— AUS（アルテミス・ユーザ・サポート）便り 2019/11/18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。

●大学卒業生等のべ1,201人分等の個人情報漏洩…Webサイトアクセス制限の設定ミス

https://this.kiji.is/565362452952958049
https://www3.nhk.or.jp/news/html/20191108/k10012169481000.html
https://www.muroran-it.ac.jp/guidance/news/post-22733.html

このニュースをザックリ言うと･･･

- 11月8日(日本時間)、室蘭工業大学より、同大学Webサーバーにおいて卒業生の一部等の個人情報が閲覧可能状態にあったと発表されました。

- 対象となるのは、2006～2013年度に在籍していた学生の一部にあたる1,187名の氏名・所属・成績およびメールアドレス等、および2013年に設置されたコースの外部評価委員会委員14名の氏名・所属等とされています。

- 同学では、9月18日にWebサーバーの設定変更を行った際の設定ミスにより閲覧可能状態となっていたとし、10月11日に外部からの指摘を受け対策を行った上で、対象となる卒業生等に個別に事情を説明しているとのことです。

AUS便りからの所感等

- 一部報道によれば、本来パスワードによるアクセス制限がかけられるべきところ、パスワードが設定されておらず公開状態になっていた模様で、個人情報の他、教職員が使用する会議資料も含まれていたとされています。

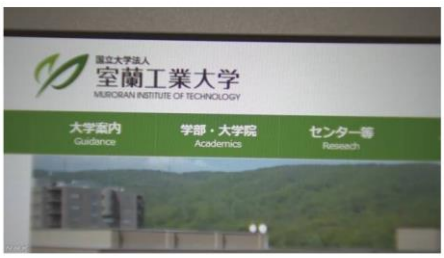
- 90年代～2000年代には、個人情報やWebフォームから入力されたアンケート回答のデータ等を含むファイルがWebサーバのドキュメントルート(DocumentRoot)以下に保存され、やはりWebからアクセス可能な状態にあったケースも頻繁に報告されていました(ディレクトリ情報が表示される設定になっていたことにより、そういったデータが保存されているディレクトリが見つけやすい状態にあったケースも珍しくありません)。

- 機密情報に対する第三者からのアクセスを防ぐため、「ディレクトリ情報を表示しないようにする等セキュアな設定を確実に行う」「パスワードにはくれぐれもすぐに推測されるような文字列を設定しない」「外部から機密情報を見つけようとする形跡がないか、随時アクセスログの確認・分析を行う」等が対策や注意点として挙げられますが、実施したアクセス制限等が機能しているかの確認のためには、とにかく「実際にアクセスしてチェックする(IPアドレスベースでの制限時は、管理者がいるネットワーク以外からもアクセスする)」ことを決して怠ってはいけません。

学生1187人分の成績など 一時誰でも閲覧可能の状態 室蘭工業大

2019年11月8日 13時54分

北海道室蘭市にある室蘭工業大学で、平成18年度から25年度に在籍していた学生のうち、1187人分の成績やメールアドレスなどの個人情報が一時、大学のホームページで誰でも閲覧できる状態になっていたことが分かりました。



室蘭工業大学によりますと先月11日、「自分の名前や成績が大学のホームページで閲覧できる」と卒業生から指摘され、詳しく調べたところ、平成18年度から25年度に在籍していた学生のうち、1187人分の名前や成績、メールアドレスなどが、大学のホームページで誰でも閲覧できる状態になっていたということです。

2019.11.08. / 大学案内

本学Ｗｅｂサーバからの個人情報の漏えいについて（お詫び）

関係各位

令和元年１１月８日
室蘭工業大学長　空閑　良壽

令和元年10月11日（金）、外部からの通報により、本学のＷｅｂサーバ上で個人情報が外部から閲覧できる状態になっていたことが判明しました。

該当のページには、平成18～25年度に本学に在籍されていた学生1,187名（建築社会基盤系学科及び建築社会基盤系専攻に所属されていた方の一部）の氏名、所属、成績等と、平成25年度に本学が設置した土木コースの外部評価委員会委員等の14名の氏名と所属等の個人情報が掲載されておりました。

調査の結果、本件の原因となるＷｅｂサーバの設定変更を行った令和元年9月18日（水）から、10月11日（金）に該当のページを閲覧不可にする措置を講ずるまでの間において、外部から閲覧できる状態となっていたことが明らかになりました。

なお、現時点において、本件の個人情報が不正に使用された事実は確認されておりません。

該当される方については、本学から順次ご連絡を差し上げ、事情を説明の上、謝罪させていただいております。

本学では、これまで全職員に対し、個人情報を含む情報管理のための研修等を行ってまいりましたが、今回、このような問題が発生したことは、極めて重大なことであると受け止めており、関係の皆様に多大なご迷惑をおかけしたことを深くお詫び申し上げます。今後はこのようなことが起こらないよう、改めて個人情報を含む情報管理の徹底に努めてまいります。

