보안 환경의 미래와 ‘서비스’로서의 보안

공격과 방어는 함께 진화한다. 네트워크가 복잡해지고 데이터가 기하급수적으로 증가할수록 보안상의 취약점과 공격방식은 다양해진다. 점점 정교해지는 생성 AI는 ‘가짜’를 구분하기 어렵게 하는 한편, 이렇게 만들어진 가짜 데이터가 학습되어 사회적인 문제로 비화할 우려도 있다. 공격 방식도 다양해져서 공급망 공격이나 파일리스, LotL과 같은 새로운 위협이 속속 등장하고 있다.

이에 대응하여 보안의 개념도 변화했다. 과거의 보안은 보호해야 할 시스템의 분명한 경계를 설정하고 경계를 넘어서는 데이터만 관리하는, 마치 담장을 따라 초소를 세워두는 것과 같은 ‘경계 보안’의 원칙을 따랐다. 대부분의 작업이 클라이언트에서 처리되고 서버는 데이터를 저장하는 역할에 그치던 시절에는 경계 보안도 문제없이 작동했다. 그러나 수많은 기기가 수시로 데이터를 주고받으며 내부 데이터와 외부 데이터의 구분이 무색해지면서, 보안의 개념도 시스템 내외부와 관계없이 모든 활동을 검토하는 ‘제로 트러스트 보안’으로 변화하고 있다.

제로 트러스트 보안은 필연적으로 관리 부담을 증가시킨다. 따라서 조직 내 보안 이벤트를 중앙집중형으로 수집, 관리하던 방식에 한계가 나타나고 있다. 조직의 모든 활동에서 보안을 고려해야 하다 보니 보안 전담 인력이 부족해졌으며, 제어해야 할 이벤트가 늘어나면서 개별적인 솔루션의 종류는 늘어났지만 이를 유기적으로 통합하는 솔루션은 제대로 갖춰지지 않았다. 더 큰 문제는 대용량의 데이터를 실시간으로 처리해야 할 필요성이 커지면서 보안 체계에 주어지는 시간은 점점 줄어든다는 점이다. 작년 미국에서 열린 RSAC 2023에서 “보안의 미래가 ‘AI를 활용한 자동화’에 있다”는 이야기도 이러한 맥락에서 나왔다.

이에 따라 빠르게 증가하는 보안 위협에 대해 신속하게 대응하는 데 필요한 전략과 기술이 절실

하다. 양자기술을 응용하여 전송 중인 데이터의 기밀성을 크게 높이는 한편 동형암호, 연합학습, 합성데이터와 같은 기술을 응용하여 곳곳에서 생성되는 데이터를 익명화하는 방법을 모색해야 한다. 한편으로는 지능화되는 공격에 대응하여 수많은 공격 시도의 패턴을 분석하고 대응방안을 제시하고 잠재적인 위협을 예측하는 AI 분석기술과 디지털트윈 기술도 필요하다. 무엇보다도 수많은 보안 관련 솔루션과 서비스를 유기적으로 연계하여 통합 운영하는 전략이 마련되어야 한다.

이러한 환경 변화에 따라 보안 시장은 솔루션 중심에서 '서비스형 보안(SECaaS)' 중심으로 이행하고 있다. 보안 환경이 복잡해질수록 더 많은 솔루션, 더 높은 수준의 보안 인력, 더 고도화된 통합 분석과 관제가 필요하다. 그러나 전문화된 보안은 자금과 인력에 여유가 있는 대규모 조직에게도 결코 만만치 않은 숙제다. SECaaS는 보안 솔루션과 관리 전반을 아웃소싱하여 정기적인 구독형 서비스로 제공하는 방식이다. 조직의 성격과 규모, 가용 자원과 예산에 따라 맞춤형으로 운영할 수 있고 점차 늘어나는 클라우드 서비스와 수직적인 통합이 가능하다는 장점이 있다.

시장 조사 전문기관인 AMR (Allied Market Research)에 따르면 2022년 전 세계 SECaaS 시장은 130억 달러 규모에 달했으며, 연평균 19.4%씩 성장해 2032년에는 750억 달러에 달할 것으로 예상된다. 보안 시장 전체를 두고 보면 여전히 솔루션 부문의 비중이 더 크겠지만 서비스 부문이 가장 빠르게 성장하리라는 전망이다. 특히 보안 부문에서 선두를 달리는 시장인 북미와 급성장하는 시장인 아시아태평양이 서비스 중심으로 재편되고 있다는 점이 주목할만하다.

물론 보안 시장이 '서비스'라는 새로운 형태로 이행하기가 쉽지는 않다. SECaaS는 개념상 기존 IT인프라에 원활하게 통합되어야 한다. 그러나 보안 환경이 복잡해지고 조직마다 네트워크 환경이 다른 만큼 호환성 문제를 겪거나 예상치 못한 취약점이 나타나는 일이 종종 있다. 오라클, 마이크로소프트, 시스코시스템즈와 같은 업무용 솔루션을 제공하는 기업들이 서비스형 보안 시장에서 우위를 점하는 이유기도 하다.

이번 TTA 저널에서는 보안 환경의 변화에 발맞춰 제로 트러스트 패러다임에서 보안을 서비스로 제공하려면 어떠한 사항을 고려해야 하는지 여러 전문가의 눈을 통해 살펴보고자 한다. 이번 기획이 미래의 보안 위협에 대응하여 우리는 무엇을 준비해야 하는지, 안전한 보안 환경을 구축하기 위해 어떤 기술과 제도가 필요한지 둘러보는 계기가 되기를 기대한다. TTA