Study on Nuclear Facility Cyber Security Awareness and Training Programs

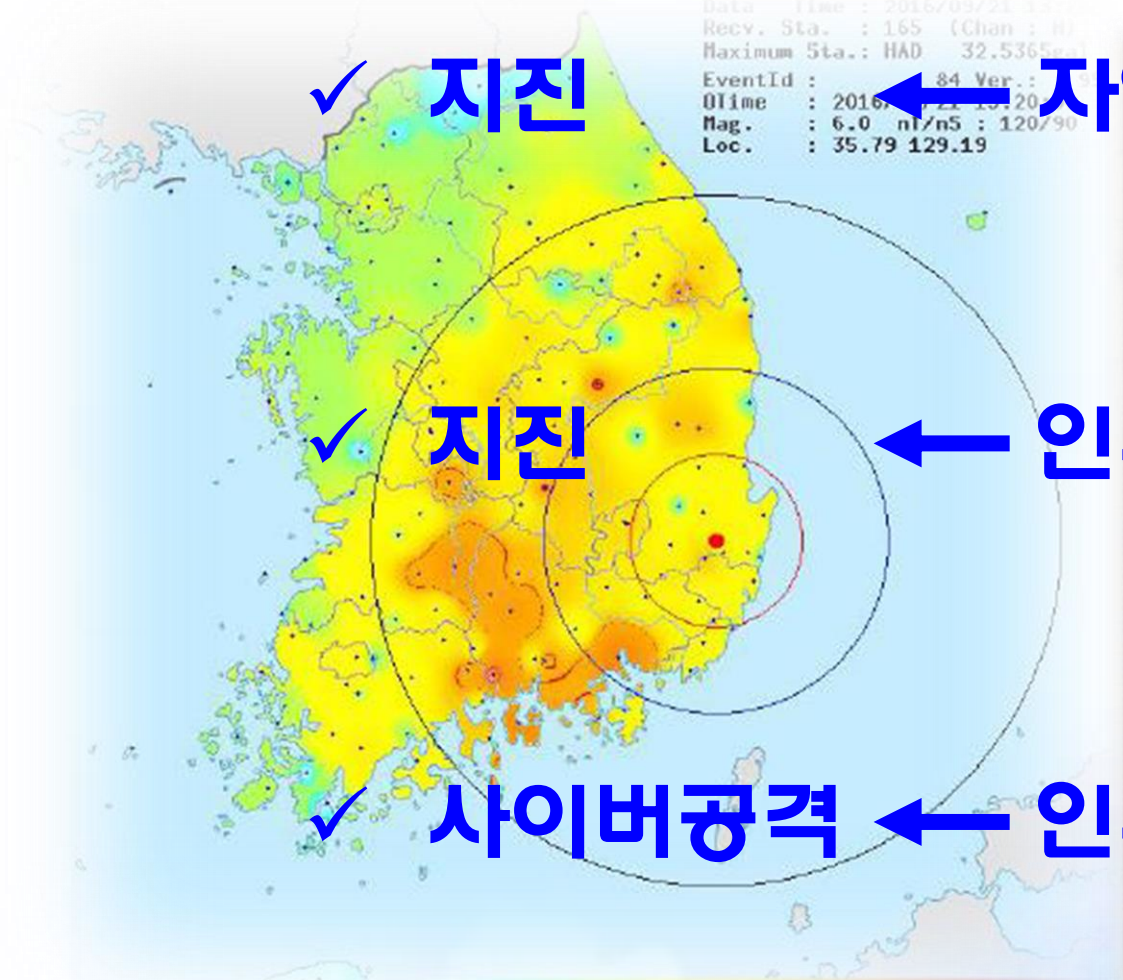
2016.10.

계측제어·인간공학연구부

이 정 운, 송 재 구, 이 철 권

KAERI 한국원자력연구원
Korea Atomic Energy Research Institute

사이버보안의 중요성



✓ 지진 ← 자연 재해

✓ 지진 ← 인위적/의도적 재해

✓ 사이버공격 ← 인위적/의도적 재해

Stuxnet worm hit industrial systems

"the worm eats away at a very specific kind of industrial control system: a configuration of the Siemens-manufactured Supervisory Control and Data Acquisition (SCADA) system that commands the centrifuges enriching uranium for Iran's nuclear program, the key step for an Iranian bomb", Wired Jan 16, 2011

사이버보안 인식 및 훈련의 중요성/시급성

- 현황
  - 규제요건 KINAC/RS-015 (2014) 공표
  - 단계별 사이버보안 프로그램 이행 계획 진행중
  - “사이버보안 인식 및 훈련”은 6단계 ‘운영적 보안조치’ 중의 하나로 이행 예정

