半径300メートルのIT:

テレワークかどうかは、もはや関係ない？　三菱重工のインシデント報告から学べる「IT管理者あるある」な反省点

https://www.itmedia.co.jp/enterprise/articles/2008/18/news040.html

テレワークが普及する中、セキュリティ対策に追われる組織や企業は多いのではないでしょうか。三菱重工が公開したインシデントレポートは、まさにテレワーク「あるある」の状況で起こった攻撃を明らかにしています。しかし、その中で挙がった要因の一つは、テレワーク以前にどうにかできたはずで、多くの組織で放置されがちなものでした。

2020年08月18日 07時00分 更新

[宮田健, ITmedia]

ほぼ全ての企業がPCとネットワークを活用し、何らかのITシステムを使っています。インターネットに接続する可能性があれば、そこにはインシデントが発生する可能性も存在します。

最近ではサイバー攻撃を受けることも当たり前になりつつありますが、インシデントが発生したあとにしっかりとその被害状況に関してのレポートも公開されるようになりました。表に出てくるレポートだけでなく、サイバー脅威情報を共有する「ISAC」（Information Sharing and Analysis Center）と呼ばれる機関の中では、さらに濃い情報が飛び交っているはず。不利とされる「守る側」も、正しく進化しています。

本コラムでもそのようなサイバー攻撃に関する被害レポートを取り上げることが増えました。ただこれは「攻撃を受けるとは情けない」と言いたいからではありません。被害を無駄にせず「レポートを自分ごととして受け止めて欲しい」という狙いがあります。今回も必ず皆さんの役に立つであろう、不正アクセスのレポートを取り上げたいと思います。

インシデントレポートを読む――三菱重工の場合

今回“教材”として取り上げるのは、2020年8月7日に公開された三菱重工のインシデントレポートです。

三菱重工が2020年8月に発表したインシデントレポート。不正アクセスを発見、対応したいきさつをまとめています（出典：三菱重工）

このレポートは、三菱重工名古屋地区のサーバと外部との間で不正な通信があったことを報告し、その原因を明らかにしています。重要な情報の流出はなく、その意味では軽微なインシデントだったかもしれません。ただ、内容を見るとPCやサーバを利用している全ての組織において、考えるべきポイントがあります。

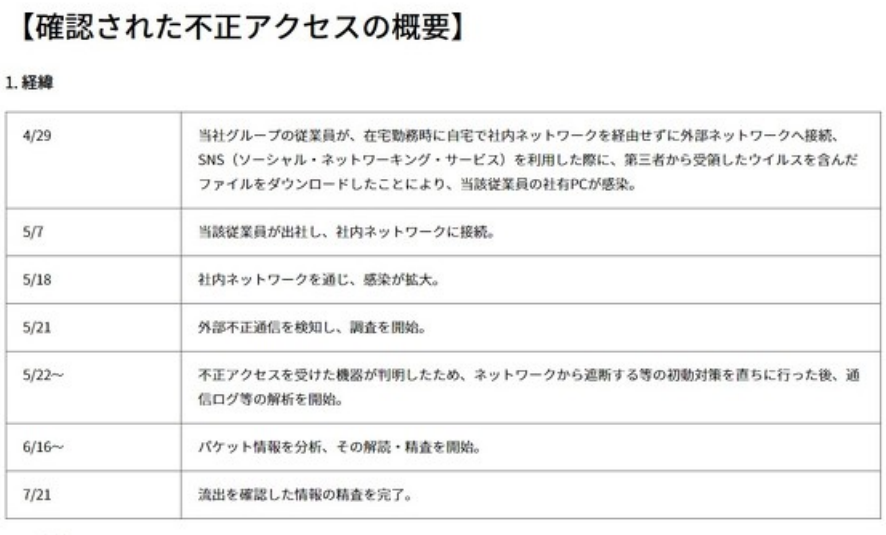
インシデントが発生したのは2020年4月29日で、同社がそれに気付いたのは5月21日でした。検知にはそれなりに時間がかかっているとも捉えられますが、個人的にはしっかりと検知できていること自体、素晴らしいと思いました。その中で気になった点は2つあります。

社用PCが自宅に存在する「テレワーク」が穴に？

まずは侵入経路です。きっかけは、社用PCからのSNS利用でした。

> 当社グループの従業員が、在宅勤務時に自宅で社内ネットワークを経由せずに外部ネットワークへ接続、SNS（ソーシャル・ネットワーキング・サービス）を利用した際に、第三者から受領したウイルスを含んだファイルをダウンロードしたことにより、当該従業員の社有PCが感染。

