클라우드 컴퓨팅 보안의 취약성과 대응 방안

지도교수 : 김 윤
연 구 자 : 정 지 원

< 목 차 >

요 약

클라우드 컴퓨팅은 온프레미스 방식의 단점을 보완하여 나온 기술이다. 하지만 보안으로 많이 이슈가 되었고 이러한 보안 위협 사례를 파악하고 사례에 따른 대응 방안을 파악하였다. 이 전에 클라우드 컴퓨팅 기술에 대한 개념 및 특징을 연구하였다.

주요어: 클라우드, IT 리소스, 온프레미스, 코로나 19, 원격 근무

1. 서론

1.1 클라우드 컴퓨팅 등장 배경

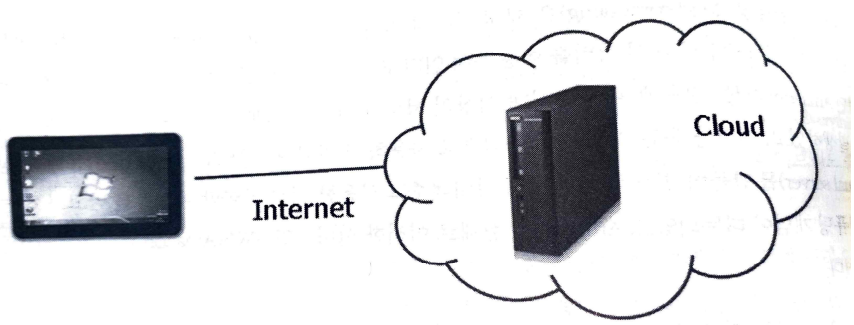
1990년대 중반부터 등장하기 시작한 다양한 검색엔진(야후!, 구글), 이메일 서비스(핫메일, 지메일), 개방형 게시 서비스(마이스페이스, 페이스북, 유튜브) 등 갖가지 소셜미디어(트위터, 링크드인)에 의해 대중들은 인터넷 기반의 컴퓨터 유틸리티의 영향을 받아왔다. 소비자 중심 서비스임에도 불구하고, 이런 서비스들로 인해 현대 클라우드 컴퓨팅의 기초를 형성하는 기본 개념이 널리 알려지고, 세상에 영향을 미치기 시작했다.

세계 최대의 인터넷 서점인 Amazon에서 시작되었다. 여러 개의 데이터 센터에서 수십만 대의 서버를 이용하여 인터넷을 통한 서적 전자상거래를 통해 이 분야를 선도하던 Amazon에서는 때에 따라 수천 대 이상의 서버가 별다른 트래픽 없이 유휴 상태가 되는 상황들이 발생하였고, 이러한 유휴 자원을 효율적으로 사용하기 위해 이러한 IT 자원들을 이용해 가상 서버(Virtual Server)를 만들어 필요한 고객에게 임대하고 사용한 시간만큼만 이용료를 받고자 하는 새로운 컴퓨팅 개념이 대두되었고 Amazon은 실제로 이러한 서비스인 AWS(Amazon Web Service)를 상용화하였다.

또한, IT 기업에서 클라우드 컴퓨팅 기술이 나오기 전까지 서비스 자동화를 위해 인프라 구축에 사용했던 방식이 있다. 일반적으로 컴퓨팅 서비스를 제공하는 기업의 경우 서비스에 필요한 IT 리소스는 데이터 센터에 구축하여 조직 내부에 위치하는 것으로 간주한다. 이렇게 기업이 IT 시스템 운용에 요구되는 데이터 센터에 다수의 H/W 및 S/W 설비를 자체적으로 보유하고 운용하는 방식을 온프레미스 시스템이라고 한다. 이는 하드웨어를 보유한 것을 의미하며, 클라우드의 반의어로 통용된다. 온프레미스 방식은 이점도 많지만 시기에 따라 온프레미스 방식은 큰 비용이 요구되기도 한다. 따라서 클라우드 방식이 발전되기 시작되었다.

1.2 클라우드 컴퓨팅 개념

클라우드 컴퓨팅을 간결하게 정의하면 클라우드 컴퓨팅은 원격지에서 제공하는 확장성이 있는 자원의 사용 모델을 도입한 분산 컴퓨팅의 특수한 형태 또는 IT 자원의 렌탈샵이라고 할 수 있다.



