危険

気をつけて！！テレワークに潜む２つの落とし穴！！

～攻撃者は脆弱性を狙っています!!～

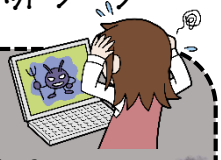
～社外から社内ネットワークに接続するとき～

その1 ⚠ VPNの脆弱性 ⚠

※VPN…インターネット回線上に作成する仮想のプライベートネットワーク

ココがキケン!!

VPN機器の脆弱性情報が出ていても、見落としたり、後回しにして最新パッチの適用を怠ってしまうと、その脆弱性を狙った犯罪者から攻撃を受けてしまいます。



窃取された認証情報で企業内部ネットワークに侵入され、ランサムウェアの被害にあってしまう可能性も！

※ ランサムウェア～パソコンをロックし、データを暗号化するウイルス

VPNの脆弱性がウイルスの侵入を許しています…

～リモートデスクトップを使うとき～

その2 ⚠ RDPの脆弱性 ⚠

※RDP…サーバコンピュータの画面をネットワークを通じて別のパソコンに転送して表示するための通信プロトコル

ココがキケン!!

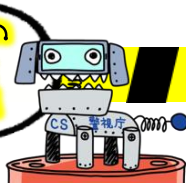
RDPを使ったリモートデスクトップ機能を公開している端末に対して、ID･パスワードを総当たりでログイン試行する攻撃をして不正ログインしようとする攻撃が増えています。

ランサムウェアの侵入経路はVPN機器からの侵入が最も多いですが、次いで多いのがリモートデスクトップからの侵入です!

攻撃者はテレワークが浸透してきている昨今の情勢をみて、セキュリティ対策が追い付いていない部分を攻撃の足がかりにしようとしています!!

～今すぐ対策をとりましょう!!～

① 脆弱性を修正したバージョンへのアップデートを必ず行う!
② パッチを適用する際は併せてパスワード変更も行うと効果的!
③ パスワードの使い回しは厳禁。推測されにくいものに!
④ 多要素認証を導入する
⑤ ログに正規の利用と異なるログイン試行が無いかを確認する
⑥ 外部からシステムにアクセス可能な端末は最小限にする
（MACアドレス･IPアドレスやポートを制限する）



警視庁サイバーセキュリティ対策本部