국가정보원 NATIONAL INTELLIGENCE SERVICE
KISA 한국인터넷진흥원

보도자료
Tel 02-3412-3412
2023. 10. 10

투·개표시스템 해킹 취약점 등 선관위 사이버보안 관리 부실 확인

- 선관위 · 국정원 · KISA 3개 기관 합동으로 7.17~9.22간 합동 보안점검 실시
- 선거인명부시스템 · 개표시스템 · 사전투표시스템 등 관련 해킹대응 취약점 다수 발견
- 선관위, 합동점검팀 권고 등을 바탕으로 총선前 사이버보안 역량 긴급 보완 예정

지난5월 국회 · 언론을 통해 선관위의 北 해킹대응 및 정보통신기반시설 관리에 대한 부실 우려가 제기된 이후, 선관위 · 국정원 · KISA가 합동보안점검팀을 구성하여 국회 교섭단체 추천 與野 참관인들 참여하에 7.17~9.22간 보안점검을 실시하였다.

합동 보안점검은 크게 △ 시스템 취약점 △ 해킹대응 실태 △ 기반시설 보안관리 등 3개 분야로 구분하여 진행되었다.

Ⅰ. '시스템 취약점 점검'은 기술적인 모든 가능성을 대상으로 가상의 해커가 선관위 전산망 침투를 시도하는 방식으로 이루어졌으며, 다음과 같은 보안 취약점들이 발견되었다.

【 투표 시스템 】

① 유권자 등록현황 · 투표 여부 등을 관리하는 '통합선거인명부시스템'에는 인터넷을 통해 선관위 내부망으로 침투할 수 있는 허점이 존재하고, 접속 권한 및 계정 관리도 부실하여 해킹이 가능한 것으로 확인되었다.

- 이를 통해, '사전 투표한 인원을 투표하지 않은 사람'으로 표시하거나 '사전 투표하지 않은 인원을 투표한 사람'으로 표시할 수 있고, 존재하지 않은 유령 유권자도 정상적인 유권자로 등록하는 등 선거인명부 내용을 변경할 수 있었다.

② 선관위의 내부시스템에 침투하여 사전투표 용지에 날인되는 廳印(선관위) · 私印(투표소) 파일을 절취할 수 있었으며, 테스트용 사전투표용지 출력 프로그램도 엄격하게 사용 통제되지 않아 실제 사전투표용지와 QR코드가 동일한 투표지를 무단으로 인쇄 가능함을 확인하였다.

③ 與野 정당 등 일부 위탁선거에 활용되는 '온라인투표시스템'에서는 정당한 투표권자가 맞는지를 인증하기 위한 절차가 미흡하여 해커가 대리 투표하더라도 확인이 되지 않는 문제점을 발견하였다.

④ 사전투표소에 설치된 통신장비에 사전 인가된 장비가 아닌 외부 非인가 PC도 연결할 수 있어 내부 선거망으로 침투가 가능함을 확인하였다.

⑤ 부재자투표의 한 종류인 '선상투표'의 경우에는 특정 유권자의 기표결과를 볼 수 없도록 암호화하여 관리하고 있으나, 시스템 보안취약점으로 암호 해독이 가능해 특정 유권자의 기표결과를 열람할 수 있었다.

【 개표 시스템 】

① 개표결과가 저장되는 '개표시스템'은 안전한 내부망(선거망)에 설치 · 운영하고 접속 패스워드도 철저하게 관리하여야 하나, 보안관리가 미흡하여 해커가 개표결과 값을 변경할 수 있음이 드러났다.

② 투표지분류기에서는 외부장비(USB 등) 접속을 통제해야 하나, 비인가 USB를 무단 연결하여 해킹프로그램 설치가 가능했고, 이를 통해 투표 분류결과를 바꿀 수 있었다. 또한 투표지분류기에 인터넷 통신이 가능한 무선 통신 장비도 연결할 수 있었다.

【 시스템 관리 】

① 선관위는 중요 정보를 처리하는 내부 중요 전산망을 인터넷과 분리하여 사전 인가된 접속만 허용하는 등 철저하게 관리해야 하나, 망분리 보안정책이 미흡하여 전산망間 통신이 가능, 인터넷에서 내부 중요망(업무망 · 선거망 등)으로 침입할 수 있었다.

② 선관위는 주요시스템 접속시 사용하는 패스워드를 숫자 · 문자 · 특수기호를 혼합하여 설정하는 등 안전하게 운영하여야 하나, 단순한 패스워드를 사용하고 있어 이를 손쉽게 유추하여 시스템에 침투가 가능하였다.

③ 선관위는 시스템 접속 패스워드 및 개인정보 등 중요정보를 암호화하여 관리해야 하나, △내부포털 접속 패스워드 △역대 선거시 등록한 후보자 명부 · 재외선거인명부 등을 평문으로 저장하고 있어 내부 주요서버 침투에 활용할 수 있었을 뿐만 아니라, 개인정보 대량 유출 위험성도 확인하였다.

II. 이미 발생했던 '해킹사고 대응' 부분에서도 후속 차단 · 보안 강화 조치가 미흡했던 사례들이 드러났다.

① 선관위가 최근 2년간 국정원에서 통보한 북한발 해킹사고에 대해 사전 인지하지 못하고 있었으며 적절한 대응조치도 하지 않았음을 확인하였다.

② 이메일 해킹사고의 피해자에게 통보조차 하지 않아 동일 직원 대상으로 사고가 연속으로 발생하였다.

③ 2021.4월경 선관위 인터넷PC가 북한 '킴수키(Kimsuky)' 조직의 악성코드에 감염되어 상용 메일함에 저장된 대외비 문건 등 업무자료와 인터넷PC의 저장자료가 유출된 사실도 확인되었다.

III. 선관위가 운영 중인 주요정보통신기반시설 보안관리 실태에 대해서도 엄정한 계량평가를 실시하였다.

① 선관위는 2022년도 '주요정보통신기반시설 보호대책 이행여부 점검' 자체 평가 점수를 100점 만점으로 국정원에 통보했으나, 합동보안점검팀이 31개 평가항목에 대해 동일기준으로 재평가한 결과, 전산망 및 용역업체 보안관리 미흡 등에 따라 31.5점에 그친 것으로 확인되었다.

② 취약점 분석평가를 관계 법령에서 정한 '정보보호 전문서비스 기업'이 아닌 무자격 업체를 통해 실시하는 등 법 위반 사례도 발견하였다.

합동보안점검팀은 국제 해킹조직들이 통상적으로 사용하는 해킹 수법을 통해 선관위 시스템에 침투할 수 있었는바, 북한 등 외부세력이 의도할 경우 어느 때라도 공격이 가능한 상황이었다고 설명하였다.

이번 점검은 국가 선거시스템 전반에 대한 보안취약점들을 선제 도출하는 계기가 되었으며, 합동점검팀은 선관위에 선거시스템 보안 관리를 국가 사이버위협 대응체계와 연동시켜 해킹대응 역량을 강화하는 방안을 제의하였다.

또한, 선관위와 함께 해킹에 악용 가능한 망간 접점, 사용자 인증절차 우회, 유추 가능한 패스워드 등을 즉시 보완하였으며, 최대한 빠른 시일내에 이번 보안점검에서 적출된 다양한 문제점을 조치할 예정이라고 밝혔다. 끝.