2023 年 10 月 24 日
富士ソフト株式会社

当社の社内システムに対する不正アクセスについて（最終報）

9 月 27 日からご報告しています当社社内システムへの不正アクセスに関しまして、第三者機関に協力いただきながら社内にて調査・緊急対策を進めるとともに、随時、関係機関やお客様に対してご報告を行ってまいりました。この度、調査が完了し、調査結果を踏まえて今回の不正アクセスの経緯、原因、再発防止策を下記の通りご報告いたします。

1. 経緯

調査の結果、今回の不正アクセスに関する一連の経緯が判明しました。

① 攻撃者により一部社員のアカウント／パスワード情報が盗まれました。これを起点に以下の 2 つの攻撃を受けました。

② 攻撃者により 6 名のアカウント／パスワードが利用されて社外から社内端末に侵入され、これを踏み台に、クラウド上に格納していた 20 ファイルが閲覧またはダウンロードされました。

③ 攻撃者によりパートナー会社向け教育サイトへ侵入され、バックドア設置を試行されました。

ただし、速やかに当社 SOC にて検知し、CSIRT が遮断したことにより被害を最小限に留めることができました。

2. 影響範囲

今回の不正アクセスにより影響を受けた範囲は、以下の通りです。

- 社員 6 名のアカウント／パスワードの悪用
- 社員 3 名の端末への侵害
- クラウド上に格納されていた当社作成の 20 ファイルの攻撃者による閲覧またはダウンロード
- パートナー会社向け教育サイトへの侵害

上記以外の端末、クラウドリソース、ファイルサーバ、お客様環境、当社標準開発環境、社内システム等については、影響はありませんでした。攻撃者に閲覧またはダウンロードされた 20 ファイルについては、全てが当社の作業上の資料であり、お客様から受領した資料やお客様に納品する資料は含まれておりません。

3. 原因

当社では、社外からのアクセスは多層防御を行っていますが、一部対応していないシステムが存在しました。また、一部の社員が攻撃者に推測可能なパスワードを使用していました。この二点が重なったことから攻撃者による不正アクセスを発生させてしまいました。

4. 再発防止策

今回の不正アクセスの発見を受け、暫定対処として、多層防御に対応していないシステムへの社外からのアクセスを停止するとともに、全社員のパスワードを強度が高いものへ変更しました。

また、侵害された端末・システムについては遮断・隔離の上、分析を行っており、利用再開に向けては対策を講じて再構築を行います。さらなる対処として、社外からアクセスされる全てのシステムへの多層防御の徹底、および攻撃のモニタリング強化を継続的に図っていきます。

今回の不正アクセスで用いられた攻撃手法の詳細については、これを模倣した攻撃による被害の発生を防ぐために公開を控えさせていただきますが、当社が加入するセキュリティ団体等を通じてセキュリティ関係者に共有を図ってまいります。当社の経験を通し、世の中の不正アクセスからの防衛とセキュリティ強化に貢献してまいります。

この度は、当社社内システムへの不正アクセスに関しまして、関係する皆様にご迷惑とご心配をおかけいたしましたことを心よりお詫び申し上げます。今後、同様の事態を起こさないよう、再発防止に努めるとともに、不正アクセスなどの犯罪行為には厳正に対処してまいります。

※1 SOC とは「Security Operation Center」の略称で、サイバー攻撃の検出・分析を行い、対応策のアドバイスなどを行う専門組織です。

※2 CSIRT とは「Computer Security Incident Response Team」の略称で、インシデント（サイバー攻撃によるセキュリティ事故）の予防及び発生後の迅速な対処を行うことを目的とした組織（機能）です。

以上

<お問い合わせ>
●ニュースリリースについて
コーポレートコミュニケーション部　広報窓口
URL：https://www.fsi.co.jp/
TEL：050-3000-2735
E-MAIL：mkoho@fsi.co.jp