[사진 1] 클라우드 컴퓨팅 개념 : 인터넷 안의 내 컴퓨터

클라우드 컴퓨팅은 사용 유형에 따라 다양하게 정의될 수 있지만, 일반적으로 개인의 PC가 아닌 인터넷상에 존재하는 클라우드 사업자 또는 클라우드 제공자에 의해 서비스가 제공되는 컴퓨팅 기술을 뜻한다.

클라우드는 확장 가능하고 측정된 IT 리소스를 원격으로 프로비저닝(provisioning)하기 위해 설계된 IT 환경이라고 할 수 있으며, 사용자는 IT의 모든 개념을 네트워크를 통해 원격으로 접속하여 이용할 수 있다.

1.2.1 클라우드의 필요성

메인프레임 기반 컴퓨팅에서 클라이언트/서버 기반 컴퓨팅으로 이동한 것에 이은 패러다임 시프트(paradigm shift)이자 새로운 산업혁명으로 단말의 경량화 추세(스마트폰, 태플릿 PC, 클라우드 디스플레이, 제로 클라이언트 등)에 따라 본격적으로 확산이 되고 있다.

클라우드 컴퓨팅은 대세이며 전 산업에 대한 파급 효과도 클 것으로 예상이 되고 서비스 모델도 다양할 것으로 예상이 된다. 스마트 자동차, 스마트 팩토리, 클라우드 로보틱스, 웨어러블 기기, IoT 기기, 빅 데이터 처리 등은 모두 클라우드를 통한 연동이 필요한 기술들이며, 알파고와 같은 인공지능도 클라우드를 기반으로 컴퓨팅 파워가 제공되고 있다. 또한, 메인 프레임급 이상의 컴퓨팅 파워를 필요로 하였던 핵심 컴퓨팅 분야까지도 클라우드 기반으로 변화가 이루어지고 있다.

또한, 사용자별로 필요성으로는 공공기관에서는 자체적으로 IT 시스템을 관리하게 되면 필요 이상으로 시스템이 구축되는 일이 발생하는가 하면 갑자기 트래픽이 몰리게 되면 사이트가 다운되는 등의 상황이 자주 발생하고, 트래픽이 몰릴 경우 해당 공공기관의 사이트가 다운되는 경우가 많아 이러한 점을 보면 클라우드가 필요하다는 것을 알 수 있다.

금융기관에서는 2011년 NH농협의 전산 사고로 인해 무려 3일간 은행 업무가 마비된 적이 있다. 이를 완전히 복구하는 데만 한 달이 걸렸는데 그동안 도입하지 못했던 이유는 보안 때문이었다. 하지만, 클라우드 기술 중에서도 크게 2가지 때문이었다. 첫째는 폭발적으로 늘어난 고객 데이터를 취합하고 용이하게 활용하기 위해서다. 둘째는 개발 단계에서 자원의 효율을 높이고 신속하게 사업을 추진할 수 있는 유연성, 새로운 신기술을 자유롭게 도입하는 확장성 때문이다.

대기업은 시장조사기관 IDC에 따르면 기업의 서비스에서 클라우드 도입률이 50% 넘는 기업이 그렇지 않은 기업에 비해 매출 성장이 2배 빠르고 총매출은 평균 1.5배 더 높다는 발표 결과를 통해 그 이유를 확인할 수 있다. 국내 주요 대기업들은 이미 클라우드 전환을 진행하고 있는 클라우드 전환은 필수적인 과정으로 보인다.

급성장하는 일반기업 역시 클라우드의 전환이 필수이다. 특히 클라우드 네이티브인 IT 스타트업에서 클라우드의 중요성을 확인할 수 있다.

1.2.2 클라우드의 장단점

클라우드의 장점으로는 첫 번째 IT 자원의 설치 공간 및 물리적 확보에 필요한 고정 비용이 IT 자원의 임대료 지급 방식으로 변경이 되므로 초기 투자 부담을 대폭 경감 할 수 있다. 두 번째로는 전력비용 감소도 있다. 서버의 통합과 가상화 기법 등의 적용을 통해 에너지 비용을 크게 절감할 수 있다. 이는 환경 관련 문제로 연결되어 지구 온난화 문제 해결에도 기여할 수 있다. 또한, IT 자원의 풀의 제공을 통해 클라우드는 동적으로 IT 자원

을 즉시 할당할 수 있다. 이러한 기능을 통해 처리 트래픽의 변동과 피크 수요에 자동으로 또는 수동으로 유연하게 대응할 수 있다. 가용성과 신뢰성은 사업 이익과 직접 관련이 되어 사용량이 많을수록 런타임 고장이 발생할 경우는 좀 더 영향이 심각하게 된다. 그러므로 클라우드 기반의 서비스와 IT 자원 계약 시 클라우드 제공자가 제안하는 SLA를 주의 깊게 살펴볼 필요가 있다. 다수의 클라우드 환경은 높은 가용성과 신뢰성을 제공할 수 있는 능력이 있지만, SLA에 표현된 정도가 의무적으로 보장된다는 것에 유의해야 한다.

