"사회공학적 기법 이용 해킹 공격 증가 예상"

지난 연말부터 국내 원자력업계는 해킹 논란에 휩싸여 있다. 그런데 그 논란의 양상이 이제는 전력계통, 발전, 스마트그리드 등 전력산업 전반으로 확산되는 추세다. 무엇보다 국민들이 가장 우려하고 있는 '안전성' 부분과 직결되는 사안이라 논란에서 쉽게 벗어나기는 어려워 보인다.

한수원에 대한 해킹 사건으로 사이버보안 침해에 대한 대책 마련이 요구되고 있다. 이에 한수원에서는 조치 훈련 실시, 보안위원회 신설 등 침해 방지책 마련에 최선을 다하고 있다.

일단 해킹 사건이 발생하자마자 원자력안전위원회, 산업통상자원부, 국정원, 원자력통제기술원, 원자력안전기술원, 인터넷진흥원, 한전KDN 등 관계부처는 전문기관과 합동으로 지난해 12월 22~26일 고리와 월성원전을 대상으로 이번 사이버 위협에 따른 운전제어망에 대한 보안체계와 운전 안전성 영향 여부 등에 대해 긴급 점검을 실시했다. 주요 점검 내용은 제어시스템 네트워크상 외부 접점 여부, 제어시스템 및 사용 중인 휴대용 매체의 악성코드 감염 여부, 제어시스템 운영 건전성 등이었다. 점검 결과, 원전 제어시스템으로 침입할 수 있는 외부 고정 접점은 없어 사내 업무망 및 사외 인터넷망과 완전히 분리된 것을 확인했으며, 제어시스템 등에서 사이버테러 공격에 사용될 수 있는 악성코드는 발견되지 않았다.

또한, 원전 주기시험결과, 운전기록 등을 통해 제어시스템이 건전하게 운영되고 있음을 확인했다. 다만 제어시스템에 사용되는 일부 휴대용 저장매체와 일부 PC에서 일반적인 웜 · 바이러스의 과거 치료기록이 확인됐다.

지난해 말 한수원 해킹 사건 전력산업 전반으로 확산 추세
대응체계 강화 · 백신 검사 생활화 등 보안 조치 수행 중요

운전제어망에 대한 정부합동 점검기간중인 지난해 12월 22~23일 한수원은 운전 제어설비에 대한 사이버 공격을 가정하고, 원전정지 및 냉각상황 등 안전상태 유지에 필요한 조치를 훈련했다. 그리고 이에 대한 대책으로 한국수력원자력은 정보보안을 강화하기 위한 계획의 일환으로 컨트롤타워 역할을 할 보안위원회를 신설키로 했다. 정부도 3월까지 근본적인 보안 강화계획을 수립키로 했다.

원자력안전위원회 관계자는 "원자력시설 등의 방호 및 방사능 방재 대책법 시행령 및 시행규칙 등 개정에 따라, 내년부터 원전제어시스템에 대한 보안체계 검사를 강화해 수행할 계획"이라며 "원전의 건설 · 운영 허가 심사항목에 사이버 보안 분야를 포함할 수 있도록 제도화해 나가겠다"고 밝혔다.

산업부의 경우 오는 6월에 시행 예정인 '원전비리 방지를 위한 원자력발전사업자등의 관리 · 감독에 관한 법'에 따라 한수원에 사이버 보안 관련 조직, 인력, 예산 운영 실태를 점검하고 미흡사항에 대해 시정조치를 요구할 방침이다.

한편 최근 미래창조과학부가 발표한 자료에 따르면 악성코드가 지속적으로 증가하고 있고, 이에 따른 새로운 보안 취약점이 빈발하고 있는 것으로 나타났다.

미래부는 올해도 단기간에 대량의 좀비 PC를 확보하기 위해 다수의 악성코드 경유지를 악용하고, 유포채널도 홈페이지 중심에서 이메일, SNS, P2P 등 다양한 방식으로 변화해 나갈 것으로 예상했다. 또한, 소프트웨어 투자비용 절감효과가 높은 오픈소스 사용이 확대됨에 따라 오픈소스 취약점을 악용한 공격도 늘어날 것으로 보인다.

아울러 최근 소니픽처스, 한수원 사고와 같이 악성이메일 유포를 통해 주요 정보를 유출함으로써 협박 수단으로 이용하거나, 유출정보 공개 등 사회적 혼란을 야기하는 새로운 양상으로 진화하고 있고, 특히 지인 · 업무사칭, 사회적 이슈를 악용하는 등 '사회공학적 기법'을 이용한 공격이 시도될 것으로 예상된다.

따라서 미래부는 "APT(Advanced Persistent Threat) 공격 등에 대비한 주기적인 모의훈련 및 통합보안 체계 구축 등 대응체계를 강화하고, 이용자들은 최신 보안 업데이트 적용 및 백신 검사 생활화 등의 보안조치 수행이 중요하다"고 지적했다.