事例で学ぶセキュリティインシデント（第14回）

管理の目が届きにくいIoTデバイスが狙われる

2024.07.16

化学メーカーのN社。神戸にある工場の保守担当者はモニターを見ていて、配管設備に設置された温度センサーの異常に気付いた。「あれっ、昨日からの温度データが制御システムに届いていない」。センサーの故障かと思ったが、異常を起こしているセンサーは同じ配管設備に設置された複数台に上る。保守担当者は工場の管理者に異常事態を伝えるとともに、本社のIT担当者に連絡した。

そして、IT担当者はIoTデバイスへの攻撃を疑った。「IoTデバイスの脆弱性を悪用した攻撃があることは知っていたが、まさかうちが」。IoTデバイス以外の制御システムや生産管理システムなどに被害が及んでいれば大変な事態になる。IT担当者は本社の役員・管理職にインシデントの疑いを報告し、神戸工場へ向かった。

IoTの利用拡大で問題になるセキュリティ対策

IoTデバイスやセンシング技術などの進化を背景に、IoTの利用が拡大している。産業用設備・機器や制御システムをはじめ、医療機器、建設機械、オフィス機器、車などのモビリティー、監視カメラ、情報家電など、さまざまな分野の製品がインターネット(ネットワーク)に接続され、IoTデバイスが収集するデータの活用や遠隔からの制御を可能にしている。

その利用拡大とともにセキュリティの問題も深刻化している。かつてはインターネットに接続することを想定していなかった機器がインターネットにつながるようになり、攻撃されるリスクが高くなっているのだ。

攻撃者がIoTデバイスの脆弱性や管理用パスワードを悪用し、不正アクセスなどの攻撃を仕掛ける。攻撃者はIoTデバイスの不正利用や不正操作を行い、IoTデバイスの設定が変更されるなど業務に支障を来す恐れもある。

そして、IoTデバイス特有の問題がセキュリティ対策を難しくしている。インターネットに接続されるオフィスや工場などのパソコンやサーバー、ネットワーク機器であれば、セキュリティパッチの適用やアンチウイルスなどのセキュリティ対策を行う。だが、IoTデバイスはインターネットに接続されているという利用者の意識が薄く、脆弱性などのセキュリティ対策がおろそかになりがちだ。

センサーなどのIoTデバイスは人目が届きにくい屋外に設置されるものもあり、攻撃されてもすぐには気付きにくい。また、数多くのIoTデバイスを長期間にわたって利用するケースもあり、IoTデバイスメーカーが脆弱性対策として提供するセキュリティパッチやファームウエアなどをすべてのIoTデバイスに適用するのが難しいといった問題もある。

セキュリティ対策としては、初期設定のパスワードを類推されにくいものに変更する、IoTデバイスメーカーから提供されるセキュリティパッチの適用やファームウエアを更新する、メーカーのサポート期間が切れたデバイスの利用は止める、IoTデバイスを接続するネットワーク機器のセキュリティ対策を再検討するなど、さまざまな方法が考えられる。

IoTデバイスの導入で設備の保守業務を効率化… 続きを読む