ランサムウェアに対する防御
PCI Security Standards Councilのリソースガイド

ランサムウェアとは、最も急激に増大しているマルウェアです。

ランサムウェアは、コンピュータファイルを盗んだり、企業のシステムやネットワークへのアクセスを妨害したりして、身代金を要求するマルウェアの一種です。ランサムウェアによる攻撃は、業務の中断による経済損失や、重要情報及びデータの損失、まは漏洩を引き起こすおそれがあります。[1]

1　出典:FBI

リスクを理解する

Cybersecurity Ventures 社の最新レポートによれば、世界のランサムウェアの経済的損失は、２０２１年には ２００億ドル に達すると予想されています。[2]

ランサムウェアの攻撃から復旧するまでにかかる総額費用の平均は、2020年の761,106ドルから2021年には. 185万ドル と2倍以上に増えています。[3]

産業界、政府、非営利団体、学会から60名以上の専門家が参加するランサムウエア作業部会によると、ランサムウェアの攻撃から企業活動が完全に復旧するには、平均 287日 かかるとのことです。[4]

2:出典:Cybersecurity Ventures Report (サイバーセキュリティ ベンチャーズ レポート)　3:出典:Sophos State of Ransomware Report 2021 (ソフォスランサムウェア現状レポート2021年度版) 4:出典:Ransomware Task Force (ランサムウェア作業部会)

攻撃

フィッシングは、昨年の違反事案の中でみられた「アクション・バリエーション」のうち、トップを占めており、違反事案の 43% は、フィッシング又はなりすましによるものでした。[5]

フィッシングメール

フィッシング メールは、マルウエアに感染させる常套手段です。これらの電子メールは、請求書や電子ファックスなど一見すると適法なものに見えますが、悪意のあるリンクや添付ファイルが含まれており、あなたのコンピュータやシステムがウイルスに感染するおそれがあります。[5]

内部アプリケーションの脆弱性の50パーセントが高リスクまたは致命的なリスクであると懸念されています。[6]

ウェブサイトやソフトウェアの脆弱性

犯罪者は、ウェブサイトにランサムウェアを仕込み、ソフトウェアの脆弱性を悪用して旧型のソフトウェア(ブラウザやブラウザのプラグイン)を使用している訪問者に攻撃を仕掛けます。

5:出典:Deloitte Cyber Intelligence Centre (デロイトサイバーインテリジェンスセンター) による報告) 6:出典:Vulnerability Statistics Report 2021 (脆弱性統計レポート2021年度版)

PCI Security Standards Council

あなたのビジネスを守る

ご注意ください

従業員の教育。PCI DSS 12.6

- このような攻撃を回避するための最善の方法及び発生した場合の認識方法や対応方法について従業員を教育する計画を立ててください。
- リスクを認識して、不審に思った時は、メールを削除して構わないことを理解しているか確認してください。
- クリックする前に確認してください。電子メールは、社内の誰かから送られてきたものであるかのようにみせかけることが可能です。疑問がある場合は、リンクをクリックしたり、ファイルを開く前に担当者に必ず確認してください。

危険に備えて警戒してください

システムをテストしてください。PCI DSS 11.3

- 最近、簡単に侵入されないかどうかシステムを確認しましたか？犯罪者は執拗なので、あなたも執拗にならなければなりません。
- 脆弱性は、犯罪者が侵入することができる「壊れた」ドアを作ってしまいます。悪意のある人物があなたのシステムに侵入することを防止するため、テストで見つかった脆弱性を修正し、他の管理も行うことが重要です。

パッチを最新のものに更新してください。PCI DSS 6.2

- 決済システムや他のシステムの問題を解決するために、ベンダーは、「パッチ」を送ってきます。
- 決済システムやソフトウェアのベンダーが送ってきた新しいセキュリティ用のパッチを最後に確認したのはいつですか？
- パッチは、犯罪者があなたのシステムに侵入するドアを塞ぎます。ベンダーの指示に従って、可能な限り迅速にパッチをインストールしてください。