レポートによれば、SNSにおいて第三者からウイルスを含んだファイルを受領、ダウンロードしたこと（恐らくファイルを実行したという意味）で社用PCが感染しました。感染したPCの持ち主はその後5月7日に“出社”したとありますので、テレワーク主体だったというわけではなさそうです。社用PCがオフィスの外でウイルスに感染し、それが社内に持ち込まれるという、非常に典型的な事例であるといえます。



【確認された不正アクセスの概要】

1. 経緯

4/29	当社グループの従業員が、在宅勤務時に自宅で社内ネットワークを経由せずに外部ネットワークへ接続、SNS（ソーシャル・ネットワーキング・サービス）を利用した際に、第三者から受領したウイルスを含んだファイルをダウンロードしたことにより、当該従業員の社有PCが感染。
5/7	当該従業員が出社し、社内ネットワークに接続。
5/18	社内ネットワークを通じ、感染が拡大。
5/21	外部不正通信を検知し、調査を開始。
5/22～	不正アクセスを受けた機器が判明したため、ネットワークから遮断する等の初動対策を直ちに行った後、通信ログ等の解析を開始。
6/16～	パケット情報を分析、その解読・精査を開始。
7/21	流出を確認した情報の精査を完了。

インシデント対応の流れをまとめたレポートの一部（出典：三菱重工）

テレワークを実施している組織なら、同じような事態が発生する可能性は非常に高いでしょう。ポリシーとしてSNSの利用を禁止するのは簡単ですが、制度で従業員の行動を制限するよりは、ITの仕組みで防いだ方が、やはり確実かと思います。

三菱重工は今回の侵入を受けた今後の対策として「強制的に社内ネットワークを経由する処置（VPN強制接続）を適用」したとしています。さらにリスクを低減しようとするならば、SIMを直接差し込めるモバイルPCを導入し、4Gからインターネットを経由しない閉域網ネットワークを活用することになるでしょう。「今後はモバイルPCの調達戦略も大きく変わるのではないか」と私は考えています。

レポートに記された「IT側にもあった落ち度」こそ、誰もが見直すべき理由

そしてもっとも注目すべきは、今回明らかになったSNS以外の要因です。その一つは、多くの人にとって覚えがありそうな“ITを管理する側の落ち度”でした。

> 影響範囲が当該従業員の社有PCから他機器に広がった要因として、同地区の一部のサーバのローカル特権アカウントに対し、同じパスワードが設定されていたことが考えられます。
>
> （特権アカウントを悪用され他機器にログインされたものと考えております。）これらに対し、ローカル特権アカウントのパスワードを全て異なるものに変更する対策を実施済みです。

これは、ウイルスに感染した社用PC内から読み取られたパスワードと、サーバの特権アカウント（administratorやrootなど）のパスワードが同じだった、つまり「パスワードの使い回しがあった」ということです。パスワードの使い回しは、どのよ

うな場合であっても推奨できるものではありません。特権アカウントならばなおさらです。これは、本当によろしくないことではあるのですが、本コラムをお読みの方も思わず目をそむけてしまう「あるある」なのではないでしょうか（私も目をそむけながらこの文章を書いています……）。

　これこそ、三菱重工のインシデントレポートが教えてくれる「あなたにも今日からできる対策」です。この事故を無駄にしないためにも、まずは特権アカウントのパスワードだけでも使い回しをしないよう、設定を見直してみてください。もちろん、サーバの管理者アカウントが「共有」されている場合は、その運用を見直すことを強くお勧めします。

人のインシデントを冷笑する前に

　自分が“普通”だと思っていることが、実は普通ではなかったーー。そんなことが、世の中には往々にしてあります。セキュリティの常識も、誰もが“当たり前”だと思っていながら、きちんとそれに沿った対策ができていないというのが現状でしょう。そのため、こういった事件、事故の原因を読むと、人ごとのように「なぜこんな単純なことができていないのだ！」と思ってしまうのではないでしょうか。自分の組織が全く同じことをしているかもしれない可能性を棚に上げながら……。

　ですので、こういったレポートを見たときには、どんなに原因が単純だったとしても、人ごととは思わず「もしも自分だったら？」と考えてみることが重要です。ぜひ、このレポートを読み直し、そこから自分ごととして学べることはないか、もう一度チェックしてみてください。きっと今日から改善できる点が見つかるはずです。その小さな一歩こそが、自分の周囲の世界をもっと安全にする最初のステップになるはずです。