ハイライトレポート

2024. 4. 18

【製造現場の最新セキュリティ対策】
「サプライチェーンの弱点を悪用した攻撃」へのセキュリティ対策

情報セキュリティの重要性　ランサムウェアの脅威から工場システムを守れ！

工場システムのDX化で新たな付加価値を生み出す取り組みが進む中、サイバー攻撃は年々脅威を増しており、情報セキュリティ10大脅威で1位となっているランサムウェアからの対策はもちろんのこと、それ以外でも被害にあえば会社として大きな損失につながりかねません。一方で、DX化には、IoTやICT技術の活用が不可欠であり、導入するIoT機器や情報端末のセキュリティ上のリスクをどう担保していくか、また、工場設備として必要な信頼性・耐久性をどう確保するかが課題です。

今回はIPA独立行政法人 情報処理推進機構が毎年発表している、組織向け情報セキュリティ10大脅威をもとに、**工場システム向け産業用PCでのセキュリティ対策と、セキュリティ運用**について事例も交えて解説いたしました。

情報セキュリティ10大脅威2位「サプライチェーンの弱点を悪用した攻撃」について

サプライチェーン攻撃の目的は、大企業の持つ機密情報の窃取、機密情報と引き換えに高額な身代金を要求する等が挙げられます。堅牢なセキュリティ対策を施す大企業は直接狙わずに、セキュリティ対策が行き届いていないグループ会社や取引業者を踏み台にして情報を窃取していきます。

■ 本日の登壇者 ■

株式会社セキュアイノベーション
事業戦略部 マネージャー
亀谷 崇 氏

事例から読み取れる課題と対策

【「サプライチェーンの弱点を悪用した攻撃」の事例】

①プロスポーツリーグ
②自動車メーカー
③総合病院

【共通する課題】

セキュリティの観点で対象となるシステムやネットワーク等の監視が機能していなかった

【対策】

SOC（Security Operation Center）の設置

出所：投影資料より一部抜粋

セキュリティ運用の重要性

セキュリティソリューションは、導入して終わりではありません。本来期待したセキュリティ強度を維持していくためには、発生したインシデントに伴う設定変更やログ解析の他、定常的な監視やレポーティング、新しい脅威に対応するためのバージョンアップ対応等の**導入後の運用オペレーションが必要不可欠です。**

セキュリティに関してお困りの方は是非お問い合わせ下さい。

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

他記事、ウェビナ、お問い合わせはこちら