— AUS（アルテミス・ユーザ・サポート）便り 2018/10/09号 —
https://www.artemis-jp.com

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。

●3社に1社でサイバー攻撃…KPMGが調査結果を発表

https://www.nikkei.com/article/DGXMZO35830110X20C18A9000000/
https://enterprisezine.jp/article/detail/11214

このニュースをザックリ言うと・・・

- 9月26日（日本時間）、KPMGコンサルティング社より、企業のサイバーセキュリティにまつわる実態調査「KPMG サイバーセキュリティサーベイ 2018」の結果が発表されました。

- 回答した企業のうち31.3%が「サイバー攻撃あるいは不正侵入の痕跡を発見した」とし、ほぼ3社に1社が攻撃を受けたとされています。

- そのうち8割以上の不正侵入については自社内部で検出できたと回答しており、内訳としては
◆サイバーセキュリティ部門による監視（31.4%）
◆社員からの通報（31.4%）
◆委託先ITベンダーからの通報（24.8%）
となっています。

- これについての前年からの変化として、「サイバーセキュリティ部門による監視というきっかけが増えてきた」「企業内でセキュリティー対策が進み不正侵入の検知率が上がっている」としています。

AUS便りからの所感等

- 見方を変えれば、十分なセキュリティ対策を行い、攻撃を受けたことを確認できたのがあくまで31.3%であり、それ以外の企業において気付かれないままに攻撃を受けている可能性も考えられます。

- この他にもセキュリティ対策への投資については、投資額が増加したと回答した企業が38.0%、投資額が不足しているとする回答も65.0%に上り、また「投資対効果がわからない(48.0%)」「どれだけ投資すべきかわからない(45.0%)」との回答もあったとされています。

- それでも今日においては「我が社はターゲットにはならない」と思い込んで何も対策しないということは決してせず、現時点でできる対策があれが一通り実施し、以後も少しでも意味や効果のある対策を取り入れるよう検討を続けて頂ければ幸いです。

日本経済新聞

3社に1社でサイバー攻撃、KPMGが調査結果

科学&新技術 BP速報
2018/9/27 23:00

保存 共有 印刷 その他

日経XTECH

KPMGコンサルティングは2018年9月26日、企業のサイバーセキュリティーにまつわる実態調査「KPMG サイバーセキュリティサーベイ 2018」の結果を発表した。3社に1社がサイバー攻撃を受けていることが分かった。

具体的には回答した企業全「（自社内で）不正侵入の と答えた。KPMGコンサル 執行役員パートナーによる 年同様の調査をしてきたが は例年とほぼ同じになった バー攻撃が高度化して、企 リティー対策を巧みにすり 析する。

不正侵入に気付いたきっかけについての質問では「自社内部での発見」が全体の87.6%を占めた。この内訳で前年との変化が見えた。「昨年は社員からの通報がきっかけとして最も多かったが、今年の調査ではサイバーセキュリティー部門による監視というきっかけが増えてきた。企業内でセキュリティー対策が進み、不正侵入の検知率が上がっている」と、大西武史ディレクターはみる。

調査ではこのほかセキュリティー対策への投資額の増減を聞いたところ、約95%の企業が前年並みか、前年より増加傾向にあると分かった。しかし、「投資対効果や適切な投資額が分からない」「投資が不足している」といった課題を抱える企業も少なくなかったという。「セキュリティー対策の投資対効果などについては、定性的ではなく、適切なKPI（重要業績評価指標）を設定して定量的に把握していく取り組みが今後必要になる」と田口執行役員は指摘する。

今回の調査は国内の上場企業と売上高が400億円以上の未上場企業を対象に、2018年4月から5月にかけて、セキュリティー対策コンサルティングを手掛けるラックと共同で実施した。8192社にアンケートを依頼して、329社から回答を得て結果をまとめた。

EnterpriseZine
データテクノロジー／情報セキュリティ ITリーダー向け専門メディア

6割の国内企業でセキュリティ投資と人材不足が課題に――KPMGサイバーセキュリティサーベイ2018

サイバーセキュリティ

33 4 G+0 B! 2 7 プッシュ通知

EnterpriseZine編集部[著] 2018/09/26 18:30

KPMGコンサルティング株式会社は2018年9月26日、国内の上場企業および売上高400億円以上の未上場企業を対象に実施した、企業のサイバーセキュリティに関する実態調査の結果をまとめたレポート「KPMGサイバーセキュリティサーベイ2018」を発表した。

EnterpriseZine

同社の発表によると、回答 イバーセキュリティ部門、社 らかになったという。

同社が発表した「KPMGサイバーセキュリティサーベイ2018」の主な調査結果は次の通り。

- 回答企業の31.3%が、過去1年間でサイバー攻撃あるいは不正侵入があったと回答
- 不正侵入に気づいたきっかけは、「サイバーセキュリティ部門による監視（31.4%）」、「社員からの通報（31.4%）」、「委託先ITベンダーからの通報（24.8%）」。8割以上が自組織内で不正侵入を検出できている
- サイバーセキュリティ対策への投資額については、38.0%が増加と回答している。しかし、投資額に対しては「大いに不足している（13.0%）」、「やや不足している（52.0%）」とも回答しており、投資額が適切であるとの評価は3割程度に留まる
- CSIRT（Computer Security Incident Response Team、シーサート）の設置に関しては、「設置済み（27.4%）」と「今後の設置予定（7.3%）」を合わせても3割程度に留まる
- 「サイバーセキュリティ経営ガイドラインVer 2.0」で言及されている事件発生時の経営報告・広報などの組織対応の実践的な演習については「十分にできている（4.0%）」、「ある程度できている（25.9%）」を合わせて3割弱に留まる
- サイバーセキュリティ対策に取り組むえでの課題として、「知見のある実務担当者が足りない」が59.9%と半数以上が回答。セキュリティ人材の不足が最も大きな課題としてとらえられている
- 「投資対効果がわからない（48.0%）」、「どれだけ投資すべきかわからない（45.0%）」と投資に関する課題も上位に