사용자의 컴퓨터, 소프트웨어, 데이터 등이 클라우드에 존재할 경우 언제 어디서나 접속해서 사용할 수 있으므로 클라우드 사용자의 이동성은 좋아진다. 또한, 프라이빗 클라우드의 경우 전사적인 IT 자원과 데이터의 통제를 통해 보안을 강화할 수 있다. 이밖에 장점으로 신속한 구현, 일관적인 서비스, 효율의 향상, 인력 문제 해소가 있다.

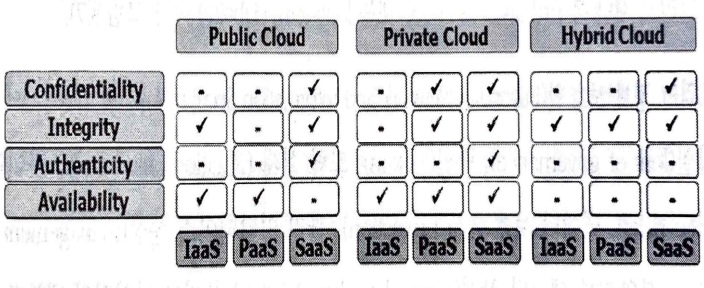
단점으로는 보안 취약성 증가가 있다. 클라우드 환경에서는 IT 리소스를 원격으로 사용하므로 기업의 신뢰 경계를 기업 내부에서 외부 클라우드의 데이터 센터까지 확대해야 한다. 이는 곧 보안 취약점(vulnerability)의 증가를 의미하며, 보안 아키텍처를 구축하는 것이 더욱 어려워진다는 것을 의미한다. 또한, 다른 조직의 데이터가 동일한 저장 공간에 놓일 수 있어 악의적인 사용자로부터 클라우드 IT 리소스 내의 데이터를 도용하고 손상시킬 수 있는 기회를 제공한다. 데이터의 안전 정도는 클라우드 소비자와 클라우드 제공자 모두에 의해 적용이 되는 보안 통제와 정책에 의해 제한이 된다.

또한, 제삼자 클라우드 제공자들은 데이터 센터를 저렴하고 편리한 지리적 위치에 구축하려 할 것이다. 클라우드 소비자들은 퍼블릭 클라우드 이용 시 대개 그들의 IT 자원과 데이터의 물리적 위치에 관심을 두지 않을 것이다. 일부 조직의 경우 이러한 상황은 데이터 개인정보 문제와 저장 정책을 명시하는 산업과 정부의 규제와 관련하여 심각한 법적 우려를 나을 수 있다. 이에 따라 다중 영역 준수 및 법적 이슈가 있을 수도 있다. 이밖에 단점으로 운영 거버넌스 제어 감소, 클라우드 제공자들 간의 이식성 제한, 과도한 비용 지출 등이 있다.

2. 클라우드 보안의 기초

2.1 클라우드 보안 요구 사항

퍼블릭, 프라이빗, 하이브리드라는 3가지 클라우드 모델이 있는데 이 전개 모델은 다시 IaaS, PaaS, SaaS라는 3가지 클라우드 서비스 모델로 세분되며, 각 모델의 CIAA 요구 정도를 다음 그림과 같이 설명한다.



[사진 2] 클라우드 전개 및 서비스 모델과 CIAA

체크 표시는 필수적인 요구 사항이며, 마이너스 표시는 선택적인 요구 조건을 의미한다. 사실, NIST에 따르면 커뮤니티 클라우드도 존재하는데, 커뮤니티 클라우드는 프라이빗 클라우드와 동일한 CIAA 요구 사항을 갖는 것으로 분석되었다. 그림을 보면 다음을 알 수 있다.

첫째, 무결성은 대부분의 클라우드 서비스에서 필수적으로 요구한다. 이는 무결성이 다른 요구 사항을 지원하기 위한 전제 조건이며, 결국 무결성이 보장되지 않으면 기밀성 등을 보장하기 어려움을 의미한다.

