서울대학교 정보화본부
Information System & Technology
Seoul National University

연구실 서버 데이터, 안전한가요?

- 교내 연구실, 사이버 침해사고 월 평균 4건 발생
  - 대부분 서버 접속 계정의 취약한 비밀번호 사용으로 사고 발생
- 이로 인해, 서버 데이터 유출 및 훼손(72%), 관리자 페이지 노출(15%), 홈페이지 변조(4%), 바이러스 감염(2%) 등 피해 발생

1 ○○연구실 피해 사례

- 사고내용: ‘23년 5월, A 서버 계정이 탈취되어 악성코드 감염
- 원　　인: 서버 계정의 취약한 비밀번호 사용(ex.1234, qwer1234!)
- 피　　해: 서버 내 중요 데이터 손실 및 유출

조치내역

- ✓ 유추 불가한 비밀번호 사용
- ✓ 외부 SSH 접근 차단
- ✓ 계정 별 접근 권한 설정

2 △△연구실 피해 사례

- 사고내용: ‘22년 12월, B 서버 내 DB 파일 강제 암호화 사고 발생
- 원　　인: DBMS(MySQL, Oracle 등)의 관리자 계정 취약한 비밀번호 사용, 미사용 포트 과다 오픈, 백신 미설치로 악성 파일 자동 대응 실패
- 피　　해: 중요 DB 파일 암호화 및 복구 불가한 피해 발생

조치내역

- ✓ DBMS 관리자 계정 비밀번호 변경
- ✓ DBMS 불필요 계정 삭제
- ✓ 미사용 포트 비활성화
- ✓ 백신 프로그램 설치

중요 데이터 보호를 위해 서버 보안은 반드시 필요합니다.
‘서울대학교 서버 운영 보안 가이드’를 참고하여 사이버 침해사고 대응 체계를 마련해주세요.

가이드 다운로드

문의: 정보화본부 IT서비스센터 880-8282