ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●三菱電機に不正アクセス…個人情報約8,000人分等流出か

https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html
https://tech.nikkeibp.co.jp/atcl/nxt/news/18/06880/
http://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf

このニュースをザックリ言うと・・・

- 1月20日(日本時間)、三菱電機より、同社ネットワークが不正アクセスを受け、個人情報および企業機密が流出した可能性があると発表されました。

- 被害を受けた個人情報はのべ8,122人分で、内訳は2011年以降の採用応募者1,987人、2012年時点の従業員4,566人、および関連会社の退職者1,569人とされています。

- 2019年6月に社内端末が不審な挙動を認識したことから不正アクセスが発覚しており、朝日新聞の報道では機密情報に触れる権限が広い中間管理職層のPCが主なターゲットとなったとされ、国内外120台超のPCおよび40台超のサーバーに不正に侵入された痕跡があるとしています。

AUS便りからの所感等

- 同社では速やかに外部からのアクセス制限等の対策および関係機関への報告を行っており、また社会インフラに関する機微、機密性の高い技術情報および取引先に関わる重要な情報は流出していないとしています。

- 不正アクセスは、同社が利用していたウイルス対策システムのセキュリティパッチ公開前の脆弱性を突かれたことが原因としていますが、アンチウイルス・UTMのようなセキュリティプロダクト自身に存在する脆弱性への対応は他のアプリケーションよりもさらに速やかに行われるべきであり、それが間に合わない間に攻撃を受けたことは痛恨と言えるでしょう。

- 監視や検知をすり抜ける高度な攻撃かつ一部端末においてログが消去され調査に時間がかかる等の事態が発生したとのことですが、もし一つのセキュリティソリューションが破られた場合にこのように攻撃者の好き放題にされてしまうことのないよう、複数のベンダーを選んだり、ネットワーク構成についても考慮したりといった、多重の防衛の実施が重要でしょう。

日経 XTECH

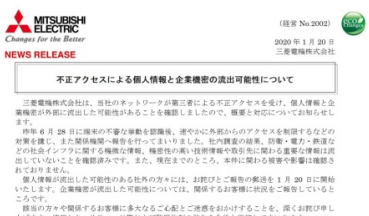
2020/01/20 20:00

ニュース

8000人の個人情報が流出した三菱電機の不正アクセス被害、採用応募者も含まれる

玄 忠雄＝日経 xTECH／日経コンピュータ　日経 XTECH

三菱電機は2020年1月20日、同日に同社が明らかにした2019年6月に把握した不正アクセスで、最大8122人の個人情報が流出した可能性がある発表した。8122人には同社の関係者以外に、社外の採用応募者も含まれていた。流出した可能性がある社外の人には報告とおわびの文書の送付を同日から開始し、電話による問い合わせの専用窓口も設けた。


MITSUBISHI ELECTRIC
Changes for the Better
NEWS RELEASE
(経営 No.2002)
2020 年 1 月 20 日
三菱電機株式会社
不正アクセスによる個人情報と企業機密の流出可能性について
三菱電機株式会社は、当社のネットワークが第三者による不正アクセスを受け、個人情報と企業機密が外部に流出した可能性があることを確認しましたので、概要と対応についてお知らせします。
昨年 6 月 28 日に端末の不審な挙動を認識後、速やかに外部からのアクセスを制限するなどの対策を講じ、また関係機関へ報告を行ってまいりました。社内調査の結果、防衛・電力・鉄道などの社会インフラに関する機微な情報、機密性の高い技術情報や取引先に関わる重要な情報は流出していないことを確認済みです。また、現在までのところ、本件に関わる被害や影響は確認されておりません。
個人情報が流出した可能性のある社外の方々には、お詫びとご報告の郵送を 1 月 20 日に開始いたします。企業機密が流出した可能性については、関係するお客様に状況をご報告しているところです。
該当の方々や関係するお客様に多大なるご心配とご迷惑をおかけすることを、深くお詫び申し上げます。情報セキュリティー対策および監視体制の強化を今後も継続してまいります。
確認された不正アクセスの概要
1. 概要

