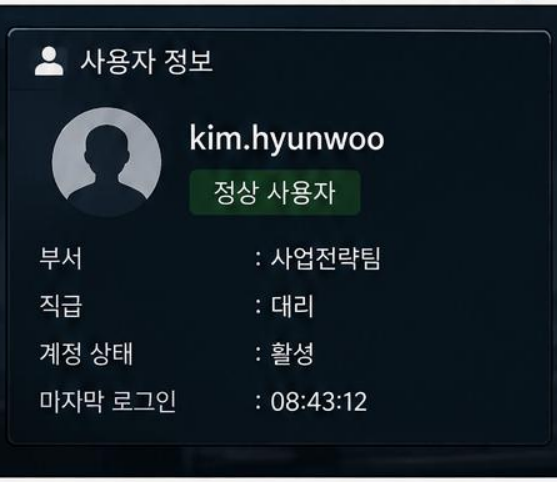
1 평범한 보안관제 화면

오전 8시 43분.
보안관제 시스템에
평범한 로그인 기록 하나가
올라온다.

계정 이름도 익숙했다.
김현우 대리.

문제는 아무도
그 이름을 다시
확인하지 않았다는
것이었다.

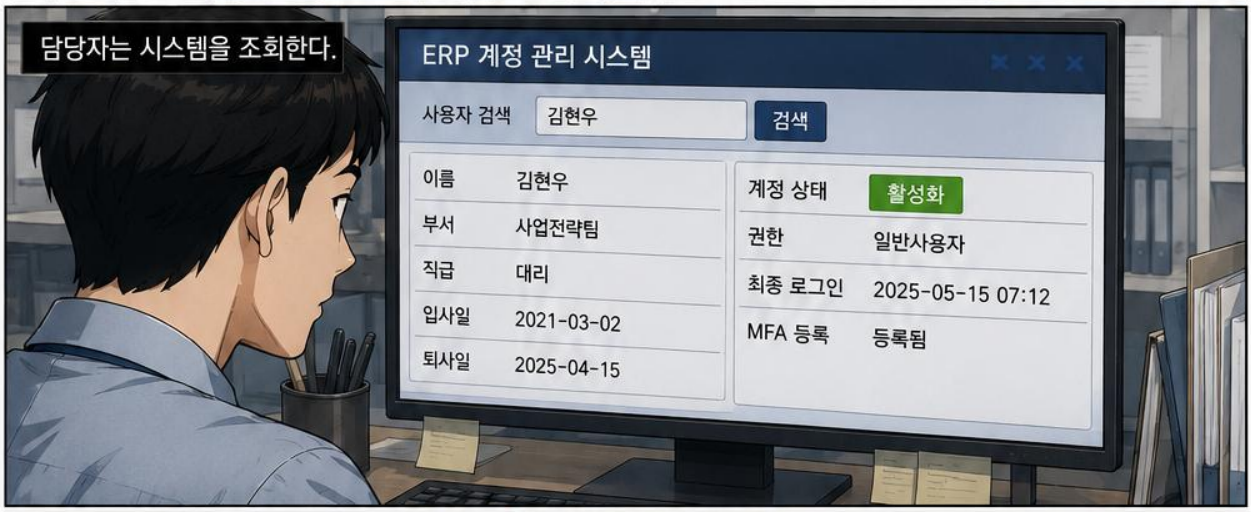


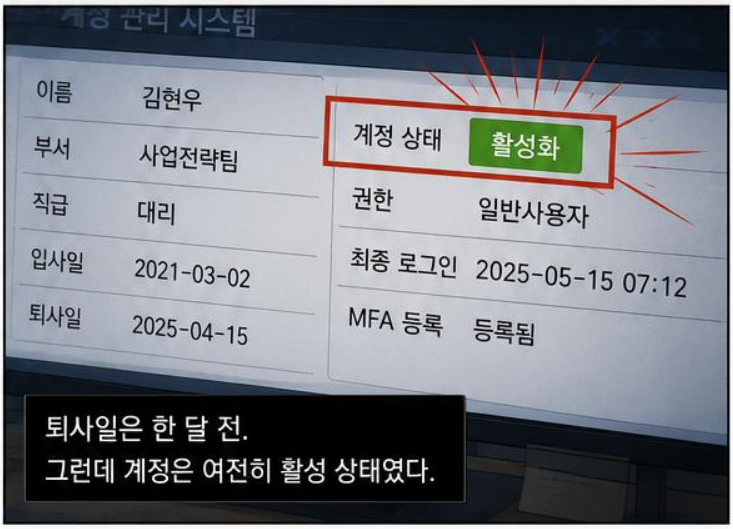
기억하세요!
퇴사자 계정이 남아 있으면 누구나 다시 회사 시스템에 접근할 수 있습니다.

퇴사자 계정 | 권한 회수 | MFA | 로그 모니터링


2 사업전략팀 긴장된 회의
같은 시각, 사업전략팀 회의실
대형 입찰 프로젝트
D-30
