

UAE, 국가 사이버 보안 전략 발표

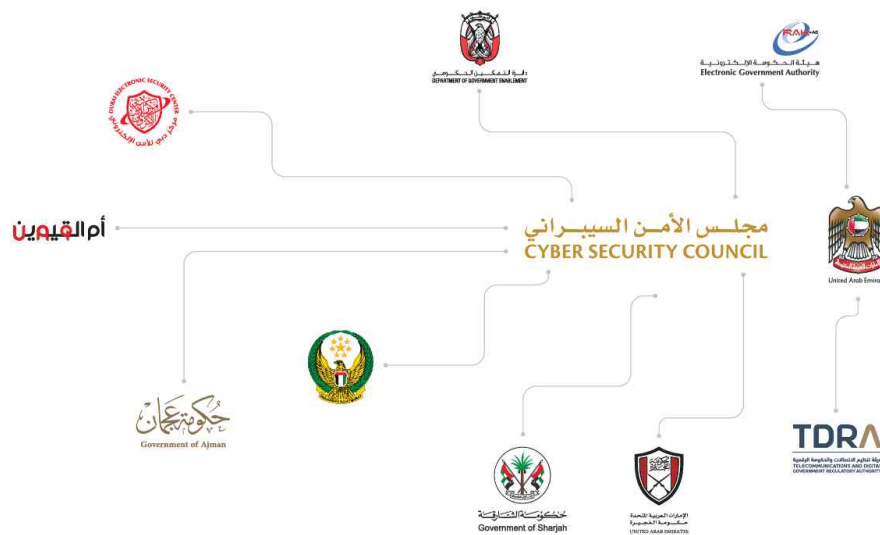
날짜 : '25년 4월 23일	무역관명 : 두바이	작성자 : 이지수 대리	
		TEL : +971)4-450-4360	EMAIL : jslee@kotra.or.kr

□ 주요내용

○ UAE 사이버 보안 위원회 (Cyber Security Council, CSC)

- CSC는 2020년 11월, UAE 내각의 결정에 따라 설립됨.
- 연방 및 지방 정부 간 사이버 보안 협력을 강화하고, 개별 기관이 운영하던 체계를 통합하여 보다 효과적인 대응 체계를 구축하고자 함.
- 주요 역할은 국가 사이버 보안 전략 수립, 관련 정책 및 표준 개발, 국내외 협력 확대, 사이버 보안 문화 확산 등임.

<UAE 사이버 보안 위원회 조직도>



출처: UAE 사이버 보안 위원회

○ CSC 주요 인사

- H.E. Dr Mohamed Al Kuwaiti는 UAE 정부 사이버 보안 책임

자(Head of Cyber Security, United Arab Emirates Government) 이자 CSC 수장으로, 특히 AI 기반 사이버 위협 대응 및 국제 협력 확대, 보안 전략 수립을 주도하고 있음.

○ 국가 사이버 보안 전략 (2025- 2031) 발표

- '25년 2월, CSC는 National Cybersecurity Strategy 2025-2031을 발표.
- UAE Vision 2031 연계 장기 전략으로, 사이버 위협 대응을 넘어 경제 성장, 국가 안보, 사회 안정을 포괄하는 방향성 제시.
- 디지털 생태계의 지속 가능성과 회복력 강화를 목표로, 다음의 5가지 핵심 축(pillars)으로 구성됨:
 - ① 효율적이고 통합적인 사이버 보안 거버넌스 구축
 - ② 안전하고 탄력적인 디지털 환경 조성
 - ③ 혁신의 신속하고 안전한 도입 지원
 - ④ 국가 차원의 디지털 및 사이버 역량 강화
 - ⑤ 국내외 협력 및 파트너십 촉진

○ 2025 UAE 사이버 보안 보고서 발간

- '25년 2월, CSC와 G42의 자회사인 보안 전문기업 CPX는 공동으로 2025 사이버 보안 보고서를 발간
- UAE는 약 223,800개의 디지털 자산을 보유하고 있으며, 절반 이상이 5년 이상 보완되지 않은 취약점을 안고 있음
- 지역별 디지털 자산 분포는 두바이(65%)가 가장 크고, 아부다비(13%), 푸자이자(11%), 샤르자(7%), 아즈만(3%), 라스알카이마(1%) 순임.
- AI 등 혁신 기술 도입과 함께 사이버 공격 표적화 증가. 특히 AI 기반 공격, 딥페이크, 자동화된 악성코드 등 고도화된 공격 기법이 확산.

○ UAE의 사이버 공격 대응 현황

- 2025년 2월, CSC의 발표에 따르면 UAE는 하루 20만 건 이상의 사이버 공격을 차단하고 있다고 발표. 공격의 주요 대상은 정부(30%), 금융 및 은행(7%), 교육(7%), 기술·항공·의료(각 4%) 등임.
- 주요 공격 유형은 IT 인프라 공격(40%), 파일 공유 공격(9%), 데이터베이스 취약점 공격(3%) 등임.
- 주요 위협 요소는 보안 설정 미흡(27%), 악성코드(22%), 스캐닝 및 로그인 시도(15%), 무단 접근(15%), 불법 행위 및 웹 공격(11%), 피싱(10%) 등임.
- 주요 해킹 수법은 서비스 거부(DoS) 공격(39%), 데이터 암호화 및 유출(37%), 인터넷 연결 애플리케이션 침해(24%), 랜섬웨어 공격(7%) 등임.
- CSC는 전통적 방식부터 AI 기반 정교한 위협까지 다양한 사이버 공격이 발생할 것으로 보고, 전 부문에 보안 표준 준수를 강조함.

□ 검토의견

- 2024년 국제전기통신연합(ITU)은 UAE를 글로벌 사이버 보안 지수(Global Cybersecurity Index)에서 80개 모든 평가 항목을 충족한 국가로 인정하며, 최고 등급인 Role-Modelling 국가로 평가함.

UAE는 사이버 보안 분야에서 빠르게 선도국으로 부상하고 있으며, 미래 지향적인 비전에 부합하는 안전하고 첨단화된 디지털 인프라 구축을 지속적으로 추진하고 있음.

특히, AI 기반 위협 탐지 기술, 사이버 인텔리전스 강화, 보안 문화 확산 등을 중심으로 전략적 대응 역량을 고도화하고 있으며, 이를 통해 디지털 경쟁력과 글로벌리더십을 강화하고 있음.

□ 출처 I

- 출처 : National Cybersecurity Strategy of the UAE
- 게시일자 : '25.2.11
- 출처:
https://csc.gov.ae/documents/d/csc/national-cybersecurity-strategy_en_ar_v11_low-compressed

□ 출처 II

- 출처: State of the UAE Cybersecurity Report
- 게시일자 : '25.2.24.
- 출처 :
<https://cpx.net/media/thbeuxk5/cpx-state-of-the-uae-report-2025.pdf>

□ 출처 III

- 출처 : 사이버 공격 하루 20만 건 차단, UAE의 사이버 보안 전략은?
- 게시일자 : '25.4.2.
- 출처:
https://dream.kotra.or.kr/dream/cms/news/actionKotraBoardDetail.do?MENU_ID=3550&pNttSn=227185