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。

●公開Webサイトのセキュリティ診断、殆どのサイトで何らかの脆弱性あり…IPA発表

https://scan.netsecurity.ne.jp/article/2021/06/10/45800.html
https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html

このニュースをザックリ言うと･･･

- 6月7日(日本時間)、IPAより、中小企業向けサイバーセキュリティ対策支援体制構築事業「サイバーセキュリティお助け隊」の、2020年度の実証実験に関する成果報告が発表されました。

- 同事業は2019年度にも実施されていたもので、今回は全国13地域および2産業分野の計1,117社の中小企業が実証に参加(2019年度は8地域・1,064社)、これらの企業に対しUTMやEDR(Endpoint Detection and Response)ソフトウェア等のセキュリティ機器を導入することにより実態を把握、計293件のインシデント対応他技術支援を実施したとのことです。

- 中小企業のセイバーセキュリティ対策の実態に関するまとめとして、インターネット上に公開しているホームページ・サービスサイト等の脆弱性診断において、対象企業の殆どで何らかの脆弱性が発見され、うち概ね2割の企業においては重大なインシデントに繋がる可能性があると診断された、等としています。

AUS便りからの所感等

- 発見された脆弱性の詳細は公開されていませんが、例えばWordPressのようなCMS(コンテンツ管理システム)あるいはECサイト構築ソフトウェア等を用いてWebサイトを立ち上げた後、ソフトウェアのアップデートを適切に行っていないケースは依然として多いとみられます。

- また、UTM等の設置により、外部からのクロスサイトスクリプティングやSQLインジェクションをはじめとするWebサイトへの攻撃、あるいは内部からのボットネット等との通信を検知したとする報告も挙がっており、多くの中小企業が実際に攻撃のターゲットとされている実情が窺い知れます。

- 2021年以降、同事業は民間でのサービス展開に移行するとしていますが、セキュリティ対策に対し多くの中小企業が最低限の予算しかかけていない、また支払い可能な金額として月額1万円程度と回答している実情に対し、セキュリティの底上げについてどういった方策がとられるか注目されるところです。

ScanNetSecurity by iid　　IPA

公開Webサイトのほとんどに何らかの脆弱性 ～ IPA 2020年度サイバーセキュリティお助け隊報告書から

独立行政法人情報処理推進機構（IPA）は6月7日、サイバーセキュリティお助け隊（令和2（2020）年度中小企業向けサイバーセキュリティ対策支援体制構築事業）の報告書について公開した。

シェア　ツイート　送る

独立行政法人情報処理推進機構（IPA）は6月7日、サイバーセキュリティお助け隊（令和2（2020）年度中小企業向けサイバーセキュリティ対策支援体制構築事業）の報告書について公開した。

IPAでは2019年度に続き2020年度も、中小企業のサイバーセキュリティ対策を支援する仕組みの構築を目的とした、全国13地域・2産業分野の中小企業を対象に、損害保険会社、ITベンダー、セキュリティ企業、地域の団体等が実施体制を組み、実証事業（サイバーセキュリティお助け隊）を実施。

IPAでは本事業を通じ、中小企業のセキュリティ対策の促進や意識喚起、攻撃実態や対策ニーズ把握を行い、対応範囲や費用等の必要なセキュリティ対策の内容とマーケティング方法や支援体制、中小企業等向けのサイバーセキュリティ対策の一つとして提供するセキュリティ簡易保険サービスのあり方、実証終了後のサービス提供の可能性等の検討を行い、報告書にまとめ公開した。

サイバーセキュリティお助け隊（令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業）の報告書について

掲載日　2021年6月7日
独立行政法人情報処理推進機構
セキュリティセンター　企画部
中小企業支援グループ

事業概要

2019年度（令和元年度）に引き続き2020年度（令和2年度）においても、中小企業のサイバーセキュリティ対策を支援する仕組みの構築を目的とし、全国13地域・2産業分野の中小企業を対象に、損害保険会社、ITベンダー、セキュリティ企業、地域の団体等が実施体制を組み、実証事業（サイバーセキュリティお助け隊）を実施しました。
本事業の実施を通じて、中小企業のセキュリティ対策の促進や意識喚起、攻撃実態や対策ニーズ把握を行い、中小企業等に必要なセキュリティ対策の内容（対応範囲や費用等）、マーケティング方法や支援体制、中小企業等向けのサイバーセキュリティ対策の一つとして提供するセキュリティ簡易保険サービスのあり方、実証終了後のサービス提供の可能性等の検討を行い、報告書にまとめました。

全体まとめ

中小企業のセイバーセキュリティ対策の実態

- 本実証事業においても、2019年度事業と同様に、**業種や規模を問わずサイバー攻撃の脅威にさらされており**、ウイルス対策ソフト等の既存対策だけでは防ぎきれていない実態が明らかとなった。
- インシデント対応ほか技術的支援は、2020年度は新型コロナウイルス感染症拡大の影響もあり、当初からリモートによる管理可能なサービス提供が多く行われたこともあり、**概ねリモートによる支援対応**となった。
- インターネット上に公開しているホームページやサービスサイト等の脆弱性診断において、対象企業のほとんどで何らかの脆弱性（弱点）が発見された。加えて、そのうち概ね**2割の企業**においては**重大なインシデントに繋がる可能性があると診断**された。
- セキュリティ対策上の課題としては、**専門人材の不足**、社員や専門人材に対する**教育**がなされていない、**費用**を捻出することが困難といった声が寄せられた。
- セキュリティ対策について予算は全くかけていない、あるいは最低限のみ対策費用をかけているという企業が多かった。セキュリティ対策に支払可能な金額としては、**月額1万円程度**と回答する中小企業が多かった。

