개정이력

차수	재(개)정 일자	시행일자	주요 개정 내용
1	2025-01-03	2025-01-03	초도 제정
2	2025-01-13	2025-01-13	목차 및 목적내용 수정
3	2025-01-16	2025-01-16	지침 전면 수정

목 차

1. 목적

취약점을 사전에 발견하여 공격 표면을 최소화하고, 데이터 유출, 서비스 중단 등의 사고를 예방한다.

2. 점검 주기 및 일정

2.1 연간 점검 주기

1)최소 1년에 1회 이상 취약점 점검을 실시한다.

2.2 점검 주기 세부화

2.2.1 월별

1) 주요 시스템 및 애플리케이션의 보안 패치 확인을 실시한다.

2.2.2 분기별

1) 네트워크 및 서버의 취약점 점검을 실시한다.

2.2.3 연간 종합 점검

1) 전체 시스템 및 네트워크에 대한 종합적인 취약점 점검을 실시한다.

3. 점검 대상

3.1 시스템

1) 운영 체제, 서버 등 시스템 전체.

3.2 네트워크

1) 방화벽, 라우터, 스위치 등 네트워크 장비.

3.3 물리적 보안

1) 서버실, 데이터 센터, 네트워크 장비 등 물리적 보안 시스템.

3.4 인프라

1) DBMS, API, 네트워크 대역폭 및 트래픽 분석.

4. 점검 방법

4.1 자동화 도구 활용

1) 보안프로그램을 사용하여 자동화된 점검을 진행한다.

4.2 수동 점검

1) 보안담당자가 수동으로 소스 코드 분석, 로그 파일 점검, 설정 파일 분석 등을 수행한다.

4.3 모의 해킹(Penetration Testing)

1) 실제 해커의 공격을 시뮬레이션하여 취약점 점검을 수행한다.

4.4 구성 관리 점검

1) 시스템 및 네트워크 장비의 구성 설정을 확인한다.

5. 점검 절차

5.1 준비 단계

1) 점검 대상 및 범위를 정의한다.

2) 점검에 필요한 도구 및 리소스를 준비한다.

3) 점검 일정 및 책임자를 지정한다.

5.2 점검 실행

1) 자동화 도구로 시스템 및 애플리케이션 취약점 점검을 진행한다.
2) 수동 점검 및 모의 해킹을 진행한다.

5.3 결과 분석 및 평가

1) 발견된 취약점의 심각도 및 위험도를 평가한다.
2) 취약점의 우선순위를 정하고 해결 방안을 제시한다.

5.4 대응 및 개선

1) 취약점에 대한 수정 작업(패치 적용, 보안 설정 변경 등)을 수행한다.
2) 패치 관리 및 시스템 재검토를 실시한다.

5.5 보고서 작성

1) 점검 결과를 보고서 형식으로 작성하여 경영진 및 관련 부서에 제출한다.
2) 취약점 해결 여부 및 후속 조치 계획을 포함한다.

6. 위험도 평가 및 우선순위 설정

6.1 취약점 분류

1) 발견된 취약점을 위험도에 따라 낮음, 중간, 높음으로 분류한다.

6.2 우선순위 설정

6.2.1 중요한 취약점부터 우선적으로 해결하도록 계획을 수립한다.

1) 높음: 즉시 패치 및 대응 필요.
2) 중간: 일정 기간 내 해결 필요.
3) 낮음: 모니터링 및 추후 점검에서 해결.

7. 패치 관리

7.1 패치 적용 주기

1) 발견된 취약점에 대해 긴급한 보안 패치를 빠르게 적용한다.

7.2 패치 테스트

1) 중요한 시스템에 패치를 적용하기 전에 테스트 환경에서 먼저 검토한다.

7.3 패치 기록 관리

1) 모든 패치 적용 내역을 기록하고 관리한다.

8. 점검 후 피드백 및 개선

8.1 점검 결과 공유

1) 점검 후 보고서를 작성하고, 관련 부서와 피드백 세션을 진행한다.

8.2 점검 프로세스 개선

1) 점검 과정에서 발견된 문제나 개선점을 반영하여 차후 점검 프로세스를 개선한다.

9. 책임자 및 팀 구성

9.1 정보보안책임자

1) 점검 활동 전반을 주관하고 검토 및 승인

9.2 기술보안담당자

1) 시스템, 네트워크에 대한 취약점 분석 및 해결

9.3 외부 전문가

1) 필요 시, 외부 보안 전문가의 도움을 받을 수 있다.

10. 문서화 및 기록 관리

10.1 취약점 점검 기록

1) 모든 점검 활동 및 결과를 문서화하여 추후 참고할 수 있도록 관리한다.

10.2 점검 일정 관리

1) 연간 점검 계획과 일정을 문서화하고 관리한다