날짜: 2019년 11월 14일

IoT Security Policy Platform은 사물인터넷(IoT)이 세상을 더 나은 곳으로 변화시킬 수 있는 큰 잠재력을 지니고 있다는 견해를 가지고 있습니다. IoT가 인터넷과 전 세계 경제에 미치는 영향에 대한 예측은 인상적입니다. IoT 기기의 수가 폭발적으로 증가하고 새롭고 흥미로운 여러 응용 분야에서 사용될 것으로 예측됩니다. 다음 선언은 이러한 IoT의 잠재력을 실현하는 데 관심이 있는 모든 정부, 시민 및 조직에 적용됩니다.

수십억 대의 IoT 기기, 애플리케이션 및 서비스가 이미 사용되고 있으며 온라인으로 연결되는 수가 점차 증가함에 따라 IoT 보안이 그 무엇보다 중요합니다. 이러한 기기 중 대다수는 기본적인 보안 기능이 부족하며, 기기 취약성이나 손상된 기기가 의도치 않게 사이버 공격의 시작점으로 사용되어 민감한 데이터를 위협하고 개별 사용자의 안전을 위협할 수 있습니다. 이는 IoT를 도입하는 사용자와 기업이 해결해야 할 위험입니다.

보안 강화로 소비자가 IoT의 이점을 실현할 수 있게 됨에 따라 위험을 해결하고 IoT의 기회를 파악하기 위한 많은 노력이 이미 진행 중입니다. 인터넷의 전 세계적인 서비스 범위와 영향력을 감안할 때 IoT 보안을 개선하기 위한 노력에 참여하는 것이 중요합니다.

지금까지 정부 기관과 조직에서는 강력한 연구, 협업 및 복수 이해 관계자와 다양한 포럼을 진행하며 강력한 IoT 보안 프레임워크를 개발하고 있습니다. IoT Security Policy Platform의 회원은 각 분야에서 IoT 보안 사례의 기준을 높이고 있습니다. 우리의 목표는 글로벌 IoT 생태계의 보안을 강화하는 것입니다.

이러한 프레임워크가 정확히 동일하지는 않지만 각각 고유한 지역 및 국가적 맥락을 반영하여 의미 있는 보안 강화를 시도하고 있습니다. 이러한 프레임워크는 다양한 애플리케이션(소비자, 산업 등) 및 IoT 생태계(네트워크, 기기 등)를 대상으로 하며, 행동 권장사항 및 모범 사례에 대한 다양한 접근 방식을 탐구합니다. 하지만 이러한 프레임워크에는 다음과 같은 특정 원칙이 공통적으로 적용됩니다.

- 위험 평가, 보안 테스트 및 평가를 포함하여 설계, 개발 및 수명 주기의 모든 단계에서 보안이 통합되도록 보장
- 개인 정보 및 중요 데이터가 보호되도록 보장
- 사용자가 개인 정보를 쉽게 삭제할 수 있도록 지원

다음과 같은 다양한 수단을 통해 이러한 원칙을 달성할 수 있습니다.

- 취약성 공개 정책 이행
- 기기에 소프트웨어 보안 업데이트가 수신되는 최소 기간을 소비자에게 분명하게 안내

- 소프트웨어를 안전하게 업데이트하는 메커니즘 제공
- 제조업체에서 고유한 암호 또는 자격 증명을 사용하여 기기를 구축
- 보안에 민감한 데이터의 통신 보호(예: 암호화된 데이터 스트림 이용)
- 자격 증명 및 보안에 민감한 데이터를 안전하게 저장

하지만 이러한 프레임워크는 단지 첫 번째 단계일 뿐입니다. IoT Security Policy Platform과 회원들은 IoT 보안에 대한 국제적 합의를 이끌어내기 위한 노력의 일환으로 전 세계적으로 직면한 과제, 특히 단편화를 해결하기 위해 협력하고 있습니다.

나아가 회원들과 플랫폼은 IoT 기기와 관련된 보안 보호 수단에 대한 인식을 제고하고 신뢰를 높이기 위해 끊임없이 진화하는 기술 세계에 발맞춰 필요할 때마다 이러한 프레임워크를 조정하고 개발할 수 있도록 지속적으로 협력해야 합니다.