Process Safety Beacon
製程安全明鑑
提供給製造業人員的訊息
www.aiche.org/ccps/process-safety-beacon
An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps
本期贊助者
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

網路安全與化工廠操作

2021年 7月號

圖 1. 佛羅里達州 Oldsmar市水處理廠

2021 年 2 月 5 日，於美國佛羅里達州奧茲馬市(Oldsmar)的某水處理廠，一名員工注意到控制電腦螢幕上的游標在奇怪地移動，最初並沒有擔心；該工廠使用可遠端使用的軟體，允許員工共享螢幕並解決 IT的問題。主管也經常連接到操作員的電腦來監控設施的系統。幾個小時之後，操作員注意到游標在移動並點擊水處理廠的控制。在幾秒鐘內，入侵者試圖將系統的氫氧化鈉設定值從百萬分之 100 (ppm) 更改為 11,100 ppm。操作員迅速發現了入侵，並將氫氧化鈉調回正常的水準。幸運的是，未影響到水質。

最近針對 Colonial Pipeline公司的勒索軟體攻擊，使美國東海岸的汽油供應中斷了幾天。

您公司的系統可能已連接到網際網路，需要保護以免受網路威脅。公司都使用多種策略來嚇阻網路威脅，例如：防火牆、防病毒軟體，以及防止惡意軟體與電腦病毒的策略。

更多的人在遠端工作；這就增加了網路攻擊的機會。

你知道嗎?

- 網路犯罪分子使用複雜的惡意軟體，以利用多個弱點而實現其目標。
- 勒索軟體攻擊越來越多，有組織的犯罪分子將其作為賺錢的工具。
- 根據最近的一項研究，每 39 秒就會發生一次網路攻擊。（參考 https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds）
- 網路釣魚會發送電子郵件，據稱來自信譽良好的公司，以誘使個人透露其個人資料。 這些攻擊是惡意軟體的主要入侵方法。
- 網路威脅可以經由電子郵件、附件和隨身儲存設備（例如拇指碟或其他隨身儲存裝置）進入公司的系統。
- 95% 的網路安全缺口是由人為錯誤所造成的。（參考 https://www.cybintsolutions.com/employee-education-reduces-risk/）

你可以做什麼？

- 隨時要與 IT 人員確認軟體更新的請求，然後再進行下去，並且及時安裝經核准的更新版軟體。
- 要確保您的防火牆和其他網路軟體都是最新版的，而且已打開使用。
- 要確保定期備份您的系統和數據。
- 所有的登入都要使用強密碼。 不要共享密碼或帳戶，並且要定期更改密碼。
- 不要在瀏覽器上儲存密碼。
- 不要點擊您不認識的人所發送的電子郵件中的超連結或附件。
- 切勿在任何公司電腦上安裝未經批准的軟體； 確保使用存取鍵和其他實體安全裝置都有適當保護。
- 如果您使用遠端存取，要遵循公司的規定要求。 如果使用公共互聯網站，要特別警惕。
- 如果您的電腦上的某些內容看起來很奇怪或異常，要尋求協助！ 有可能是駭客試圖獲得使用權限。

網路攻擊是真實存在的。你就是防衛的重要份子。