Process Safety Beacon
Messages for Manufacturing Personnel
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

サイバーセキュリティと化学プラントの運転

2021年7月

図1. フロリダ州Oldsmarの水処理プラント

2021 年 2 月 5 日、フロリダ州Oldsmarの水処理プラントで、ある従業員は制御コンピューターの画面上でカーソルが奇妙な動きをしていることに気付いた。 プラントでは、リモート アクセス ソフトウェアを使用して、スタッフが画面を共有し、IT の問題をトラブルシューティングできるようにしていた。また監督者も、しばしば自分のコンピュータを接続して、施設のシステムを監視していた。初めは気にしていなかったが、数時間後、オペレーターはカーソルが水処理プラントのコントロール画面上を移動してクリックしていることに気付いた。数秒も経たない内に、侵入者はシステムの水酸化ナトリウムの設定値を 100ppm から 11,100ppm に変更しようとした。オペレーターはすぐにその侵入に気付き、水酸化ナトリウムを通常のレベルに戻した。幸い、水質には影響しなかった。

最近、コロニアル・パイプラインがランサムウェアの攻撃を受けて、米国東海岸へのガソリンの供給が数日間停止される事態が発生した。

あなたの会社のシステムもおそらくインターネットに接続されており、サイバー攻撃からの防御が必要であろう。企業がサイバー攻撃をかわすための戦略には、ファイアウォール、ウイルス対策ソフトウェア、マルウェアやコンピュータ ウイルスから保護するための方策などがある。

リモートで働く人が増えており、 その為、サイバー攻撃の機会も増加している。

知っていますか

- サイバー犯罪者たちは、巧妙なマルウェアを使用して、いくつもの脆弱性を突いて彼らの目的を果たそうとする。
- 金銭目的のツールとして、組織犯罪者たちによるランサムウェア攻撃が増加している。
- 最近の調査によると、サイバー攻撃は 39 秒に 1 回発生している。 (参考. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- フィッシングは、信頼できる企業からと思わせる電子メールを送信して、個人に個人情報を開示させるように誘導する。 この攻撃は、マルウェア侵入の常とう手段である。
- サイバー攻撃の脅威は、電子メール、添付ファイル、および USB ドライブやその他のポータブル の記憶媒体 など、可搬式の外付け機器から会社のシステムに侵入する可能性がある。
- サイバー セキュリティの穴の 95% は人のミスが原因となっている。(参考. https://www.cybintsolutions.com/employee-education-reduces-risk/)

あなたにできること

- ソフトウェア のアップデートの要求が来たら実行する前に必ず IT 部門に確認を取り、承認されたら迅速にインストールすること。
- 自分のファイアウォールやその他のネットワーク 用ソフトウェアが最新で、有効になっていることを確認すること。
- システムとデータを定期的にバックアップすること。
- すべてのアクセスに強力なパスワードを使用すること。 パスワードやアカウントは他人と共有せず、定期的にパスワードを変更すること。
- ブラウザ上にパスワードを保存しないこと。
- 知らない人から送信されたメールのリンクや添付ファイルをクリックしないこと。
- 会社のコンピュータに未承認のソフトウェアをインストールしないこと。 アクセス キーやその他の物理的なセキュリティ デバイスが適切に機能していることを確認すること。
- リモート アクセスをする場合は、会社のルールに従うこと。公共のインターネット サイトを使用する場合は、特に注意すること。
- コンピューターが何かおかしい、またはいつもと違うと思われる場合は、助けを求めること。 ハッカーがアクセスを試みている可能性がある。

サイバー攻撃は現実のものだ。 あなたは防御の重要な一員である。