제로 트러스트, 그 누구도 믿지 마라

권오현 계간 스켑틱 편집자

정보통신(IT) 기술이 우리 사회와 삶을 지배하는 오늘날, 사이버 보안은 개인의 안전을 넘어 기업과 국가의 존립을 좌지우지하는 근본 과제가 되었다. 2021년 5월, 랜섬웨어 공격으로 인하여 송유관 가동을 중단하는 초유의 사태를 맞은 미국 최대 송유관 업체 '콜로니얼 파이프 라인' 사례가 대표적이다. 이 회사는 범죄 단체에 거액의 돈을 지불할 수밖에 없었다.

코로나19로 인한 비대면 문화의 확산, 클라우드 기술에 따른 원격 접속, 인공지능을 이용한 데이터 활용의 확대는 앞으로 사이버 보안 문제가 더욱 중요해질 것임을 시사한다. 이런 상황에 대한 인식을 통해 최근 대두되고 있는 사이버 보안 정책이 바로 '제로 트러스트(Zero Trust)'다.

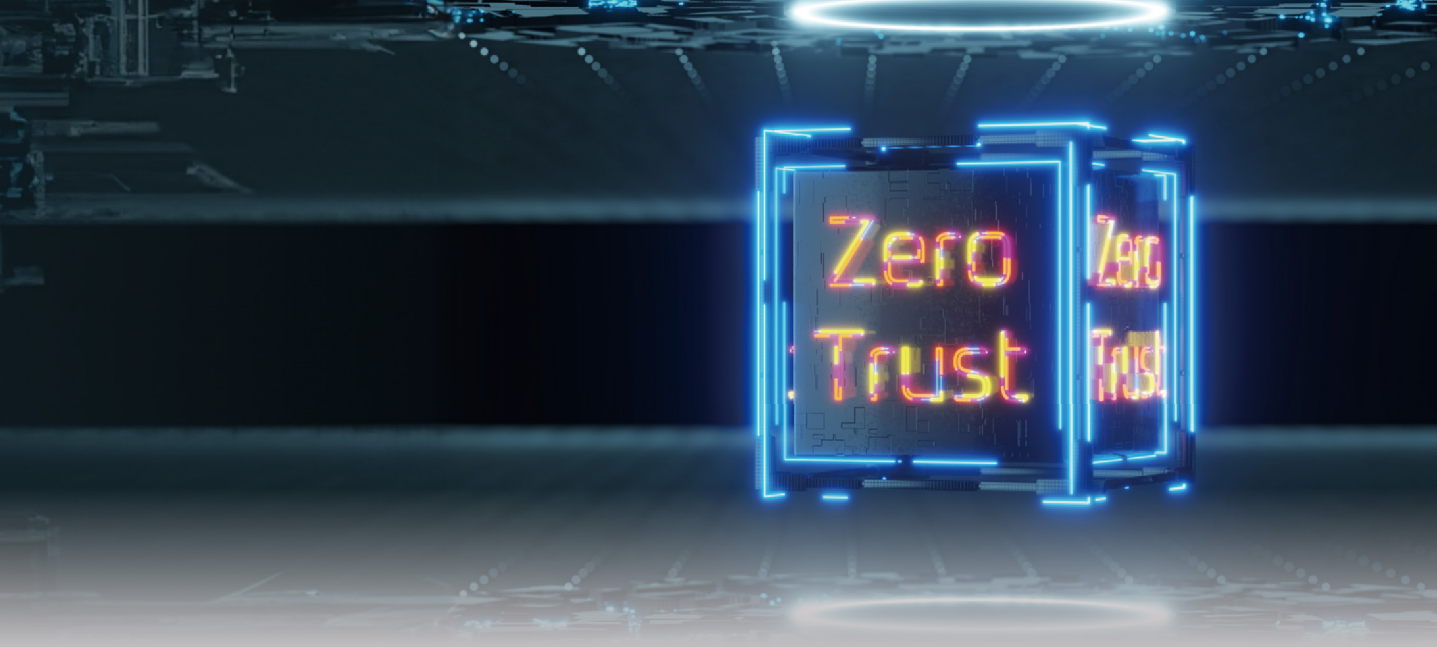
제로 트러스트란 무엇인가

제로 트러스트는 글자 그대로 '아무것도 신뢰하지 않는다'를 사이버 보안 정책의 기조로 삼는 것을 말한다. 이는 사이버 보안의 취약점이 기술 수준이 떨어져서 생기는 것이 아니라, 보안 정책이 허술하고 내부자를 무비판적으로 신뢰하는 데서 발생한다는 인식에서 촉발됐다. 기본적으로 사용자가 시스템이나 데이터에 접근을 요청할 때 철저히 검증하고 검증을 통과했다고 해도 최소한의 신뢰만 부여하는 것을 말한다. 이 용어는 2010년 사이버 보안 전문가 존 킨더버그(John Kindervag)가 제시했는데, 그는 보안 취약점은 신뢰에 있다고 주장했다.

