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。

●NTTコムに不正アクセス…621社の工事情報流出か

https://www.itmedia.co.jp/news/articles/2005/28/news124.html
https://www.ntt.com/about-us/press-releases/news/article/2020/0528.html

このニュースをザックリ言うと・・・

- 5月28日(日本時間)、NTTコミュニケーションズ社(以下NTTコム)より、同社法人向けサービスに関する情報が、不正アクセスにより流出した可能性があると発表されました。

- 被害を受けたのは同社法人向けサービス「Bizホスティング エンタープライズ」「Enterprise Cloud1.0オプションサービス」(以下BHE/ECL)の顧客621社に関する工事情報で、現在までに顧客管理情報や個人情報の流出は確認されていないとのことです。

- 5月7日に不正アクセスを検知して遮断、その後アクセスログの解析により、同11日に情報流出の事象を確認したとのことです。

AUS便りからの所感等

- 発表によれば、まずNTTコムの海外拠点が不正アクセスを受け、そこを踏み台にしてBHE/ECLの管理サーバーが置かれたセグメント、さらにNTTコムの社内セグメントに侵入されたとしています。

- また、BHEにおいて、ユーザーの環境を新サービスへ移行しており、その過程で撤去を控えていたサーバー等が、攻撃者の侵入経路として利用されたとのことで、NTTコムでは移行中の設備についても物理的な撤去が終わるまでセキュリティ対策の適用を徹底するとしています。

- 組織が管理するあらゆるサーバー・機器について、アップデートが行われていない等の理由で何らかの侵入を許すような脆弱性や設定が存在していないか、およびあるサーバーやネットワークセグメントに侵入した攻撃者が、他のサーバーのあらゆるサービスへ認証なし等で容易にアクセス可能となるようなネットワーク構成でないかについて、それぞれ十分に確認し、適宜対策をとることが肝要です。

NTT Communications Go the Distance.

2020 年 5 月 28 日

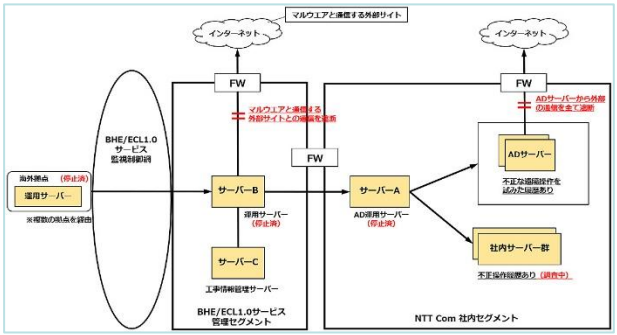
当社への不正アクセスによる情報流出の可能性について

NTT コミュニケーションズ(以下 NTT Com)は、当社の設備が攻撃者からの不正アクセスを受けたことを 5 月 7 日に検知し、一部の情報が外部に流出した可能性があること（以下 本事象）を 5 月 11 日に確認しました。

社内調査の結果、当社の一部サービス（「Biz ホスティング エンタープライズ（以下 BHE）」[※1]、「Enterprise Cloud1.0（以下 ECL1.0）オプションサービス」[※2]）に関する工事情報管理サーバーおよび、当社の社内業務で利用しているサーバー群（以下 社内サーバー群）において、一部の情報が外部に流出した可能性があることが判明しました。

現時点においては、踏み台となったサーバーの停止などの初動措置を終えておりますが、影響を受けた可能性があるお客さまには、順次連絡を差し上げております。あわせて、再発防止に向けた対応を実施しております。

また、個人のお客さまに関する情報は含まれておりません。



ITmedia NEWS

NTTコムに不正アクセス　法人の工事情報が漏えいした疑い

2020年05月28日 17時13分 公開　[井上輝一，ITmedia]

印刷　見る　Share　B! 25

NTTコミュニケーションズは5月28日、自社のサーバ設備が外部から不正アクセスを受け、一部の情報が漏えいした可能性があると発表した。漏えいの可能性が分かっているのは法人の工事に関する情報で、現在までに顧客管理情報や個人情報の漏えいは見つかっていないとしている。

漏えいの可能性があるのは、同社の法人向けサービス「Bizホスティング エンタープライズ」と「Enterprise Cloud1.0オプションサービス」に関する工事情報。

攻撃者は、2つのサービスの管理サーバが置かれたセグメントに接続する海外拠点サーバを踏み台に侵入。NTTコムが調査した結果、同セグメント内の運用サーバ（サーバB）に到達していたことが分かった。このサーバBに接続していた工事情報管理サーバから、外部へ情報が漏れた可能性があるという。

