2022 年 5 月 17 日

Venture Solution

コラム記事

セキュリティー担当者からよく聞く悩みとして、人手不足・予算不足が挙げられるかと思います。
日本企業の傾向として、セキュリティー対策への意識が希薄な傾向である言われています。
セキュリティー部門の重要性を各企業で今一度見直し、対策を強化することでランサムウエア被害に合わない体制つくりが必須だと感じております。
そこで、日本のセキュリティー対策についての記事が掲載されておりましたのでご紹介いたします。

ランサムウエア標的、日本２万台　脆弱性対応世界に後れ

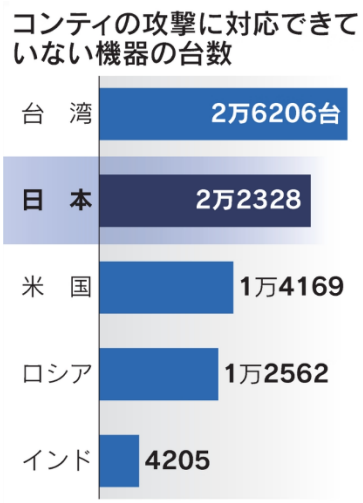
（日経電子版 2022/5/17(火) 02:00 配信より引用）

「様々な脆弱性を組み合わせて攻撃をする」などと幹部同士で議論している様子が確認できる（画像を一部加工）（日経電子版より引用）

世界最大のランサムウエア（身代金要求型ウイルス）犯罪集団「コンティ」の標的になりかねないコンピューターが少なくとも日本に約 2 万 2 千台あることが日本経済新聞の調査で判明した。4 月下旬時点で台湾に次ぐ多さで、3 位の米国の 1.5 倍以上だ。事業継続を重視して修正対応を後回しにする短期的な視点が日本の防衛力を下げている。

コンティから漏洩したチャットの情報などから、脆弱性対策大手の米テナブルが、コンティが使う脆弱性を特定。このうち侵入経路となる 9 個の脆弱性について、日本経済新聞がセキュリティー大手トレンドマイクロの協力を得て調査した。インターネットにつながる機器の検索ツール「SHODAN」を利用した。

脆弱性が放置された機器は、SHODAN で検索可能なものだけでも世界に 13 万 8968 台だった。その 16%の 2 万 2328 台が日本にあった。台湾の 2 万 6206 台に次ぐ多さだ。



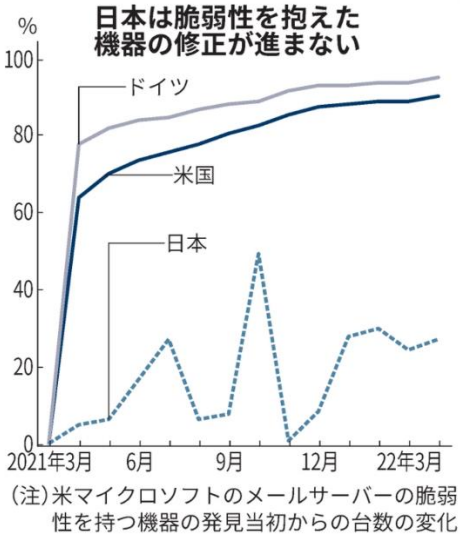
（日経電子版より引用）

見つかったのは米マイクロソフトのメールやファイル共有サービス向けのサーバーを遠隔から操作できる脆弱性だ。実証用の攻撃プログラムが公開されているため、容易にハッキングを実行できるものもある。機微な情報の抜き取りなどにつながる恐れがある。世界のサイバー防衛チームの連合組織 FIRST の基準では、これらの危険度を示すスコアは 9.8～10（最高値は 10）となる。

脆弱性は通常、公表時に製造元から修正ソフトが配布される。「修正せずに放置しておくと重大なリスクにさらされる」とテナブルのサットナム・ナラン氏は警告する。しかし、コンティが利用する脆弱性には 7 年前の発見から修正されていないものもある。

特に日本は脆弱性の修正ソフトを組み込む対策が進んでいない。メールサーバーに脆弱性がある台数は、脆弱性が発見された 2021 年 3 月から 27%しか減っていない。世界平均の 84%と比べて見劣りする。

この脆弱性は中国政府とのつながりが疑われるハッカー集団に実際に悪用されているとマイクロソフトは指摘する。欧米各国の多くは 9 割以上のメールサーバーで修正対応済みだ。



（日経電子版より引用）

テナブル日本法人の貴島直也・カントリーマネージャーは「日本企業は事業継続を優先しすぎて脆弱性対策がおろそかになることが多い」と指摘する。修正ソフトの適用により、機器が一時的に停止することがあるためだ。「日本企業ではセキュリティー部門の立場が低く、事業部門に修正を止められてしまう」

貴島氏は、

① セキュリティー部門が経営トップに直接リスクを報告する
② サービスの一時停止が受け入れられる風土をつくる
③ 海外の先進企業を参考に対策を進めること
を提案する。

脆弱性は重要度の低いものも含めると 21 年に約 2 万件が見つかった。5 年前の 3 倍以上の水準だ。修正ソフトの適応は企業の重い負担になる。特にセキュリティーの予算と人員を十分に確保できない中小企業は対応が困難だ。

高い攻撃技術を持つセキュリティー技術者「ホワイトハッカー」を多数抱える GMO サイバーセキュリティ　by イエラエ（東京・渋谷）の牧田誠社長は「攻撃者の視点を持ち、防御する IT（情報技術）資産の優先順位を決めることが必要になっている」と語る。

このように日本企業はセキュリティー対策において、世界の先進国内では後れを取っております。
サイバー犯罪者へももちろん、その情報は入っているはずです。
ただし、セキュリティー部門がいくら危機感を感じていても、企業として対策に乗り出さなければ本当の対策効果を得ることは出来ないと思っています。
セキュリティー部門の情報・知識を社内で共有し、1 部門の問題ではなく企業としての問題ととらえ、対策を今一度検討する必要があると感じています。