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

ความปลอดภัยบนโลกไซเบอร์และการดำเนินการผลิตในอุตสาหกรรมเคมี

กรกฎาคม 2564

รูปที่ 1. โรงบำบัดน้ำเสีย เมืองโอลสมาร์ รัฐฟลอริดา

เมื่อวันที่ 5 กุมภาพันธ์ 2564 พนักงานในโรงบำบัดน้ำเสียที่เมืองโอลสมาร์ รัฐฟลอริดาสังเกตุเห็นว่าเคอร์เซอร์บนจอคอมพิวเตอร์ของเขาเคลื่อนไหวแปลก ๆ ในตอนแรกเขาไม่ได้กังวลใด ๆ ; โรงงานมีการใช้ซอฟท์แวร์การเข้าถึงจากระยะไกล (remote access) เพื่อให้พนักงานสามารถแชร์หน้าจอและแก้ปัญหาด้านไอทีได้ บ่อยครั้งที่หัวหน้างานเชื่อมต่อเข้ามากับคอมพิวเตอร์เพื่อตรวจสอบระบบของโรงงานด้วย หลังจากนั้นไม่กี่ชั่วโมง โอเปอเรเตอร์สังเกตเห็นว่าเคอร์เซอร์มีการเคลื่อนไหวและคลิกไปที่ระบบควบคุมของโรงบำบัดน้ำเสีย ภายในไม่กี่วินาที ผู้บุกรุกพยายามที่จะเปลี่ยนค่าโซเดียมไฮดรอกไซด์ของระบบจาก 100 ppm เป็น 11,000 ppm โอเปอเรเตอร์ตรวจพบการบุกรุกอย่างรวดเร็วและปรับค่าโซเดียมไฮดรอกไซด์กลับสู่ระดับปกติ โชคดีที่ไม่มีผลกระทบอะไรกับคุณภาพของน้ำ

การโจมตีด้วยซอฟท์แวร์เพื่อเรียกค่าไถ่ (ransomware) ครั้งล่าสุดบนท่อส่งก๊าซโคโลเนียล ทำให้ไม่มีน้ำมันจ่ายไปยังชายฝั่งตะวันออกของสหรัฐฯ เป็นเวลาหลายวัน

ระบบของบริษัทคุณอาจเชื่อมต่อกับอินเตอร์เน็ทและต้องการการป้องกันจากภัยคุกคามทางไซเบอร์ มีกลยุทธ์มากมายที่บริษัทใช้เพื่อป้องกัน เช่น : การใช้ firewalls, ซอฟท์แวร์ป้องกันไวรัส และ นโยบายในการป้องกัน malware - ซอฟท์แวร์ที่ออกแบบมาเพื่อสร้างความเสียหายกับระบบคอมพิวเตอร์ และไวรัสคอมพิวเตอร์

มีคนที่ทำงานจากทางไกล (work remote) มากขึ้น; ยิ่งเพิ่มโอกาสในการถูกโจมตีทางไซเบอร์มากขึ้น

คุณทราบหรือไม่?

- อาชญากรในโลกไซเบอร์ใช้ malware ที่ซับซ้อนเพื่อใช้ประโยชน์จากช่องโหว่ทั้งหลายเพื่อให้บรรลุเป้าหมายในการก่อเหตุ
- การโจมตีด้วยซอฟท์แวร์เพื่อเรียกค่าไถ่ (Ransom ware attack) กำลังเพิ่มขึ้นจากกลุ่มอาชญากรที่ใช้มันเป็นเครื่องมือในการหาเงิน
- จากผลการศึกษาล่าสุด, การโจมตีในโลกไซเบอร์เกิดขึ้นทุก ๆ 39 วินาที (อ้างอิง : https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Phishing คือการส่งอีเมล์จากบริษัทที่ดูเหมือนจะมีชื่อเสียง เพื่อชักจูงให้บุคคลเปิดเผยข้อมูลส่วนบุคคล การโจมตีแบบนี้เป็นวิธีเริ่มต้นสำหรับ malware.
- ภัยคุกคามทางไซเบอร์สามารถเข้ามาในระบบของบริษัทผ่านทางอีเมล์ สิ่งที่แนบมา และ จากอุปกรณ์จัดเก็บข้อมูลแบบพกพาต่าง ๆ เช่น thumb drives หรือ อื่น ๆ
- 95% ที่ทำให้ความปลอดภัยทางไซเบอร์เกิดช่องโหว่เกิดจากความผิดพลาดของมนุษย์ (อ้างอิง : https://www.cybintsolutions.com/employee-education-reduces-risk/)

คุณสามารถช่วยอะไรได้?

- ตรวจสอบคำขออัปเดตซอฟท์แวร์กับฝ่ายไอทีเสมอก่อนดำเนินการ และ ติดตั้งการอัปเดตที่ได้รับการอนุมัติในเวลาที่เหมาะสม
- ตรวจสอบให้แน่ใจว่า firewall และ ซอฟท์แวร์เครือข่ายอื่น ๆ ของคุณทันสมัยและเปิดใช้งานอยู่
- ตรวจสอบให้แน่ใจว่าได้ทำการสำรองข้อมูลระบบและข้อมูลของคุณอย่างสม่ำเสมอ
- ใช้รหัสผ่านที่รัดกุมสำหรับการเข้าถึงระบบทั้งหมด อย่าแชร์รหัสผ่านหรือ ชื่อบัญชี และ เปลี่ยนรหัสผ่านเป็นประจำ
- อย่าบันทึกรหัสผ่านบนบราวเซอร์
- อย่าคลิกบนลิงค์ หรือ สิ่งที่แนบมาในอีเมล์ที่ส่งมาจากคนที่คุณไม่รู้จัก
- อย่าติดตั้งซอฟท์แวร์ที่ไม่ได้รับอนุมัติลงในคอมพิวเตอร์ใด ๆ ของบริษัท; ตรวจสอบให้แน่ใจว่า access keys และ physical security devices อื่นๆ อยู่ในจุดที่ปลอดภัย
- หากคุณใช้ remote access, ปฏิบัติตามข้อกำหนดของบริษัท ระมัดระวังเป็นพิเศษหากใช้บริการอินเตอร์เน็ตสาธารณะ
- หากบางอย่างในคอมพิวเตอร์ของคุณดูแปลกหรือแตกต่างไปจากเดิม ขอความช่วยเหลือ! อาจเป็นแฮคเกอร์ที่พยายามเข้าถึงข้อมูลของคุณ

การโจมตีทางไซเบอร์มีอยู่จริง คุณเป็นส่วนสำคัญในการป้องกัน