KISA 한국인터넷진흥원	**보도자료**	대체불가 대한민국
2026. 11. 4.(수) 조간[온라인: 11. 3.(화) 15:00]부터 보도 가능합니다.		

담당부서	지역AX산업보안팀 서민석 팀장(전화:061-820-3850, 전자우편: msseo@kisa.or.kr) 지역AX산업보안팀 김지명 책임(전화:061-820-3853, 전자우편: jimyungkim@kisa.or.kr)	
참고자료	사진 있음 ■ 사진 없음 □	총 2매

선박 사이버 침해사고 대응 모의훈련 실시

- 국내 해운사 · 관계 기관 · 기업 참여…위협 정보 공유부터 사고 분석 · 복구까지 공동 대응 체계 점검 -

한국인터넷진흥원(KISA)은 국내 해운사* 및 관계 기관·기업**과 함께 '해운사 협력형 침해사고 모의훈련'을 부산 벡스코에서 실시했다고 2026. 11. 3.(화) 밝혔다.

* (훈련 참여) 에이치엠엠오션서비스, 포스에스엠, 현대엘엔지해운, 케이엘엔지, 지마린서비스 / (참관) 팬오션

** (훈련 참여) 해양경찰청, 한국해운협회, 한국선박관리산업협회 / (참관) 국립한국해양대학교, 이글루코퍼레이션, 한국선급

최근 위성통신 기술의 발전과 원격지원 활용 등으로 선박과 육상과의 연결이 확대되면서, 악성 메일을 통한 공격, 선박용 기자재·소프트웨어 공급망을 악용한 사이버 위협에 대비할 필요성이 커지고 있다. 특히 여러 해운사가 같은 시스템이나 서비스를 이용하는 경우, 한 곳에서 발견된 보안 취약점이나 공격 수법이 다른 해운사에도 발생할 수 있어 신속한 정보 공유와 공동 대응이 중요하다.

이에 한국인터넷진흥원은 개별 해운사의 사고 대응 절차와 함께 해운사 간 위협 정보 공유와 관계 기관의 분석·수사 지원으로 이어지는

공동 대응 체계를 점검하기 위해 이번 모의훈련을 마련했다. 한 해운사가 확인한 위협 정보를 다른 해운사의 탐지와 차단에 활용하고, 대응 과정에서 확보한 정보를 다시 공유하는 협력 절차에 중점을 뒀다.

훈련은 공격자가 항만 기관을 사칭한 악성 메일을 해운사와 선박에 발송하고, 감염된 협력사 컴퓨터를 통해 선박용 소프트웨어 업데이트 파일을 변조하는 상황을 가정해 진행됐다. 변조된 업데이트로 선박 내 컴퓨터와 통신 서버가 감염돼 육상과 선박 간 통신에 장애가 발생하는 상황도 포함됐다.

훈련 과정은 ▲해킹 의심 메일 인지 및 위협 정보 공유(지마린서비스) ▲악성코드 제거, 시스템 복구 등 해킹 의심 메일 첨부파일 실행에 따른 감염 대응(현대엘엔지해운, 케이엘엔지) ▲인공지능(AI) 기반 공격 도구를 활용한 공급망 침투 대응(에이치엠엠오션서비스, 포스에스엠) ▲사고 분석 지원 및 위협 정보 공유(한국인터넷진흥원, 해양경찰청, 한국해운협회, 한국선박관리산업협회) 등 네 단계로 구성됐다.

한국인터넷진흥원은 이번 훈련에서 확인된 개선 사항을 참여 해운사와 공유하고, 각 사의 침해사고 대응 절차에 반영할 수 있도록 지원할 계획이다.

한국인터넷진흥원 이용필 디지털위협예방본부장은 “선박 사이버 침해사고는 선내 정보시스템 장애에 그치지 않고 운항과 물류 서비스까지 영향을 미칠 수 있는 만큼, 해운 업계와 관계 기관의 긴밀한 공조가 중요하다”며 “앞으로도 선박 운항 환경을 반영한 실전형 훈련을 이어가 해운 현장의 사이버 위협 대응 역량을 강화해 나가겠다”고 말했다.