ASAMA あさまセキュリティニュースレター
Security Newsletter
2023年12月12日
Vol.103

2023年セキュリティニュースまとめ

攻撃手法は様々、基本的な対策を確実に、万が一のバックアップとインシデント時の対策の確認を

人為的なミスによる情報漏洩

メール誤送信、ノートPC・USBメモリ、紙書類の置忘れや紛失
業務委託先からの情報漏洩、個人利用の端末やサービスから漏洩

起こることを想定して事前に対策を

マルウェア被害による情報漏洩

Emotet　添付ファイルはウイルス対策検知を回避するように進化
（暗号化ZIP、ショートカットリンク、大容量ファイル、OneNote形式等）
攻撃の波があり、今後も取引先からのメール＝安全ではなく不審な点は確認を

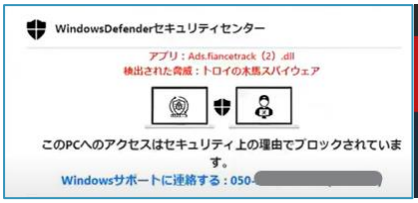
ランサムウェア　お金を払えば誰でもランサムウェアによる攻撃が行える仕組みが確立
暗号化を行わずに脅迫するケースも。社会的インパクトも大きく被害も甚大

脆弱性の脅威　日常では気づきにくく悪用されているケースが多い

ルータ、VPN機能、無線LAN、NAS、WEBカメラ等のネットワーク機器、HPサイトの**脆弱性**
自動でアップデートされないものは更新の確認・サポート終了しているものは見直しを

WEBブラウザ閲覧中の脅威

偽の警告画面でサポート詐欺　警告画面の電話番号にかけさせ遠隔サポートで金銭要求・情報漏洩も



不正送金被害急増

偽メール・SMS（不在通知など）手口が巧妙化　個人被害が急増中
（フィッシング・スミッシング）

POINT

2023年のサイバー攻撃も、終息したと思われたEmotetの再開とともに添付ファイルがウイルス対策の検知を回避するために巧妙化
ランサムウェア被害は、社会的なニュースになる被害が多発、データセンターや港のシステムが被害にあい、何日も業務停止になるケースも
また、様々な情報漏洩やインターネット経由の詐欺被害も話題となりました。
2024年のサイバー攻撃は、AI技術を悪用した攻撃が増えると考えられており、
より巧妙化したフィッシングメールやビジネスメール詐欺といった攻撃が行われると予想されます。
100%防ぐことは困難なため、基本的な対策・既存セキュリティ対策の見直し・バックアップ、
社員のセキュリティ教育、インシデント時の連絡や対応については、明確化し確認を

対策

参考URL　迷惑メール相談センター
https://www.dekyo.or.jp/soudan/index.html

- **フィッシングメール・SMS経由のスミッシングは、常に最新の情報を確認…**
- **不審なメール、WEB閲覧中の警告表示などは、社内で情報を共有・確認を**
- **利用するソフトやデバイスは必要最小限にし、OS、ソフト、ファームウェアなど定期的にアップデートを**
- **サポート切れのパソコンやソフト、古いネットワーク機器は使用をやめ、定期的に見直しを**
- **業務で使用するデバイスやサービスは公私を分けての利用を。フリーWiFiのビジネス利用は避けましょう**
- **バックアップは必ず取りましょう。社内ネットワーク以外の場所（クラウドなど）へのバックアップの検討を**

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414