단계	이행 항목	내용
1단계	사이버보안 조직 구성	• 사이버보안 이행조직 구성 • 비상사건 대응 조직 구성
2단계	필수디지털자산 식별	• 필수시스템 식별 • 필수디지털자산(CDA) 식별
3단계	심층방호 및 비상대응	• 등급분류 및 분류기준 이행 • 비상사건 대응 계획 및 이행
4단계	매체통제	• 이동형 매체 및 모바일 기기(PMMD) 통제 • 유지보수 및 시험 기기 통제
5단계	무결성 유지	• 내부위협에 대한 CDA 무결성 유지조치 • 불법접근 방지 조치
6단계	보안조치 #1	• 운영적 보안조치 이행 • 관리적 보안조치 이행
7단계	보안조치 #2	• 기술적 보안조치 이행

사이버보안 인식 및 훈련의 중요성/시급성

- 사이버보안 업무는 사이버보안팀만의 업무가 아님
- 관련 기관 전체직원(협력사, 제작사 등 포함)의 노력이 필요
- 초기단계부터 인식 교육 전파가 필요
- 사이버 안전문화의 확보

- 사이버보안 활동의 효과적 이행을 위해 사전 교육 필요
  - 필수계통/필수디지털자산 식별,
  - 심층방호 전략 수립 및 적용,
  - 101개 보안조치 현황평가 및 필요한 보안조치 적용,
  - 변경관리,
  - 비상대응 등

- 현재 관심 밖에 있음

규제요건(RS-015)의 관련 항목

- 본문
  - 2.2.1 사이버보안 조직의 구성 및 역할
  - 2.2.5.2.5 인식제고 및 훈련
  - 2.3.1.2 비상사건대응 훈련
  - 2.3.2.3 비상 복구계획 점검 및 훈련
  - 2.3.2.4 비상 복구 교육

- 부록1. 사이버보안계획 작성 양식
  - 4.3 교육 및 훈련에 관한 사항
  - 4.3.1 교육 및 훈련
  - 4.3.1.1 비상사건 대응 훈련
  - 4.3.1.2 비상 복구계획 점검 및 훈련
  - 4.3.1.3 비상 복구 교육

- 부록 2. 사이버 보안조치
  - 2.5 인식제고 및 훈련
  - 2.5.1 인식제고 및 훈련 범위
  - 2.5.2 인식제고 프로그램
  - 2.5.3 기술적 훈련
  - 2.5.4 특화된 사이버보안 훈련
  - 2.5.5 교육훈련 피드백

사이버보안 인식 및 훈련 프로그램의 종류 및 대상

교육 및 훈련의 종류	교육 및 훈련 대상
1. 인식제고 프로그램	계약업체 직원을 포함하는 전직원
2. 기술적 훈련	1) 계통담당자 : – 필수디지털자산 설계, 설치, 운영, 유지보수 혹은 관리에 책임과 역할을 가지는 직원 – 시스템 관리자, 시스템 사용자, 네트워크 관리자 및 기타 필수디지털자산에 접근가능한 직원 2) 사이버보안조직
3. 특화된 사이버보안 훈련	사이버보안조직 및 비상사건대응조직
4. 비상사건대응 및 복구를 위한 교육 및 훈련	비상사건대응조직 및 계통담당자

사이버보안 인식제고 교육 내용(안)

인식제고 프로그램 내용
1) 일반적 사이버 위협 및 방법 또는 공격 기술 (‘새로운 위협 및 기술’이 있다면 분석하여 추가)
2) 사이버 침해사례의 공격방법, 공격 영향 등 (원자력시설 또는 이와 유사한 산업제어시스템에 대해)
3) 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 의미와 침해되었을 경우의 위해성
4) 다섯가지 공격 벡터 (네트워크, 무선, 이동형 매체 및 장비, 공급경로(Supply Chain), 물리적 접근)
5) 사이버보안 프로그램 (CSP) 이해 (목적, 범위, 조직구성, 자산식별 및 분석, 단계별 보안 전략, 보안성 평가, 기술적, 운영적, 관리적 보안조치 적용, 지속적인 감시와 평가, 변경통제 등)
6) 기술적, 운영적, 관리적 보안조치의 이해 (정책 및 요건 개요, 보안조치 부재 시의 영향 등)
7) 사이버보안 정책, 절차, 요건의 위배 및 의심스러운 활동, 비상사건 등에 따른 보고 절차
8) 앞의 교육내용에 포함되지 않은 기타 용어 정의

