# EQST insight

## 최신 ICT 기술에 따라 확대되는 공격 표면 관리의 중요성 및 대응 방안

공격 표면 관리 (Attack Surface Management, 이하 ASM)는 인터넷을 통해 공격의 경로가 될 수 있는 기업의 모든 디지털 자산을 관리하는 것을 의미한다.

공격 표면은 의외로 범위가 넓다. 기업의 내부 자산 뿐만 아니라 소프트웨어 공급망, 그리고 협력업체의 인력에서부터 기업의 브랜드와 평판 등의 Digital Risk까지도 공격 표면에 포함될 수 있다. 그 중에서 이번 헤드라인에서의 공격 표면 관리는 인터넷에 연결된 자산을 위주로 설명한다.

공격 표면 관리의 중요성을 설명하기 전에 조금 다른 이야기로 풀어 나가고자 한다. 영화 스타워즈 세계관에서 연력(年歷)의 기준이 되는 야빈 전투 (Battle of Yavin)를 다룬 에피소드 IV – 새로운 희망 (A New Hope)을 보신 분들은 기억하시겠지만 반란군 연합의 루크 스카이워커가 탑승한 X윙 스타파이터 1대에 의해 제국의 거대한 전략 자산인 '죽음의 별 (Death Star)'이 파괴된다.

반란군 연합은 루크의 쌍둥이인 레아 공주가 어렵게 입수한 '죽음의 별' 설계도를 분석하여 치명적인 취약점(원자로)을 찾아내고, 고작 몇 대의 전투기로 이루어진 편대가 양자 어뢰 공격을 감행해 '죽음의 별'을 우주의 먼지로 사라지게 만든다.


지난해 말 인터넷 역사상 최악의 취약점이라 불리는 'Log4j' 취약점이 발견돼 온 사회가 떠들썩했다. 실제 공격으로 인한 피해 사례가 밝혀지지 않았지만 그 여파는 상당했다. 'Log4j' 취약점은 원격코드 실행 취약점으로 인가받지 않은 사용자가 원격으로 접속해 악성코드를 실행할 수 있어 위험도가 매우 크다. 해커는 이 취약점을 악용해 원격으로 목표 대상의 모든 권한을 탈취하는 것이 가능하며 서버를 통해 내부망에 접근해 데이터를 약탈하는 등 기업의 전체 네트워크까지 장악할 수 있다. 이렇게 기업에 매우 심각한 문제를 야기할 수 있는 취약점이었으나, 대부분 빠르게 대응하지 못했다. 여기엔 몇 가지 이유가 있다.


① 취약점을 가진 Log4j가 사용된 애플리케이션을 식별하는 데 많은 시간을 소모했다. 취약점 분석 소프트웨어 전문 업체인 Qualys에 의하면 완전한 패치까지 평균 17일이 소요된 것으로 보고된 바 있다.


② 취약점을 가진 Log4j 가 사용된 애플케이션이 공격을 받을 경우 발생할 수 있는 비즈니스 영향에 대해 평가가 이루어지지 않아 어떤 순위로 대응해야 하는지 알 수 없었다. 발견된 애플리케이션 중 50%가 수명을 다한 (End of Life) 상태였던 것도 매우 흥미로운 일이었다.

보안 컨설팅에서도 기업이 보유하고 있는 디지털 자산의 식별은 매우 기초적인 위험평가의 관리 방안으로 소개되고 있으나, 실제 현실 세계에서는 동작하지 않은 것이다.

Enterprise Strategy Group (ESG Research)에서 보고한 바에 의하면 공격 표면을 적극적으로 모니터링한다고 믿는 기업은 9%에 불과했다.