✓ 경쟁사 대비 선제 제안
✓ 가격 전략 및 공급 조건 수립
제안서 완성 및 제출
이번 건 반드시 따야 합니다.
경쟁사보다 먼저 제출해야 해...
가격 전략이 핵심인데...
수치 하나라도 틀리면 안 돼...
입찰 제안서 핵심 항목
01 가격 정책 및 수익 구조 극비
02 공급 조건 및 일정 극비
03 협력사 단가표 극비
04 리스크 분석 및 대응 방안 극비
대외비
모든 자료는 '극비'로 분류되어 접근 권한이 엄격히 제한되어 있다.
대외비
입찰 제안서
대형 입찰 프로젝트, 모든 정보는 극비! 단 하나의 실수도 용납되지 않는다.

3 퇴사자 계정 정리 요청 메일





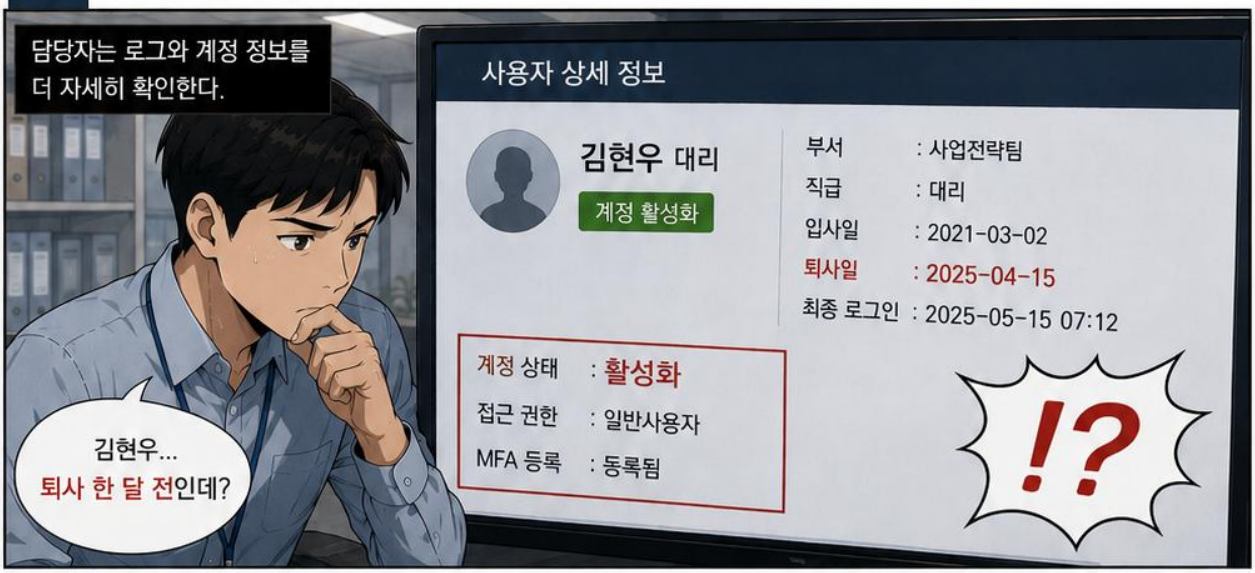
여기서 잠깐!

