베니스 영화제 참가자 대상 해킹, 해커 개인정보 탈취

▶ 베니스 영화제, 기자와 참석자 개인정보 서버에서 유출

침해사고 일시	7.7	발생국가	이탈리아
침해사고 유형	개인정보 유출	침해사고 규모	-

- 7월 7일, 이탈리아 베니스 영화제 조직위에서 영화제 참가자 및 언론인 개인정보가 외부 공격자에 의해 무단 접근 및 복사되는 침해사고가 발생함. 이번 사건으로 이름, 이메일 주소, 전화번호, 우편 주소, 부가가치세 환급 대상자의 경우 세금 코드까지 유출 가능성이 확인됨. 피해자는 수백 명 이상으로 추정되며 특히 언론인과 영화 관계자 등 민감 인적 네트워크가 포함되어 있음. 사고 원인은 영화제 서버의 접근제어 취약점 또는 인증 우회 가능성이 지목됨.
- 조직위 IT팀은 침입이 탐지되자 즉시 해당 시스템을 격리하고 보안 조치를 적용함. 침해 범위 분석과 복구 작업을 병행했으며 유럽 GDPR 제33조에 따라 관계 감독기관에 신고를 진행함. 그러나 당국에 최초 보고가 언제 이루어졌는지에 대해서는 불명확하며 피해자 통보는 8월 5~6일 사이에 개별 발송됨.
- 유출된 정보 특성상, 표적형 피싱과 사칭 연락, 세금 사기 등의 2차 피해 위험이 높음. 특히 VAT 환급 대상자의 세금 정보 노출은 재정 사기 가능성을 키움. 사고 직후 영화제 측은 참가자들에게 비밀번호 변경과 다중인증(MFA) 설정을 권고하고, 베니스 영화제 관련 주제를 사칭한 이메일과 메시지에 주의할 것을 요청함.
- 이번 사건의 대응 과정에서 조직위는 침해된 데이터베이스가 행사 운영 데이터, 결제, 예약 발권 시스템에는 영향을 미치지 않았다고 강조함. 다만 공격자 신원은 아직 밝혀지지 않았으며, 2022년 칸 영화제 온라인 예매 시스템을 마비시킨 봇 공격 사례와 유사한 문화행사 대상 위협 확산 우려가 제기됨.
- 베니스 영화제 측은 현재 포렌식 분석과 서버 보안 강화 작업을 지속 중이며, 향후 인증과 접속 관리 체계를 재정비하고 외부 보안 자문을 확대할 계획임.

1) https://www.techradar.com/pro/security/venice-film-festival-hacked-attendee-data-leaked-online
2) https://www.hollywoodreporter.com/movies/movie-news/venice-film-festival-hacked-data-compromised-1236338374/

미국 미네소타주 세인트폴 시정부, 랜섬웨어 공격 발생

▶ 미국 미네소타주 세인트폴 시정부, 랜섬웨어 공격으로 내부 네트워크 및 주요 행정 서비스 마비

침해사고 일시	7.25	발생국가	미국
침해사고 유형	랜섬웨어	침해사고 규모	-

- 7월 25일, 미국 미네소타주 세인트폴 시정부가 랜섬웨어 조직 '인터락(Interlock)'의 공격을 받아 시청 내부 전산망과 온라인 행정 서비스가 전면 중단되는 사태가 발생함. 공격자는 시정부 서버에서 약 43GB의 데이터를 탈취했다고 주장하며 금전적 요구를 했으나, 시정부는 협상 없이 네트워크를 차단하고 즉각 비상 대응 체계를 가동함.
- 사고 원인은 노후화된 네트워크 장비와 미적용 보안 패치를 통한 침투로 분석됨. 공격 방식은 데이터 암호화와 유출 위협을 병행하는 '이중 갈취(Double Extortion)'였으며, 표적에는 시민 개인정보, 내부 행정 문서, 재정 자료, 내부 이메일 등이 포함된 것으로 알려짐. 이는 시정부의 디지털 인프라 취약성이 공격에 직접적으로 악용된 사례임.
- 공격 직후 시정부는 FBI와 미네소타 주방위군 사이버보안 부대의 지원을 받아 피해 범위를 조사했고 모든 서버와 단말기의 보안 점검, 데이터 백업 및 계정 초기화를 실시함. 약 3,500명 직원의 계정 비밀번호 변경 작업이 'Operation Secure St. Paul'이라는 명칭으로 진행됐으며, 잠재적 침투 경로 차단을 위해 외부 네트워크 연결이 전면 중단됨.
- 대응 조치에는 구형 서버 교체, 최신 보안 패치 적용, 재해 복구(DR) 프로세스 검증, 전 직원 보안 교육 강화, 피싱 이메일 경고 발송이 포함됨. 긴급 911 대응 시스템은 정상 가동됐으나 수도 요금 납부, 도서관 네트워크, 각종 인허가 업무는 장기간 오프라인 처리로 전환됨. 이번 사건은 미국 지방정부가 여전히 랜섬웨어의 주요 공격 표적임을 재확인시켰으며, 예방적 보안 투자와 지속적 모니터링 체계 강화의 필요성을 부각시킴.

