정보보안 취약점 분석 지침

제정 2017. 11. 20.
개정 2022. 7. 1.

제1조(목적) 본 지침은 「교육부 정보보안 기본지침」에 의거 AX·정보화혁신본부 정보시스템(IDC 입주시스템 포함)에 대한 보안 취약점을 진단하고 분석하여, 사이버침해사고의 예방을 위한 대책을 수립하고, 안정적인 정보보안 체계를 확립하기 위한 절차를 마련하는데 목적이 있다.

제2조(용어 정의) 본 지침에서 사용하는 용어의 정의는 다음과 같다.

① “보안 취약점”이란 정보시스템에 비인가자의 접근을 허용하거나 정상적인 서비스를 방해하는 위협 또는 사이버공격에 악용되어 관리자가 설정한 접근 권한 外 정보를 열람·취득하게 하거나 보안기능을 회피 가능하게 하는 정보통신망·정보시스템의 결함 및 정보시스템에서 관리하는 중요한 데이터의 유출, 변조, 삭제에 대한 위협을 말한다.

② “정보시스템”이란 정보의 수집, 가공, 저장, 검색, 송신, 수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계로서, 「모바일 전자정부 서비스 관리 지침」의 모바일 앱, 하이브리드 앱을 포함한다.

제3조(범위) 보안 취약점 진단 및 분석은 시스템, 네트워크, 응용프로그램 분야를 그 대상 범위로 한다.

제4조(대상 시스템 및 진단 방법 결정) 정보화기획운영과 또는 정보시스템 운영 담당자는 정기적으로(연1회 기준) 정보시스템에 대한 보안 취약점 분석을 실시하며, 정기적 보안 취약점 분석 이외 필요하다고 판단되는 경우에는 추가적으로 보안 취약점 진단을 실시하고 대상 시스템에 따른 진단 방법을 결정한다.

제5조(사전 업무협의 및 작업 일시 결정) 정보화기획운영과는 보안 취약점 진단 및 분석 계획을 수립하기 위하여 대상 시스템 및 운영 관련 업무부서와 사전 협의하고 작업 일시를 결정한다.

제6조(취약점 분석 계획서 작성 및 보고) 정보화기획운영과는 대상 장비, 진단 방법 및 작업 일시가 결정이 되면 보안 취약점 진단 및 분석 계획을 수립하여 정보보안담당관에게 보고하여 승인을 받는다.

제7조(작업 공지) 정보화기획운영과는 취약점 진단 및 분석 작업으로 인해 관련 서비스의 중단 혹은 차질이 예상되는 경우, 작업에 관한 내용을 업무포털(코러스 등)의 공지사항 또는 학교 공지사항에 안내·게시한다.

제8조(분석작업 실시) 정보화기획운영과는 정해진 일시에 진단 및 분석 작업을 수행하며 이와 관련하여 협력 업체의 지원을 받을 수 있다. 단, 외부 업체일 경우 부산대학교 정보통신보안 기본지침을 준수하여야 한다.

제9조(분석결과 처리) ① 정보화기획운영과는 보안 취약점 분석 결과를 서면으로 정리하여 정보보안담당관에게 보고하고, 필요시 결과 보고회를 통하여 해당 서비스팀에 취약점 및 보완·조치사항을 통지하여 보완하도록 한다.

② 취약 위험성이 높은 사항에 대하여는 정보시스템 담당자에게 직접 통보하여 빠른 조치를 취하도록 하여야 한다.

제10조(기타사항) 본 지침에서 명시되지 않은 사항은 아래 각 항에 따른다.

① 교육부 정보보안 기본지침

② 부산대학교 정보보안 기본지침

③ 기타 관계 법령 등

부 칙

이 지침은 2017년 11월 20일부터 시행한다.

부 칙

이 지침은 2022년 7월 1일부터 시행한다.