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。

●内閣府にサイバー攻撃、231人分の個人情報流出…サーバー機器の「ゼロデイ脆弱性」を突かれる

https://www.asahi.com/articles/ASP4Q730CP4PUTIL06P.html
https://www.cao.go.jp/others/csi/security/20210422notice.html
https://www.cao.go.jp/others/csi/security/20210423notice.html
https://www.soliton.co.jp/news/2021/004393.html

このニュースをザックリ言うと･･･

- 4月22日(日本時間)、内閣府より、同府が設置したファイル共有サーバーが不正アクセスを受け、個人情報が流出した可能性があると発表されました。

- サーバーは内閣府や内閣官房の職員が外部と情報をやりとりするために設置されたアプライアンス(専用機器)で、不正アクセスは今年1月に検知されて発覚したとのことですが、その後の調査により、遅くとも2020年3月には始まっていたとされ、被害を受けた個人情報は231人分(公開されていない氏名・所属・連絡先等)とされています。

- アプライアンスにはソリトンシステムズ社開発の「FileZen」を利用していたこと、不正アクセスはその時点で修正パッチが出ていなかった、いわゆる「ゼロデイ脆弱性」を悪用して行われたことが発表や報道等で明らかになっています。

- 同23日にはソリトン社からもこれに関連して発表がされ、FileZen利用者に対し脆弱性を修正した最新のファームウェア(バージョン4.2.8および5.0.3)へのアップデートを行うよう呼び掛けられています。

AUS便りからの所感等

- 不正アクセスの原因となった脆弱性は2点で、前述の通りいずれも不正アクセスが開始した時点で未対策であったもので、パッチがリリースされたのは2020年12月から今年4月にかけてとなっており、とにかくFileZenを利用している各社においては、速やかに状況を確認の上ファームウェアの更新を行うことが肝要です。

- 内外の利用者ないし不特定多数からのサーバーへのアクセスについて監視を行い、分析する体制を整えることは、今回のようなゼロデイ脆弱性の恐れに対し、速やかに攻撃を発見し、ベンダーへの連絡・対策を実施することを鑑みるならば、特に重要なことと言えるでしょう。

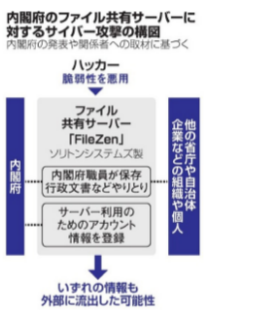
- ここ数年、社外との文書等のデータを安全にやり取りする手段については特に議論が続いていますが、FileZen等いわゆるオンプレミスでの運用、クラウドの利用、それぞれにおいて運用・利用時に発生し得る問題を洗い出し、安全性と利便性のいずれも欠くことなく十分に満たすシステムを構築することが重要です。

朝日新聞 DIGITAL

内閣府にサイバー攻撃　サーバーに「ゼロデイ」の痕跡

会員記事

編集委員・須藤龍也、吉沢英将　2021年4月22日 21時37分



内閣府の共有ファイルサーバーに対するサイバー攻撃の構図

内閣府（は22日、内閣府 や内閣官房の職員らが外部とファイルの送受信をする際に使うファイル共有サーバーに 不正アクセス があったと発表した。不正アクセス を受けたファイルには231人分の個人情報が含まれており、これらが流出した可能性があるという。

中国の影、たどり着いた雑居ビル　三菱電機サイバー攻撃 →

朝日新聞の取材に応じた複数の関係者によると、不正アクセス は遅くとも昨年3月には起きていたことが確認された。内閣府 が 不正アクセス を検知するまでの間、外部に向けてサーバーから大量のデータが送信されていた痕跡が見つかった。データのサイズは一度の送信で数ギガバイトに及んだといい、流出の規模はさらに増える恐れがある。

●「ニコニコ」の偽サイト？に注意喚起…「プロキシーサイト」のURLが検索結果に表示される事態

https://www.itmedia.co.jp/news/articles/2104/21/news133.html
https://blog.nicovideo.jp/niconews/151137.html

このニュースをザックリ言うと･･･

- 4月21日(日本時間)、ドワンゴ社より、同社が運営する動画サイト等のサービス群「ニコニコ」の一部サイトと内容が全く同じ「コピーサイト」が確認されたとして注意喚起が出されています。

- 注意喚起に挙げられていたのは「ニコニコ大百科」「ニコニ立体」のもので、この時点ではGoogle等サーチエンジンの検索結果において、コピーサイトが上位に表示されるケースもあった模様です。

- 同社では、これらのサイトには悪意のあるコンテンツやツールが仕込まれている可能性があり、またニコニコのアカウント情報を乗っ取られる恐れもあるため、これらのサイトからログインしないよう呼び掛けています。

AUS便りからの所感

- 注意喚起中でコピーサイトとされるものはいずれもドメイン名に「proxy」という単語を含んでおり、厳密には「アクセス元IPアドレスを隠したい」「本物のサイトへのアクセス遮断を回避したい」等の目的で利用される「プロキシーサイト」とみられます。

- 同社ではニコニコへのアクセス時、アドレスバーに「nicovideo.jp」と表示されていることを確認することも呼び掛けています(ニコニコ大百科は「https://dic.nicovideo.jp/ 」、ニコニ立体は「https://3d.nicovideo.jp/ 」となります)が、プロキシーサイトの仕様によっては「https://dic.nicovideo.jp.proxy.*******/ 」のようにURLの一部(さらにはFQDNの先頭)にこれらのドメイン名が含まれる可能性もあることには注意が必要です(そしてそのようなURLはフィッシングサイトでも度々使われます)。

- 検索結果に表示されるようになった経緯は不明で、現在表示される様子は確認されませんが、サイト内の個々の動画や記事へのリンクとしてこういったプロキシーサイトのものが表示される恐れもあるため、「自分が意図したサイト」に確実にアクセスするための自衛手段として、フィッシングサイトと同様にあらかじめ登録したブックマークからアクセスすること、検索等についても結果のアクセス先が本物であることを確認するか、本物のサイト内で行うことを強く推奨致します。

●ゴールデンウィークにおける情報セキュリティの注意喚起、IPAより発表

https://www.ipa.go.jp/security/topics/alert20210421.html
https://www.ipa.go.jp/security/measures/vacation.html

このニュースをザックリ言うと･･･

- 4月21日(日本時間)、IPAより、多くの企業・組織が長期休暇となるゴールデンウィークを迎えるにあたっての、情報セキュリティに関する注意喚起が出されています。

- 長期休暇においては、組織内に常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象にした基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

- IPAは毎年のこの時期および夏季・冬季休暇の時期に注意喚起を行っている他、特に最近相談が多く寄せられている事例として「ブラウザ通知機能による不審な通知」および「iPhoneカレンダーへの不審な通知」についても注意を呼び掛けています。

AUS便りからの所感

- 注意喚起の内容は、システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性から、従業員が旅行先等でSNSへの書き込みを行った場合に、最悪関係者にも思わぬ被害が及んでしまう可能性まで、多様なものとなっています。

- 一方で、挙げられているセキュリティ対策の内容は毎回大きく異なるようなものではなく、この他にも長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策(https://www.ipa.go.jp/security/measures/everyday.html)」として別途まとまっており、GWまでに十分な対応が間に合わなかったとしても、GW明け以降に点検すべきことは多く存在しますし、以後も夏季休暇等に備えて、準備・点検を行うよう意識していくことが肝要です。