둘째, 전반적으로 SaaS는 좀 더 많은 보안 요구 사항이 필요로 한다. 예를 들어 퍼블릭 클라우드에서 SaaS는 기밀성, 무결성, 진정성을 필수 조건으로 요구하나, IaaS의 경우 무결성과 가용성을 필수 조건으로 요구한다.

셋째, 프라이빗 클라우드는 다른 클라우드 전개 모델보다 좀 더 많은 요구 사항을 필수적으로 요구한다.

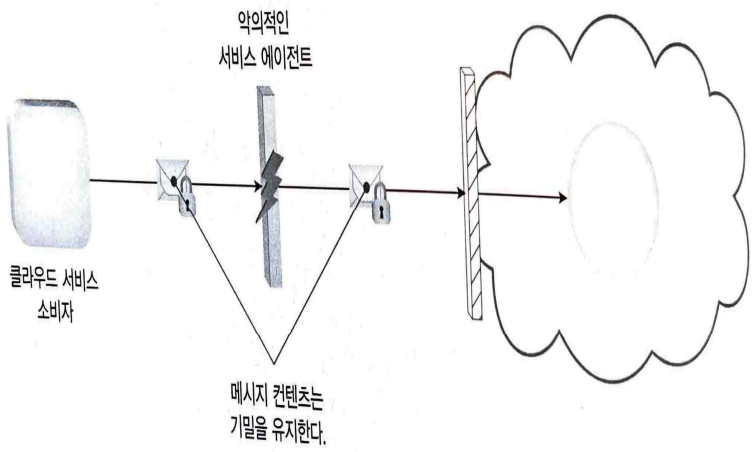
넷째, 보안책임 및 신뢰 공유가 요구된다. 신뢰는 공유 보안 모델의 목표를 유지하기 위해 클라우드 파트너를 선택하는 데 있어 가장 중요하다. 조직은 역할과 책임을 명확하게 이해하고 독립적인 타사 보안 감사 및 증명에 액세스할 수 있어야 한다.

마지막으로 기존의 엔터프라이즈 보안이 사람의 속도로 분석하고 대응하는 동안 클라우드 위협은 기계의 속도로 움직이고 있다. 클라우드 환경의 최신 보안은 위협 감지 및 대응을 자동화해야 한다. 지능형 위협에는 머신러닝을 통한 위협 예측, 예방, 탐지 및 대응에 새로운 수준의 정교함을 제공하는 보안 솔루션이 필요하다.

2.2 클라우드 보안 메커니즘

2.2.1 암호화

기본적으로 데이터는 평문으로 알려진 읽을 수 있는 형식으로 코드 된다. 네트워크를 통해 전송될 때, 평문은 공인되지 않고 잠재적으로 악의적인 접근에 취약하다. 암호화 메커니즘은 데이터의 기밀과 무결성을 보존하기 위한 전용의 디지털 코딩 시스템이다.



[사진 3] 클라우드 보안 메커니즘 중 암호화

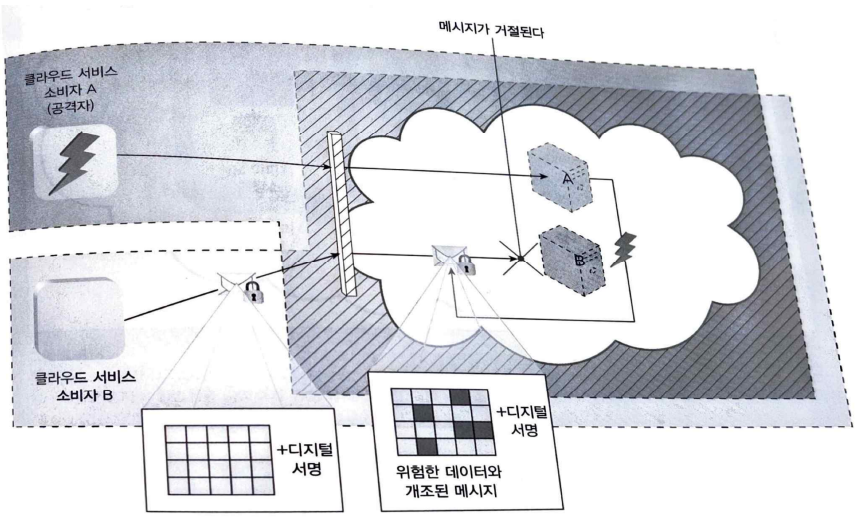
암호화는 대칭 암호화와 비대칭 암호화 두 가지 유형이 있다. 대칭 암호화는 하나의 공유된 키를 사용하는 공인된 부분에 의해 수행되는 암호화와 복호화 모두를 위해 같은 키를 사용한다. 또한, 보안키 암호 방식으로 알려진 특별한 키와 함께 암호화된 메시지는 같은 키에 의해서만 복호화 될 수 있다. 데이터를 정당하게 복호화 하는 부분은 본래의 암호화가 키를 정당하게 소유한 부분에 의해서 수행됐다는 증거와 함께 제공된다. 키를 가지는 유일하게 공인된 부분이 메시지를 생성할 수 있기에 기본 권한 확인은 항상 수행된다. 이것은 데이터 기밀을 유지하고 입증한다. 비대칭 암호화는 개인키와 공개키로 명명된 두 개의 다른 키의 사용에 의존한다. 비대칭 암호화(공개키)와 함께, 공개키는 일반적으로 사용할 수 있는 반면 개인 키는 소유자에게만 알려진다. 개인키와 암호화된 문서는 상응하는 공개키로만 정확하게 복호화 될 수 있다. 역으로 공개키와 암호화된 문서는 상대 개인키를 사용해서만 복호화 될 수 있다. 한 개 대신에 사용된 두 다른 키의 결과로, 비대칭 암호화는 대체로 항상 대칭 암호화보다 계산적으로 느리다.