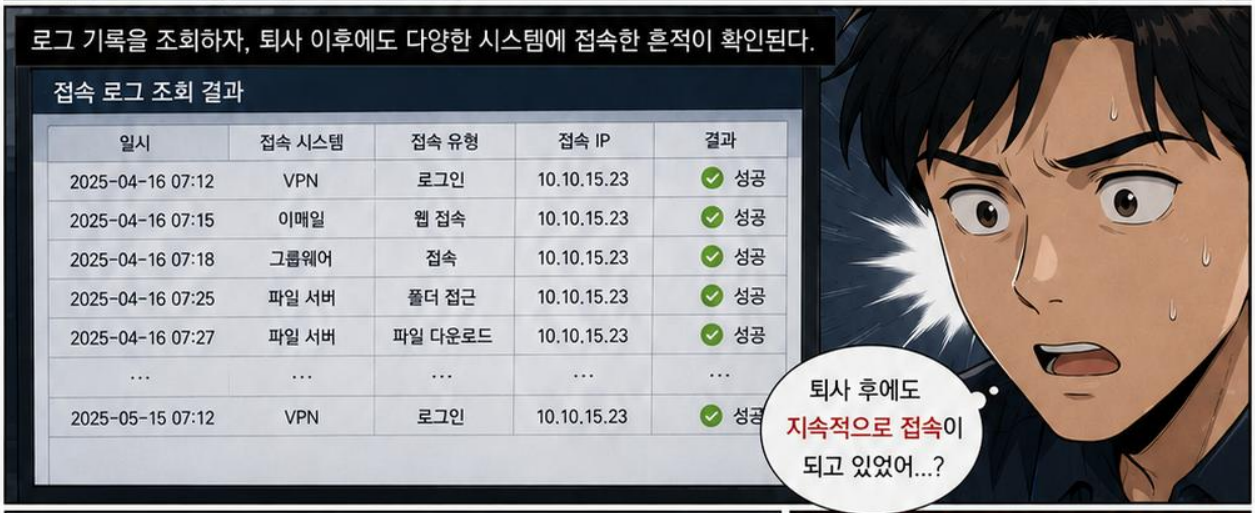
퇴사 처리 후에도 계정이 남아있으면, 권한이 그대로 유지되어
내부 정보 유출의 위험이 발생할 수 있습니다!

퇴사자 계정 관리 체크 포인트

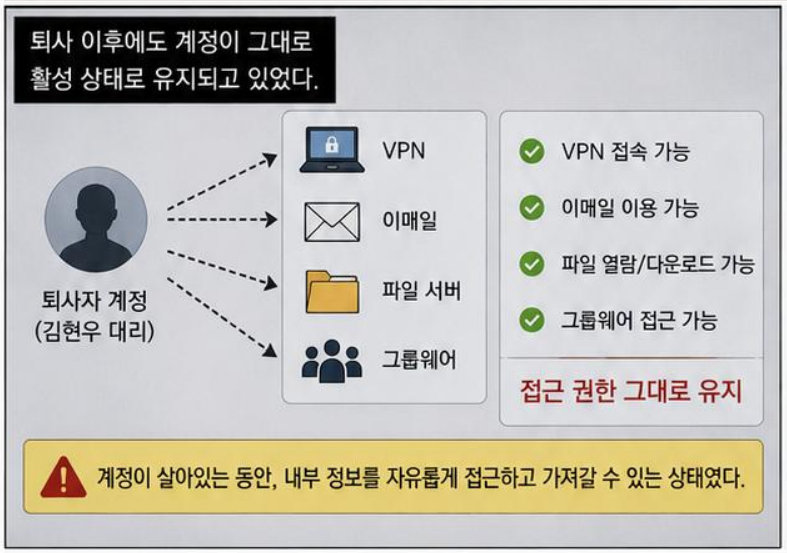
- ☑ 퇴사 사실 통보
- ☑ 계정 비활성화/삭제
- ☑ 권한 회수 확인

