'클라우드 보안인증제 개선방안'에 대한

BSA | The Software Alliance 의견서

August 8, 2019

BSA | The Software Alliance (**BSA**)[1] 는 행정안전부와 과학기술정보통신부가 7 월 23 일 발표 한 '클라우드 보안인증제 개선방안'[2] 에 의견을 전달하고자 합니다.[3]

BSA 소개

BSA 와 BSA 회원들은 데이터 분석, 기계 학습, 사물 인터넷 등 데이터를 기반으로 이루어지는 혁신의 최전선에서 활동하고 있습니다. 소비자와 기업 모두가 이러한 혁신을 신뢰하고 이를 통해 최대한의 이익을 얻을 수 있도록, 우리 회원들은 플랫폼과 서비스 전반에 걸쳐 높은 품질의 서비스를 유지하는데 심혈을 기울이고 있습니다.

BSA 의 회원들은 사이버 위협으로부터 고객을 보호하기 위해 암호화 기술을 포함한 필수적인 보안 기술을 제공함으로써 사용자의 신뢰를 얻고 있습니다. 이러한 위협들은 넓은 범위의 악의적 위협자들에 의해 행해지게 되며, 그들은 시민들의 신분을 훔치고, 우리에게 소중한 사람들을 해치며, 상업적으로 가치 있는 기밀을 훔치거나, 국가 안보에 즉각적 위험을 가합니다.

이에, BSA 와 회원들은 클라우드 보안인증제 요건에 대해 큰 관심을 가지고 있으며, 더욱 개선될 수 있도록 다음과 같은 의견과 권고사항을 제언 드립니다.

---

[1] BSA (www.bsa.org)는 국제 시장에서 글로벌 소프트웨어 산업을 주도하고 있습니다. BSA 의 회원들은 데이터 분석, 기계 학습, 사물 인터넷 등 데이터 중심 혁신의 최전선에서 활동 중이며 사이버 위협으로부터 고객을 보호하기 위해 암호화와 같은 필수적인 보안 기술을 제공함으로써 사용자의 신뢰를 얻고 있습니다.

BSA 회원사: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] 클라우드 보안인증제: https://isms.kisa.or.kr/main/csap/intro/index.jsp

[3] 클라우드 보안인증제 개선방안: https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939

개요

BSA 는 SaaS(Software-as-a-Service) 클라우드 서비스에 대한 인증 요구사항을 간소화하여 SaaS 서비스 제공자의 부담을 줄여줌으로써 공공 부문 SaaS 의 사용을 촉진하려는 행정안전부와 과학기술정보통신부의 노력이 올바른 접근 방법이라고 생각합니다. 이와 같이, 공공 부문에서 클라우드 서비스의 힘과 이점을 점점 더 많이 활용하게 하는 접근 방식을 채택 한다면 한국의 클라우드법 [4]에 강한 영향을 줄 것으로 사료 됩니다. 또한, 이러한 정책은 전 세계 정부들이 채택하고 있는 '클라우드 우선' 정책들과도 잘 연계되어 있습니다 [5].

행정안전부와 과학기술정보통신부의 목표를 보다 확실히 성취하기 위해서는, 클라우드 보안인증 요건의 개정을 추가 채택함으로써 인증제를 더욱 개선 시켜야 합니다. 이에 BSA 는 다음 항목들의 제외를 고려해 주실 것을 요청 드립니다.

- **14.2.1 (물리적 위치 및 분리)** 클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정하고, 공공기관용 클라우드컴퓨팅서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 일반 이용자용 클라우드컴퓨팅서비스 영역과 분리하여 운영하여야 한다.

- **14.3.1 (네트워크 암호화)** 클라우드 서비스를 통해 생성된 중요자료를 암호화하는 수단을 제공하는 경우에는 검증필 국가표준암호화 기술을 제공하여야 한다.

두 요건에 대한 자세한 의견은 아래 내용을 참고 부탁 드립니다.