2.2.2 해싱

해싱 메커니즘은 데이터 보호의 단방향, 비역전 형태가 요구될 때 사용된다. 일단 해싱이 메시지에 적용되면 잠기고, 키도 메시지가 잠금 해지하는 것을 제공하지 않는다. 이 메커니즘의 보통 애플리케이션은 비밀번호의 스토리지다.

2.2.3 디지털 서명

디지털 서명 메커니즘은 인증과 부인 방지를 통해 데이터 진위와 무결성의 제공 수단이다. 메시지는 메시지가 연속되는 공인되지 않은 수정을 경험하면 무효하게 만들어주는 전송에 앞선 디지털 서명을 할당한다. 디지털 서명은 받은 메시지가 정당한 전송자에 의해 생성된 것과 같다는 증거를 제공한다. 또한, 악의적인 중개자와 불충분한 권한, 중복된 신뢰 경계 보안 위협을 완화하는 것을 돕는다.



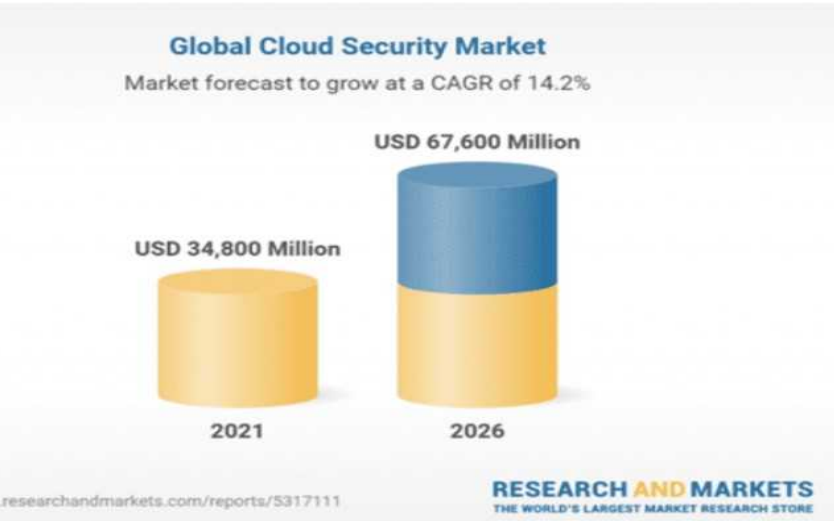
[사진 4] 디지털 서명 메커니즘

2.2.4 공개키 인프라

비대칭 키의 배포를 관리하기 위한 일반적인 접근은 공개키 암호 방식을 안전하게 사용하기 위해 대규모 시스템을 가능하게 하는 프로토콜과 데이터 형식, 규칙, 실행 시스템으로써 존재하는 공개키 인프라(PKI) 메커니즘에 기반을 둔다. 이 시스템은 키 유효성을 확인할 수 있게 하는 동안 상응하는 키 소유주와 공개키를 연관 짓기 위해 사용된다. PKI는 사용자 ID와 유효성 기간과 같은 연관된 정보를 증명하기 위해 공개키를 묶는 디지털 서명된 데이터 구조인 디지털 인증서의 사용에 의존한다. 디지털 인증서는 일반적으로 제삼자의 인증서 권한(CA, Certificate Authority)에 의해 디지털 서명된다.

