2022 年 6 月 23 日

当社グループ従業員を装った不審メールに関する調査報告書

株式会社 SDS ホールディングス

2022 年 6 月 8 日頃より発生しておりました弊社グループ従業員を装い送信されていました「なりすましメール」に関しまして、関係者の皆様には、多大なご迷惑とご心配をおかけしておりますことを深くお詫び申し上げます。
この件につきまして、外部のセキュリティ専門機関を起用し、被害状況や感染経緯等について詳細な調査を実施いたしましたので、その結果を下記のとおりご報告いたします。

記

1.概要
当社を装った第三者からの不審なメールが複数の方へ発信されている事実を確認し、当社従業員のパソコンがマルウエア（Emotet）に感染していることを確認しました。

2.経緯
・6 月 8 日（水）当社を装った第三者からの不審なメールが複数の方へ発信されている事実を確認。全従業員の端末のウイルススキャンを実施し、従業員 1 名の端末がマルウェア（Emotet）に感染していたことを確認、直ちに該当 PC をネットワークから遮断しウイルス対策ソフトにて駆除を実施。該当従業員のメールサーバーと業務システムのパスワードを変更。ホームページにて注意喚起を掲載
・6 月 9 日（木）　JPCERTCC が提供する「EmoCheck」による再スキャンをに実行し、他の端末に感染がないことを確認。ファイルサーバーや社内システムに影響がないことを確認
・6 月 10 日（金）　セキュリティ専門の調査会社にフォレンジック調査を依頼。内閣府の個人情報保護委員会へ相談し、「個人情報流出のおそれ」として報告書（速報）を提出
・6 月 20 日（月）　調査会社より報告書を受領
　＊エモテット以外のマルウエアには感染していないことを確認
　＊社内ネットワーク内の他の端末やサーバーへ横展開した形跡はない
　＊窃取されたデータを特定するための痕跡はマルウエアによって消失していた
　＊該当端末にはアドレス帳含む顧客リストや決済情報の保存はなかった

3. 被害状況
現時点では本件を悪用した被害は確認しておりません。
不審メールの報告件数は感染直後には多かったものの、ここ数日は新規の報告もなく現在は収束に向かっているものと判断しております。

4. 今後の対応
同様の事象が発生しないよう、定期的なウイルスチェックと OS のアップデートの励行し、情報セキュリティに関する基本動作の確認と徹底を図り、教育プログラムの充実を図ってまいります。

お客様ならびに関係者の皆様には多大なご迷惑をおかけいたしましたことを深くお詫び申し上げます。

以上