서울대학교

서버 운영 보안 가이드

2023. 12.

서울대학교
정보화본부

상세 가이드 다운로드

Windows 서버

Unix(Linux) 서버

□ 개 요

○ 학내 정보자산(웹 및 DB, 네트워크 서버 등) 취약점 사전 조치를 통한 중요 데이터 보호 및 유출 사전 방지

○ 학내 구성원 보안 수준 제고를 통한 사이버 침해사고 대응 체계 강화

○ **(조치대상) Windows/Linux 서버를 운용 중인 기관**

○ **(조치내용)** Windows/Linux 서버 운영 시, 기본 **서버 보안 실시**

> **< 서버 보안 >**
> 데이터가 실제 존재하는 서버에 대해 외부 공격으로부터 보호하고,
> 중요한 데이터의 무단 접근 및 손상을 방지하기 위한 방어 조치를 하는 것

○ **(조치항목 및 방법)** 1페이지 '상세 가이드 다운로드' 클릭 후 파일 참고

※ 중요도 '상' 항목에 대해 최소한의 서버 보안은 반드시 실시

- Windows 서버 : 전체 82개 항목

분류	번호	점검항목	항목 수 (중요도)			
			상	중	하	합계
Windows	1	계정 관리	6	12	-	**18**
	2	서비스 관리	25	10	1	**36**
	3	패치 관리	2	1	-	**3**
	4	로그 관리	2	1	1	**4**
	5	보안 관리	10	9	1	**20**
	6	DB 관리	-	1	-	**1**
	합계		**45**	**34**	**3**	**82**

- Linux 서버 : 전체 72개 항목

분류	번호	점검항목	항목 수 (중요도)			
			상	중	하	합계
Linux	1	계정 관리	4	5	6	**15**
	2	파일 및 디렉터리 관리	14	3	2	**19**
	3	서비스 관리	23	9	3	**35**
	4	패치 관리	1	-	-	**1**
	5	로그 관리	1	-	1	**2**
	합계		**43**	**17**	**12**	**72**

□ 학내 침해사고 사례

○ 최근 3년간 총 139건의 사이버 침해사고 발생

- 대부분의 침해사고는 학과 연구실 내 서버에서 발생하며, 취약한 패스워드 사용에 의한 피해는 매년 증가하고 있음

- 또한 학내 50% 이상의 서버가, 외부 어디서든 원격 접근 가능한 취약 정책으로 사이버 위협에 노출되어 있음

- 이로 인해 서버 데이터 유출 및 훼손(72%), 홈페이지 변조(4%), 바이러스 감염(2%) 등의 피해가 매월 발생함

< 주요 침해사고 발생 현황 >

(2021년) Hadoop YARN Resource Manager 취약점을 이용한 **악성코드 유입**
(2022년) 암호화폐 채굴 악성파일 설치로 인한 서버 **자원 악용**
(2022년) 홈페이지 내 파일업로드 취약점을 통한 **악성 웹쉘 업로드** 발생
(2023년) **취약한 서버 계정 탈취** 후 다른 서버 원격 접속하여 **2차 피해** 발생