2.3 기업에 따른 클라우드 보안

사이버 보안으로 국내에서 유명한 주요 3개 회사는 최근의 고성장 기조를 계속해서 이어나가고자 클라우드 보안으로 사업 영역을 확대, 강화하고 있다. 지난 2년간 코로나 19 상황에 따른 비대면 환경 전환으로 사이버 보안 수요가 증가하였다. 이 기업들은 사이버 보안 중 클라우드 보안에 비중을 두고 또한, 전체 사이버 보안 시장 중에서도 빠르게 성장이 기대되는 분야이다.



[사진 5] 클라우드 보안 시장 전망

2.3.1 Google

클라우드 회사 중 세계적으로 유명한 주요 3사 회사 중 하나인 구글은 구글 만의 엔지니어링과 글로벌 운영 역량을 기반으로 구축되었다. 강력한 빌트인 보안 도구로는 클라우드 데이터 손실 방지, 키(Key) 관리, 자산 인벤토리(Inventory), 암호화, 방화벽, 차폐 가상 머신(VM)이 있다. 구글 보안 커맨드 센터(Google Security Command Center)는 중앙 집중식 관리와 가시성을 제공한다. 이를 통해 고객들이 잘못된 구성 및 취약점을 발견하고 컴플라이언스를 모니터링하며 위협을 감지할 수 있도록 지원한다.

구글은 2014년 클라우드 모니터링 기술 업체 스택 드라이버(Stack driver) 인수를 바탕

으로 최고 수준의 모니터링 및 로그 분석을 제공한다. 현재는 구글 클라우드 오퍼레이션으로 확장 및 브랜드가 변경되었다.

구글 클라우드의 아쉬운 점은 보안 전문가가 적고 도구가 부족하고 보안 기능도 다양하지 않은 점이라는 것이다.

2.3.2 해커원(HackerOne)

해커원은 해커들이 시작한 일종의 해커 기반 보안 플랫폼이다. 글로벌 해커 커뮤니티를 통해 보안 이슈들을 찾아내는 것이 서비스의 핵심이다. 화이트 해커 서비스를 지공하며 동시에 보안 소프트웨어 개발 서비스, 컴플라이언스 이슈 대응 서비스 등도 함께 수행한다. 샌프란시스코에 본사를 두고, 런던, 뉴욕, 싱가포르, 네덜란드에서도 사무실을 운영하고 있다. 주요 활용 방안으로는 새로 클라우드 서비스를 도입하는 기업의 경우 기존의 컴플라이언스 이슈 대응, 알려지지 않은 보안 위협에 대한 사전 분석 등 클라우드 도입 시 우려되는 보안 이슈를 우선 풀어야 한다. 이럴 경우 해커원의 전문 서비스가 활용될 수 있다. 특히 SaaS로 넘어가는 경우 데이터 유출이나 안전성 등에 대한 사전 테스트로도 적합한 서비스이다. 주요 파트너로는 미 국방성, 유럽 위원회와 같은 공공기관, 구글 플레이, 스포티파이, 페이팔, 트위터와 같은 서비스 기업, 도요타, GM과 같은 제조사, HBO, 버라이즌, 스타벅스 등 다양한 분야의 고객 스펙트럼을 보유하고 있다.

2.4 클라우드 보안의 핵심 기술

클라우드 보안은 조직에 보안 요구 사항을 해결하고 조직이 규정 준수 요구 사항을 준수하도록 하는 접근 방식을 제공한다. 효과적인 클라우드 보안을 구축하려면 다음으로 구성된 클라우드 기술 스택 전체에 걸쳐 여러 계층의 방어가 필요하다.

구성 조건으로 첫째는 민감한 시스템 및 데이터에 대한 승인된 액세스를 차단하도록 설계된 예방적 제어가 있다. 둘째는 감사, 모니터링 및 보고를 통해 무단 시스템과 데이터 액세스 및 변경 사항을 도출하도록 설계된 감지 제어가 있다. 셋째로는 정기적이고 중요한 보안 업데이트를 방지, 감지 및 대응하도록 설계된 자동화된 제어가 있다. 마지막으로 보안 정책, 표준, 관행 및 절차를 처리하도록 설계된 관리 제어가 있다.

