２０２６年4月8日

お客様、お取引先様　各位

エフワン株式会社

ランサムウェア攻撃に関するお知らせとお詫び（最終報）

本年１月３０日のランサムウェア攻撃に関する被害につき、侵入経路、手法が確定しましたのでご報告いたします。

当社は今回の被害を受け、外部調査機関にデジタルフォレンジック調査を依頼しました。調査は３月３日より行われ２３日に報告を受けました。その結果において判明した事と今後の対策についてご報告いたします。

ランサムウェアに関して

ランサムウェアは『Black Shrantac』と呼ばれるものと推定されます。２０２６年１月２９日午後１１時５０分頃から翌日３０日午前１時頃の間にサーバー内のファイルが暗号化され、拡張子が[,shrt]に変更され、脅迫文が残されていました。

侵入経路と被害事由

暗号化、及び被害が発覚する前、２０２６年１月２６日及び２８日の深夜に、外部より VPN 経由で不正なリモートデスクトップ接続が行われていた事が確認できました。侵入された機器は主に通信トラブル等が発生した際にバックアップの為に準備された回線と接続する物であり、該当機器のセキュリティーホールを衝き侵入される事に至ったと考えられます。更に該当機器の情報から管理者権限が漏洩し甚大な被害をうけました。

情報の漏洩

外部へのデータ送信等は今回の調査範囲に於いて確認ができませんでしたが、暗号化実行時にログが大量に発生し上書きが行われている事、一部ログそのものが暗号化された事、一部機器の再起動等が実行された事でメモリ上の情報が消失した事等で漏洩を否定する事ができません。３月６日に海外のサイバー脅威インテリジェンスの提供や、ダークウェブに流出していないかを監視するサイバーセキュリティ企業等が当社の事案を公開している事実を踏まえ漏洩があったと判断いたします。

個人情報に関しましては第２報で報告した通り、同一人物の重複を踏まえて約１７万件となります。誠に申し訳ございませんでした。

お客様におかれましては詐欺やなりすましのリスクが高まります。流出した情報を悪用した「なりすましメール」や「フィッシングメール」が送付される、不審な郵便物や電話がかかってくる可能性も否定できません。十分にご注意頂きますよう改めてお願いいたします。

今後の対策に関して

今回の被害を受け当社の情報セキュリティに関して下記の見直しを実施いたします。

- 機器の一新

  今回の事案で現存機器にウィルス等が残存している可能性を払拭する為、新しい機器への入替ます。

- リモートアクセスの管理強化

  認証設定に用いる方法に二段階認証等を用いる方法に変更します。

- 認証情報・アカウントの一新

  新たなアカウントの作成、パスワード強度を上げ等、適切に運用するようにいたします。

- ログ・監査の強化

  今回の被害を受け、ログ・監査情報の保存方法、保有期間、容量を見直します。

- OS・ファームウェア、ウィルス対策ソフト等の管理の徹底

  全ての機器の情報を定期的に検査し、最新の物に更新が行われるかを改めて管理します。

- その他

  セキュリティ教育の実施。インシデント発生時の組織的な対応方法の確立。

最後に

この事案については警察へ被害届の提出、法令に測り個人情報保護委員会へ報告を済ませております。又、第二報で記した様に、復旧は被害資産を戻すのではなく、新しく構築していく事となります。その為に、お客様、お取引様におかれましては、ご迷惑をお掛けする期間が長期に渡ると考えらえます。当社も可能な限り速度を以て対応していく所存ですので、ご理解、ご容赦賜りたくお願い申し上げます。

今回の件では、お客様、お取引様に多大なるご迷惑とご心配をおかけする事態となりましたことを、心より深くお詫び申し上げるとともに、再発防止に努めてまいります。

お問い合わせ

本件に関しましてご不明な点がございましたら、下記までご連絡頂きたく存じます。

エフワン株式会社　統括管理部

電話番号　06-6454-1222

E-mail　webmaster@f-one.co.jp

受付時間　午前１０時～午後４時半　※土日祝日を除く