콜드체인 관련 냉장·냉동설비 사이버보안 강화 요청

□ 배경

○ 프랑스의 다수 슈퍼마켓(수백여곳)에서 사용중인 냉장·냉동설비 제어 시스템이 해킹되어 식품 변질, 설비 손상 등 물리적 피해 발생(10.11)

* 해킹 당했던 시스템은 Danfoss社 및 Dixell/Copeland社 제품으로 관리 편의(원격에서 온도 감시·조절 등)을 위해 인터넷에 연결되어 있었으며, 해커가 동 시스템에 침투(고급 해킹 기법이 아닌 기본적인 보안수칙 미준수 악용), 제상기능 및 온도설정 무단 조작

□ 요청 사항

○ ▵콜드체인 설비를 직접 운영하는 기관, ▵온도 감시 등 통합관제 서비스 제공 업체, ▵콜드체인 제조업체 등에 하기 보안대책 전파 및 준수 권고

○ 콜드체인 설비 제조업체에 대해서는 인터넷 연결 냉장·냉동설비에 대해 한국인터넷진흥원의 '정보통신망연결기기등 정보보호인증' 획득 권고

□ 보안대책

○ 모니터링 및 제어를 위한 원격접속 시 가상사설망*(VPN) 활용

* 시스템의 공인 IP주소가 인터넷에 직접 노출되는 것을 방지하고, 인증서·패스워드 등을 통한 사용자 인증을 거쳐야만 접속을 허용하는 보안기능

○ ▵관리화면이 인터넷에 직접 노출되지 않도록 조치, ▵관리기능에 대한 접속은 허용된 IP에 대해서만 허용 등 관리기능 접속 강화

○ ▵디폴트 패스워드 변경, ▵추측하기 어려운 패스워드 사용, ▵시스템마다 각기 다른 패스워드 사용, ▵주기적 변경 등 패스워드 관리 강화

○ 이상 온도변화·설정변경 등을 감지·대응할 수 있도록 대응체계 수립

○ 제조사 보안공지문 등 수시 확인, 취약점 보안패치 적시 적용