組織を守るための ASM

(Attack Surface Management)

参加者向け資料

第 1 章：ASM とは

【定義】

ASM（Attack Surface Management）は組織の攻撃対象となりうる範囲を特定・評価・管理する取り組みです。

【重要ポイント】

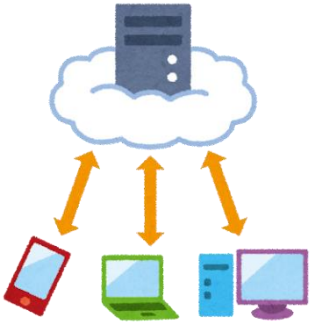
・インターネットに公開されている自社資産の把握

・潜在的な脆弱性の特定

・攻撃可能な経路の理解と対策

【対象となる主な資産例】

1. Web サイト・サービス
2. クラウドリソース
3. メールシステム
4. 社外向けサーバー
5. リモートアクセス環境



6.本来公開されるべきではないコンフィグ情報など

7.サポート終了済みのソフトウェア

【ASM が必要な理由】

・ サイバー攻撃の高度化・複雑化

・ IT 環境の急速な変化

・ クラウドサービスの増加

・ リモートワークの普及

第2章：攻撃者から見た組織

【攻撃者が収集する情報】

1. ドメイン情報
    - Webサイト構成
    - メールサーバー設定
    - ドメイン名
    - サブドメイン一覧
    - IPアドレス一覧
    - ポートとプロトコル
    - APIエンドポイント
    - ソフトウェア情報
    - 認証情報 など

2. 公開サービス
    - クラウドストレージ
    - 開発環境
    - テスト環境

3. 従業員情報
    - メールアドレス

・職務情報

・SNS アカウント

【よくある脆弱性】

・古いソフトウェアバージョン

・不適切なアクセス制御

・設定ミス

・未認識の公開サーバー

第3章：シャドーIT とリスク

【シャドーIT とは】

情報システム部門の把握・管理外で利用されている IT 資産やサービス

【具体例】

・個人で契約したクラウドサービス

・承認されていないアプリケーション

・私用デバイスでの業務データ処理

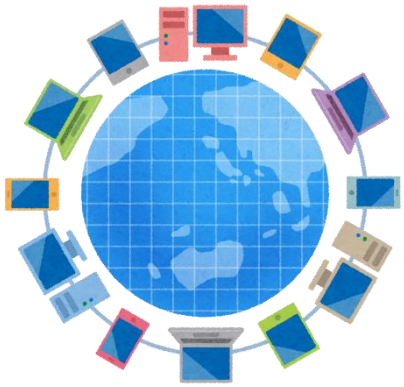
・非公式なコラボレーションツール

【組織へのリスク】

1. データ漏洩
2. コンプライアンス違反
3. セキュリティホール
4. 管理不能なアクセス経路

第 4 章：実践的対策

【日常的な確認事項】



☐ 利用サービスの棚卸し

☐ アクセス権限の確認

☐ 設定の定期確認

☐ 更新プログラムの適用

【報告すべき事項】

・ 新規サービスの利用開始

・ 設定変更

・ 異常な動作

・ 不審なアクセス

【適切な管理のために】

1. 定期的な資産棚卸
2. 使用ルールの確認
3. セキュリティ更新の徹底
4. 適切な申請・承認

第5章：参考情報

【用語集】

・ Attack Surface：攻撃対象となりうるIT資産

・ Asset Management：資産管理

・ Vulnerability：脆弱性

【問い合わせ先】

・ セキュリティ関連：内線XXXX

・ システム管理：内線YYYY

・ インシデント報告：内線ZZZ

[勉強会担当者]

第８システム開発本部　部門担当 ××〇〇

mail ：system8@zzz.com

※主催者向け資料については、機密情報を含むため別途提供させていただきますが、必要でしたら勉強会担当者までお申し付けください。