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。

●中小企業のセキュリティ支援「サイバーセキュリティお助け隊」の実証実験開始

https://cybersecurity-jp.com/news/31742
https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

このニュースをザックリ言うと・・・

- 6月4日（日本時間）、情報処理推進機構（IPA）より、中小企業のサイバーセキュリティ対策支援を行う「サイバーセキュリティお助け隊」の実証事業について発表されました。

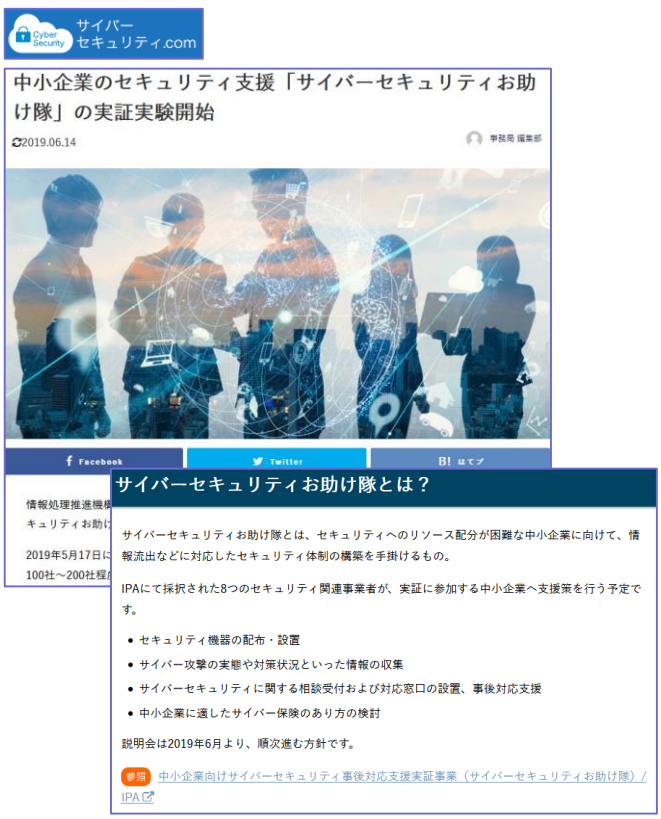
- IPAでは、「サプライチェーン」を構成する中小企業のサイバーセキュリティ対策の強化について、我が国の産業に対する世界の信頼に直結する重要な課題であるとしています。

- 8地域15府県の中小企業を対象として、サイバーセキュリティに関する悩みや、対策のニーズ、サイバー攻撃被害の実態等を把握するとともに、サイバーインシデントが発生した際の支援体制の構築等に向けた実証を行うとしており、IPAにて採択された8つのセキュリティ関連事業者が実証に参加する中小企業へ支援策を行う予定です。

AUS便りからの所感等

- 大企業のみならず中小企業においてもサイバー攻撃を受ける可能性があることは言うまでもありませんが、攻撃者がターゲット企業を介し、そことやり取りを行っている企業へ、マルウェアの伝播を含めたさらなる攻撃を行うこと等に着目しているものと考えられます。

- 今回の実証事業の対象となる地域は限定的なものですが、その結果に基づいて実施地域が拡大され、最終的には全国の中小企業におけるセキュリティ強度の底上げに貢献するよう期待したいものです。



●Windowsではパスワードの定期的な再設定は不要…MSが改定へ

https://japan.zdnet.com/article/35138170/

このニュースをザックリ言うと・・・

- 5月23日（現地時間）、マイクロソフト（MS）より、Windows 10（およびWindows Server）のセキュリティベースラインにおいて、「パスワードに期限を設定すべき」としていた推奨事項を削除する意向が発表されました。

- 同社では「定期的なパスワードの失効はパスワード(またはハッシュ)が有効期間中に盗まれ不正な主体によって使用される場合に対する防御にしかならない。そもそもパスワードが盗まれなければ失効させる必要もない。また、パスワードが盗まれたことを示す証拠があればおそらく有効期限が来て失効するのを待つよりも直ちに行動する方が問題を解決するためには望ましい」等と説明しています。

- 一方で同社では、以前より「パスワードは企業にとって不便であり、安全性が低く、コストが高い」と主張しており、複数の形態の認証手段やバイオメトリクス（生体認証）に置き換えられるべきともしています。