4 충격적인 발견





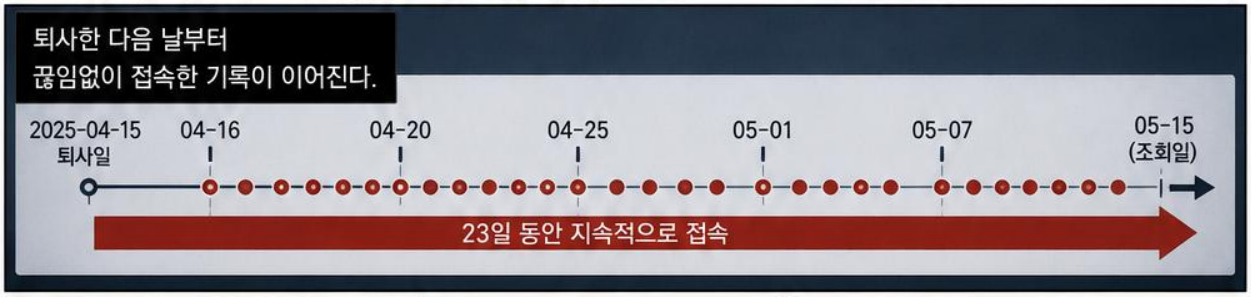
일시	접속 시스템	접속 유형	접속 IP	결과
2025-04-16 07:12	VPN	로그인	10.10.15.23	성공
2025-04-16 07:15	이메일	웹 접속	10.10.15.23	성공
2025-04-16 07:18	그룹웨어	접속	10.10.15.23	성공
2025-04-16 07:25	파일 서버	폴더 접근	10.10.15.23	성공
2025-04-16 07:27	파일 서버	파일 다운로드	10.10.15.23	성공
…	…	…	…	…
2025-05-15 07:12	VPN	로그인	10.10.15.23	성공

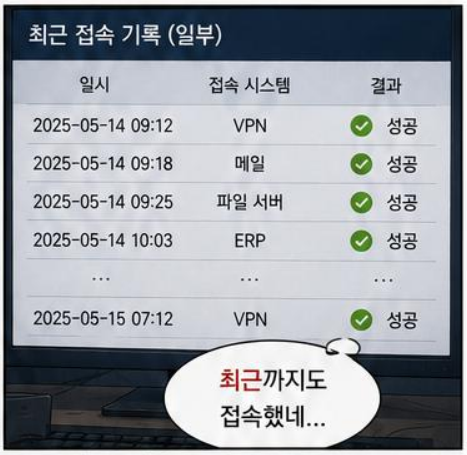


퇴사자 계정이 그대로 살아있으면, 회사의 핵심 정보가 무방비로 노출됩니다.

#퇴사자 계정 #계정 활성화 #접근 권한 #내부 정보 유출 #로그 분석

5 과거 접속 기록 확인





퇴사자 계정이 그대로 남아 있으면,
언제든 내부 시스템에 접근할 수 있습니다.

#퇴사자 계정 #지속 접속 #계정 활성화
#접근 권한 #로그 분석 #내부 정보 유출

6 인사팀 vs 운영팀 통화

부서 간 인계 · 협업 절차가 명확하지 않으면,
퇴사자 계정은 그대로 남아 위험이 됩니다.

