2023 年 6 月 2 日

Venture Solution

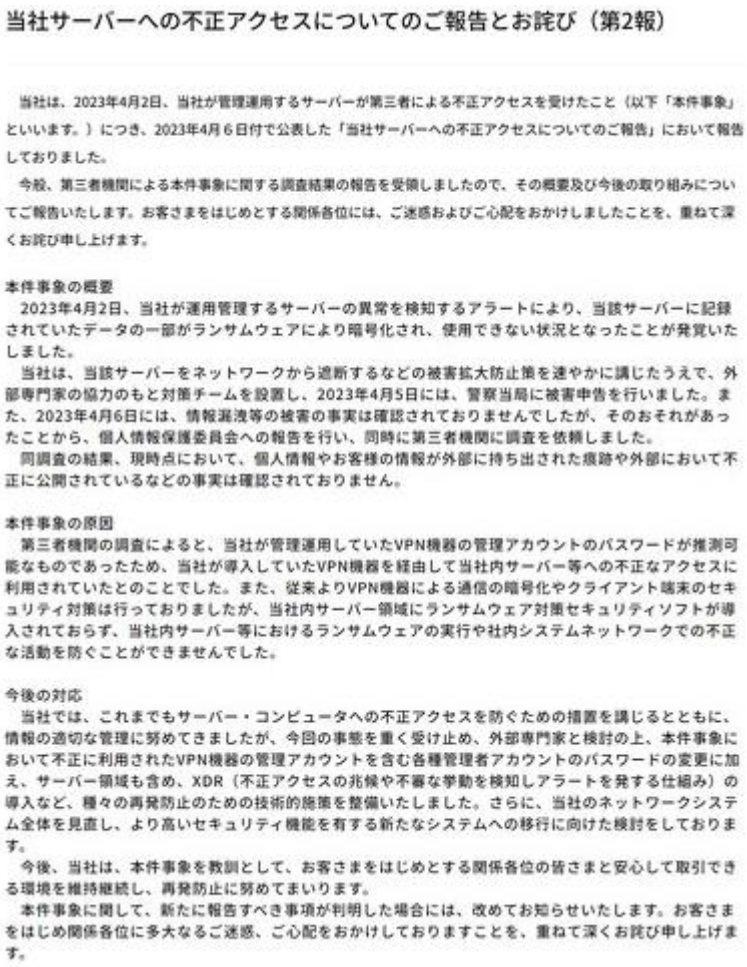
コラム記事

働き方改革や新型コロナウイルスの影響により、人々の働き方は大きく変化しております。
特に 2~3 年の中での変化として真っ先に挙げられることは「リモートワーク」ではないでしょうか。
企業によっては、全社員リモート対応としてオフィス費用を削減していたり、ワークライフバランス向上のために積極的に導入していたり、様々な変化をつくることで独自の社風を形成している企業も多く存在すると伺っております。
このリモートワークを支えているシステムの 1 つが VPN です。
そんな中、VPN を経由して社内サーバが不正アクセスを受けた記事が掲載されておりましたので、ご紹介いたします。

「推測可能な VPN パスワード」でランサムウェア被害 村本建設

（ITmedia NEWS 2023/6/2(金) 12：11 配信 より引用）
村本建設は、4 月に同社のサーバが不正アクセスを受け、データが暗号化されるランサムウェア攻撃を受けた原因の調査結果を、5 月 31 日付で発表した。

VPN 機器の管理アカウントのパスワードが推測可能なものだったため、VPN を経由して社内サーバが不正アクセスされたという。



当社サーバーへの不正アクセスについてのご報告とお詫び（第2報）

当社は、2023年4月2日、当社が管理運用するサーバーが第三者による不正アクセスを受けたこと（以下「本件事象」といいます。）につき、2023年4月６日付で公表した「当社サーバーへの不正アクセスについてのご報告」において報告しておりました。
今般、第三者機関による本件事象に関する調査結果の報告を受領しましたので、その概要及び今後の取り組みについてご報告いたします。お客さまをはじめとする関係各位には、ご迷惑およびご心配をおかけしましたことを、重ねて深くお詫び申し上げます。