기존의 사이버 보안은 방화벽 개념으로 보안을 구축한다. 특정 사용자나 기기가 어떤 IT 시스템에 접근을 요청할 때 보안 절차를 요구하고 이를 통과하면 해당 사용자나 기기를 신뢰하여 시스템 전체를 자유롭게 열람할 수 있도록 한다. 이런 방식을 '경계 보안 모델'이라 한다. 아이디와 패스워드를 올바로 적으면 접속을 가능하게 해주는 시스템이 대표적인 예다.

이러한 경계 보안 모델은 허락받지 않은 외부인의 접근을 막는 데 치중되어 있다. 만약 부적절한 외부 접근을 한 번이라도 허용하게 된다면 시스템 전체가 위험해질 수 있다. 누군가 불순한 목적으로 방화벽을 우회하는 방법을 개발하거나 발견한다면 이는 그대로 보안 취약점이 되며, 이 취약점을 해결할 때까지 허용되지 않는 사용자나 기기가 들어올 가능성은 사라지지 않는다.

제로 트러스트는 바로 이러한 난점을 타개하기 위한 시스템이다. 그렇기에 방화벽 시스템을 통과해서 시스템에 접속한 사용자나 기기라도 전적으로 신뢰하지 않는다. IT 시스템에 접근한 이후에도



각각의 하위 시스템에 들어갈 때마다 처음에 했던 검증을 다시 반복해야 한다. 시스템 내에 있는 데이터를 열람할 때도 다시 인증을 수행해야 한다.

이러한 제로 트러스트의 특징은 '미세 분할'이라는 단어로 표현할 수 있다. 즉 시스템 전체를 한꺼번에 지켜야 할 하나의 큰 덩어리로 보지 않고 모든 부분을 세분화하여 각 요소에 대하여 독립적으로 보안을 시행하는 것이다.

이를 잘 보여주는 예시로 제로 트러스트의 신원 인증이 있다. 제로 트러스트는 기존 방화벽 시스템에서 사용하는 아이디와 패스워드 기반 인증을 비롯하여 OTP나 보안키를 활용한 인증, 지문이나 홍채, 얼굴 인식 등 생체 기반 인증 등을 복합적으로 사용한다. 사용자에 대한 철저한 신원 인증이 가능한 이런 복합적 신원 인증 방법을 멀티 팩터 인증(MFA, Multi-Factor Authentication)이라고 한다. 사용자가 소유한 기기 역시 기존에 등록했다고 하더라도 이 기기에 정부나 기업에서 요구한 보안 애플리케이션이나 안티바이러스 솔루션이 설치되어 있는지, 기기 자체의 보안 수준이 높은지를 또 한 번 검증한다.

제로 트러스트는 이미 현실이다

마이크로소프트(MS)는 자사 보안에 제로 트러스트를 도입했다. MS 액티브 디렉터리(Azure Active Directory)는 아이디를 기반으로 사용자 인증을 진행하고, 싱글사인온을 통해 기업 아이디로 클라우드 접속을 진행하며 이와 동시에 보안키, 지문, 얼굴 등을 인증하는 MFA 구조로 되어 있다. 또한 모든 접근 요청은 보안을 위반하며 내외부 접근 구분 없이 개방형 네트워크에서 발생했다고 가정한 채로, 즉 전혀 신뢰하지 않는 채로 반복해서 확인한다. 네트워크 트래픽 일체를 검사하고 기록하는 것은 물론이다.

제로 트러스트는 기존 사이버 보안 방식처럼 단순히 데이터를 보호하는 데서 그치는 것이 아니라 사용자, 디지털기기, 시스템, 네트워크까지 개념을 확장하여 보호하고 보안 위협 분석과 통합 기능까지 포함하는 전사적인 개념이다. 따라서 기존 기술을 활용하여 장기적인 계획을 수립하고 시행에 나서는 개념 전환이 필요하다.

현재 우리나라도 최근 발표한 「디지털플랫폼정부 실현계획」에서 새로운 디지털 환경에서의 사이버 보안을 위하여 국가적 차원의 제로 트러스트 도입을 추진하겠다고 선언하며, 「제로트러스트 가이드라인 1.0」을 발표했다. 급변하는 IT 환경에서 '누구도 믿지 마라'라는 선언이 보안의 새로운 패러다임이 되었다.