不審なアクティビティを監視してください。PCI DSS 11.5

- 現在、システムの変更を監視していますか？不審な変更や不正、または未承認の変更を調査しましたか？
- システムの変更を調査することで、承認又は認可していない変更を誰かが行った時に知ることができます。変化が生じたら、すぐに調査することで、問題をより迅速に発見し、攻撃をシャットダウンする可能性を高めることができます。
- 変更管理プロセスは、変更が承認されるかどうかを判断するのに役立ちます。もし、変更が承認されなかった場合や不明の場合は、システムがウイルスに感染していないかどうか速やかに確認すべきです。

システムをバックアップしてください。PCI DSS 9.5.1, 12.10.1

- バックアップをする際は、以前の良好なバックアップを上書きしないよう注意してください。これは、ランサムウェアによって暗号化されたデータをバックアップし、良好なバックアップを上書きしてしまうことを防ぐことに役立つかもしれません。どのようなバックアップ方法であっても、定期的にディスク全体のバックアップと、追加されたバックアップ(前回のバックアップ以降に新しくなったデータのみをバックアップ)することは、最良の慣行です。
- リスクを軽減するために、バックアップデータをオンラインの状態(バックアップされるシステムに接続したままの状態)にしておくことは避けるべきです。代わりに、バックアップデータをオフサイトのオフラインで保存してください(バックアップを「クラウド」に保存することは、オフライン保存の一般的な方法ですが、最後の箇条書きを参照してください)。これにより、ランサムウェアによって身代金を要求されたとしても、最新のバックアップを簡単に復元することができます。
- 複数の世代のバックアップを保存し、あなたの組織がランサムウェアを検出する能力や古い記録を使用し、再構築する能力に応じた保存期間を設定してください。
- 最近、パックアップが完全にされているか確認しましたか？最近、バックアップとリカバリーのプロセスを確認しましたか？ランサムウェアによってシステムがロックされてしまった場合、バックアップからデータを復元できるか確認することは必須です。
- クラウドのバックアップを使用する際には、クラウドサービスのプロバイダがあらゆる種類のマルウェアからの保護に努めていることを確認してください。クラウドのストレージは、永続的な同期を行うバックアップシステムに接続されている場合、攻撃者によってロックされる可能性もあります。

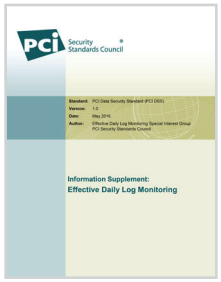
計画を立てる

準備しましょう。PCI DSS 12.10

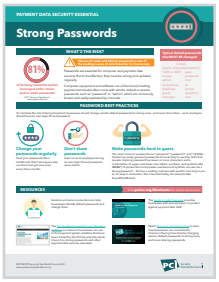
- あなたと貴社の従業員は、攻撃にどう対処するか、誰に連絡するかなど、攻撃が起きた時にどのように対応するかについて知っておくべきです。
- 計画を立て、従業員にそれを伝えましょう。
- この計画を定期的に見直し、スタッフの教育に継続的に取り組んでください。

PCIの詳細な参考資料

PCIデータ セキュリティ基準 バージョン3.2.1

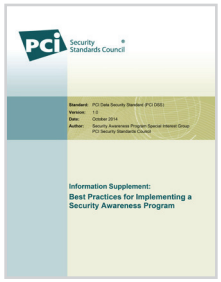


情報の補足:効果的なデイリーログのモニタリング



決済データ・セキュリティ・エッセンシャル:強力なパスワード

決済データ・セキュリティ・エッセンシャル:パッチをインストールする



セキュリティ意識向上プログラムの導入に対する最善慣行

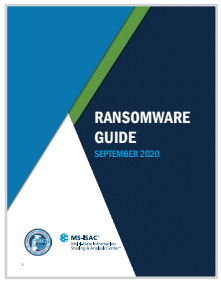
小規模加盟店のための決済保護リソース:安全な決済のためのガイド

関連業界資料

次のランサムウェアの犠牲者にはならないでください。あなたの組織の保護に役立つ最善慣行。

ランサムウェア:その内容と対処方法

ランサムウェア撲滅プロジェクト



CISA MS-ISAC ランサムウェアガイド

専門家のコメント及び質問は press@pcisecuritystandards.org までご連絡ください。
PCI基準及びリソースに関する詳しい情報は www.pcisecuritystandards.org をご確認ください。