2024년 크라우드스트라이크발 전산마비 사태

2024. 8. 20. 법무법인 린 TMT팀

'죽음의 블루스크린' 사태

지난 7월 19일 미국의 클라우드 기반 사이버 보안회사인 크라우드스트라이크(CrowdStrike)가 배포한 소프트웨어 ' Falcon Sensor' 의 업데이트가 MS 윈도우와 충돌하면서 수백만대의 윈도우 시스템에 화면 전체가 파란색으로 채워지는 현상인 '죽음의 블루스크린'(Blue Screen of Death) 오류가 발생했습니다.

이로 인해 미국의 주요 항공사인 아메리칸 항공 등 5천편 이상의 항공기 운항이 지연되거나 취소되었고, 은행과 주식 거래소의 운영에도 차질이 생겼으며, 방송사에서는 손으로 지도를 그려 일기예보를 하는 일까지 발생했습니다. 10억달러(약 1조4천억원)가 넘는 복구 비용이 들 것으로 예상되고 있고, 이미 법적 소송 절차에 착수한 델타 항공을 포함해 관련 소송이 잇달아 제기될 가능성이 높아 보입니다.

전문가들은 피해 보상과 관련해 다수의 소송이 제기될 가능성을 높게 보면서도, 크라우드스트라이크가 고객과 체결한 계약에 면책조항이 들어가 있을 경우 법적으로 보호를 받을 수 있는 가능성도 염두에 두고 있습니다.

우리나라에 미친 영향은?

한국은 크라우드스트라이크를 사용하는 기업 수가 상대적으로 적어 피해가 제한적이었지만, 일부 저가 항공사의 항공권 예약 및 발권 시스템에 오류가 발생하거나, 게임사의 서버에 장애가 발생해 긴급 점검을 실시하기도 했습니다.

이번 사태로 인해, 국내에서도 소프트웨어 업데이트의 철저한 테스트와 품질 보증의 중요성이 다시 한 번 강조되었고, 이러한 대규모 장애의 영향을 최소화하기 위한 비상 계획과 신속한 대응 매커니즘을 구축할 필요가 있다고 지적되고 있습니다.

EU에서 제정한 '사이버복원력법'(CRA, Cyber Resilience Act)을 아시나요?

이와 관련하여, 유럽연합(EU)이 제정한 CRA도 주목을 받고 있습니다.

CRA는 유럽연합이 사이버 보안사고가 미치는 막대한 영향력을 고려하여 디지털 요소를 포함한 제품의 사이버 보안을 강화함으로써, 소비자와 기업을 보호하기 위해 제정한 규제법률 입니다.

이 법에 따르면, 디지털 제품은 그 설계 단계에서부터 보안을 고려해서 개발되어야 하고, 제품의 수명 주기 동안 정기적인 보안 업데이트를 제공해야 하는 등 엄격한 사이버 보안 요구사항을 준수하여야 합니다. 또한, 제조업체는 제품의 취약점을 신속히 식별하고 해결해야 하며, 이를 위한 취약점 관리 프로세스를 갖추어야 합니다.

심각한 사이버 보안사고가 발생한 경우, 24시간 이내에 유럽연합 사이버 보안청(ENISA, EU Agency for Cybersecurity)과 국가 컴퓨터 보안 사고대응팀(CSIRT, Computer Security Incident Response Team)에 보고하도록 의무화하고 있습니다. 2024년 3월 12일 유럽의회에서 승인되어, 하반기에 발효될 예정입니다.

Legal Insights

'사이버공급망'(Cyber Supply Chain)의 중요성을 인식해야 합니다.

이번 사태는 정상적인 기업활동의 일환인 사이버공급망 내에서 발생될 수 있는 잠재적 리스크의 실체를 여실히 보여주었습니다. 사이버테러나 해킹으로 인한 것이 아니라, 공급받은 보안프로그램을 업데이트하는 과정에서 발생되었기에 더욱 충격적이었습니다.

이를 계기로, 복잡한 사이버 공급망에 잠재된 위험을 식별하고 관리하는 것이 중요하다는 점을 인식하고, 제3자(Third-party) 소프트웨어 사용에 따른 리스크 평가 및 관리체계를 갖추어야겠습니다. 신뢰할 수 있는 공급업체를 선택하고, 필수적인 업계 표준 및 규정에 따르는 엄격한 품질관리 프로토콜을 준수하도록 요구하는 한편, 공급망을 다각화하여 다양한 기술생태계를 구축함으로써, 단일 실패 지점(SPOF, Single Point of Failure)의 영향을 최소화시키는 것도 필요하겠습니다.

'비즈니스 연속성 계획'을 수립하고, '사이버복원력'을 높여야 합니다.

예상하지 못한 사고발생시에도 비즈니스의 주요 기능 운영의 장애를 막아 손실을 최소화하고, 고객신뢰를 유지할 수 있는 '비즈니스 연속성 계획'(BCP, Business Continuity Plan)을 수립하여야 합니다.

이를 위해, 사고 발생을 가정하여 신속하게 대응하고 정기적인 시뮬레이션과 훈련을 통해 준비상태를 점검하고 개선하는 등의 사이버복원력(Cyber Resiliency)을 높이기 위한 노력을 지속하여야겠습니다.

법적 분쟁에 대비하여야 합니다.

사고 발생으로 인한 복잡한 법적 분쟁에 선제적으로 대응할 필요가 있습니다.

먼저, 분쟁발생에 대비하여 서비스수준협약(SLA, Service Level Agreement)을 체결하여 서비스 제공자와 고객의 책임과 의무를 명확히 규정하여야겠습니다. 위반시 제재나 보상방법을 명시하고, 재해복구, 비상상황 대응 절차, 중요시스템의 경우 업데이트 전 테스트를 의무화하는 규정 등을 포함시킬 필요성이 있습니다. 사고와 관련된 계약상의 면책 조항 포함여부 및 그 규정방식에 대해서도 유념하여야겠습니다.

다음으로, 현행 제조물책임법, 정보통신망법, 개인정보보호법 등 관련 법령에서 정한 규제의무를 위반한 것은 없는지 등을 잘 살펴, 사고로 인한 책임을 최소화할 수 있도록 미리 대비할 필요가 있습니다. 국경을 초월한 피해가 발생할 수 있는 만큼, 국제소송 및 준거법 결정 등 국제사법 절차에 대한 이해가 필요하고, 다양한 이해관계자들이 개입된 복잡한 분쟁양상이 전개될 수 있다는 점에서, 적시에 적절한 법적 조력을 받아야 한다는 점을 꼭 기억하시기 바랍니다.

***

관련 구성원