脆弱性管理の始め方

Vulnerability Management 101

v0.2 preview

hogehuga
脆弱性対応勉強会

目次

脆弱性管理について、全く手を付けていない状況からどう始めるのかを、順を追ってまとめました。

初めに

脆弱性管理とは何か、なぜ必要なのか、目指すゴールは何か、を考えます。

脆弱性管理とは何か

- 企業・組織が持つIT資産のリスクを減らし、攻撃から守るための取り組み

なぜ

- 脆弱性を放置すると、攻撃者に悪用され、システム停止・情報漏洩・金銭的損失などのリスクがある

目指すゴール（現実的な到達点）

- 「自分たちが対応すべき脆弱性を把握し、優先順位をつけ、適切に対応できる状態」
- まずは「最低限対処すべき脆弱性があるかどうかを把握する」ことから始める

おそらく、ここが一番重要であり、検討や理解に時間を掛ける必要がある。

- 必要に応じてコンサルティングやベンダとのディスカッションを行う
- 弊 脆弱性対応研究会への相談でも可能（非営利活動範囲で限界はある）

脆弱性管理の進め方

まだ管理を始めていない組織でもできる、小さく始めるパターン

この章は重要ではないかもしれない

1章を重点的に書くべきであり、本章は補足的に記載する方向とする

概要

本章では、脆弱性管理をどのように始めていくかのSTEPを記載していく

1. 対象範囲（スコープ）を決める
2. 資産を把握する
3. リスクを把握し、優先順位をつける

採用する手法は重要ではなく、どのように進めるのか、何を把握しておく必要があるのかを重点的に検討する

また、本項目でも完璧を求めないことを優先し、抜け漏れはありつつも管理が始まることを優先して進めるべきと考える

STEP1. 対象範囲（スコープ）を決める

いきなり全てのシステムを対象にするのは無理なので、まずは「どこを管理するか」を決める

- 最初の対象
  - 社内で重要なシステム（基幹システム、インターネット公開のシステムなど）
- 次の対象
  - 業務端末やネットワーク機器など、管理の幅を広げる

注意点

- 最初から、"全て"を"完璧に"はできない
- 1システムでSTEP3まで実行し、そこから対象を必要に応じて増やす

最初に見るべきスコープはどう決めるのか

- どのシステムが最も"リスク"が高いか？
  - リスクとは？
    - 先ずは、サイバー攻撃の被害にあったとき最も事業に影響があるもの
    - 通常、事業影響をもってリスクと呼んでいる
  - 例えば
    - インターネットに公開されているWEBサーバ
    - 社内の認証基盤
    - 重要なデータを扱うサーバ
    - etc...
- 運用が回せる範囲か？
  - 「まずはこの範囲だけでも把握し、対応する」という意識が大切

STEP2. 資産を把握する

「知らないものは守れない」ので、何を持っているかを把握することが最優先

- まずは対象範囲の「管理対象の資産リスト」を作る
  - 資産とは？
    - どのようなホストがあるか
      - オンプレミスサーバ、物理サーバ、仮想サーバ、クラウド上のインスタンス、etc
    - ホストがどのようなもので動いているか
      - OS（Windows/Linux/etc）、ソフトウェア（OpenSSL, httpd）
        - OSのパッケージ、自組織で作ったアプリ/WEBアプリで利用しているライブラリ、etc
        - バージョン番号等の情報が必要の情報が必要
  - どこまで対象にするかは、STEP1.の対象範囲と併せて検討が必要

まずは、完璧を目指さない事も重要。やりながら過不足を修正する。

また、「あるべき資産リスト」と「実際の稼働状況」を定期的に確認する必要もある

- 実際の稼働状況とあるべき資産リストは、乖離することがある
  - その為、定期的な棚卸のような整理が必要
- 資産管理台帳＋自動スキャン、が可能なら望ましい
  - まずは基となる台帳を作り、アップデートのタイミングで更新を行う
    - 更新を手動で行うのは手間がかかる為、コスト等で余裕があれば自動スキャンができる脆弱性管理製品の導入をお勧めする
    - 自動スキャンは、対象となる範囲がどこまであるのか（カバレッジ）に注意して選定する

todo.やり方を書く

- まずはExcelでも構わないので、機器/ソフトウェア一覧をまとめる
  - FortOS、等がわかればまずは良い？

STEP3. リスクを把握し、優先順位をつける

リスクを基に優先順位をつける

- リスク？
  - リスク = 機会（攻撃の可能性） x 脆弱性（深刻度） x 資産（影響度）
  - 資産については利用者の環境によるので一旦後回しとして、機会と脆弱性で評価する

但し、見つけた脆弱性すべてを理解して優先順位をつけることは不可能

- その為、対応力に応じて、ステップアップしていく事を推奨する

これも完璧を求めない

- 「決めた評価軸に従い対応する」「対応しきれなければ、評価軸を組織のポリシーとして調整する」事が重要
- 抜け漏れがありつつも重大なものには対応できている、という状況を作る

優先度付けのステップ

1. まずはKEV Catalogに記載のあるものをチェックする
2. 慣れてきたら、CVSS Base Scoreの高いものを対応する
3. 数が多くて運用が回らなくなるので、EPSSやシステムの置かれている状況を考慮した優先度付けを行う

最初は単純かつシンプルな`KEV Catalogに対象ソフトウェアが該当すれば対応する`を行い、
徐々に対応範囲を広げつつ優先順位を考えた対応に変えていく

STEP3.1. KEV Catalogを基にした対応

KEV Catalogとは？

- 米国CISAがメンテナンスしている、`Known Exploited Vulnerabilities Catalog`（悪用が確認されている脆弱性のカタログ）
  - 実際に悪用が確認されている脆弱性で、米国政府機関のシステムでは対応必須となっているもの
  - 攻撃者によって使われているものを優先的に対応する、のが基本なので、これを利用する

どうすればよいか？

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog で公開されているリストを見る
- 利用している製品が該当すれば、アップデートなどを行う

メリット等

- 登録される脆弱性の数は、他の手法ほど多くはないので、確認の手間は低い
- ここに登録されない悪用の危険のある脆弱性もあるので、慣れてきたらステップアップする

todo.やり方を書く

- KEVCatalogのcsvなりを取得
- 前回チェック日以降に絞り込み、保有製品と比較し、該当製品が無いかを確認

STEP3.2. CVSS Base Scoreを基にした対応

todo.このページの必要性を検討

- 101だったら概要だけでよい？
- そもそも要らないのかもしれない
  - 次のステップだから、別の資料でよい？

STEP3.3. EPSS等を利用したトリアージ

todo.このページの必要性を検討

- 101だったら概要だけでよい？
- そもそも要らないのかもしれない
  - 次のステップだから、別の資料でよい？

まとめ

まとめ

- まずは、スモールスタートとする
  - スコープを決めて、資産を把握し、KEV Catalogに載っている脆弱性から対応する。
- 全てを、一度に、完璧に、管理しようとは思わない。
  - 限られたリソースで「本当に危険なものから対応する」事が大切。
- 脆弱性自体の深刻度と攻撃される可能性を組み合わせて優先度を決める。
- 定期的なチェックを習慣化する
  - KEV Catalog、脆弱性スキャン、対応状況の確認

更新履歴

版	日付	概要
0.2	2025-02-24	preview版リリース