流出した個人情報の概要を公表した三菱電機の発表文
出所：三菱電機
[画像のクリックで拡大表示]

MITSUBISHI ELECTRIC
Changes for the Better

(経営 No.2002)

2020 年 1 月 20 日
三菱電機株式会社

NEWS RELEASE

不正アクセスによる個人情報と企業機密の流出可能性について

三菱電機株式会社は、当社のネットワークが第三者による不正アクセスを受け、個人情報と企業機密が外部に流出した可能性があることを確認しましたので、概要と対応についてお知らせします。

昨年 6 月 28 日に端末の不審な挙動を認識後、速やかに外部からのアクセスを制限するなどの対策を講じ、また関係機関へ報告を行ってまいりました。社内調査の結果、防衛・電力・鉄道などの社会インフラに関する機微な情報、機密性の高い技術情報や取引先に関わる重要な情報は流出していないことを確認済みです。また、現在までのところ、本件に関わる被害や影響は確認されておりません。

個人情報が流出した可能性のある社外の方々には、お詫びとご報告の郵送を 1 月 20 日に開始いたします。企業機密が流出した可能性については、関係するお客様に状況をご報告しているところです。

該当の方々や関係するお客様に多大なるご心配とご迷惑をおかけすることを、深くお詫び申し上げます。情報セキュリティー対策および監視体制の強化を今後も継続してまいります。

確認された不正アクセスの概要

1. 概要

昨年 6 月 28 日に、当社内端末で不審な挙動を検知し調査した結果、第三者による不正アクセスを受け、外部にデータを送信されていたことが分かりました。監視や検知をすり抜ける高度な手法であり、かつ一部の端末において、送信されたファイルを特定するためのログ（操作記録）が攻撃者によって消去されていたため調査に時間を要しました。不正アクセスにより、個人情報と企業機密が外部に流出した可能性があることが分かりました。なお、関係機関にはご報告済みです。

●中学校生徒等約1,200人分の個人情報が入ったUSBメモリー一時紛失…千葉県

http://www.chibanippo.co.jp/news/national/661290

このニュースをザックリ言うと・・・

- 1月22日(日本時間)、千葉県教育委員会より、山武市立中学校の生徒等のべ1,239人分の個人情報が入ったUSBメモリーを一時紛失する事案が昨年11月に発生していたと発表されました。

- USBメモリーは同中学の教諭の私物で、出張先の県総合教育センター(千葉市)にメモリーが入ったポーチが置き忘れられていましたが、同センター職員が見つけ中学校に連絡されていたとのことです。

- 教諭が勤務してきた中学校3校の生徒、職員の氏名・成績および学校行事の写真等が保存されていましたが、流出はなかったとされています。

AUS便りからの所感

- 県教育委員会によれば、昨年8月にも別の教諭がUSBメモリーを紛失する事案が発生しており、その際の再発防止策として県立校と各市町村教委に私物USBデバイスの校内持ち込み禁止および過去データの消去の徹底が指示されていました。

- 紛失のリスクが高い私物のUSBメモリーを持ち込み禁止にした結果、結局はその状況での情報の取り扱いが不便であったことから結局密かに使われてしまったものと推測されますが、こういったルール違反あるいはそれによる情報漏洩が発生する可能性を抑えるには、データ保存時の暗号化をはじめとした、適切に管理された有用な代替手段を提供することが大事と言えるでしょう。

千葉日報

生徒情報のＵＳＢ紛失　千葉県教委、中学教諭を減給処分

2020年1月23日 05:00 | 無料公開

千葉県教委は２２日、生徒ら延べ１２３９人分の個人情報を入れた私物のＵＳＢメモリーを一時紛失したとして、山武市立中学校の男性教諭（３４）を減給１０分の１（１カ月）の懲戒処分にした。