기술적 훈련 내용(안)

계통담당자의 사이버보안 연계업무	기술적 교육훈련 내용
1) 필수시스템 식별 및 필수디지털자산 식별	– 필수시스템 및 필수디지털자산의 정의 – 식별 방법 및 절차
2) 심층방호전략에 따른 필수디지털자산 등급분류 및 위반구역 조사	– 심층방호전략의 의미 – 등급분류 기준 및 등급분류 결과 – 위반 구역 조사 방법 및 해결방안
3) 필수디지털자산의 사이버보안조치 규제요건 부합 현황 평가	– RS-015의 101개 보안조치 항목에 대한 요건 설명 – 평가 방법 및 절차 – 보안조치 항목의 해당여부 및 요건 만족 판단 기준
4) 추가 또는 보완이 필요한 사이버보안조치의 적용을 위한 구현방안 수립 및 타당성 분석, 보안조치 구현 및 실효성 시험	– 사이버보안조치 구현방안 선정 방법 및 절차 – 적합성 및 적용성 판단 기준 – 실효성 판정 기준
5) 필수디지털자산 및 관련 디지털자산에 대해 부여된 사이버보안조치 이행 가. 해당 기술적 보안조치에 관한 운영 나. 해당 운영적 및 관리적 보안조치의 이행	– 해당 보안조치의 이행 절차
6) 변경통제 이행	– 이행 절차 – 변경 시 사이버보안 영향성 평가 방법

특화된 사이버보안 훈련

- 요건
  - 가. 데이터보안, 운영체제 보안, 응용시스템 보안, 네트워크 보안, 보안조치, 침입 분석, 비상사건 관리 및 대응, 디지털 포렌직, 침투테스트, 시스템 기능 등에 대한 최신의 기술 및 지식
  - 나. 취약점 제거, 필수디지털자산에 대한 사이버보안 강화 및 사이버공격에 따른 영향을 최소화하기 위한 기술 및 도구의 사용에 관한 사항
  - 다. 다른 직원들에게 사이버보안 가이드, 지침 및 훈련을 제공할 수 있도록 하기 위한 기술
  - 라. 사이버보안계획 및 이행을 검토하기 위한 기술
  - 마. 필수디지털자산이 사이버보안계획을 준수하는지 평가하기 위한 기술
  - 바. 보안조치의 설계, 획득, 설치, 운영, 유지보수 및 관리하기 위한 기술
- 국내 프로그램 개발 필요
- 해외 유사 훈련 프로그램 활용

해외 유사 프로그램

- SANS 프로그램
  1. ICS410: ICS/SCADA Security Essentials
  2. ICS515: ICS Active Defense and Incident Response
  3. Hosted: Assessing and Exploiting Control Systems
  4. Hosted: Critical Infrastructure and Control System Cybersecurity
  5. FOR508: Advanced Digital Forensics and Incident Response
  6. FOR572: Advanced Network Forensics and Analysis
  7. FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
  8. SPECIAL: Introduction to Malware Analysis: Hands-on and Technical

- ISA 프로그램
  1. Assessing the Cybersecurity of New or Existing IACS Systems (IC33)
  2. IACS Cybersecurity Design & Implementation (IC34)
  3. IACS Cybersecurity Operations & Maintenance (IC37)
  4. Industrial Networking and Security (TS12)
  5. Advanced Industrial Networking and Cyber Security (TS20)

해외 유사 프로그램

- Black Hat 2016 Conference의 관련 사이버보안 Training
  1. Assessing and Exploiting Control Systems
  2. Attacking, Defending And Building SCADA Systems
  3. Advanced Infrastructure Hacking: 2 Day
  4. Advanced Infrastructure Hacking: 4 Day
- Cansec West Conference Training

- Infosec Institute의 SCADA/ICS Security Boot Camp
- Cybati의 Control System Cybersecurity Course 및 Training Kit CybatiWorks™

비상사건 대응 및 복구 훈련

- 주기적 점검 및 훈련(최소 년 1회 이상)
- 개발된 비상사건대응 절차 및 가상 시나리오를 기반으로 한 모의훈련
  - 비상사건 처리
  - 비상사건의 모니터링
  - 필수디지털자산 백업
  - 복구 및 재구성

- 현재 가용한 탐지 및 분석 방법을 기준으로 비상사건대응 절차 개발
- 탐지 및 분석 관련 보안조치의 구현 상황, 분석 기술의 개발 정도 등에 맞추어 비상사건대응 절차 보완
- 발전되는 비상사건대응 절차에 따라 비상대응 및 복구 훈련 시나리오 보완

Questions & Comments ?