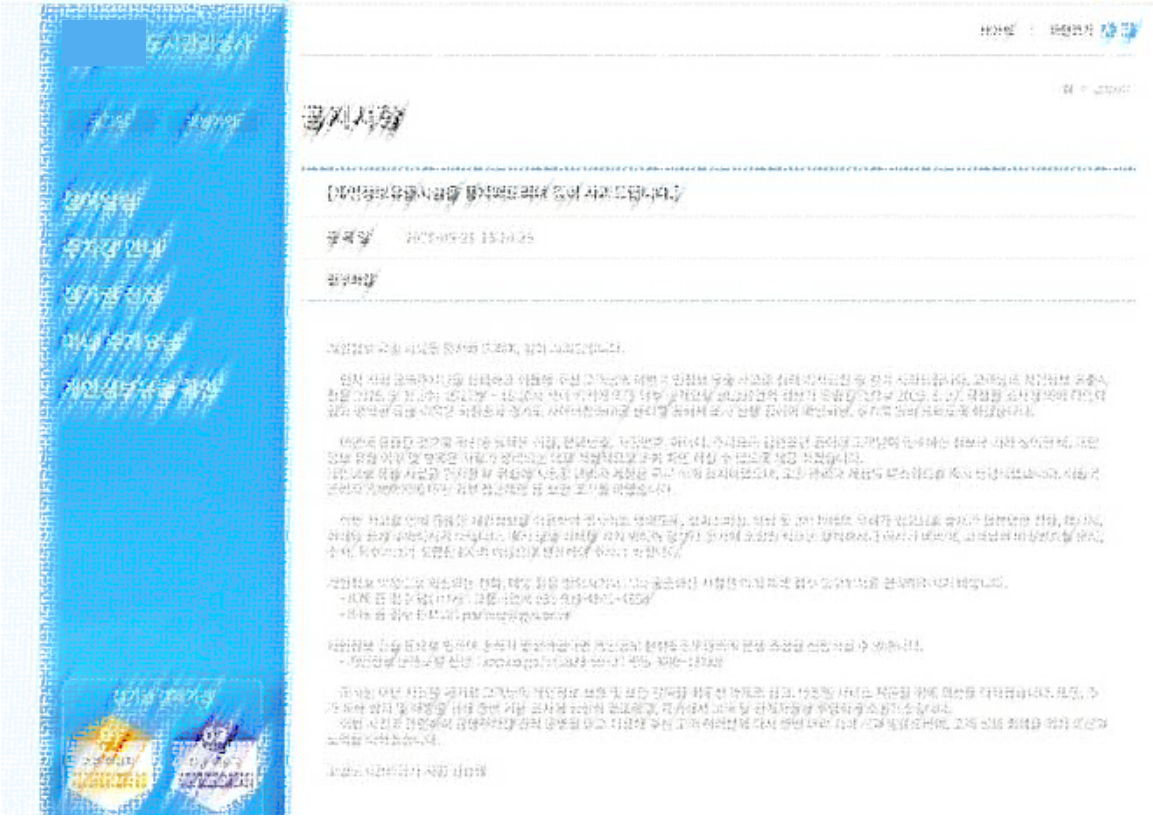
A 시 공영주차장 이용 고객 정보 해킹 사고 보고서



1. 개요

2025 년 5 월, A 시 산하기관 B 도시관리공사는 공영주차장 시스템을 운영하던 외주업체의 관리자 계정 정보가 외부 공격자에게 탈취되어 약 1 만여 명의 시민 개인정보가 유출된 사건이 발생. 해당 사고의 원인, 해킹 유형, 예상 경로, 그리고 대응 및 방어 방안에 대해 요약 설명함.

