで、ウイルスに感染したり、フィッシングサイトに誘導されたりしてしまう可能性**があります。休暇明けはメールが多数溜まっていることが想定されますので、**特に注意してメールチェック**を行ってください。**不審なメールを受信していた場合、“添付ファイルは開かず”、”本文中のURLにはアクセスせず”**、IT Expert Servicesサービスデスクにご連絡ください。

■ こんなときは、マルウェアやウイルス感染が疑われます

1.不審なメールの添付ファイルやURLをクリックしてしまった

2.アプリケーションをインストールしたら急にパソコンが重たくなった

3.勝手にメールが送信されている

4.急にファイルが増えたり、減ったりしている

IT Expert Servicesにご相談ください

■ 万が一、マルウェアやウイルス感染がわかったら

✓PCの利用をただちに中止しましょう

冒頭にもあるようにマルウェアなどは、皆さまのPC操作を記録している場合もあります。また、PC操作を続けることで被害が拡大する場合もありますのでPCの利用を中止し、下記の適切な対処を進めましょう。

✓PCをネットワークから隔離しましょう

PCのウイルス感染が危惧される際は、PCのネットワークを切断します。
LANケーブルを抜いたり無線LANのスイッチを切ったりなどの方法で、職場、家庭を含めるネットワーク環境から感染したPCを切り離してください。
ただし、ウイルスによる被害状況を保存するためにPCの電源は切らないように注意しましょう。

※電源OFFについては、企業によって対応が異なる場合もあります。
ご担当者様へのご確認や皆さまの企業の対応方針をご確認ください。

✓ウイルス対策ソフトでウイルス駆除をしましょう

ウイルス対策ソフトによるウイルス駆除を実施しましょう。“ウイルス駆除の仕方がわからない”、“ウイルスが駆除されたのか不安”といった方は、IT Expert Servicesサービスデスクまでご連絡ください。

✓IT Expert Servicesサービスデスクまでご連絡を

サービスデスクとエンジニアが連携し、ウイルス駆除や障害解消に向け、皆さまをご支援いたします。

今回は、休暇明けのセキュリティー対策についてご紹介しました。今後も休暇の際には特に注意が必要ですので、ぜひご参考になさってください。
また、日常のIT機器管理でお困りごとやご不明点がございましたら、いつでもIT Expert Servicesサービスデスクまでお気軽にお問い合わせください。

（2024年5月発行月次レポート「ITトピックス」の内容を一部修正して掲載しております。）