1) https://therecord.media/ransomware-gang-behind-minnesota-attack
2) https://www.govtech.com/security/st-paul-minn-breach-confirmed-as-ransomware-attack

유럽 항공사 에어프랑스와 KLM, 고객 정보 유출

▶ 에어프랑스와 KLM이 공동으로 사용하는 제 3자 고객 서비스 플랫폼 해킹으로 항공사 고객 정보 유출 발생

침해사고 일시	7.28	발생국가	프랑스,네덜란드
침해사고 유형	개인정보 유출	침해사고 규모	-

- 7월 28일, 유럽 항공사 에어프랑스(Air France)와 KLM이 공동으로 사용하는 제 3자 고객 서비스 플랫폼이 해킹돼 다수 고객의 개인정보가 유출되는 사건이 발생함. 두 항공사는 공동 성명을 통해 외부 플랫폼에서 비정상 활동이 탐지됐으며 이를 통해 공격자가 고객 데이터에 접근했다고 밝힘. 내부 항공사 네트워크는 직접 침해되지 않았으나 유출된 데이터는 성명, 연락처, 플라잉 블루(Flying Blue) 회원 번호와 등급, 고객 서비스 이메일 제목 등으로 확인됨. 다만 여권번호, 결제 정보, 비밀번호, 항공편 세부 정보 등 민감 데이터는 포함되지 않았음.
- 사고 원인은 고객센터에서 사용하는 제 3자 시스템의 보안 취약점 악용으로 분석됨. 최근 디올, 샤넬, 판도라, 구글, 콴타스 등 다른 대형 기업들이 동일한 유형의 제 3자 플랫폼 침해를 보고한 사례와 유사성이 있음. 일부 보안 전문가는 이번 사건이 세일즈포스(Salesforce) 인스턴스를 노린 사이버 범죄 조직 샤이니헌터스(ShinyHunters) 또는 스캐터드 스파이더(Scattered Spider)의 연계 공격일 가능성을 제기함.
- 두 항공사는 즉시 해당 플랫폼 접근을 차단하고 네덜란드와 프랑스 개인정보보호 당국에 침해 사실을 보고함. 피해 고객에게는 피싱 및 사기 시도 가능성을 경고하고 수상한 이메일과 연락에 주의할 것을 당부함. 향후 재발 방지를 위해 제 3자 보안 감사 강화, 침입 탐지 및 차단 시스템 개선, 데이터 접근 권한 최소화 조치 등을 진행 중임.
- 이번 사건은 글로벌 항공사조차 제 3자 의존으로 인한 공급망 보안 위협에서 자유롭지 않음을 보여줌. 특히 고객정보 유출이 신뢰도와 브랜드 가치에 미치는 영향이 큰 만큼, 다층 보안 전략과 상시 모니터링 체계 구축이 필수적임.

1) https://www.theregister.com/2025/08/07/klm_air_france_latest_major/
2) https://www.darkreading.com/cyberattacks-data-breaches/air-france-klm-data-breach

프랑스 이동통신사 Bouygues Telecom, 고객 개인정보 유출

▶ 프랑스 이동통신사 Bouygues Telecom, 약 640만 명의 고객 정보 유출

침해사고 일시	8.4	발생국가	프랑스
침해사고 유형	개인정보 유출	침해사고 규모	약 640만 명

- 8월 4일, 프랑스 3위 이동통신사인 Bouygues Telecom이 대규모 사이버 공격을 받아 약 640만 명 고객의 개인정보가 유출됨. 회사 측은 침해 사실을 인지한 직후 내부 보안팀과 외부 보안 전문가를 투입해 조사를 개시하고, 악성 접근을 즉시 차단했으며 프랑스 개인정보보호위원회(CNIL)와 사법 당국에 신고를 완료함. 유출된 데이터에는 고객의 이름, 주소, 이메일, 전화번호, 계약 정보, 신분 관련 데이터(또는 기업 정보)와 IBAN 번호 등이 포함되었으나 비밀번호와 결제 카드 정보는 유출되지 않은 것으로 확인됨.
- 사건의 구체적인 침투 방식은 아직 공개되지 않음. 그러나 해커가 내부 시스템의 소프트웨어 취약점을 악용하거나 권한이 탈취된 계정을 통해 무단 접근한 것으로 추정됨. 특히 IBAN과 계약 정보는 피싱 이메일, 사칭 전화, 계정 탈취 시도에 활용될 수 있으며, 이를 통한 금융 사기나 대규모 스팸과 스미싱 공격으로 이어질 가능성이 높음.
- 이번 공격이 랜섬웨어 형태인지, 혹은 특정 국가 연계 위협 그룹의 소행인지는 확정되지 않았으나, 최근 유럽 및 글로벌 통신업계를 겨냥한 지능형 지속 위협(APT) 사례가 늘고 있어 연관 가능성이 제기됨.
- Bouygues Telecom은 피해 고객 전원에게 이메일과 문자 메시지를 통해 개별 통지를 진행함. 고객들에게 계정 로그인 시 다중 인증(MFA) 적용, 의심 연락 차단, 금융 계좌 모니터링 등 보안 수칙을 안내함. 통신사 내부적으로는 침투 경로를 추적해 차단하고, 서버 접근 제어 강화, 데이터 암호화 수준 상향, 로그 분석 고도화 등 장기적인 보안 대책을 추진하고 있음.

1) https://therecord.media/bouygues-telecom-france-cyberattack-data-breach
2) https://www.techradar.com/pro/security/bouygues-telecom-data-breach-could-affect-millions-of-customers-heres-what-we-know