●「緊急事態宣言解除後のセキュリティ・チェックリスト」、JNSAが公開

https://www.nikkei.com/article/DGXMZO59366820R20C20A5000000/
https://www.jnsa.org/telework_support/telework_security/

このニュースをザックリ言うと・・・

- 5月19日(日本時間)、日本ネットワークセキュリティ協会(JNSA)より、「緊急事態宣言解除後のセキュリティ・チェックリスト」が公開されています。

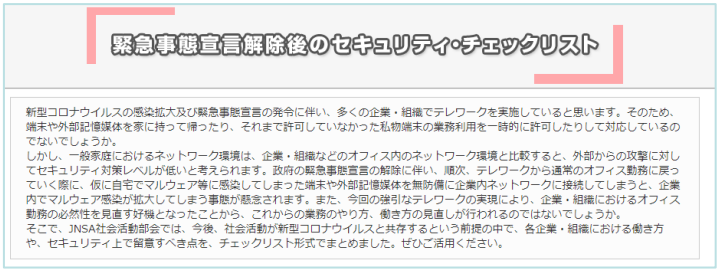
- 新型コロナウイルスの感染拡大およびそれに対する緊急事態宣言の発令により多くの組織でテレワーク(リモートワーク)が実施されていた状況から、宣言解除による通常のオフィス勤務に戻っていくにあたり、自宅に持ち込んでいた端末や外部記憶媒体に密かに感染していたマルウェアが企業ネットワークに拡散する等の懸念があることや、今後のオフィス勤務の必然性を見直す機会となり得るとしています。

- こういった状況を踏まえ、今後、社会活動が新型コロナウイルスと共存するという前提の中で、各企業・組織における働き方や、セキュリティ上で留意すべき点を、チェックリスト形式でまとめたものとなっています。

AUS便りからの所感

- チェックリストは大きく「停止したシステムの再稼働における注意事項」「テレワークで社外に持ち出した機器を社内ネットワークに接続する際の注意事項」「緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い」「Withコロナフェーズに向けた、業務見直しとセキュリティ対策」の4つに分類された計24項目からなっています。

- テレワーク等への対応を「今回限りの特別なもの」と見なして元の状況に戻すか、以後も発生が予想される感染の新しい波(いわゆる第二波)を鑑み「特別でないこと」にするための整備を行うかに拘らず、ネットワークシステムが安全な状態に保たれるよう、このチェックリストを適切に活用して頂ければ幸いです。



●公的機関を模倣した偽サイト？ NISCが注意喚起

https://twitter.com/nisc_forecast/status/1260476206270558209
https://www3.nhk.or.jp/news/html/20200513/k10012428901000.html
https://this.kiji.is/633629831045088353

このニュースをザックリ言うと・・・

- 5月13日(日本時間)、内閣サイバーセキュリティセンター(NISC)より、日本の公的機関や企業等を模倣した多数のWebサイトが存在するという情報が寄せられているとして、Twitter上で注意喚起が出されています。

- 注意喚起によれば、サイトはURLに海外のドメイン名が含まれる一方、「本物のサイトとURL以外見分けがつかない」ものがあり、サイバー犯罪等に用いられる可能性」があるとしています。

- これらの偽サイトについては、一般的なフィッシングサイトのような模倣ではなく、CDNサービスの悪用により、寸分違わぬ内容を表示している可能性が指摘されており、いずれにしろこういったサイトにはアクセスしないよう呼び掛けられています。

AUS便りからの所感

- このような形の偽サイトは2014～2015年にも注意喚起が出され(https://eset-info.canon-its.jp/malware_info/qa/detail/150202.html)、このときは正規サイトとの間に存在するプロキシーサーバーが実態とされていましたが、今回は正規のサイトと関係ない組織がCDNでコンテンツをキャッシュするサーバーを立ち上げたものとされています。

- また、偽サイトはいずれもドメイン名の末尾が「.tk」「.ml」「.ga」「.cf」「.gq」となっており、これらを無料で登録可能なサービスを悪用している模様です。

- 現時点で偽サイトは個人情報の詐取を目的としているようには見受けられないものの、今後より有害な攻撃が行われる可能性も指摘されており、他のフィッシングサイトへの対応と同様、不審なドメイン名のURLを含むリンクについては検索エンジン等で正規のサイトのURLを確認する、あるいはブラウザー・アンチウイルス・UTMのアンチフィッシング機能による防御を行うことを推奨致します。