ハイライトレポート

2024. 1. 23 Day2

【IoTセキュリティ対策の最前線】押さえておきたい！！IoTセキュリティ対策の最前線

日々巧妙化・多様化するサイバー攻撃にどう立ち向かうか

サイバー攻撃は年を追うごとに増加の一途を辿り、2023年には攻撃対象の偵察行動が全世界で1日あたり7,000件以上観測されています。また、サプライチェーンの弱点を突く攻撃がランサムウェアに次ぐ脅威になるなど攻撃手段が巧妙化し、ライフサイクル全体を通した今までより高度で包括的な脆弱性管理が必要になってきています。本セッションはこうしたサイバー攻撃に伴う各国の動向や、実際に脆弱性管理で抑えるべきポイントをご紹介しました。

サイバーセキュリティ規格の動向

加速するサイバー攻撃情勢を踏まえ、世界各国でサイバーセキュリティ規格や法案の策定が推進されています。IEC62443をはじめ、欧州サイバーレジリエンス法、FIPS、NISTなど挙げ始めればキリがなく、早いものでは2024年から規制開始となる法案も存在します。中でも共通して求められる要件は「脆弱性の少ない安全なIoT機器の開発および脆弱性に対する迅速な対応」です。

一方、現実的には日々発見される新たな脆弱性に対して、製品開発・保守部門のみで対処することは容易ではありません

サイバーセキュリティ対策の要点を抑える

どの業界のサイバーセキュリティガイドライン・規格に対応するにも、まずは理想とのGAP分析、言わば「現状把握」から取り組み始めることを推奨いたします。先にゴールと課題を明らかにすることで、時間、費用、人員などのリソースを効率的に投入することが可能です。

もちろん評価・分析だけではなく、次のフェーズで求められる具体的な脆弱性への対応や、脆弱性テストなどの規格準拠に向けた道のりを、総合的にご支援いたします。

迅速かつ持続的な脆弱性対応、SBOM管理

メーカは製品に該当する脆弱性の把握とその対処方法を迅速に判断することが必要です。かつ開発時だけでなく、運用フェーズにおいても厳格に対策することが求められています。その手掛かりとして以下の2点を紹介いたしました。

「Timesys Vigiles」はお客様のソフトウェアプラットフォームに合わせ、自動化されたセキュリティ脆弱性管理と対策パッチの通知により、現状把握やソフトウェアセキュリティの維持にかかる時間とコストを大幅に削減することが出来ます。

「EMLinux」は標準的に脆弱性検査機能を有しており現状把握が容易な上、脆弱性の修正パッチを10年間提供することにより、長期間を前提とした運用が可能です。

また、上記はいずれもSBOMに対応しています。お客様の迅速かつ持続的な脆弱性対応実現に大きく寄与します。

■ 本日の登壇者 ■

サイバートラスト株式会社
OSS/IoT事業統括 IoT技術本部
執行役員本部長
岸田 茂晴 氏

VIGILES™
脆弱性通知&パッチ情報提供ツール

EMLinux
10年間の脆弱性サポートを提供する組込みOS

他記事、ウェビナ、お問い合わせはこちら

リョーサンテクラボ
エンジニアによりそうマガジンサイト