취약점점검지침

취약점점검지침

문서번호: 가비아-GL-09

개정번호: VERSION 1.2

정보보호 책임자	정보보호 최고책임자

개정이력

개정 번호	개정일자	담당자	개정 내용
Version 1.0	2016.10.26	안광해	정보보호책임자 · 최고책임자 승인 정보보호위원회 의결 및 지침 시행
Version 1.1	2016.12.22	안광해	정보보호위원회 의결 및 개정 지침 시행
Version 1.2	2017.04.21	안광해	이행심사 조치 사항 제14조 예외적용 책임자 변경 기존: 정보보호관리자, 개정: 정보보호최고책임자

목 차

제1장 일반사항

제1조 (목적)

본 지침은 (주)가비아 (이하 "회사"라 함)의 클라우드 서비스 공공 zone 정보시스템에 대한 주기적인 보안 점검을 수행함으로써 주요 자산의 위협에 대한 노출을 최소화하는데 그 목적이 있다.

제2조 (적용범위)

본 지침은 회사의 모든 클라우드 서비스 정보시스템자산을 대상으로 한다.

제3조 (용어정의)

1. 취약점: 정보시스템자산 내에서 일반사용자가 권한 상승하여 관리자 권한을 획득하거나 비인가 외부자가 특정 권한을 획득할 수 있는 보안상의 결함을 의미한다.
2. 포트: 일반적으로 포트는 다른 장치에 물리적으로 접속되는 특정한 부위를 말하나, 네트워크에서는 인터넷이나 기타 다른 네트워크 메시지를 서버에 전달 혹은 도착하는 출입구를 의미한다.
3. 취약점점검: 정보시스템의 보안정책을 위반하기 위해 악용되는 시스템의 설계, 구현, 운영, 관리상의 취약점의 존재 여부를 확인하는 일련의 업무를 의미한다.
4. 취약점 점검도구: 보안 취약점 점검 기술 중의 한 분야로서 시스템 기반의 보안 취약점을 점검하는 기능을 가진 도구를 의미한다.

제4조 (책임사항)

1. 정보보호책임자

1.1 정보시스템자산에 대하여 주기적(연1회 이상)으로 취약점 점검이 이루어지도록 수행·관리·감독을 수행한다.
1.2 점검결과는 정보보호최고책임자에게 보고하고 발견된 취약점은 제거하도록 조치한다.
1.3 취약점 점검업무를 자체적으로 수행하기 어려운 경우 관련기관이나 외부 정보보호업체를 통해 지원을 받도록 한다.
1.4 서버, 네트워크, 정보보호시스템 등 정보시스템자산에 대하여 해당 관리자는 발견된 취약점을 제거할 의무를 갖는다.

제2장 취약점점검

제5조 (취약점점검 대상)

1. 취약점점검 시기

1.1 정보시스템의 취약점점검은 매년 1회 이상 진행하는 것을 원칙으로 한다.

2. 취약점점검 대상

2.1 서버: 웹서버, DB서버, NC서버 등의 서버
2.2 네트워크: 라우터, 스위치, IP공유기 등
2.3 정보보호시스템: UTM, 웹방화벽, 방화벽, IPS, IDS 등
2.4 DB : DBMS
2.5 PC(전사 자원 대상) : 노트북, 테블릿PC 등
2.6 웹서비스

제6조 (취약점점검방법의 결정)

1. 네트워크기반 취약점 점검: 시스템 취약점 분석 방법에는 자동화된 스캐닝 도구를 사용해 원격으로 점검하는 방법
2. 시스템기반 취약점 점검: 체크리스트 기반으로 로컬에서 점검하는 방법으로 구분할 수 있으며 외부 정보보호업체 등을 통하여 수행할 수도 있다.
3. 모의해킹: 애플리케이션 레벨 및 시스템의 취약점을 내부 보안 전문가의 모의해킹을 통해 파악한다. 외부 업체를 이용하여 진행할 수도 있다.
4. 취약점 점검도구의 이용은 특정한 소수의 취약점 탐지보다는 다수의 취약점 항목을 자동으로 점검할 수 있다.

제7조 (취약점점점도구의 선정)

취약점 정보, 취약점 데이터베이스, 신규 취약점 업데이트 기능, 취약점 점검결과의 정확성, 취약점 점검결과 보고서, 사용자의 편의성, 한글의 지원, 점검도구의 안정성을 고려하여 점검도구를 선정한다

제8조 (취약점점검 도구)

1. 네트워크 취약점 점검도구

    1.1 Nessus 등

2. 시스템 취약점 점검도구

    2.1 LSOF(List Open File) 등

3. 공개 취약점 점검도구를 다운로드 받기 위해서는 다음 사이트를 참조한다.

    3.1 http://www.krcert.or.kr 의 자료실 → 보안도구 메뉴에서 다운

4. 기타 취약점 점검 도구: 아큐네틱스, 시큐아이스캔 등

제9조 (취약점점검도구 관리)

1. 취약점 점검도구의 사용 및 관리는 정보보호책임자로 제한한다.
2. 정보보호책임자는 취약점 점검도구의 접근통제에 대한 관리책임을 지며, 새로운 취약점이 발견될 경우 취약점 점검도구의 취약점 데이터베이스에 대한 업데이트를 실시한다.

제10조 (취약점 점검항목의 선정)

정보시스템자산에 문제가 발생하거나 또는 발생할 수 있는 위협요인을 식별하여, 점검에 필요한 취약점은 '안전 행안부 취약점 항목' 기준으로 점검항목으로 선정한다..

제11조 (취약점점검의 수행)

침해사고대응팀은 분석.평가 시 발견된 미 준수 항목 및 정보보호 취약점을 평가한 후 취약점 분석.평가 결과를 취약점과 관련된 각 관리부서에 전달한다. 취약점 분석. 평가 결과에는 다음 각 항목의 내용이 포함되어야 한다.

1. 취약점 분석 평가 수행 일시

2. 취약점 분석 평가 대상
3. 취약점 분석 방법
4. 취약점 점검 내용 및 결과
5. 취약점 조치 가이드 라인

제12조 (발견된 취약점의 조치)

1. 취약점 점검을 통해 발견된 취약점에 대해서 적절한 조치와 해결책을 마련하도록 한다.
2. 취약점 점검결과에 대해 기존 정보보호대책의 적정성, 효율성 및 문제점을 평가하고 분석한다.
3. 정보보호대책(방침, 절차, 시스템) 등의 보완이 필요할 경우 기존 대책과 연계하여 효과성, 경제성을 바탕으로 가장 효율적인 대책과 추진방법을 선정한다.

제3장 부칙

제13조 (시행일)

본 지침은 정보보호위원회 의결 완료일부터 시행된다.

제14조 (예외적용)

다음 각 호에 해당하는 경우에는 본 지침에서 명시한 내용일지라도 정보보호 최고 책임자의 승인을 받아 예외 취급할 수 있다.

1. 기술환경의 변화로 적용이 불가능할 경우
2. 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우
3. 기타 재해 등 불가항력적인 상황일 경우

제15조 (경과조치)

특별한 사유에 의하여 본 지침에 정하는 요건을 충족하지 못한 경우에는 발생일로부터 3 개월 이내에 개선방안을 강구하여야 한다.