2026년 사이버 보안 전망: 일본 및 아시아 태평양

Google Cloud
Security

Google Cloud의 2026년 사이버 보안 전망 스페셜 리포트는 JAPAC 지역 기업들이 내년에 마주할 수 있는 위협과 과제를 미리 파악하고 대비하는 데 도움을 드리고자 합니다.

외교관을 겨냥한 정치적 사이버 스파이 활동: 국제 회의 집중 공략

2026년에는 아태지역 전역에서 개최될 주요 정치 및 안보 정상회의들이 사이버 스파이 활동이 급증하는 주 표적이 될 것으로 예상됩니다. 필리핀 아세안(ASEAN) 정상회의, 중국 APEC 정상회의, 팔라우 태평양 도서국 포럼(PIF) 등의 행사에서 협상 우위를 점하고 후원 국가의 정치적 입지 강화 및 의사 결정에 필요한 정보를 확보하기 위해 정치, 산업, 군사 정보 탈취 작전을 더욱 가속화할 것입니다.

동남아시아 국가의 외교관을 노린 2025년 첩보 활동과 미국-타이완 방위산업 회의를 미끼로 활용해 행사 관계자를 표적으로 삼은 2024년 작전을 토대로 더 진화된 스파이 사이버 공격이 전개될 것입니다.

차량 탑재형 불법 기지국 스캠

2026년에도 차량 탑재형 불법 기지국(FBS)을 악용한 위협은 지속될 전망입니다. 공격자들은 셀룰러 브로드캐스트 메시지 체계에 내재된 보안 취약점을 익스플로잇하는 사기 전술을 활용합니다. 이러한 이동형 기지국은 정상적인 이동통신 네트워크를 사칭하여 인근 기기들이 자신들에게 접속하도록 유인합니다.

일단 연결되면, FBS는 위협 행위자가 통제하는 사이트로 사용자를 유도하는 링크가 포함된 피싱 SMS 메시지(주로 할인이나 기타 콘텐츠를 약속하는 내용)를 전송할 수 있습니다. 이러한 범죄는 주로 Telegram과 같은 소셜 메시징 애플리케이션을 통해 말단 '자금 운반책'을 고용하는 중국 연계 사이버 범죄자들에 의해 주로 자행됩니다.

쉽게 돈을 벌 수 있다는 유혹과 범인 검거의 어려움으로 인해 이러한 위협 추세가 계속 이어질 것으로 보입니다. 2025년 1분기 태국 및 인도네시아 등지에서 성공적인 단속 작전과 검거가 있었음에도 불구하고 3분기에 해당 활동이 빠르게 재출현했습니다. 이는 FBS 전술의 수익성과 복원력을 보여주는 사례이며 내년에도 전 세계적으로 이 위협이 계속될 것임을 시사합니다.

공급망 사이버 보안 의무화

2026년, 일본과 한국에서 활동하거나 해당 국가와 비즈니스 관계를 맺고 있는 조직들은 새롭고 강력한 선제적 공급망 보안 의무 조치를 이행해야 할 것입니다. 이는 최근 발생한 대형 보안 사고들에 대응하여 양국이 국가적 차원의 방어 태세를 강화하고 있기 때문입니다.

일본은 2026 회계연도까지 '사이버 보안 대책 평가 제도'를 도입할 예정입니다. 이 제도는 기업들, 특히 반도체 제조와 같은 제조업 분야 기업들에게 국제 표준인 ISO/IEC 15408에 기반한 보안 유효성 기준을 충족하도록 요구합니다. 이를 위해 기업들은 자사 공급망의 보안 상태를 가시화하고 검증해야 합니다. 아울러 일본 정부는 새로운 사이버 보안 등급 제도를 활용하여 기업들의 전반적인 보안 태세를 평가할 계획입니다.

한국은 잇따른 대규모 침해 사고 이후 통신 등 핵심 기반 시설 분야에 대한 사이버 방어 태세를 전면 재정비하고 있습니다. 이는 정부의 관리 감독 강화로 이어질 것이며, 광범위한 기술 공급망 전반에 걸쳐 견고한 보안 시스템 구축을 위한 투자가 의무화될 전망입니다.

'2026년 사이버 보안 전망' 전체 보고서를 다운로드하여 Google Cloud 보안 리더와 현장에서 실제 위협을 대응해 온 전문가들이 예측하는 내년도 글로벌 트렌드를 확인해 보세요. AI부터 사이버 범죄, 국가 배후 활동(nation-state activity)을 포함한 내용을 담고 있습니다.

Google Cloud