2026년 상반기 국내 랜섬웨어 동향 분석

공격 벡터 · 협상 실태 · 복구율 통계

요 약

본 보고서는 2026년 1월부터 6월까지 국내에서 접수된 랜섬웨어 침해사고 412건을 분석한 결과를 담고 있다. 초기 침투 경로는 외부 노출 RDP(38.2%), VPN 장비 취약점(24.5%), 피싱 메일 첨부파일(19.1%) 순으로 나타났다. 특히 백업 데이터가 동일 도메인에 마운트되어 함께 암호화된 사례가 전체의 61%를 차지해, 오프라인·불변 백업의 부재가 복구 실패의 결정적 요인임을 확인했다.

1. 조사 개요

조사 대상은 KISA에 신고된 침해사고 중 랜섬웨어로 분류된 412건이며, 기업 규모별로는 중소기업이 78.4%를 차지했다. 데이터 수집은 신고 접수 시점의 초기 진술과 현장 분석 결과를 교차 검증하는 방식으로 진행했다.

2. 초기 침투 경로

외부에 노출된 원격 데스크톱 서비스가 여전히 가장 큰 위협으로 확인됐다. 해당 사례의 82%에서 관리자 계정에 다단계 인증이 적용되어 있지 않았으며, 비밀번호 재사용이 확인된 경우도 절반을 넘었다.

3. 백업 및 복구 실태

백업을 보유했다고 응답한 조직 중 실제로 복구에 성공한 비율은 34.7%에 그쳤다. 실패 사유는 백업 대상 누락, 동일 네트워크 내 보관, 복구 절차 미검증 순이었다.

4. 권고 사항

3-2-1 백업 원칙 준수, 관리 인터페이스의 외부 노출 차단, 관리자 계정 MFA 강제, 분기별 복구 훈련 시행을 권고한다.