本件事象の概要
2023年4月2日、当社が運用管理するサーバーの異常を検知するアラートにより、当該サーバーに記録されていたデータの一部がランサムウェアにより暗号化され、使用できない状況となったことが発覚いたしました。
当社は、当該サーバーをネットワークから遮断するなどの被害拡大防止策を速やかに講じたうえで、外部専門家の協力のもと対策チームを設置し、2023年4月5日には、警察当局に被害申告を行いました。また、2023年4月6日には、情報漏洩等の被害の事実は確認されておりませんでしたが、そのおそれがあったことから、個人情報保護委員会への報告を行い、同時に第三者機関に調査を依頼しました。
同調査の結果、現時点において、個人情報やお客様の情報が外部に持ち出された痕跡や外部において不正に公開されているなどの事実は確認されておりません。

本件事象の原因
第三者機関の調査によると、当社が管理運用していたVPN機器の管理アカウントのパスワードが推測可能なものであったため、当社が導入していたVPN機器を経由して当社内サーバー等への不正なアクセスに利用されていたとのことでした。また、従来よりVPN機器による通信の暗号化やクライアント端末のセキュリティ対策は行っておりましたが、当社内サーバー領域にランサムウェア対策セキュリティソフトが導入されておらず、当社内サーバー等におけるランサムウェアの実行や社内システムネットワークでの不正な活動を防ぐことができませんでした。

今後の対応
当社では、これまでもサーバー・コンピュータへの不正アクセスを防ぐための措置を講じるとともに、情報の適切な管理に努めてきましたが、今回の事態を重く受け止め、外部専門家と検討の上、本件事象において不正に利用されたVPN機器の管理アカウントを含む各種管理者アカウントのパスワードの変更に加え、サーバー領域も含め、XDR（不正アクセスの兆候や不審な挙動を検知しアラートを発する仕組み）の導入など、種々の再発防止のための技術的施策を整備いたしました。さらに、当社のネットワークシステム全体を見直し、より高いセキュリティ機能を有する新たなシステムへの移行に向けた検討をしております。
今後、当社は、本件事象を教訓として、お客さまをはじめとする関係各位の皆さまと安心して取引できる環境を維持継続し、再発防止に努めてまいります。
本件事象に関して、新たに報告すべき事項が判明した場合には、改めてお知らせいたします。お客さまをはじめ関係各位に多大なるご迷惑、ご心配をおかけしておりますことを、重ねて深くお詫び申し上げます。

（ITmedia NEWS 2023/6/2(金) 12：11 配信より引用）

攻撃は 4 月 2 日に発覚。同社が運用するサーバに記録されていたデータの一部がランサムウェアにより暗号化され、使用できない状況になった。

第三者機関の調査によると、同社が運用していた VPN 機器の管理アカウントのパスワードが推測可能なものだったため、VPN 機器を経由して社内サーバに不正アクセスされたという。

社内サーバは、ランサムウェア対策やセキュリティソフトの導入がされておらず、ランサムウェアの実行を防げなかったという。

個人情報や顧客情報が外部に持ち出された痕跡や、外部で不正公開されているといった事実は確認していないという。

再発防止策として、VPN 機器を含む各種管理者アカウントのパスワードの変更、サーバ領域も含めた不正アクセス検知システム（XDR）の導入などを行った他、ネットワークシステム全体を見直し、高セキュリティな環境に移行することを検討している。

今回ご紹介した記事については、VPN 機器の管理アカウントパスワードが推測可能であったことが原因とされていますが、どれだけ難解なパスワードを設定していても、VPN 等が感染経路となり不正アクセス被害にあってしまったとの公表事例は後を絶ちません。

また、VPN や認証技術の脆弱性を利用されてランサムウェアなどに感染してしまう事例も多く報告されています。
働き方が変化してきたからこそ、改めてセキュリティ対策、特に侵入を防ぐと言ったような観点で対策を講じることが重要であると考えます。