Red Hat

양자 내성 암호화 준비를 위한 핵심 4단계

양자 컴퓨팅 분야의 발전은 빠르면 2029년에 암호화 표준의 안전을 위협할 것으로 예상됩니다.[1] 이는 양자 컴퓨팅 기반 해독 기술에도 뚫리지 않는 암호화가 모든 비즈니스에 반드시 필요해짐을 의미합니다. 이 중대한 위협과 이미 현실화된 '선탈취, 후해독' 공격에 대응하기 위해 조직은 양자 내성 암호화에 대비하는 다음 주요 4단계를 고려해야 합니다.

1 조직의 민감한 데이터와 기존 암호화 프로토콜 평가

양자 내성 암호화에 대비하려면 조직이 보호해야 하는 데이터의 현재 취약점을 평가해야 합니다.

이를 수행하는 가장 좋은 방법은 비즈니스 운영, 법률, 컴플라이언스, IT 및 기타 관련 부서의 담당자가 모두 참여하는 다각적인 팀을 구성해 그러한 데이터에 대한 모든 액세스 경로를 추적하는 것입니다. 팀은 조사 결과를 바탕으로 다양한 고려 사항 중에서도 특히 현재, 근미래, 먼 미래에 민감한 데이터로 분류되는 데이터를 시기별로 알아낼 수 있습니다.

그런 다음 조직이 현재 시행 중인 암호화 프로토콜에 대한 실사를 진행하여 업데이트가 시급한 프로토콜, 수정의 여지가 있는 프로토콜, 하드웨어 또는 소프트웨어 관련 제한 사항으로 인해 현재와 동일하게 유지해야 하는 프로토콜을 평가해야 합니다.

2 우선순위를 지정해야 하는 자산 결정

팀이 조직의 민감한 데이터를 완벽하게 파악했다면 즉시 보호해야 하는 자산에 대한 우선순위를 지정할 수 있습니다.

다양한 모든 자산의 보안을 한 번에 해결하는 것은 실용적이지도, 현실적이지도 않습니다. 따라서 팀이 이미 수행한 작업에서 얻은 인사이트를 바탕으로 실용적인 계획을 수립하여 먼저 조치해야 하는 자산 및 시스템과 나중에 처리해도 되는 자산 및 시스템을 신중하게 검토하는 것이 중요합니다.

1 Horvath, Mark. "지금부터 양자 내성 암호화로 이전하세요." Gartner, 2024년 9월 30일

3 기존 환경에서 새로운 양자 내성 알고리즘 테스트 시작

대부분의 규제 기관은 조직이 가능한 한 빨리 새로운 양자 내성 암호화 프로토콜 및 알고리즘으로 마이그레이션할 것을 권고하고 있으며, 여기에는 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)가 2024년 8월에 공표한 1차 확정 표준이 포함됩니다.[2]

팀이 더 빠르게 알고리즘 테스트를 시작하고 조직의 성공적인 마이그레이션에 걸림돌이 되는 문제를 해결할 수 있다면 곧 필수 컴플라이언스 요건으로 시행될 규정에 더욱 빈틈없이 대비할 수 있으며, '선탈취 후해독' 공격의 위험을 더 효과적으로 완화할 수 있을 것입니다.

조직이 새로운 양자 내성 알고리즘의 테스트를 시작할 수 있도록 도우려면 Red Hat® Enterprise Linux® 10을 채택하거나 해당 버전으로 업그레이드할 것을 고려해 보세요. 이 운영 체제(Operating System, OS)에는 OpenSSL, ML-KEM(FIPS 203), ML-DSA(FIPS 204)를 비롯한 1차 양자 내성 알고리즘이 탑재되어 키 교환, 암호화, 서명 기능을 제공하며 향후 릴리스를 위한 추가적인 기능도 계획되어 있습니다.

4 전면적인 마이그레이션을 시작하고 프로덕션 단계로의 이행 시작

이 프로세스의 마지막 단계이기는 하지만, 새로운 양자 내성 알고리즘을 구현하는 것은 전체 프로세스에서 가장 광범위하고 복잡한 부분입니다.

즉각적인 결과를 얻기 위해 단기간 전력 질주를 하기보다는 장기적인 이점을 얻는 것을 목표로 꾸준한 노력을 기울이면서 이 단계를 진행해야 합니다.

환경 전반에서 모든 암호화 알고리즘을 업데이트하는 것은 지금 당장은 불가능하겠지만, 미리 작업한 단계에서 얻은 인사이트와 확인된 우선순위를 통해 지속적인 성공을 위한 기반을 마련할 수 있을 것입니다.

암호화 프로토콜에 변경 사항을 적용하고 프로덕션에 양자 내성 알고리즘을 통합하는 작업을 시작할 때 의도치 않은 결과나 다운타임을 완화하려면 테스트 단계에서 확인된 상호 의존성에 특별한 주의를 기울여야 합니다.

오늘 바로 양자 내성 암호화에 대비하세요

이 페이지에서 조직이 양자 내성 암호화 시대에 대비하는 것을 도울 수 있는 양자 내성 알고리즘을 탑재한 Red Hat Enterprise Linux 10에 대해 자세히 알아보세요.

2 "NIST, 1차 확정된 양자 내성 암호화 표준 3종 공표." 미국 국립표준기술연구소(National Institute of Standards and Technology), 2024년 8월 13일.