사이버 보안이 실제 보안에 중요한 이유

Axis는 실생활에서 실제 보안에 도움을 주는 유용한 제품을 만드는 것으로 이미 잘 알려져 있는데, 왜 사이버 보안에 대한 이야기를 하려 할까요? 할리우드 영화의 세상에서 살펴봐야 할 한 가지는 세계를 구하고/미녀를 반하게 만들고/전리품을 챙겨 달아나기 위해 스파이나 비밀 요원, 카지노 절도를 계획 중인 도둑과 심지어 수퍼히어로까지 보안 카메라, 스마트 도어, 생체 인식 키패드 및 불빛이 번쩍이는 다양한 키트를 사용하거나 남용하고 있다는 것입니다.

하지만 그런 영화 속에서 사용자 인터페이스가 아무리 비현실적으로 억지스럽고(영화에서 M16나 CIA가 사용하는 그런 컴퓨터를 저도 '정말' 갖고 싶네요), 필요한 기술이 과도하게 단순화되어 있을 수 있다 해도("펜타곤을 해킹하려면 이 버튼을 누르세요"처럼 말이죠), 그 속에는 상당한 진실이 있습니다.

사이버 보안은 실제 보안에 중요합니다.

이 포스트와 이어지는 몇 개의 포스트에서, 21세기에 사이버 보안이 실제 보안에 중요한 이유와 상황에 맞는 사이버 보안의 기본 매개변수는 무엇인지, 그리고 비즈니스나 조직을 위해 실제 보안 시스템을 계획할 때 알아두어야 할 일반적인 사이버 보안의 개념에 대해 알아보려고 합니다.

알아두어야 할 가장 중요한 것은 **사이버 보안은** 제품이 아닌, **과정이라는 것**입니다. 시스템 수준, 네트워크와 장치를 보호할 책임, 전체 벤더 공급 체인에서 지원하는 서비스를 통해서뿐만 아니라, 네트워크 관리자와 사용자 자신이 위협을 관리해야 합니다. 기술이 중요한 역할을 하지만, 모든 위험과 위협을 제거하지는 못합니다.

단순하게 얘기하면 사이버 보안은 위험 관리에 관한 것이며, 모든 위험을 제거하는 것은 불가능합니다.

[여담으로 간단한 심리 실험을 할 수 있습니다. 오늘 아침에 일어났을 때부터 발생 가능성이 있는 '모든' 위험을 나열해 보십시오. 개에 걸려 넘어지거나 샤워 중에 화상을 입는 것뿐만 아니라 운석이나 갑작스런 개구리 홍수가 일어난다면 어떨까요? 어떤 위험은 전혀 예상할 수 없을뿐더러 모든 위험에 대처하는 계획을 세우는 일은 불가능에 가깝습니다.]

더구나 어떤 위험으로부터 보호하려면 엄청난 비용이 필요하기 때문에 [몇 달러로 당신의 집에 운석 충돌 방지 기능을 갖출 수 있을까요?] 무엇이 자신과 조직에게 중요한지에 대해 생각하면서 시작할 필요가 있습니다. 왕관에 박힌 보석의 개수를 파악하고 철저하게 감시하고 지켜야 합니다(실제로 런던 타워에서 근무하지 않을 테니 그냥 비유로 하는 말입니다). 어떤 위험이 허용 가능 수준인지 확인하고, 일부 위험의 영향을 완화할 방법을 찾아 내며, 다른 위험을 예방 형태로 전환해야 합니다.

다음 포스트에서는 실제 보안 시스템의 위험을 분석할 수 있는 방법과, 어떤 완화 노력이 실제로 효과가 있는지, 다양한 공격 유형 및 서로 다른 규모의 조직이 위험에 맞서 무엇을 할 수 있는지를 살펴 보겠습니다.