取引先各位

2020 年 11 月 27 日

株式会社サイダス

弊社 WEB サイトへのハッキングについて

2020 年 10 月 11 日より、弊社の公式 WEB サイト（https://www.cydas.com/）にマルウェアが混入していることが発覚し、対応を行いました。件の概要についてまとめます。

発覚の経緯

2020 年 10 月 26 日、2020 年 10 月第 2 週（10 月 8 日～14 日）サイトへのアクセス数（オーガニックサーチ経由での流入セッション数）が、過去 3 週間の移動平均線より大きく乖離していることを発見しました。さらに、アクセス先のページを調査した結果、マルウェアによって意図しないページが WEB サイト内に作成されていることが判明しました。

特定された被害の範囲と内容

アクセスログを解析した結果、特定の管理者ユーザーへのリスト型攻撃により CMS の管理画面へアクセスされていたことが判明しました。これにより、ディレクトリの一部が改竄され、マルウェアによって意図しないページが WEB サイト内に作成されていました。

このマルウェアは、意図しないページを作成することにより検索流入を不正な形で増やし、Google 等の検索エンジンからのペナルティを受けさせることを目的としたもので、個人情報、その他機密情報の流出を目的としたものではありませんでした。

また、この攻撃は、WEB サイトの管理画面に対するものであり、弊社が提供するクラウドサービス（CYDAS HR、CYDAS PEOPLE ほか）や、弊社が保有する情報資産とは完全に切り離された領域へのものです。**そのため、個人情報や営業の機密等、情報資産の流出等の影響はありません。**

対応の時系列

- 10 月 26 日 18:00

問題の特定

- 10 月 26 日 21:00

被害範囲と内容の特定

- 10 月 26 日 21:30

対応と対策の実施

- 10 月 27 日～

再発防止策の検討と恒久対策の実施

対応と対策について

- 改竄が確認されたファイルの削除
- すべてのユーザーのパスワードのリセット
- リスト型攻撃、ブルートフォース攻撃によって突破されない認証情報の設定