●福島信金Webサイトが一時改ざん被害…外部サイト誘導で不正ツールをダウンロード

https://www.nikkei.com/article/DGXMZO36058840T01C18A0000000/

このニュースをザックリ言うと･･･

- 9月28日（日本時間）、福島信用金庫より、同信金のWebサイトが改ざんの被害を受けていたことが発表されました。

- 発表によれば、Webサイトの一部ページへのアクセスにより外部Webサイトに誘導され、誘導先において「Windowsシステムが古くなり破損していることが検出されました。」というメッセージと共に不正なツールをダウンロードするよう表示されていたとのことで、さらにこのツールの実行によりフリーダイヤルへ電話するよう誘導され、カード情報を詐取される可能性があったとしています。

- 同信金では9月26日に改ざんに関する連絡を受け、現在は修正されているとのことです。

AUS便りからの所感等

- サイト作成を委託された業者が不正アクセスを受けたことが改ざんの原因とされています。

- ソフトウェアの開発において、開発者のアカウントを乗っ取る等の行為により、配布物にマルウェアを混入させることを「サプライチェーン攻撃」と呼びますが、今回のケースは「Webサーバ自体に直接攻撃を行う以外の経路で行われた」ことから、それに似通っていると言えます。

- いずれにしろWebサイトを閲覧する側にとっては、いつ訪問したサイトに仕掛けられた罠で攻撃を受けるかわからないものと心得て、アンチウイルスやWebブラウザおよびUTMのセキュリティ機能を有効にして防御を確実に行うことが肝要です。


日本經濟新聞

福島信金HP改ざん被害　別サイト誘導、県警が捜査

社会

2018/10/3 11:06

福島信用金庫（福島市）は3日までに、ホームページ（HP）が不正アクセスを受け、改ざんされたと発表した。修正しており、現在問題はない。相談を受けた福島県警は、不正アクセス禁止法違反容疑で捜査を始めた。

信金によると、HPの「店舗一覧」「ふくしんこども応援賞」にアクセスすると「システムが古くなり破損していることが検出された」と表示される。修正のためにソフトをダウンロードするよう指示され実行するとフリーダイヤルに電話するよう誘導されるという。

実際に電話すると、カード情報を聞き取るなどの詐欺被害に遭う可能性があるとしている。これまでに被害は確認されていない。

サーバー管理会社からの連絡で9月26日に発覚。信金は、HP作成を委託した企業が不正アクセスされ、HPに被害が出たとみており「お客さまにご迷惑をお掛けしないよう、セキュリティーを強化する」と話した。（共同）

●新潟大学でフィッシングによるメールアカウント乗っ取り…スパムメール送信の他、個人情報漏洩の可能性も

https://www.niigata-u.ac.jp/news/2018/47488/

このニュースをザックリ言うと･･･

- 9月27日（日本時間）、新潟大学より、同大学職員の複数のメールアカウントが不正アクセスにより乗っ取られたと発表されました。

- 発表によれば、4月17日～5月14日に職員に対しメール管理者をかたるフィッシングメールが送信され、同学のメールシステムに偽装したフィッシングサイトでパスワードを入力した教職員6名がアカウントを乗っ取られたとのことで、被害を受けたうち2名のメールアドレスから約36万件のスパムメールが送信された他、3名のメールボックスにあった学内関係者の名簿・メールアドレス等の個人情報のべ116件にアクセスされた可能性があると発表されています。

- 既に不正アクセスを受けたメールアカウントは停止し、教職員に対しパスワード変更や不審なメールに関する注意喚起等を行う、等の対応をとったとしています。

AUS便りからの所感等

- 今年4月～6月、複数の国公私立大学で同様の事件が発生し、のべ1万件以上の個人情報の流出が発表されており、このときは「Office 365」が提供するメールシステム上のアカウントが奪取されましたが、今回がその一環であるかについては不明です。

- マルウェアへの感染等でも言えますが、単に「ユーザが気を付ける」だけではなく、サーバ側・クライアント側共に利用できる対策を確実に行うこと、あるいはUTMを含めた新たなソリューションを導入すること、ブラウザやセキュリティソフト等のアンチフィッシング機能、システムが2段階認証（多要素認証）を提供しているならば可能な限りそれらを有効にしフィッシングに備えること、等が肝要です。


新潟大學

新潟大学におけるフィッシングメール被害による情報漏洩の可能性及び迷惑メール送信に関するお詫びについて

2018年09月27日 木曜日　お知らせ

本学の電子メール管理者を装ったフィッシングメールにより複数の電子メールアカウントのパスワードが窃取され、不正アクセスを受ける事案が発生しました。一部の電子メールアカウントのメールボックス内には個人情報を含む情報があったことが判明しており、アカウントの利用を停止するまでの間、攻撃者が覗き見ることが可能な状態になっていました。また、不正アクセスを受けた電子メールアカウントの一部からは迷惑メールが送信されました。

現時点では、個人情報漏洩の被害報告は確認されておりませんが、関係者の皆様に多大なご心配をお掛けする事態を招いたことを、深くお詫び申し上げます。