백악관 보고서, 미 연방 기관, 양자 암호화 이후 마이그레이션 대비

(2024.08.22., 양자정보연구지원센터)

□ 미 연방 기관, 양자 암호화 이후(PQC) 마이그레이션(migration) 대비

○ 양자 컴퓨팅과 그 위협

- 양자 컴퓨팅은 도구이자 위협으로, 기존 암호화 시스템을 무너뜨릴 수 있는 큰 잠재력을 지니고 있음
- 비록 완전한 양자 컴퓨터는 아직 개발되지 않았지만, 그 위협은 이미 현재에 영향을 미치고 있음

○ 백악관 보고서와 연방 정부의 대응

- 최근 백악관 보고서에 따르면, 미 연방 기관들은 양자 컴퓨터에 대비한 암호화 인프라 전환 과제를 맡게 됨
- 보고서는 양자 후 암호(PQC, post-quantum cryptography)로의 전환 전략을 제시, 향후 10년 동안 약 71억 달러가 소요될 것으로 추산

○ **긴급성: ‘record-now, decrypt-later’ 위협**

- 보고서는 양자 컴퓨터 등장 이전에도 ‘record-now, decrypt-later 공격이 발생할 수 있다고 경고함
- 적들은 지금 데이터를 해킹한 후, 미래에 양자 컴퓨터로 이를 해독하려 할 수 있어, PQC로의 전환이 시급함

○ 우선 순위 및 시스템 식별

- 연방 기관들은 PQC 전환 우선순위를 설정하고, 취약한 암호화 시스템을 식별해야 함
- 일부 구형 시스템은 새로운 암호화 알고리즘을 지원하지 못해, 교체 또는 업그레이드가 필요할 수 있음

○ 비용과 과제

- **PQC로의 전환 비용은 약 71억 달러로 추산**되며, 특히 구형 시스템의 교체가 큰 비중을 차지할 것임

- 국방부 및 국가 안보 기관들의 추가 비용 추산도 필요하며, 전체 예산이 더 늘어날 가능성 있음

ㅇ 지속적인 과정

- PQC 전환은 일회성 프로젝트가 아니며, 지속적인 업데이트와 관리가 필요함
- 연방 기관들은 암호화 시스템을 꾸준히 점검하고, 최신 PQC 기술을 반영해야 할 것임

□ 백악관 보고서: PQC로의 전환 전략

ㅇ 네 가지 주요 원칙

- 포괄적이고 지속적인 암호화 시스템 목록 작성은 PQC로 성공적인 전환을 위한 중요한 기준임
- ’ recoed now, decrypt later’ 공격의 위협으로 인해 양자 컴퓨터가 운영되기 전부터 PQC 전환이 시작되어야 함
- 기관들은 PQC 전환을 위한 시스템과 데이터를 우선적으로 정리해야 함
- PQC 알고리즘을 지원하지 못할 시스템은 가능한 빨리 식별되어야 함

ㅇ PQC 표준 개발을 위한 NIST 조정 노력과 일정(보고서 참조)

- CRQC(cryptanalytically relevant quatnum computer)로 인한 위험으로부터 보호되기 위해서는 수년간 지속적인 정부 차원의 노력이 필요함
- 암호화는 모든 연방 정보 시스템이 필수적이고 보편적으로 내장된 구성 요소임
- 현재와 미래 위협으로부터 암호화를 보호하는 것은 핵심 사이버 방어를 배포하고 유지하며, 연방 기관들이 공공에 필수 서비스를 제공할 수 있는 능력에 중요함

(원문)

1. https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/