- ☑ 퇴사 통보
- ☑ 계정 종료 요청
- ☑ 권한 회수
- ☑ 시스템 반영 확인

퇴사 처리의 마지막 단계는 **'계정 종료 및 권한 회수'**입니다.

7 보안팀 긴급 분석

다운로드한 주요 문서 목록

파일명	문서 유형	용량
신규 사업 전략 문서	내부 전략	4.2 GB
가격 정책 자료	영업 기밀	3.6 GB
협력사 단가표	영업 기밀	2.8 GB
입찰 제안서 초안	입찰 자료	5.1 GB
내부 조직 개편안	내부 문서	2.3 GB
…	…	
총 다운로드 용량		18.0 GB

접속 타임라인 (퇴사 이후)

04-16 07:12	VPN 접속	성공
04-16 07:15	이메일 접속	성공
04-16 07:18	그룹웨어 접속	성공
04-16 07:25	파일 서버 접근	성공
04-16 07:27	파일 다운로드 시작	성공
…		
05-15 07:12	VPN 접속(마지막)	성공

하루, 이틀, 일주일...
아무 차단 없이 계속 접속했다.

주요 접근 시스템

김현우 대리
(퇴사자 계정)

메일 시스템	정상 접근
그룹웨어	정상 접근
파일 서버	정상 접근
ERP 시스템	정상 접근
문서관리 시스템	정상 접근

퇴사자 계정이 남아 있어, 현직 직원과 동일한 권한을 사용했다.

퇴사 후에도 계정이 남아 있으면,
중요 정보는 언제든 외부로 유출될 수 있습니다.

#퇴사자 계정 #권한 회수 #로그 분석
#접근 권한 #내부 정보 유출 #계정 관리

8 경쟁사 제안서 비교

보안팀은 유출된 자료가
경쟁사 제안서에 반영되었을 가능성을
확인하기 시작한다.

유출 의심 자료

입찰 제안서 초안_v3.pptx
최종 수정일 : 2025-04-10 22:47

2025년 A 프로젝트 제안서 (초안)

3. 제안 범위

- 시스템 통합 및 구축
- 데이터 이관
- 유지보수 3년

01 분석 | 02 설계 | 03 구축 | 04 운영

경쟁사에서 제출한 제안서의 내용과
유사한 부분이 다수 발견된다.

당사 제안서 (초안)

3. 제안 범위

- 시스템 통합 및 구축
- 데이터 이관
- 유지보수 3년

01 분석 | 02 설계 | 03 구축 | 04 운영

4. 추진 일정

분석 2주 — 설계 3주 — 구축 8주 — 운영 3년

VS

경쟁사 제안서

3. 제안 범위

- 시스템 통합 및 구축
- 데이터 이관
- 유지보수 3년

01 분석 | 02 설계 | 03 구축 | 04 운영

4. 추진 일정

분석 2주 — 설계 3주 — 구축 8주 — 운영 3년

동일한 오탈자/표현 비교

당사 제안서 (초안)	경쟁사 제안서
5. 기대 효과	5. 기대 효과
• 운영 효율성 향상	• 운영 효율성 향상
• 비용 절감 효과	• 비용 절감 효과
• 고객 만족도 제고 (응답속도 개선)	• 고객 만족도 제고 (응답속도 개선)

내부 자료가 외부로 유출되어
경쟁사 제안서에 반영된 정황 확인!

퇴사자 계정이 남아있으면,
핵심 정보가 경쟁력을 잃고 회사의 신뢰가 무너집니다.

내부 문서 유출은 곧
기업의 경쟁력 손실로 이어집니다.