그만큼 공격 표면 관리에 어려움이 있다는 이야기도 될 수 있다. 불행하게도 Cloud, IoT 등의 발달로 인해 우리가 상상할 수 없을 만큼 공격 표면은 확대되고 있고, 특히 Cloud 환경은 더욱 복잡하다. On-Premise 와 Cloud 를 동시에 사용하며, 하나 이상의 CSP (Cloud Service Provider)에 의존하는 소위 Multi-Cloud 가 확산되고 있기 때문이다. 또한 Cloud 시대에 기업은 수많은 워크로드로 이루어진 웹사이트뿐만 아니라, 네이티브 애플리케이션, 개인정보와 같이 민감한 데이터, 자격증명, SSL 인증서 등 인터넷에 연결된 자산을 보유하고 있다.

공격자는 자동화된 툴을 사용해 빠르게 기업 전반의 공격 표면을 분석해 취약점을 식별하고 공격을 감행한다. 이러한 공격은 대부분 성공적이며, 공격의 결과로 약 80% 이상이 주요 데이터의 유출이라는 최악의 상황을 야기한다.


이러한 추세에 대응하기 위해 이미 글로벌 업체는 ASM(Attack Surface Management) 전문 업체 인수를 진행하고 있다. 지난 6월 RSA Conference 2022에서 IBM은 Randori의 인수를 공표했으며, 이외에도 Microsoft (RiskIQ), Mandiant (Intrigue), Palo Alto Networks (Expanse Networks) 등이 이미 ASM 전문 업체를 인수했다.

특히 IBM이 인수한 Randori의 경우 ASM 기능 외에 CART(Continuous Automated Red Teaming)를 선보이며, 기업의 보안 역량을 강화할 수 있도록 지원하는 공세적인 보안 기술을 강조하고 있다.

최근 코로나 팬데믹으로 인한 원격근무, Cloud 도입의 확산 등 지속되는 디지털 트랜스포메이션에 맞춰 보안업체에서도 혁신의 움직임을 보이고 있는 것이다.

ASM의 주요 기능은 ① 자산의 검색과 식별, ② 자산의 분류를 통한 우선순위 지정 (공격 가능성에 따른 비즈니스 영향도 평가 등) ③ 적극적인 대응 (Remediation) ④ 지속적인 모니터링이다.

위의 주요한 4가지 기능을 지속적으로 관리할 수 있도록 많은 부분의 자동화를 지원하며, 최근 Vendor와 Technology의 통합(Consolidation) 추세에 맞춰 하나의 플랫폼으로 제공된다는 점이 주목할 만하다.

이미 기업은 보안을 위해 많은 투자를 진행하고 있으며 평균 40~80개의 벤더와 협력하고 있다. 그러나 너무 많은 벤더를 관리하는 툴로 인한 내부 인력 교육, Network, Endpoint 등 영역별 Silo, 비효율적인 예산 집행 등의 문제로 계속해서 벤더와 벤더가 제공하는 기술의 통합을 원하고 있고, 글로벌 기업은 이미 CISO뿐만 아니라 구매 단계에서 Consolidation을 진행하고 있다.

한편, 최근 공격 기법은 계속해서 진화하고 있으며 기업의 다양한 공격 표면을 활용해 랜섬웨어와 같이 기업에 실질적인 피해를 유발하고 있다.

따라서 Cloud 도입과 전환으로 계속해서 확장되고 있는 공격 표면에 대한 관리가 절대적으로 필요한 상황이며, SK쉴더스도 글로벌 업체와의 긴밀한 협력을 통해 국내 환경에 부합하는 새로운 보안 서비스를 준비 중에 있다.

SK쉴더스는 AI, Big Data, 클라우드 등 New ICT 확산으로 복잡해지는 보안환경과 지능화되는 보안 위협에 신속히 대응할 수 있도록 사이버보안 및 기술을 지속적인 연구, 개발하고 내재화를 통해 경쟁력을 높이고 있다. 국내 사이버보안 1위 역량을 바탕으로 보안 컨설팅, 모의해킹, 침해 사고 분석 역량과 경험이 반영된 SK쉴더스에 차별화된 서비스를 제공해 고객의 보안 투자를 보호하고, 대응의 단계를 향상시키는데 기여할 수 있는 기회가 되길 희망한다.