지식경제부 보도참고자료 함께하는 공정사회! 더 큰 희망 대한민국
http://www.mke.go.kr
문의 : 정보화담당관실 박영삼과장(02-2110-5231), 이학동 사무관(02-2023-1812)

전력망 해킹 장면의 진실과 거짓

□ 최근 SBS 드라마 "유령"은 불순분자가 사용자PC를 원격 조정하고 전력망을 장악해 대규모 정전사태가 발생하는 장면을 방영함

o 기본적으로 드라마는 시청자들의 흥미와 재미를 위해 다소의 픽션 요소를 담고 있는 바, 주요 장면의 진실과 거짓을 가려냄으로써 국민들의 이해를 돕고 해킹에 대한 불필요한 불안감을 해소코자 함

※ 지경부에서는 지난 '09년 **'Black Friday'**라는 제목으로 유사한 시나리오를 동영상으로 제작하여 모의훈련 실시 후 관계자들에게 보안 경각심 고취를 위해 배포

□ (장면 1) 불순분자가 대한전력 직원 집에 잠입, PC에 전력 제어시스템을 공격하는 스턱스넷을 심어 놓아 USB를 꽂으면 스턱스넷에 감염되도록 하고 이를 대한전력 직원이 회사에서 전력제어용 PC에 꽂으면 전력제어망이 감염되어 대규모 정전사태가 발생(그림 1)

→ (거짓) 전력 제어용 PC는 USB포트를 사용할 수 없도록 물리적으로 봉인·운영하고 있어 감염된 USB를 사용할 수 없는 환경임

→ (진실) 가정에서 사용 중인 USB가 스턱스넷에 감염되는 상황은 가능

□ (장면 2) 해커가 전력자동화시스템을 해킹하여 원격에서 파괴명령을 내리고, 해당 시스템의 파괴로 인하여 발전소의 발전량이 늘어남에 따라 원자력발전소 폭발을 시도하는 시나리오 (그림2)

→ (거짓) 전력제어시스템 및 전력자동화시스템은 인터넷망과 분리되어 폐쇄망으로 운영하고 있으므로, 외부에서 접근이 불가능

* 일반 제어시스템이 인터넷망과 연결되어 있는 경우 해당 시나리오는 가능할 수 있음

□ (장면 3) 해커가 발송한 메일의 첨부파일에 멜리사 악성코드가 숨겨져 있어 사용자가 첨부파일을 열어보는 순간 악성코드에 감염되어 메일 수신함의 주요 메일을 해커에게 전달하는 시나리오 (그림3)

→ (진실) 멜리사 악성코드는 해커들이 자주 사용하는 기술로서 이를 일부 변형하여 개인 메일을 탈취할 수 있으므로 주의가 필요


(그림1)


(그림2)



(그림3)

□ 지경부에서는 전력·가스 등 정보통신기반시설 보호를 위해 지식경제사이버안전센터를 통해 365일 24시간 보안 모니터링을 실시하고 있으며, 사전적인 보안 취약점 점검활동을 상시적으로 진행하고 있음

○ 국가가반시설을 외부 인터넷망으로부터 분리하고 외부저장매체(USB) 접속용 포트를 물리적 봉인하는 등 해킹사고 예방에 만전을 기하고 있음

□ 다만, 해킹기술이 하루가 다르게 발전하고 있으므로 우리가 사이버안전에 조금이라도 방심한다면 드라마에서와 같이 엄청난 재앙을 초래할 수 있으므로 보안에 대한 관심과 실천이 필요함