#내부 정보 유출 #퇴사자 계정 #접근 권한
#경쟁사 유출 #정보보호 #로그 분석

9 긴급 임원회의

핵심 쟁점

퇴사자 계정 관리 실패	권한 회수 미흡	부서 간 책임 공백	내부 정보 유출 위험
퇴사 후에도 계정이 활성 상태로 유지됨	접근 권한이 그대로 남아 모든 시스템 이용 가능	인사팀과 운영팀 사이 요청·확인 절차 부재	핵심 문서 유출 가능성으로 회사 신뢰·매출 타격 우려

단 한 개의 계정, 단 한 번의 누락이 회사 전체를 위협할 수 있습니다.
계정 관리와 권한 회수는 선택이 아닌 필수입니다.

10 사고 원인 정리

누구도 악의가 없었지만, 결과는 심각했다.

퇴사자 계정은 정리되지 않았고,	계정, 권한 회수 요청은 그대로 남아,	퇴사 이후에도 지속적인 접속이 가능했고,	내부 정보에 대한 접근이 자유로웠다.
			
계정 활성 상태 유지	접근 권한 회수 누락	로그인 · VPN 접속 가능	내부 정보 접근 가능

"보냈다"와 "안 받았다" 사이에서,
회사의 핵심 정보가 유출될 수 있는 길이 열려 있었다.

사고 원인 핵심 요약

1	인사팀	퇴사자 공지 메일 발송	→	요청이 전달되었다고 판단
2	IT 운영팀	계정, 권한 회수 요청 메일 미수신	→	요청 없음으로 계정 유지
3	퇴사자 계정	계정 상태 '활성화' 유지	→	접근 권한 회수되지 않음
4	결과	퇴사 후에도 시스템 접속 및 내부 정보 접근 가능	→	정보 유출 위험 발생

업무 처리의 '착각'이 만든 책임 공백이 회사의 핵심 정보를 위협합니다.

- ☑ 퇴사자 계정 관리 절차 명확화
- ☑ 계정 종료 및 권한 회수 확인 프로세스 필수
- ☑ 부서 간 커뮤니케이션 및 기록 관리 강화

11 추가 분석 결과

보안팀은 추가 분석을 통해,
퇴사자 계정이 그대로 활용되고
있었음을 확인했다.

퇴사자 계정 추가 분석 결과

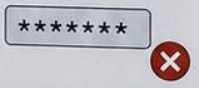
김현우 대리
퇴사자 계정

퇴사일 : 2025-04-15
최종 로그인 : 2025-05-15 07:12

MFA 기기 유지

동록된 MFA 기기가
여전히 활성 상태

비밀번호 변경 없음

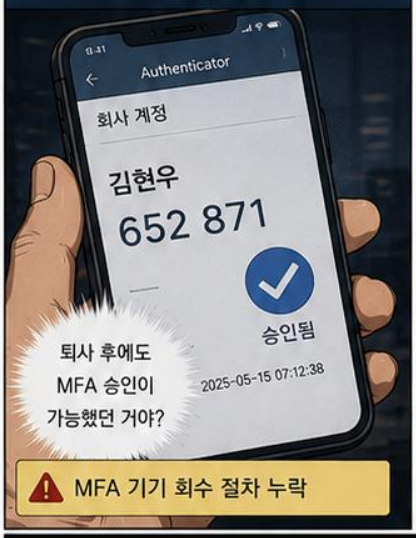


퇴사 이후에도
비밀번호 변경 기록 없음

권한 회수 없음

파일 서버, 그룹웨어 등
접근 권한 그대로 유지

MFA 기기 상태 확인



⚠ MFA 기기 회수 절차 누락

비밀번호 변경 이력

변경 일시	변경자	변경 결과
2025-03-02	김현우	성공
2025-03-15	김현우	성공
2025-04-01	김현우	성공
2025-04-15	-	-
2025-05-15	-	-

퇴사일 이후로
변경 기록이
전혀 없어...