3. 클라우드 보안 취약성 및 대응 방안

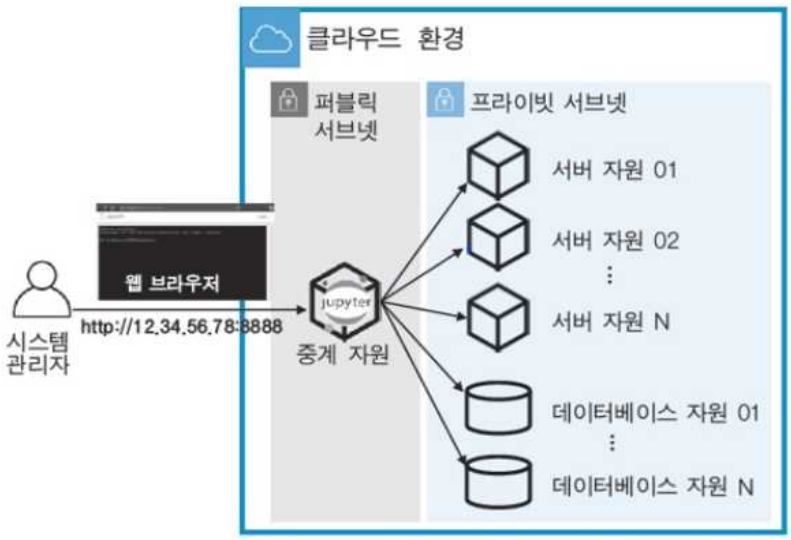
3.1 클라우드 보안 위협 사례

클라우드 서비스를 사용하는 환경에서 발생하는 보안 이슈는 크게 3가지 유형이 있다. 첫째는 클라우드 서비스를 운영하는 과정에 발생하는 이슈이다. 이 유형은 보통 인력과 조직의 변화로 발생하는 상황이다. 일반적으로 담당자의 업무가 변경되어 새로 배정되면, 할당받은 IP 주소를 방화벽에 등록하고 권한을 신청하는 일련의 프로세스 과정을 거치게 된다. 반면, 이전 담당자는 다른 업무로 이동하기 때문에 사용하던 방화벽 등록과 사용 권한을 반납, 회수하지 않고 바로 이동하는 경우 이전 업무의 서버나 시스템에 접근 할 수 있고 임의적으로 접근할 수 있게 되어 보안 문제가 발생한다.

둘째는 클라우드 서비스의 현황을 관리하는 과정에 발생하는 이슈다. 클라우드 서비스의 신청과 해지 프로세스가 미흡한 환경에서 발생하는 문제점이다. 보통 테스트나 임시용으로

활용한 클라우드 서비스는 어느 순간 사용하지 않는 시점에서 무관심의 대상이 된다. 이는 권한이 오픈된 채로 그대로 방치될 가능성이 높다.

마지막으로는 클라우드 구성에 존재하는 취약점으로 인한 이슈이다. 이 보안 이슈로는 스스로 인지하기 어렵다는 특징이 있다. 요즘은 각자 취향에 맞는 방식으로 클라우드 서비스를 활용하고 있는 시대이다. 대표적인 사례로 문제점을 파악하면, 최근 데이터 분석에 활용하려고 파이썬(Python) 언어 기반의 주피터(jupyter notebook) 소프트웨어를 설치하여 활용하는 경우가 있다. 해당 소프트웨어는 서버를 접속할 수 있는 터미널(terminal) 기능도 제공하기 때문에 주의가 필요하다. 문제의 시작은 퍼블릭 서브넷(subnet)에 있는 중계 서버(bastion-host)에는 데이터 분석 목적으로 주피터 노트북 소프트웨어를 설치하고, 악의적 사용자는 원격으로 주피터 노트북을 접속하기 위해 중계 서버에 할당된 공인 IP 주소로 접속한다. 단순히 데이터 분석을 수행한다면 문제가 없겠지만, 주피터 노트북에는 서버에 접속하는 통로가 있기에 사실상 프라이빗 서브넷(private subnet)에 있는 모든 자원을 마음대로 접근할 수 있게 된다. 보안 관점에서 매우 취약한 상태가 된다.



[사진 6] 주피터 노트북을 통한 클라우드 접속 취약점

3.2 대응 방안

첫 번째 보안 이슈에 대한 해결방안으로는 IP 기반이 아닌, 사용자 중심의 ID 기반으로 시스템과 보안의 통합된 처리가 가능한 계정관리 시스템과 솔루션을 활용하는 것이다. 업무가 변경될 때마다 업무를 따라가는 것이 아닌, 사람이 주체가 되는 체계로 권한 처리가 이루어지는 방식으로 이는 클라우드 환경이 아닌 온프레미스 환경에서도 동일하게 발생하는 사례이다.