14.2.1 (물리적 위치 및 분리)

데이터와 서버의 위치를 국내로 한정하고 시스템을 분리 운영하는 사항은 한국의 디지털 생태계에 부정적인 영향을 미치고 세계 디지털 경제에 효과적으로 참여할 수 있는 능력을 저해 할 것입니다. 이러한 요구사항은 서비스 제공 업체들이 데이터와 서버의 위치를 국내로 한정하고 시스템을 분리하기 위해 중복되고 잠재적으로 활용도가 낮은 서버 및 기타 관련 인프라를 배치해야 하기 때문에 결과적으로 서비스 제공 비용을 높이게 됩니다. 서비스 제공자들은 이러한 기반구조 관련 비용을 회수해야 하며, 이는 궁극적으로 최종 소비자의 비용을 증가시킬 것 입니다.

또한, 데이터/서버의 위치를 국내로 한정하고 네트워크 분리를 요구 하는 항목은 최종 사용자와 정부기관을 포함한 조달 업체가 사용 가능한 기술의 선택을 억제 시킬 수 있습니다. 서비스 제공업체가

---

[4] 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률, [제 14839, 2017. 7. 26.]

[5] 호주, 뉴질랜드, 필리핀, 미국 등

국내에 호스팅 시설을 갖추게 된다 하더라도 서비스의 일부 기능은 억제 될 가능성이 높아지게 됩니다. 대부분의 경우, 모든 데이터를 국내에서 처리할 수는 없는 경우에도, 국내에서 모두 처리할 수 있는 경우와 같은 서비스 품질을 제공 할 수 있습니다 (예: 상업용 하이퍼스케일 클라우드 컴퓨팅 서비스의 분석력에 의존하는 특정 부정 행위 탐지 서비스).

데이터 보안이 데이터/서버 현지화 및 네트워크 분리 요구사항(상업용 하이퍼스케일 클라우드 서비스의 사용을 허용하는 것이 아니라)에 대한 주요 우려 사항으로 지목 되고 있다면, 이에 대한 근거가 확실한 것인지 살펴 보아야 합니다. 잘 관리되는 클라우드 서비스는 사내 클라우드 서비스보다 더 안전합니다. 클라우드 서비스 제공업체들은 그들의 시스템이 물리적으로나 디지털적으로나 안전하게 보호될 수 있도록 상당한 투자를 합니다. 이들은 일반적으로 국제 보안 인증에 부합하기 위해 엄격한 감사 프로세스를 거치며, 첨단 위협 보호 기술을 제공하고, 유휴 상태 및 전송 중인 데이터를 보호할 수 있습니다.

전 세계적으로 운영되는 클라우드 서비스 제공업체들은 전 세계의 사이버 위협에 대한 가시성을 확보하고, 새롭게 발견된 사이버 위협에 대한 사이버 방어를 신속하게 업데이트 하고 있습니다. 하지만, 클라우드 서비스 제공자가 데이터/서버를 현지화하고 네트워크를 물리적으로 분리해야 하는 경우 이러한 모든 보안상의 이점을 상실하게 될 것입니다. 더 나아가 잠재적으로 조직이 사용하는 시스템의 보안과 복원력을 감소시킬 것입니다 - 사이버 위협자들은 이러한 서비스 제공자들을 쉬운 목표물로 삼을 것이며, 제공자들이 지능적 위협 보호 기술에 접근할 수 없기 때문에 위협 벡터를 식별하고 다루는 것은 더 어려워 지게 될 것입니다.

데이터와 서버의 현지화 및 네트워크 분리 정책은 국경을 넘어 데이터를 전송하는 능력에 의존하고 상업용 하이퍼스케일 클라우드 컴퓨팅 서비스를 활용하는 기술에 대한 접근을 제한함으로써 국내에서의 AI 와 그 밖의 신흥 기술들의 이용과 발전에 부정적인 영향을 미치고 궁극적으로 한국의 경제 경쟁력에 부정적인 영향을 미치게 될 것입니다.

이에, BSA 는 행정안전부와 과학기술정보통신부에 14.2.1 항목 제외 고려를 요청 드립니다.

14.3.1 (네트워크 암호화)

행정안전부와 과학기술정보통신부가 잘 알고 있듯이 암호화는 신원 도용에 사용될 수 있는 개인 식별 정보, 사기 및 기타 금융 범죄에 이용될 수 있는 금융 데이터, 독점적인 사업 정보와 지적 재산, 심지어는 정부 기밀까지 포함한 중요한 데이터 보호를 위한 중요한 기술입니다. 강력한 암호화로 인해 데이터 침해를 직접적으로 막을 수 있는 것은 아니지만, 침해 이후 사이버 위협자가 중요한 데이터에 액세스하는 것을 차단하여 위험을 완화할 수 있습니다.