⚠ 비밀번호 변경 및 무효화 미실시

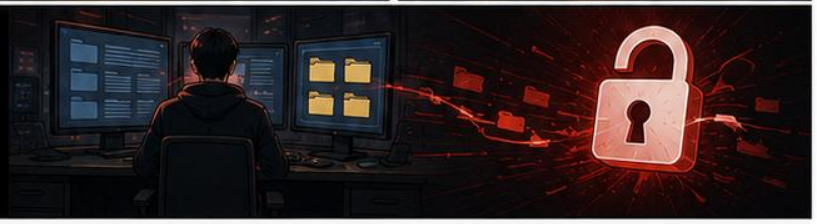
계정 권한 현황

시스템	권한 상태
파일 서버	읽기/쓰기
그룹웨어	관리자
ERP	사용자
메일 시스템	사용자
사내 메신저	사용자
...	...

민감 시스템까지
모두 접근 가능
상태였어...

⚠ 권한 회수 절차 누락

누군가의 부주의가 만든 작은 틈,
그 틈으로 퇴사자는 아무런 제약 없이
회사의 핵심 정보에 접근할 수 있었다.



퇴사자 계정, 반드시 다음 사항을 확인하세요!

MFA 기기 회수 확인
등록된 MFA 기기
반드시 회수

비밀번호 변경/무효화
퇴사 즉시 비밀번호
변경 또는 무효화

접근 권한 회수
모든 시스템의 접근
권한 즉시 회수

로그 모니터링 강화
퇴사 이후 비정상 접근
지속 모니터링

퇴사자의 계정을 방치하는 순간, 내부 정보 유출은 현실이 됩니다!
계정 관리의 작은 실수가, 회사의 미래를 위협합니다.

12 교훈과 마무리

퇴사자 계정 관리 미흡

퇴사 처리 후에도
계정이 활성 상태로
남아 있었다.

권한 회수 누락

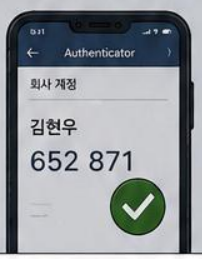
시스템 접근 권한과
데이터 접근 권한이
회수되지 않았다.

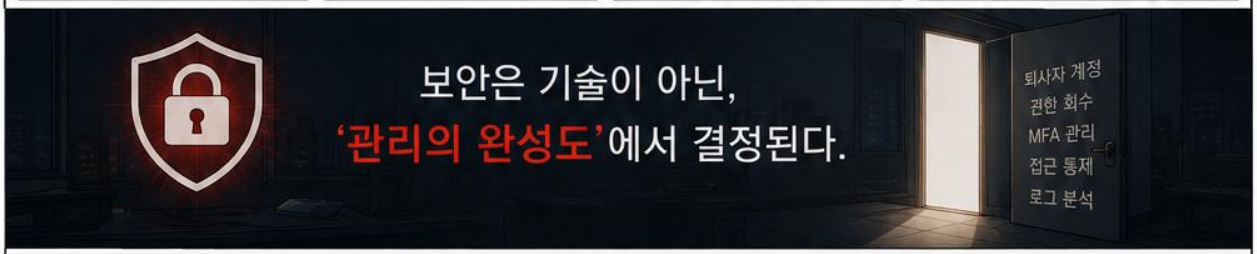
부서 간 책임 공백

인사팀과 운영팀의
커뮤니케이션 부재로
책임이 공백이 생겼다.

MFA 및 보안 통제 미흡

MFA 기기 유지, 비밀번호 변경
없음으로 내부자처럼
접근이 가능했다.





우리가 반드시 기억해야 할 교훈

- 퇴사 처리는 '메일 발송'으로 끝나지 않습니다.
- 계정 종료와 권한 회수는 반드시 확인되어야 합니다.
- 사용하지 않는 계정은 가장 위험한 계정입니다.
- 내부 계정 관리 부주의는 대규모 정보유출로 이어질 수 있습니다.

지금 바로, 퇴사자 계정 관리 프로세스를 점검하세요!
우리의 작은 관심이 회사를 지키는 가장 확실한 보안입니다.