[붙임] RDP(윈도우) 접속 관련 서버 및 단말 보안 체크리스트

○ 체크리스트

순번	점검내용	확인 여부	비고
1	불필요한 원격 접속 서비스 등 포트 점검 및 제거		RDP 불필요시
2	원격 접속 서비스용 단말기(IP) 제한		
3	접속로그 점검 및 침해유무 파악		
4	복잡한 비밀번호 및 임계값 설정, 정기적 변경		
5	소프트웨어 최신 보안 업데이트 적용		
6	중요 데이터 정기 백업 및 복구 절차 점검 등		

○ 각 항목 확인 및 점검 가이드

※ 윈도우 서버 및 단말 버전에 따라 상이할 수 있음

1. 불필요한 원격 접속 서비스 등 포트 점검 및 제거

- 설정 화면 이동

· Win + R → sysdm.cpl 입력 → "원격" 탭 이동

· 이 컴퓨터에 대한 원격 연결 허용" 체크 여부 확인

- RDP 비활성화 (설정 시, 원격 접속 불가)

· 위의 "원격" 탭에서 "이 컴퓨터에 대한 원격 연결 허용 안함" 체크, 저장

2. 원격 접속용 단말기(IP) 제한

- 화면 이동

· Win + R → wf.msc 실행

· "인바운드 규칙" → "원격 데스크톱 - 사용자 모드 (TCP-in)" 우클릭>속성

- IP 제한

· "영역" 탭에서 "원격 IP 주소" 에 “다음 IP 주소‘ 클릭 후 제한 된 IP만 추가

3. 접속로그 점검 및 침해유무 파악

- 화면 이동

· Win + R → eventvwr.msc 실행

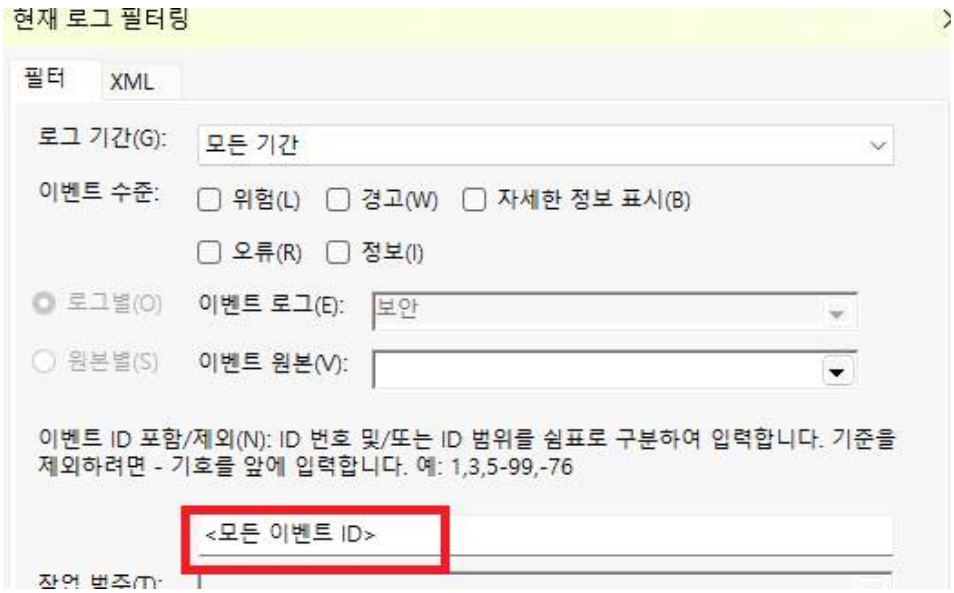
· 좌측 목록에 "Windows 로그" → "보안" 선택

· 우측 ”현재 로그 필터링“ 클릭 후 ”<모든 이벤트 ID>“에 검색

4624: 성공 로그인 / 4625: 실패 로그인

- 점검 사항

· 다수의 실패 로그인 혹은 관리자 미접속 시간에 성공 로그인 이력 유무 확인



4. 복잡한 비밀번호 및 임계값 설정, 정기적 변경

1) 복잡한 비밀번호 설정, 사용기간 제한

- 화면 이동

· Win + R → gpedit.msc 실행

· "컴퓨터 구성">"Windows 설정">"보안 설정">"계정 정책">"암호 정책" 이동

- 설정

· “암호는 복잡성을 만족해야 함” : 사용

· “최대 암호 사용 기간” : 90일

· “최소 암호 길이” : 8문자

· “최소 암호 사용 기간” : 1일

2) 임계값 설정

- 화면 이동

· Win + R → gpedit.msc 실행

· "컴퓨터 구성">"Windows 설정">"보안 설정">"계정 정책">"계정 장금 정책" 이동

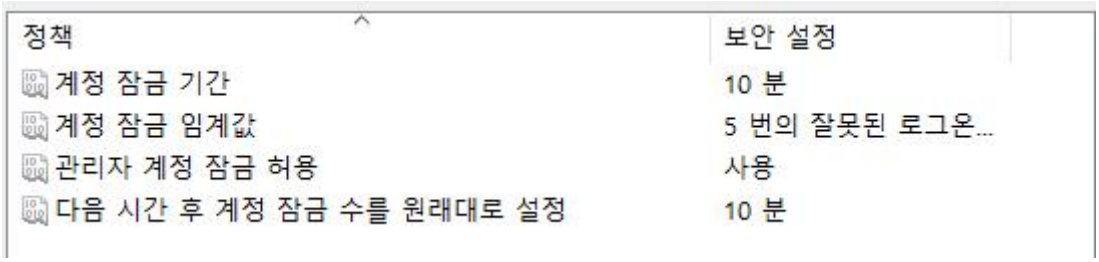
- 설정

· “계정 잠금 기간” : 10분

· “계정 잠금 임계값” : 5번의 잘못된 로그온 시도

· “관리자 계정 잠금 허용” : 사용

· “다음 시간 후 계정 잠금 수를 원래대로 설정” : 10분



5. 소프트웨어 최신 보안 업데이트 적용
  - 화면 이동
    · Win + I → "Windows 업데이트" 클릭
  - 조치
    · "업데이트 확인" 클릭 후 적용

6. 중요 데이터 백업
  - 별도 서버 및 단말 보관 시 데이터/파일 암호화 등 개인정보 유출에 유의