2025年2月26日
東京都板橋区板橋4-2-3
株式会社ソーゴー

「弊社ファイルサーバへの不正アクセスによるサイバー攻撃に関する調査結果のご報告」

弊社社内にある複数台のファイルサーバが、第三者の不正アクセスによるサイバー攻撃を受けた件につきまして、多大なるご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。原因究明のための調査を続けてまいりましたが、専門の調査機関よりフォレンジック調査完了の報告を受け、下記の通り調査結果および今後の再発対策についてご報告いたします。

1. 事案の概要

2024年11月11日午前8時頃、弊社社員が社内に設置されているファイルサーバにアクセスできない旨の報告を受け確認を行なったところ、当該ファイルサーバが第三者の不正アクセスによるサイバー攻撃を受けたことが発覚しました。直ちに調査を開始し、警察への被害申告を行い、個人情報の漏洩の有無・原因究明、および復旧に向けて対応を進めておりました。

2. フォレンジック調査(※1)の結果について

専門調査機関によるフォレンジック調査の結果、2024年11月8日に初期侵入と想定される外部からの不正ログオン施行が確認されました。VPN機器の脆弱性を狙った不正アクセスである可能性が高いとのことでしたが、該当日付以前のログが消失していたこと、不正アクセスによって一部のデータの消失があったことなどから、VPN機器の脆弱性を介したサイバー攻撃であった可能性に留まり、原因の特定には至りませんでした。

3. ダークサイト調査(※2)の経過報告について

専門調査機関による調査を継続的に実施しておりますが、現時点で情報漏洩がされている事実はございません。現在も常時監視にて、万一情報漏洩が疑われる内容がダークサイト上で発見された場合は、アラートにより通知される体制としており、今後も継続して調査を続けてまいります。

4. 今後の再発防止に向けた取り組み

- (1) VPN 機能の停止並びにネットワーク機器のファームウェアアップデートの実施
- (2) 全 PC 端末およびサーバ端末へ EDR 製品の導入および監視体制の整備
- (3) セキュリティ専門会社の支援による現状のセキュリティ対策状況の網羅的な確認
- (4) 再発防止のためのセキュリティ運用体制の見直しおよび強化
- (5) 個人情報の取扱いルールの見直しおよび教育の実施

今回、明確な原因特定には至らなかったものの、想定される原因への対策として、ネットワーク機器のファームウェアアップデートを実施いたしました。また、セキュリティ専門会社からの支援を受け、今後、同様の被害を起こさないための組織づくりを進めております。

現在、業務で利用する PC 端末およびサーバ端末への EDR 製品(※3)の導入は完了しており、監視体制の仕組みは整えました。あわせて組織全体のセキュリティ状況における網羅的な確認も行い、追加で行うべき対策および組織体制の強化、教育の実施を進め、再発防止策に取り組んでまいります。

※1.コンピュータやデジタル媒体からデータを抽出・解析し、犯罪やセキュリティ侵害の証拠を 確認する科学的手法

※2.一般的な検索エンジンではアクセスできないダークウェブを対象にした違法活動や情報流出の監視・調査

※3.EDR (Endpoint Detection and Response) : 端末の不正な挙動を監視し、ウイルス感染の早期検知を目的とした
セキュリティ対策製品

5. お問い合わせ先

本件に関するお問い合わせは、下記窓口にて承ります。

株式会社ソーゴー 情報セキュリティ対策窓口

電話：0120-720-117

受付時間：平日 9:00～18:00

皆様には多大なるご心配とご迷惑をおかけしておりますことを深くお詫び申し上げます。
弊社は本事態を厳粛に受け止め、皆様の個人情報保護に全力で取り組んでまいります。
何卒ご理解とご協力を賜りますようお願い申し上げます。

また、今後、新たな調査結果が判明した場合には、弊社ホームページにて発表いたしますので、随時ご確認いただきますようお願い申し上げます。

以上