●不正アクセスで個人情報40万件流出、3年半後に脅迫メールで発覚-

https://www.itmedia.co.jp/news/articles/2106/08/news095.html
https://www.yupiteru.co.jp/corp/important/210607.html

このニュースをザックリ言うと･･･

- 6月7日、自動車向け無線通信機器等を取り扱うユピテル社より、同社サーバーが2017年に不正アクセスを受けた際に、会員サイト「My Yupiteru」利用者の個人情報が流出していたと発表されました。

- 被害を受けたとされるのは、2017年10月以前に会員登録された405,576人分の個人情報(住所・氏名・性別・生年月日・電話番号・メールアドレス)とのことです(クレジットカード情報は保有していなかったため、対象外とのことです)。

- 今年5月になって当時の犯人とみられる相手から金銭を要求する脅迫メールを受信し、メールに記載されたリンク先において、流出したとみられる個人情報の存在を確認したことから、警察に被害の届出を行い、今回の発表となったとのことです。

AUS便りからの所感

- 2017年に不正アクセスを受けた時点では、それ自体は検知していたものの、データがダウンロードされた形跡までは確認できなかったことから、同社では発表をしていなかったとしており、これに対し流出の可能性の発表を早期に行わなかったことを指摘する声もあります。

- サーバー上の各種ソフトウェアを最新に保つことはもちろんですが、外部からの不審なアクセス、内部から外部への正規でない通信によるデータ流出について確実に検知し遮断できるよう、UTMの設置やサーバー上へのソリューションの導入あるいはサーバー自身の適切な設定を検討することが重要と言えます。

ITmedia NEWS

ユピテル、40万人分の会員情報流出　不正アクセス確認から3年以上報告せず、脅迫メール受信で公開

2021年06月08日 12時26分 公開　[ITmedia]

印刷　1144　Share　B! 91

自動車用品などを手掛けるユピテル（東京都港区）は6月7日、2017年10月にサーバが不正アクセスを受け、同社が運営する会員サイト「My Yupiteru」に登録する約40万人分の個人情報が外部に流出したと発表した。攻撃者とみられる人物から、金銭要求の脅迫メールを受信していることも併せて公表した。クレジットカード情報は含まれておらず、7日時点で、個人情報の悪用も確認されていない。

事態が急転したのは、不正アクセスから約3年半後の21年5月。社員が攻撃者とみられる人物からのメールを受信。文面を確認すると「2017年末にサーバをハッキングし、顧客情報を持っている」とする文面とともに「私はお金が必要です。私は金銭を尋ねます。入手した情報を競合他社に渡します。彼らは購入するでしょう。私はあなたのために2週間待ちます」（原文ママ）と金銭を要求する記載があった。メールに記載されたリンク先に、約52万件のデータを確認した。

●チケット購入者411人分のメールアドレス流出…中止メールに全員分のアドレス表示

https://www.at-s.com/news/article/shizuoka/912873.html
http://k-kousya.or.jp/

このニュースをザックリ言うと･･･

- 6月8日(日本時間)、掛川市文化財団より、同市内で開催予定だったイベントのチケット購入者411人分のメールアドレスが誤って外部に流出したと発表されました。

- 発表によれば、同日にイベント中止のお知らせをチケット購入者にメールで一斉送信した際、他の送信先全員のメールアドレスが表示される設定となっていたとのことです。

- メールを受信したチケット購入者からの指摘で流出が発覚し、同財団では対象となる全員に謝罪の連絡をし、メールを削除するよう依頼しているとのことです。

AUS便りからの所感

- メール送信の際に宛先のアドレスを、送信されたメールには表示されない「Bcc:」ではなく「Cc:」に入れて送ったものと考えられます。

- 大量のメールアドレスをCc: やTo: に入れてしまうという事故は専らメーラーから手入力でメールを送信しようとした場合に発生するものであり、このような潜在的リスクの高い単純な方法をとるのではなく、メーリングリストやメール配信サービス等、同報メール送信のためのシステムを導入すること、どうしてもメーラーで対応せざるを得ない場合はメーラー自身あるいはアドオンで提供される誤送信防止機能を有効にすることが肝要です。

あなたの静岡新聞

メールアドレス４１１人分が漏えい　掛川市文化財団

2021.6.9

掛川市文化財団は８日、市内で開催予定だった講談のチケット購入者４１１人に開催中止を伝える電子メールを一斉送信した際、ほかの送信先全員のメールアドレスが表示される設定で送ってしまうミスがあったと発表した。財団は個人情報の漏えい事案として全員に謝罪の連絡をし、メールの削除を依頼している。メールを受信した購入者から指摘があり、設定ミスに気づいたという。