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

후원사
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

사이버 보안과 화학공정 운영

2021년 7월

플로리다주 올즈마 수처리 플랜트

2021년 2월 5일 플로리다주 올즈마 수처리 플랜트의 한 직원이 제어 컴퓨터 화면에서 커서가 이상하게 움직이고 있는 것을 감지했습니다. 이 플랜트는 원격 액세스 소프트웨어를 사용하여 직원들이 화면을 공유하고 IT 문제를 해결할 수 있도록 하고 있어 처음엔 대수롭지 않게 여겼습니다. 관리자가 종종 운영인원의 컴퓨터에 접속해 시설의 시스템을 모니터링합니다. 몇 시간 후, 운전원이 커서가 이동하여 수처리 플랜트의 제어 기능을 클릭하는 것을 발견했습니다. 몇 초 만에 침입자는 시스템의 수산화 나트륨 설정치를 100 ppm에서 11,100 ppm으로 변경하려고 시도했습니다. 운전원은 신속하게 침입을 감지하고는 수산화 나트륨 수치를 정상 수준으로 복구했습니다. 다행히도 수질엔 영향이 없었습니다.

최근 미국 송유관 업체인 콜로니얼 파이프라인이 랜섬웨어 공격을 받아 며칠 동안 미국 동부 해안에 휘발유 공급이 차단되었습니다.

회사 시스템은 대개 인터넷에 연결되어 있으며 사이버 위협으로부터 보호가 필요합니다. 방화벽, 바이러스 백신 소프트웨어 및 악성 코드(멀웨어)와 컴퓨터 바이러스로부터 보호하기 위한 정책과 같은 사이버 위협을 억제하기 위해 회사는 많은 전략을 활용합니다.

더 많은 사람들이 원격으로 일하게 되면서, 이로 인해 더 많은 사이버 공격에 노출되고 있습니다.

알고 계셨나요?

- 사이버 범죄는 정교한 악성 코드를 사용하여 여러 취약점을 활용해 목표를 달성하려고 합니다.
- 랜섬웨어 공격은 조직적인 범죄자들의 돈을 버는 도구로 사용되면서 빈도가 증가하고 있습니다.
- 최근 연구에 따르면 사이버 공격은 39초마다 발생하고 있습니다.(참고 https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- 피싱은 평판이 좋은 회사로 가장해 개인에게 개인 정보를 공개하도록 유도하는 이메일을 보내고 있습니다. 이러한 공격은 악성 코드의 주요 입질 방법입니다.
- 사이버 위협은 이메일, 첨부 파일 및 소형 메모리 드라이브나 기타 휴대용 저장 장치를 통해 회사의 시스템으로 유입될 수 있습니다.
- 사이버 보안 침해의 95%는 인적 오류로 인해 발생합니다. (참고 https://www.cybintsolutions.com/employee-education-reduces-risk/)

무엇을 할 수 있을까요?

- 소프트웨어 업데이트를 실행하기 전에 항상 IT담당자에게 업데이트 요청이 사실인지 확인하고, 승인 된 업데이트는 신속하게 설치하십시오.
- 방화벽 및 기타 네트워크 소프트웨어가 최신 상태로 작동하고 있는지 확인합니다. 시스템과 데이터를 정기적으로 백업해야 합니다.
- 모든 액세스에 강력한 암호를 사용합니다. 암호나 계정을 공유하지 말고 정기적으로 암호를 변경하십시오.
- 브라우저에 암호를 저장하지 마십시오.
- 모르는 사람이 보낸 이메일에서 링크나 첨부 파일을 클릭하지 마십시오.
- 회사 컴퓨터에 승인되지 않은 소프트웨어를 설치하지 마십시오. 액세스 키나 다른 물리적 보안 장치가 제대로 꽂혀 있는지 확인합니다.
- 원격 액세스를 사용하는 경우 회사의 요구 사항을 따릅니다. 공용 인터넷 사이트를 사용하는 경우 특히 경계하십시오.
- 컴퓨터 상에 무언가가 이상하거나 평소와는 달리 보이는 경우 도움을 요청하십시오! 액세스 권한을 얻기 위한 해킹 시도일 수 있습니다.

사이버 공격이 실제로 벌어지고 있습니다. 당신이 사이버 방어의 주역입니다.