그러나 암호화에 대한 국가적인 접근방식은 인터넷의 세계적인 특성과, 범죄나 테러 행위가 국경에 의해 제한되지 않기 때문에 분명한 한계가 있습니다. 실제로, 국내에서 인증된 암호화 표준의 사용만 허용하는 개별 국가의 단편적인 접근방식은 제공자가 동급 최강의 암호화 기술을 사용하지 못하게 할 수 있으며, 이는 민감한 데이터의 보호를 강화하기 보다 약화 시킬 수 있습니다.

이에, 국내 인증 암호화 기술만 사용할 수 있는 요건을 부과하는 대신, **14.3.1 항목 제외 고려를 요청 드리며, 대안으로 행정안전부와 과학기술정보통신부가 암호화를 통해 정보의 보안을 보장하는 원칙적인 접근법을 채택할 것을 제언 드립니다.** 이와 관련하여 BSA 는 추가적인 제언으로 행정안전부와 과학기술정보통신부가 암호화 [6]에 관한 정책과 관 구현을 고려할 수 있는 8 가지 원칙을 제공하고 있습니다.

1. **데이터 보안 개선:** 데이터 서비스 제공자(개인 또는 기업 — 데이터 저장, 관리 또는 전송)는 해당 데이터 또는 해당 서비스에 의존하는 기업 및 개인에 대한 공격을 차단하기 위해 사용 가능한 최선의 기술을 사용할 수 있도록 허용해야 한다**.**
2. **법 집행 및 대테러 역량 강화:** 사생활과 시민의 자유를 보호하는 법을 집행 하는 기관은 테러리스트와 범죄 행위를 방지하고 기소하기 위해 이용할 수 있는 최선의 자원, 정보 및 기술에 접근할 수 있어야 한다.
3. **사생활 보호 향상:** 개인은 그들의 공공, 사적, 상업적 삶과 만남들 속에서 안전 해야 할 권리가 있다.
4. **정부 기밀 정보 보호:** 국가, 주 및 지역 기관은 보유 중 인 데이터가 국내외 침입 위협에 대해 안전한지 확인해야 한다.
5. **혁신 촉진:** 혁신적 데이터 보안 기술의 개발자와 제공자는 디지털 보안을 위한 기술 제품과 도구를 설계하는 방법에 대한 정부의 규정에서 벗어나야 한다.
6. **주요 시설 방어:** 은행, 의료, 전기, 수도 및 기타 중요 인프라 제공자와 같은 필수 서비스 제공자는 사용자에게 최상의 보안 기술을 제공할 수 있도록 해야 한다. 모범 사례는 널리 공유되어야 한다**.**
7. **세계적 영향 이해:** 범죄와 테러 행위는 국경에 의해 제한되지 않기에, 법과 정책은 보안 기술이 개발되고 사용되는 모든 국가에서 일관성과 명확성을 만들어내야 한다.
8. **투명성 증대:** 기술 의무나 암호화의 미래에 관한 입법 제안이 채택되기 전에 공공(이해관계자)과의 완전하고 투명한 대화가 먼저 있어야 한다**.**

[6] BSA 가 개발한 암호화 관련 자료는 우측 페이지를 통해 참고하시길 바랍니다. https://encryption.bsa.org.

Conclusion

BSA 는 소비자 보호, 데이터 보호, 사이버 보안, 암호화 정책 및 법률 개발과 관련하여 전 세계 정부와 긴밀하게 협력해왔습니다. 이러한 경험들을 바탕으로 BSA 는 혁신을 효과적으로 장려하는 동시에 소비자의 이익과 권리를 보호하는 정책과 법률의 가능성을 직접 목격하였습니다.

BSA 는 추후 행정안전부, 과학기술정보통신부와 클라우드 보안인증제 개선을 목적으로 만나고 협력할 수 있는 기회를 환영할 것이며, 이는 두 부처의 목표와도 상응 할 것이라 믿고 있습니다. 이를 위해, BSA 는 해당 부처와의 대화를 요청 드리는 바입니다.

BSA | THE SOFTWARE ALLIANCE