●Windowsの脆弱性「BlueKeep」を悪用した攻撃開始か…MSも警告

https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/
https://wired.jp/2019/11/05/bluekeep-hacking-cryptocurrency-mining/
https://japan.cnet.com/article/35145189/

このニュースをザックリ言うと･･･

- 11月2日(現地時間)、イギリスのセキュリティ研究者より、Windowsの脆弱性「BlueKeep」を悪用しPCをマルウェアに感染させる攻撃を確認したと発表されました。

- BlueKeepはWindows 7以前のリモートデスクトップサービス(RDS)に存在する脆弱性で、今年5月にMicrosoft(以下MS)より修正パッチがリリースされています(AUS便り 2019/5/20号参照)。

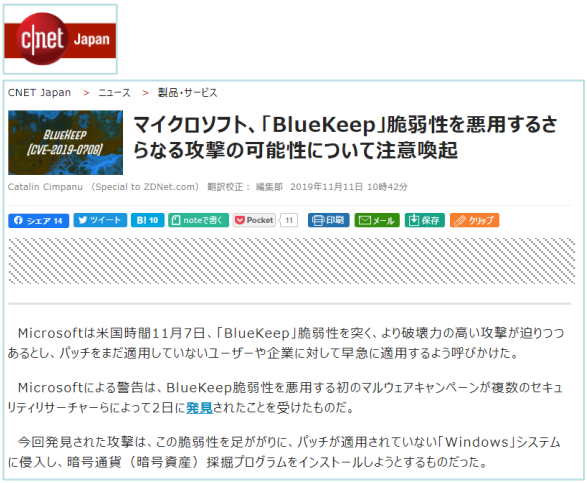
- 今回確認された攻撃の内容は、暗号通貨(仮想通貨)を採掘するプログラムをPCに不正にインストールさせる程度のものとされていますが、同7日にはMSより、自己拡散能力を持つワーム等破壊力の高い攻撃が今後登場する可能性もあるとして注意喚起が出されています。

AUS便りからの所感

- MSは8月にもBlueKeepを悪用する大規模攻撃の可能性があるとし、パッチの早期適用を呼び掛けています(AUS便り 2019/8/19号参照)。

- 前述のとおり、もうすぐ無償のサポートが終了するWindows 7を含む古いOSで発生する脆弱性であり、よほどの理由がない限り、全てのパッチを適用するか、最新のWindows 10に更新するかを選択することが、根本的な対策として肝要です。

- RDSが使用するTCP/UDPポート3389番を探索する動きはBlueKeep以前からありますので、RDSが不要なクライアントPCで有効になっていれば無効化し、また他のサービスポートも含め不特定多数が外部から直接ポートにアクセスできないよう、PC自体やルーター・UTM等のファイアウォール機能でアクセス遮断を行うことも可能な限り行うようにしましょう。



●気象庁公式を騙る偽防災アプリに注意喚起

https://www3.nhk.or.jp/news/html/20191107/k10012166961000.html
https://www.buzzfeed.com/jp/yutochiba/fake-aplication
http://www.jma.go.jp/jma/press/1911/06b/1106_press_spam_mails.html

このニュースをザックリ言うと･･･

- 11月6日(日本時間)、気象庁より、同庁の報道発表を装った迷惑メールが拡散しているとして注意喚起が出されています。

- 同庁に問合せがあったというメールの一例として、「地震早期警告」を受け取れるようにする公式防災アプリを騙り不審なファイルをダウンロードさせようとするものが挙げられています。

- 同庁からはこうしたアプリは配布しておらず、不特定多数の人にアプリのダウンロードを促すメールを送ることもないとしており、金銭的な被害などを受けた場合は最寄りの警察署に被害届を出すよう呼びかけています。

AUS便りからの所感等

- 気象庁を騙る攻撃の事例は、昨年11月にも「津波警報発表」と称してマルウェアをダウンロードするWebサイトへ誘導するものが確認されています(AUS便り 2018/11/19号)。

- 今回のメールも、最初の文言が拙いところに気付かない限りは騙される可能性がある巧妙な偽装となっていますが、ともあれこのような不審なメールを受け取った場合は、安易にメール上のリンクをクリックせず、公式サイトで同様の情報が掲載されていないか、あるいはSNS等でこのようなメールが他でも拡散しているという報告がないか、確認するのが重要です。

- 併せて悪意のあるサイトへのアクセスが可能な限り遮断されるよう、ブラウザーやセキュリティソフトあるいはUTM等でのセキュリティ機能を有効にすることによる防御を行うことを推奨致します。