두 번째 보안 이슈에 대한 해결방안으로는 전체 클라우드 서비스를 대상으로 사용 중인 서비스를 로깅(logging) 하며, 사용률(usage) 수치를 통해 미사용으로 예측되는 서비스 등은 자동으로 비 활성화시키는 정규 프로세스를 갖추도록 한다. 즉, 활성화된 클라우드 서비스를 상시 모니터링하고 서비스 접속 이력을 검토하여 일괄 비 활성화하는 방식으로 보안 수준을 향상한다.

마지막 보안 이슈에 대한 해결방안으로는 현재 사용하고 있는 클라우드 서비스와 구성된 자원 현황이 눈에 드러나지 않다는 비가시성을 기억해야 한다. 따라서 시각화된 모니터링 체계와 관리자에 의해 검토해야 할 최소한의 프로세스를 정착시키는 것을 우선으로 해야 한다.

4. 결론

본 논문에서는 클라우드 서비스에서 발생할 수 있는 클라우드 보안 위협을 사례에 따라 정리함으로써 이에 대한 대응 방안을 연구하였다.

최근 코로나 19로 인하여 비대면 환경이 많이 떠오르고 있다. 이에 따라서 사이버 보안 중에서도 클라우드 보안이 많이 화제가 된 바가 있다. 가속화에 따라 공공과 민간 등 전 영역에서의 원격 근무가 확산이 있다. 데이터 수집부터 분석, 공급망 관리, 유통까지 직원의 모든 업무 절차가 전통 기업에서도 오프라인에서 온라인으로 옮겨 가면서, 모든 업무가 클라우드를 기반으로 작동하게 됐다. 코로나 19가 완화되고 있음에도 국내 IT 기업 중에서는 원격 근무 체제를 유지하겠다고 밝힌 기업이 있다.

클라우드 시장이 성장하면서 클라우드 서비스에 대한 외부 사이버 공격 횟수는 전보다 630% 증가했다. 이를 해결하기 위해 국내외 기업은 클라우드 보안에 특히 더 투자하고 있다. 판매량 역시 한 회사는 115% 증가하였다고 밝혔다.

현재 상황에 맞게 클라우드 보안을 더욱 연구하여 위협 유형 및 대응 방안을 지속적해서 파악해야 할 필요가 있다.

참고문헌

[1] 토마스 얼, 자이엄 마흐무드, 리카르도 푸티니, '클라우드 컴퓨팅: 개념에서 설계, 아키텍처까지', 에이콘, 2015년
[2] 정재화, 클라우드 컴퓨팅, 한국방송통신대학교출판문화원, 2020년
[3] 나연묵, 최종무, 박기웅, '클라우드 컴퓨팅 개념, 기술, 구축체험', 홍릉과학출판사, 2016년
[4] IMOXION, 4차 산업혁명 시대의 클라우드 서비스가 필수인 이유, https://www.imoxion.com/resources/tech-insight/?mod=document&uid=805, 2022.10.01
[5] 고수현, 금융권 화두로 떠오른 '클라우드 기술 도입'...왜?, 시사오늘시사온, 2022.05.19, https://www.sisaon.co.kr/news/articleView.html?idxno=139039
[6] 임유경, 국내 사이버 보안 빅3, '클라우드'에 미래 걸었다, ZDNET Korea, 2022.04.28, https://zdnet.co.kr/view/?no=20220428135843
[7] Neal Weinberg, 닮은 듯 다른 '보안' 전략… 클라우드 빅3 비교해보니, 2021.06.16, https://www.ciokorea.com/news/197799
[8] 윤대균, 클라우드 보안서비스 기업 총정리 (feat. 오픈소스), slownews, 2020.06.24, https://slownews.kr/76799
[9] SAMSUNG SDS, 현장에서 발생하는 클라우드 보안 이슈와 해결 방법, https://www.samsungsds.com/kr/insights/yje-cloud211224.html, 2022.10.01
[10] 이소연, 비대면 흐름 속 몸집 커진 클라우드 보안… 1000兆 시장 열린다, 조선일보, 2022.06.16, https://biz.chosun.com/it-science/ict/2022/06/16/J7U6AVNTKJE4NMZ4E7UXOLHS6I/