2. 사고 개요

- 발생 일시: 2025 년 4 월 21 일 오후 3 시 27 분 ~ 4 시경
- 피해 규모: 이용객 10,399 명의 개인정보
- 유출 정보: 성명, 전화번호, 차량번호, 주차장 ID, 요금 감면 조건 등
- 공격 수단: 외부에서 관리자 계정 탈취 후 시스템 접근

3. 사고 원인 가능성 분석

1) 외주 유지보수 업체의 계정 보안 관리 소홀

- 관리자 계정 ID/PW 가 평문 저장 또는 취약한 형태로 노출되었을 가능성

2) 시스템 접근 통제 미흡

- 관리자 페이지에 대한 IP 차단, 인증 강화 등 기본적인 보안 설정 미비

3) 공격 탐지 실패

- 해커의 최초 침입 및 활동을 실시간으로 탐지하지 못함

4. 해킹 유형 및 매커니즘

- 공격 유형: 인증정보 탈취 후 시스템 침투 (Credential Theft → Privilege Escalation)
- 가능성 높은 침입 경로:

a) 피싱 또는 스피어피싱 이메일을 통한 관리자 계정 탈취 (멀웨어 침투,로그인 정보수집)

b) 외주업체의 VPN 또는 원격접속 시스템에 대한 무차별 대입(Brute Force) 공격

c) 관리자 계정 정보가 포함된 내부 자료 유출 또는 클라우드 저장소 노출

5. 2 차 피해 가능성

- 유출된 전화번호 기반 스미싱 공격
- 차량번호 기반 위치 추적/사생활 침해 우려
- 유출 정보 악용한 사회공학적 공격

6. 방어 방안 및 대응책

보안 유형	관련 기술	기술적 조치용 솔루션
관리자 계정 다중 인증	MFA(다중 인증)	NexBe Sign 통합인증
고객 (개인/민감)정보보안	DLP	PCFILTER
관리자 페이지 접근제어	NAC/제로트러스트 보안	엑소스피어
해킹,랜섬,바이러스 등 각종 사이버 위협 방지	선천면역 종합 사이버위협 차단(무학습형, 알고리즘)	파라솔(trueEP)
	후천면역 안티바이러스 (학습형, 분석엔진)	MS 디팬더(윈도우 기본) 엑소스피어
키보드 보안	가상 키패드	INNOVER Keypad
이메일 보안	수시 해킹메일 모의훈련	머드픽스
	악성 스팸메일 차단	스팸스나이퍼

1) 기술적 조치:

- 관리자 계정에 다중 인증(MFA) 도입
- 관리자 페이지 접근 IP 화이트리스트 설정
- 비인가 접속/행위 탐지를 위한 EDR/XDR 또는 실시간 행위 기반 방어체계 도입
- 외주업체 계정 분리 및 모니터링 강화
- 내부 중요 로그 및 계정 접근 이력 상시 모니터링

2) 기술적 조치용 솔루션 대응 (TrueEP/파라솔 솔루션 적용 가능 영역):

- 비정상 행위 탐지 및 자료 유출 실시간 차단 (Self/Non-Self 구분 기반)
- 알려지지 않은 랜섬웨어 및 악성코드 활동 즉시 탐지 및 차단
- 외부 저장장치, 메신저, 이메일, 네트워크 통한 자료 전송 통제
- 정책기반 USB, 테더링, 외부접속 차단
- 전송 로그 및 개인정보 포함 문서 감시 기능

3) 제도적/관리적 대응:

- 외주 유지보수 업체 대상 보안 교육 및 보안준수 협약 강화
- 사고 대응 시나리오 구축 및 주기적 모의훈련
- 개인정보보호법 준수 여부 상시 감사체계 구축

7. 결론

본 사고는 기본적인 계정 보안 관리 소홀과 외주업체 통제 부재에서 기인한 것으로, 향후 유사 사고 방지를 위해 기술적·관리적·제품적 다중 방어체계 마련이 필수적이다.

8. 솔루션 문의

파라솔(PARASOLE) 도입 문의

E help@parasole.co.kr

(주)제이커넥트

서울시 종로구 평창문화로 75, 글로리아타운 A동 407-2호 (03009)