○ 사이버 침해사고 발생 전, 서버 보안 강화 필요

- 기본적인 서버 보안을 통해 침해사고 사전 방지 가능

- '[붙임] OS 별 서버 보안 가이드라인'에 따라, 패스워드 복잡성 및 외부 SSH 원격접속 차단 등의 **서버 보안 설정 반드시 적용**

□ 추가 보안조치

○ (필수) 학내용 V3 백신 설치

- 사용용도 : 악성 파일 자동 검출 및 삭제, 유해 사이트 등의 악성 네트워크 차단 기능 제공

- 다운로드 : mySNU - S/W다운로드 - V3백신

※ 학내 정보 자산(서버, PC, 노트북 등)에서만 다운로드 및 사용 가능

○ TCP Wrapper

- 사용용도 : 특정 호스트(Domain) 또는 네트워크 주소(IP)로부터의 접속을 허용·차단하는 접근 제어(ACL) 프로그램

- 사용방법

분류		접근 차단	접근 허용
파일 구성		/etc/hosts.deny	/etc./hosts.allow
파일 설명		접근 차단에 대한 설정	접근 허용에 대한 설정
사용 방법		서비스 : 접근 대역(IP or Domain)	
예시	Ex1	ALL : ALL 모든 서비스에 대하여 모든 접근 차단	httpd : ALL 웹 서비스에 대하여 모든 접근 허용
	Ex2	sshd : 1.1.1.1 2.2.2.2 ssh 서비스에 대하여 1.1.1.1과 2.2.2.2에서 접근 차단	sshd : 192.168.10. ssh 서비스에 대하여 192.168.10.X에서 접근 허용
	Ex3	Httpd : 192.168.10.0/255.255.255.0 웹 서비스에 대하여 192.168.10.X에서 접근 차단	sshd : 192.168. EXCEPT 192.168.100. ssh 서비스에 대하여 192.168.X.X 대역 접근 허용 단, 192.168.100.X 대역은 허용 제외

□ 정보자산 관리 방안

○ **정보자산 관리대장** 작성 및 주기적 관리

연번	소속	취급자	책임자	용도	운영체제 및 모델명	IP	도입 일자	비고 (자산위치 등)
물품 번호	*정보화지원과*	*홍길동*	*고길동*	*000용 연구 서버*	*Windows Server 2022*	*147.47.x.x*	*22.7.1.*	
물품 번호	*정보화지원과*	*홍길동*	*고길동*	*학과 홈페이지 운영 서버 (000.snu.ac.kr)*	*Linux (Centos 7)*	*147.46.x.x*	*23.8.1.*	

- 연번: 각 기관에서 관리하기 위한 일련번호
- 소속: 취급자의 소속
- 취급자/책임자: 취급자 및 책임자 성명
- 용도: 정보자산의 운용 용도
- 운영체제 및 모델명: 운영체제 정보 및 HW 모델명
- IP: 정보자산에 설정된 IP
- 도입일자: 해당 정보자산의 도입년도, 월, 일
- 비고: 도입 및 폐기 상태, 자산 위치 등 기타 필요한 사항

○ 학내 **IP 정보 및 담당자 현행화**

- 정보화본부 ITSM 시스템 내 IP 정보(취급자, 책임자) 현행화
- 신청방법 : ITSM - 서비스 요청 - 네트워크 서비스 - IP서비스 - IP정보변경 신청

  ※ 세부 내용 '[별첨] IP주소 신청 및 담당자 변경 방법' 참고

별첨 | **IP주소 신청 및 담당자 변경 방법**

□ IP주소 신청 및 담당자 변경 방법

○ 메뉴 : 포털(mySNU) → 스누인지원 → 서비스요청 → 네트워크서비스 → IP서비스

메뉴	신청 조건	비 고
IP 신청	· 컴퓨터 추가(신규) 구매 · 다른 건물로 연구실/사무실 이전	· 절차 : 웹 신청 → 책임자에게 확인메일 → 책임자 회신 → IP할당 (할당 시 신청자에게 자동 메일 송부) ※ 책임자 "거부" 회신 시 할당된 IP주소 강제반납함 · **다른 건물 이전 시, 기존 IP 반납 필수**
IP 반납	· 졸업/퇴직 등 더이상 IP를 사용하지 않을 경우 · 컴퓨터 불용 · 장기간 해외 출장 (귀국 후 IP신청)	· IP신청자는 직접 반납신청 · IP신청자 부재시 반납요청 : IT센터에 메일 또는 전화(반납 사유 명시) IT센터 : 880-8282 (itsc@snu.ac.kr , snunet@snu.ac.kr) · **IP 신청자만 반납 신청 가능** · 타인에게 IP할당을 위해 반드시 반납 요망
IP 정보변경	· 랜카드 교체 or 컴퓨터 교체 · 전화번호, OS 등 정보변경 시 · 졸업, 퇴직, 인사이동 등	· **IP 신청자만 정보변경 신청 가능** · 졸업/퇴직 등의 경우, 본인이 신청한 IP들의 "신청자정보"를 타인으로 변경(인계)해야 함
IP 명의변경	· 사용 IP의 신청자를 모르는 경우 현재 사용자가 할당된 IP 계속 사용	· 단, 위치정보(동/호수) 또는 컴퓨터의 정보 등 비교 가능한 데이터일 경우 명의변경처리 가능함(관리자 처리 시 기존 데이터와 비교함)

□ IP주소 등록 확인 및 변경 절차 (도식)