2023 年 11 月 20 日

全国社会保険労務士会連合会御中

株式会社エムケイシステム

令和 5 年 11 月 10 日付、社労連第 637 号にて頂いたご質問につきまして、下記の通り回答いたします。尚、文書回答のみでは分かり辛い点、説明が不十分な点も多いと存じます。本件につきまして、別途説明会を実施させていただきたく、ご検討の程よろしくお願いいたします。

記

１.

弊社システムへの侵入の経緯等に関しましては、弊社から利用者の方に 6 月 28 日付でメールマガジンにて配布している資料 「項目５ ：侵害状況の概要」をご参照ください。

（ 添付資料：セキュリティに関する報告書 2023.6.28 発信）

２.

従前の仕様では、利用者のアクセス制限はグループポリシー等で権限を制限しておりましたが、侵入経緯の説明にある通り正規のログインから何らかの方法でドメインコントローラーに接続され、管理者権限を奪取されました。そのため改めてアクセス制御に対する対策を見直すことを対策として列挙させていただきました。

３.

従来のセキュリティパッチの適用運用は物理サーバー37 台、仮想サーバー278 台を人海戦術で実施しており、パッチ適用の完了まで 2 週間から 3 週間の時間を要しておりました。そのため、パッチ適用が完了するまでの間脆弱な状態が維持されることとなり今回の事態の要因の一つである可能性も否定できないと考えております。

今回の事例を受け、システムの基盤を AWS に移行することで OS を必要とするコンポーネントの大幅な減少、AWS のサービスを活用することによる脆弱性情報の取得および適用状況の可視化や自動化などが可能になりました。これにより短時間でパッチ適用が行われるようになり、システムが潜在的に持つ脆弱な状態を短縮することができております。

また、システム稼働再開するにあたりペネトレーションテストを実施することでアプリケーション起因の脆弱性を現時点でなくしております。

脆弱性は永久的にゼロになることはありませんので、定期的（半年に 1 回）に脆弱性診断を実施していくことで最新の脆弱性情報をもとに不具合がないかを点検していく予定です。

４．

強固な認証方法は多要素認証を意味しています。インシデント発生以前から有償にてワンタイムパスワード方式の多要素認証を取り扱いしておりましたが、多くのユーザーは ID/パスワード認証のみの認証方式でした。パスワードについても、初回パスワードの発行時は 8 桁のランダムな文字列を郵送にて利用者に配布しておりましたが、ユーザー側にてパスワード変更が可能なため、類推可能なものやパスワード強度が弱いものが存在していることを今回の件を契機に弊社を支援いただいているセキュリティ専門事業者から指摘を受けております。

これらの脆弱性を改善するため、

１）証明書発行サーバーによるデバイス認証による認証方式の無償提供

２）パスワードのポリシーを最低文字列 10 文字以上、英大文字・英小文字・数字・記号から 3 種類以上の文字列を必須とする運用に変更いたしました。

これらの対策により、

万が一、ID/パスワードの流出が発生した場合でもデバイスによる認証で接続元を制限することができるとともに、パスワードの複雑性が向上いたしました。

５．

システムのアカウント管理については請求処理と密接に関係するために削除、登録については厳密に管理しております。

ただ、ユーザーアカウントにおいて長期にわたってログインされていない有休アカウントの存在が確認できており、これらのアカウントについては契約が有効である以上弊社として勝手に操作をすることを控えている状況でありました。しかしながら今回の件で、6 か月以上アクセスの無い有休アカウントについては契約者の同意を得たうえでアカウントの無効化を実施し、再び利用する場合には弊社にて再有効化する運用に変更しております。

６．

インシデント発生前のログレビューは、弊社と契約している SOC サービス事業者とネットワークログのリアルタイム監視とログの分析結果について 4 半期ごとにレビューを実施しておりました。しかしながら今回のインシデント発生により監視の粒度、対象、間隔に課題があることが判明し、ログレビューを根底から見直すことと致しました。

具体的には、SOC 監視サービス事業者を変更し WAF、EDR など通信およびコンポーネントもリアルタイムで監視し、毎月レポートを発行してもらう体制に変更しています。

７．

インシデント発生から 2 か月を経過していない状況の中で発表させていただいた対策であって、基礎的な内容であり、短期間で実施できるものが中心となっております。

中長期的には、CIS Controlv8 をベースに対策を進めているところです。また、ISMS 27001 を取得し社内および提供サービスのセキュリティ維持管理に努めております。

以上