MOTEX

VPN経由の攻撃が増加

高い頻度で公表されるOSやネットワーク機器の脆弱性

漏れなく対応できていると言えますか？

既出の脆弱性を悪用した「Nデイ攻撃」が増加中

OSやネットワーク機器の定期的なチェックでできる対策があります

例えば・・VPNの脆弱性は攻撃者にとってのチャンス
機密情報窃取のきっかけを与えてしまうかもしれません

某情報通信業のインシデント事例

コロナ禍でテレワーク勤務を推進する際にネットワークの負荷が高まったため、
緊急対応で旧型のVPN機器を利用。
結果、不正アクセスに遭い顧客や個人情報が流出する被害が発生した。

「Nデイ攻撃」とは？

ゼロディ攻撃が、修正プログラムが提供される前の脆弱性を悪用する攻撃であるのに対し、Nデイ攻撃はすでに修正プログラムが公開されている脆弱性に対して行われる攻撃です。金銭や情報を目的とした攻撃の場合、公開されていて悪用しやすい脆弱性を狙うNデイ攻撃が好まれる傾向にあります。

LANSCOPE
Professional Service
ネットワーク脆弱性診断パッケージ

稼働中のシステムに負荷を与えることなく
自社ネットワークの脆弱性を診断できます！

ネットワークを安全に保つためには？詳細はこちら → → →

自社ネットワークの**現状を把握**し
内在する脆弱性に対処しましょう

LANSCOPE
Professional Service

ネットワーク脆弱性診断で見つかりやすい脆弱性とは？

不要なポート

意図しないログイン画面の表示

管理用Webページに不特定多数がアクセスできることにより、サーバーを不正操作される恐れがあります。

暗号化通信の不備

強度の弱い暗号化方式の利用

暗号化通信のバージョンが古い場合、通信内容を盗聴し、機密情報や個人情報を窃取される恐れがあります。

OSの脆弱性

サポート切れバージョンの利用

サポート切れの製品を利用していると、セキュリティパッチが提供されず新たな脆弱性に対処ができません。

実施事例　システム会社C社様　診断期間：3週間

緊急度の高い脆弱性が公表され、
サービスの安全性を心配する問い合わせが入ったが
自社内で調査をするには時間もスキルも足りなかった。

最新の脆弱性情報も診断項目へ**即時に反映**されるから
脆弱性の公表から**2週間**で問題がないことを確認できた。

Q：ネットワーク脆弱性診断は1度で十分ですか？

A：ネットワークの脆弱性は、約2週間に1回の頻度で新たなものが発見されます。
定期的に診断を行うことで新たな脅威の見逃しを防ぐことができます。
半年に1回のペースでの診断がおすすめです！

需要の高い脆弱性診断をパッケージ化！

- Webアプリケーション脆弱性診断パッケージ
- ネットワーク脆弱性診断パッケージ
- クラウドセキュリティ診断パッケージ
- サイバーセキュリティ診断診断パッケージ
- グループセキュリティレポーティングパッケージ

お問い合わせはこちら
https://go.motex.co.jp/l/320351/2022-09-05/7zggwn

エムオーテックス株式会社　●お問い合わせ窓口：営業部

【大　阪】〒532-0011 大阪市淀川区西中島5-12-12　エムオーテックス新大阪ビル
【東　京】〒108-0075 東京都港区港南1-2-70　品川シーズンテラス5F
【名古屋】〒460-0003 名古屋市中区錦1-11-11　名古屋インターシティ3F
【九　州】〒812-0011 福岡市博多区博多駅前1-15-20　NMF博多駅前ビル2F
06-6308-8980(大阪・九州)　**03-5460-1371**(東京)　**052-253-7346**(名古屋)

●お問い合わせ先