2. ASM(Attack Surface Management)の動向について

要約

- 侵入前提の対策である EDR だけではなく、組織内部への侵入阻止を目的とした ASM が注目されている。
- 国内での導入はまだ進んでいないが、総務省のガイドラインなどの公表により今後の導入拡大が見込まれる。

背景と目的

デジタルトランスフォーメーションの進展により、クラウド利用の拡大やテレワークの増加などが一般的になった結果、サイバー攻撃の起点が増加しています。

本冊子の第 2 部でも紹介したように、ランサム攻撃により大きな被害が発生しています。これらのランサムウェアの原因として、警察庁の発表(*1)では、「国内で発生したランサムウェア被害の感染経路は、2022 年と 2023 年上半期のいずれも、80%以上が管理不十分な外部公開資産(VPN 機器やリモートデスクトップ)」とされています。

悪意ある攻撃者の入り口となりうる外部に公開された資産を漏れなく管理し、タイムリーなパッチ適用などの適切な管理・運用を行うことは容易ではありません。

このような環境変化に対応するため、外部から把握できる情報を用いて、IT 資産の適切な管理を可能にするソリューションとして、ASM(Attack Surface Management)が注目されています。

経済産業省のガイダンス紹介

2023 年 5 月、『ASM(Attack Surface Management)導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～』(*2)が公表されました。本ガイダンスでは ASM の特徴を以下のように紹介しています。

- 情報システムを管理している部門が把握していない IT 資産を発見できること。
- 情報システムを管理している部門の想定と異なり、公開状態となっている IT 資産を発見できること。

ASM は、「組織の外部(インターネット)からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス」(ガイダンスの定義)となりますが、具体的な手法としては次のようなものがあります。

(*1) 出典:警察庁ウェブサイト　令和4年におけるサイバー空間をめぐる脅威の情勢等について
出典:警察庁ウェブサイト　令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について

(*2)https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

① 自動的なアセット特定:
ツールを活用することで、自社や関連企業のアタックサーフェスを自動的かつ継続的に特定。未把握の機器や意図しない設定ミスを攻撃者視点から発見でき、リスク低減に寄与

② 脆弱性スキャン:
アセットに対して定期的な脆弱性スキャンを実施、脆弱性情報を収集し、適切な対応策を検討

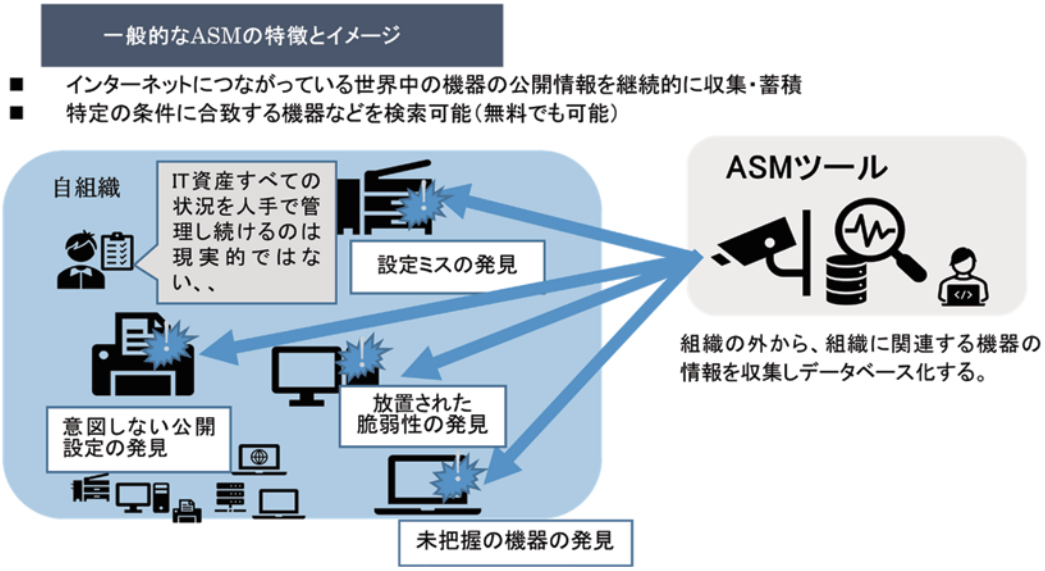
③ 設定の評価:
アセットの設定を評価し、セキュリティベストプラクティスに準拠しているかどうかを確認

④ 攻撃シナリオのモデリング:
アセットを攻撃者視点で分析し、潜在的な攻撃シナリオをモデリング

⑤ リスク評価と優先順位付け:
検出されたリスクを評価し、優先順位を付けて対応

ASM は自社のセキュリティ向上のために有効なソリューションではありますが、導入するツールの選択時には事前検証などの実施により、自社に適したツールの見極めも重要です。主に発生する課題は以下のとおりです。

- 自社と関係のない IT 資産(ノイズ)に関する通知の精査
- 収集された情報の発見理由や根拠の説明不足
- 対応すべき箇所を優先順位付けるための判断指標の追加



出典: ASM(Attack Surface Management)導入ガイダンス(経済産業省)

ASM を取り巻く国内の状況

国内の普及度に関する具体的な統計データは限られているが、トレンドマイクロ社が調査した「法人組織のアタックサーフェスに関するセキュリティ意識調査」(*1)によると、「アタックサーフェス（攻撃対象領域）が多様化することに懸念がある法人組織は 7 割以上」で「安全性に盲点があると答えた日本組織は約半数」というものでした。

一般的なセキュリティ対策への意識は高まっているようですが、ASM の普及が進んでいる、特に欧米諸国の企業や組織と比較すると、国内においては一部の大企業や金融機関、政府機関などでの利活用が始まったばかりで、中小企業や一般的な組織においてはまだまだ導入が進んでいないようです。それには他のセキュリティ対策と同様、以下のような原因が想定されます。

- 日本の一般的な企業や組織において、ASM の重要性やメリットに対する認識がまだ不十分
- 十分なスキルと経験を持った専門家の不足
- 組織全体でセキュリティ意識を高め、ASM を継続的に実施する文化の醸成がまだ不十分

最後に

ASM 製品の多くは、グラフを利用したアセットの状況の可視化ができ、リスクに対するアラートの通知などを 24 時間 365 日体制で監視する SOC（Security Operation Center）のスピーディーなインシデント対応の助けになります。

EDR（Endpoint Detection and Response）のような侵入されたことを前提とした事後的な対応だけではなく、そもそも侵入されないことを目的とする予防的な対応に位置する ASM の重要性は、今後ますます高まっていくものと考えられます。

（水谷　浩樹）

(*1)https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220629-01.html