KISA 한국인터넷진흥원	**보도자료**	대체불가 대한민국
2026. 8. 26.(수) [배포 시점]부터 보도 가능합니다.		

담당부서	위협대응정책팀 김은성 팀장(전화: 02-405-4710, 전자우편: eun-sung@kisa.or.kr) 위협대응정책팀 백은주 수석(전화: 02-405-4716, 전자우편: beunju@kisa.or.kr)	
참고자료	사진 있음 □ 사진 없음 ■	총 2매

한국인터넷진흥원, 아·태 지역 사이버공격 대응 공동 훈련 실시

- 원격 모니터링·관리(RMM) 도구 악용 공격 대응·20개국 25개 팀 참가 -

한국인터넷진흥원(KISA, 원장 이상중)은 아·태침해사고대응팀협의회(APCERT)*와 함께 원격 모니터링·관리(RMM) 도구를 악용한 사이버 공격에 대응하기 위한 국제 공동 모의훈련을 실시했다고 2026. 8. 26.(수) 밝혔다.

* 아·태침해사고대응팀협의회(APCERT, Asia Pacific Computer Emergency Response Team): 2003년 창립한 아시아·태평양 지역 내 국가를 대표하는 기업·기관 침해사고대응팀(CERT)이 모인 협의체로, 현재 25개국 35개 팀이 참여

아·태침해사고대응팀협의회(APCERT)는 매년 주요 사이버보안 이슈를 주제로 공동 모의훈련을 실시해, 아·태 지역의 사이버 위협 대응 역량을 점검·강화하고 있다. 협의회 창립부터 함께해 온 한국인터넷진흥원은 2024년 지능형 지속 위협(APT) 공격 그룹 식별, 2025년 대량 언어모델 악용 랜섬웨어 대응을 주제로 모의훈련을 주관한 데 이어 올해는 원격 모니터링·관리(RMM) 도구 악용 공격을 주제로 모의훈련을 개최했다. 올해 모의훈련에는 아·태 지역 20개국 25개 팀이 참가했다.

원격 모니터링·관리(RMM) 도구는 정보기술(IT) 관리자가 원격으로 시스템을 점검·관리하고 유지보수를 하는 데 사용하는 솔루션으로,

기업 정보기술(IT) 운영에 널리 활용되고 있다. 하지만 인터넷에 노출된 원격 모니터링·관리(RMM) 도구가 공격자에게 장악될 경우, 정상적 관리 활동으로 위장한 공격이 내부망 전반으로 확산할 수 있다는 점에서 사이버 위협요인으로도 주목받고 있다.

이에 따라 올해 모의훈련은 가상의 제조기업이 외부에 노출된 원격 모니터링·관리(RMM) 도구를 통해 침해당하는 상황을 가정해 진행됐다. 훈련에 참여한 각국 침해사고대응팀은 공격 단계별로 제공된 디스크 이미지를 분석해 침해 원인과 공격 경로를 규명하고, 이를 토대로 대응 방안과 보안 권고문을 마련했다.

한국인터넷진흥원은 오는 11월 부산에서 열리는 아·태침해사고대응팀 협의회(APCERT) 연례 총회에서 이번 훈련 결과를 공유해, 회원 팀이 침해사고 대응 절차를 점검·보완하는 데 참고하도록 할 계획이다.

한국인터넷진흥원 박용규 디지털위협대응본부장은 “이번 훈련은 기업 현장에서 널리 쓰이는 원격 모니터링·관리(RMM) 도구가 사이버공격의 통로로 악용되는 상황에 대비해 실제 대응 절차를 점검하는 데 중점을 뒀다”며 “앞으로도 새로운 사이버 위협을 반영한 훈련을 지속하고, 해외 침해사고 대응 기관과의 정보 공유와 협력을 강화해 나가겠다”고 말했다.