最新セキュリティマネジメント（第19回）

産業用制御システムのセキュリティ強化

2022.12.20

電力、ガス、水道、鉄道といった社会基盤や、石油、化学、鉄鋼など多くの工場・プラントにおいて、産業用制御システムが監視、制御などに用いられている。こうした産業用制御システムは、これまでスタンドアローン型で利用されてきた。しかし近年、インダストリー4.0やIoTの進化によってインターネットに接続されるケースが増えている。

インターネットに接続されればセキュリティリスクは増大する。重要な社会基盤や多くの産業で用いられている産業用制御システムを守るために何が必要なのか。IPAが公開した、ドイツ連邦政府がまとめた「産業用制御システム（ICS）のセキュリティ－10大脅威と対策2022－」を参考に考えてみよう。

インターネット経由で広がるマルウエア感染

IPAは2022年12月に、ドイツ連邦政府の情報セキュリティ庁（BSI）がまとめた「産業用制御システム（ICS）のセキュリティ－10大脅威と対策2022－」の日本語版を発表した。そこでは、近年セキュリティリスクの増大が指摘される産業用制御システムがさらされている10の脅威とその原因、脅威のシナリオ、そして脅威を軽減するための対策を解説している。

10の脅威のうち特に注目したいのは、2019年から増加傾向にある脅威だ。その多くがインターネットなど外部と接続されるようになったことに起因している。ここでは中でも増加傾向が顕著な「インターネットやイントラネット経由のマルウエア感染」と「サプライチェーンにおけるソフトウエアおよびハードウエアの脆弱性」について取り上げてみたい。

「インターネットやイントラネット経由のマルウエア感染」の原因は企業ネットワークで使われているOSやデータベース、ブラウザ、電子メールなどのコンポーネントの脆弱性にある。これらのコンポーネントにはほぼ毎日新たな脆弱性が発見され、サイバー攻撃者はその脆弱性を突いてくる。

攻撃者がインターネット上の脆弱性を悪用してイントラネットに侵入し、悪意を持ったソフトウエアであるマルウエアをイントラネット上に忍ばせる。産業用制御システムが接続されているネットワークに攻撃者が侵入しても、必ずしも従業員が気付くとは限らない。

想定される脅威のシナリオとしては、電子メールの添付ファイルやオフィス文書などを介したり、細工された外部サイトに誘導されたりすると、産業用制御システムが感染する。感染すると産業用制御システムのコンポーネントがマルウエアの操作によって悪用されたり、企業Webサイトが攻撃されたりする。

対策としては従来のようなファイアウォールやウイルス対策ソフトなどの水際対策に加えて、ネットワークを最大限分離して攻撃経路をできるだけ限定したり、産業用制御システムのネットワークに定期的かつタイムリーにパッチを適用したり、侵入検知システムで通信状況をモニタリングしたりするなどが挙げられる。

サプライチェーンの脅威はより複雑で広範囲… 続きを読む