AUS便りからの所感等


ZDNet Japan

Windowsではパスワードの定期的な再設定は不要--MSがガイドラインの改定へ

Steve Ranger（ZDNet.com） 翻訳校正：石橋啓一郎 2019年06月11日 06時30分

いいね！215 B! 59 Pocket 53

印刷 メール ダウンロード クリップ

パスワードに有効期限を設定することは、ユーザーアカウントを保護する方法としては時代遅れであり、有害無益だとさえ言えるかも知れない。30日か60日ごとにパスワードの変更を迫られることは、新しいパスワードをひねり出して覚えておかなければならないユーザーにとって頭痛の種である上に、セキュリティの向上にもほとんど役に立たない。

今ではMicrosoftもスタンスを変え、「Windows 10」と「Windows Server」のセキュリティベースラインに含まれていた、パスワードに期限を設定すべきであるという推奨事項を削除することになった。米ZDNetのLiam Tung記者が別の記事でも書いた通り、Microsoftは、新しいガイドラインのドラフトを公表する際、有効期限に関するポリシーを廃止する意向を明らかにした。

- ほんの数年前まで、パスワードは「定期的に変更すべき」という意見が強く、国内の多くのセキュリティ機関で推奨事項とされていましたが、頻繁な変更の要求に対しユーザが簡単なパスワードを設定してしまうという問題も指摘されていました。

- 特に2014年、複数のサイトで同じパスワードを設定していたユーザが連鎖的に不正ログインの被害を受ける事件が多発したことにより、パスワード管理に関するこれまでのセオリーの見直しが進み、2018年には総務省やPマーク認定機関等も定期的な変更を推奨する方針から転換しています。

- 多くの社内システムにおいては、依然IDとパスワードの入力によりログオンする形式をとっていると思われますが、その中でも、パスワードの管理等についても改善を行える箇所はきっとあるはずですので、適宜見直しを行って頂ければ幸いです。

●フィッシング対策協議会、「フィッシングレポート」「フィッシング対策ガイドライン」2019年度版を公開

https://www.antiphishing.jp/report/wg/phishing_report2019.html
https://www.antiphishing.jp/news/info/guideline2019.html

このニュースをザックリ言うと・・・

- 5月29日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、フィッシングの被害状況、フィッシングの攻撃技術・手法等をとりまとめた「フィッシングレポート」および「フィッシング対策ガイドライン」の2019年度版が公開されました。

- レポートによれば、フィッシング届出件数は2018年3月以降急激に上昇して以降比較的高い水準で推移しており、フィッシングサイトのURL件数およびブランドを悪用された企業の件数も増加傾向にある、等としています。

- ガイドラインについては事業者向けと利用者向けがそれぞれ用意されており、昨今のフィッシング動向を反映して内容が改訂されています。

AUS便りからの所感等


フィッシング対策協議会
Council of Anti-Phishing Japan

資料公開：フィッシングレポート 2019 の概要について

2019年05月29日

フィッシング対策協議会の技術・制度検討ワーキンググループでは、フィッシングの被害状況、フィッシングの攻撃技術・手法などをとりまとめた「フィッシングレポート 2019」を公開しました。

■本レポートの主な内容は以下のとおりです。

資料公開：フィッシング対策ガイドラインの改訂のお知らせ

2019年05月29日

フィッシング対策協議会の技術・制度検討ワーキンググループでは、2018 年度のフィッシング動向や新しい対策技術等をふまえ、事業者向けと利用者向けのフィッシング対策ガイドラインをそれぞれ改訂し、2019 年度版として公開いたしました。

詳細は以下 URL をご覧ください。

- ガイドラインでは、利用者として「フィッシングに引っかからないための対策」だけでなく、Webサイト運営者として「被害の発生を抑制するための対策」「被害の発生を迅速に検知するための対策」および「被害が発生してしまった際の対策」等にも言及されています。

- 例えば、「被害の発生を抑制するための対策」において「利用者が正規メールとフィッシングメールを判別可能とする」ために推奨されている対策だけでも多くの項目が挙げられています。

- ともあれ、ガイドラインを一通り読み込み、実施可能な対策から順次実行を検討していくこと、また対策の実施にあたっては、適宜ホスティングやクラウドサービスと契約することも視野に入れるのが良いでしょう。