県教委は昨年８月に別の教諭がＵＳＢを紛失した際に、再発防止策として県立校と各市町村教委に私物ＵＳＢの校内持ち込み禁止と過去データの消去を徹底するよう指示。男性教諭も校長から使用状況の確認を受けたが、所持していないと回答し、過去のデータも消去していなかった。

県教委教職員課によると、教諭は昨年１１月２１日に出張先の県総合教育センター（千葉市美浜区）にＵＳＢを入れたポーチを置き忘れた。同センターの職員が見つけ、教諭の勤務先の校長に連絡して発覚。ＵＳＢには教諭が勤務してきた中学校３校の生徒、職員の氏名や成績、学校行事の写真などを保存していた。情報流出はないという。

県教委は、私物ＵＳＢの持ち込み禁止と過去データの消去を徹底するよう各校、各市町村教委に改めて通知した。本年度の懲戒処分は監督責任を除き１６件目。

●チェックポイント社の月例レポート、最も危険なマルウェアは3ヶ月連続で「Emotet」に

https://scan.netsecurity.ne.jp/article/2020/01/23/43575.html

このニュースをザックリ言うと・・・

- 1月21日(日本時間)、セキュリティベンダーのチェック・ポイント・ソフトウェア・テクノロジーズ(以下チェックポイント)社より、2019年12月度の月例レポート「Global Threat Index(世界の脅威指標)」が発表されました。

- 「最も危険なマルウェア」はインターネットバンキングを狙う等様々な行動をとる「Emotet」が3ヶ月連続でトップとなっており、12月には環境運動家グレタ・トゥーンベリ氏のサポート呼び掛けを騙るスパムメール等での拡散が確認されたとしています。

- この他「最も危険なモバイルマルウェア」は不正な広告を表示する「xHelper」をはじめAndroidに感染するものがトップ3に、「エクスプロイト数が最も多かった脆弱性」では「HTTPを介したOSコマンドインジェクション」がトップとなっています。

AUS便りからの所感

- Emotetは2019年9月以降一貫して頻繁な活動を続けていますが、前述のようなインターネットバンキングを狙う以外にも、他のマルウェアの媒介となったり、感染したPC上のメールデータ等を読み込んでなりすましメールを送信したり(AUS便り2019/12/09号参照)と、刻々と手口を変容させています。

- マルウェアを含めたネット上で発生している攻撃について随時情報収集や啓発を行うとともに、アンチウイルスやUTM等による侵入防止、PC自体のソフトウェアアップデート等による感染防止等の防御策を確実に固める体制が整っているか、適宜確認することが肝要です。

ScanNetSecurity

マルウェアは「Emotet」が3カ月連続でトップに--月例レポート（チェック・ポイント）

チェック・ポイントは、2019年12月の「Global Threat Index（世界の脅威指標）」を発表した。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社（チェック・ポイント）は1月21日、2019年12月の「Global Threat Index（世界の脅威指標）」を発表した。レポートによると、12月は「Emotet」が「Support Greta Thunberg - Time Person of the Year 2019（2019年の今年の人に選ばれたグレタさんを応援しよう！）」と「Christmas Party!」を含む各種のスパムメール キャンペーンを使って拡散されていた。

もっと「チェック・ポイント」のニュース
「非公開」動画も公開、「TikTok」の脆弱性を発…
標的型ランサムウェア、モバイル、5G、AIなど20…
ボットネット「Emotet」が3カ月ぶりに活動を再…
編集部にメッセージを送る

12月の「もっとも危険な」マルウェアの上位3種は、「Emotet」「XMRig」「Trickbot」となり、「Emotet」が3カ月連続でトップのマルウェア脅威となった。Emotetは12月に世界中の企業や組織のうち13%（11月は9%）に影響を及ぼし、XMRigとTrickbotはそれぞれ企業や組織の7%に影響を及ぼした。