EQST insight

클라우드로의 전환, 알맞은 보안 대응 방안은?

클라우드 컴퓨팅은 4차 산업 혁명의 핵심 기반으로 최근 그 활용률이 증가하고 있다. 그러나 클라우드 보안에 대한 우려가 완전히 해소되지 않아 기업들은 여전히 클라우드 도입과 확산에 신중한 상태이다. 쉽게 말해, 정확한 위치 파악도 안 된 외부 어딘가에 기업의 주요 데이터를 저장하는 것에 대해 불안감을 갖고 있는 것이다. 이에 클라우드 보안 위협 요소와 환경 변화, 보안 사고, 공격 유형들을 알아보고, 클라우드 환경에서는 어떤 보안 대책을 마련해야 하는지 살펴보고자 한다.

클라우드 보안 위협 요소와 환경 변화

클라우드 보안 위협에는 권한 및 계정 관리, 구현 오류, 시스템 오류, 디도스(DDoS) 등의 기술적 측면과 내부관리자의 실수나 부정행위, 저장소 관리 미흡 등과 같은 관리적 측면, 그리고 자연재해와 같은 물리적인 측면에서 발생하는 위협들이 있다. 대부분의 클라우드는 기존 인프라에서 발생하는 것과 같은 보안 문제를 가지고 있으며 해결 방안도 기본적으로 유사하다. 하지만 가상화, 네트워크 연결, 분산처리 환경 등과 같은 '자원 공유'라는 특수성으로 인해 복합적인 보안 위협이 존재한다. 특히 클라우드 서비스 공급 업체를 겨냥한 보안 침해 및 공격과 공유 인프라로 인한 취약성 증가는 클라우드의 보안 위협으로 가장 많이 언급되는 요소이다.

클라우드로의 환경 전환으로 인한 컨테이너화가 늘고 있는 것도 클라우드의 보안 위협을 가중하고 있다. 다양한 서비스 영역의 확장으로 인해 고객 애플리케이션 제공 주기 단축과 효율적 개발/운영이 이뤄지기 위해서는 컨테이너화가 필수적이다. 그런데 클라우드 내 컨테이너화를 통해 개발/운영의 효율성 증대와 다양한 서비스 제공 등이 가능해졌지만, 클라우드/컨테이너 플랫폼의 서버, 가상화, 이미지, 저장장치, 네트워크 등의 보안 문제도 함께 증가하고 있는 추세이다. 공유된 리소스 관리, 계정, 설계상의 취약점과 같은 보안 이슈 역시 컨테이너화가 늘면서 증가하고 있다. '2019년 Cyber Threat Defense Report'에서 IT 조직 담당자를 대상으로 영역별 조직의 전반적인 보안 상태를 설문 조사했을 때도 컨테이너 보안은 가장 낮은 것으로 드러났다.

클라우드 보안 사고 사례

클라우드에서 실제로 발생한 보안 사고는 접근 권한 우회/탈취, 네트워크 트래픽 위/변조, 디도스(DDoS) 공격, 시스템 오류 등의 문제로 발생했다. 클라우드의 특수적 환경에 기반한 보안 사고로는 공유 자원을 활용한 암호화폐 채굴 사고가 대표적이다.

서비스 제공자	보안 사고 사례
A社	연예인들의 계정 탈취와 민감한 사진 노출
	아이클라우드의 계정 탈취와 자료 삭제
	마이그레이션 과부하로 인한 아이클라우드 서버 접속 장애
B社	클라우드 환경 설정 오류로 인한 기업 정보 노출
C社	서비스 이용자의 메시지와 주소록 삭제
	태국 ISP를 이용한 세션 하이재킹 공격
	자연재해로 인한 Gmail과 앱스토어 장애 발생

D 社	이용자 이메일 정보 유출 및 스팸메일 전송
E 社	디도스 공격으로 인한 서비스 장애
F 社	이미지에 CRSS 악성코드 삽입
G 社	컨테이너 환경 설정 오류로 인한 악성코드 배포 및 암호화폐 채굴
H 社	클라우드 네트워크 관리 미흡으로 인한 고객 정보 노출

[클라우드 서비스 보안사고 사례]

클라우드에서 발생한 보안 사고는 주로 클라우드의 특수성을 고려하지 않은 설정 오류나 관리 미흡으로 인해 발생하였다. 그리고 이는 고객 서비스에 직접적 영향으로 이어진 경우가 많았다.

클라우드 사이버 공격 유형

글로벌 사이버 보안 연구소 SANS(SANS Institute)는 RSA Conference (RSAC) 2018에서 '가장 위험한 5가지 최신 공격 기법'을 발표했다. 이를 기반으로 클라우드 서비스 환경을 노리는 사이버 공격들을 살펴보면 다음과 같다.

1) **크립토마이닝(Cryptomining) 공격**

암호화폐(Cryptocurrency) 열풍과 더불어 크립토 마이닝(Cryptomining)의 피해 또한 급격히 증가하는 추세이다. 비트코인 또는 이더리움 코인은 온라인을 통해 채굴하는데, 공격자는 스텔스

기능을 가진 원격 접근 도구를 활용해 처리 능력을 하이재킹(hijacking)하여 클라우드 컴퓨팅 리소스를 무단으로 암호화폐 채굴을 수행하는 데 사용한다.

2) **크로스테넌트 공격(Cross-tenant Attack)**
동일한 클라우드 플랫폼을 사용하는 기업이나 기관에서 업무를 위해 공유 채널을 이용할 경우 클라우드의 테넌트(Tenant) 간 경계가 흐려지게 된다. 이때 한 명의 사용자를 통해 침해가 발생한다면,해당 클라우드 플랫폼 내 공유 채널을 사용하는 기업이나 기관 전체가 영향을 받을 수 있다.

3) **클라우드 랜섬웨어(Cloud Ransomware) 공격**
현재까지 많은 기업들에게 재앙처럼 발생한 랜섬웨어는 비교적 간단한 형태의 멀웨어로 방어벽을 뚫고 아주 강력한 암호화를 통해 서버의 모든 파일을 암호화시켰다. 클라우드 영역에서 발생할 경우 특정 기업에 국한되지 않고, 클라우드 플랫폼 전체에 영향을 줄 수 있다.

4) **인스턴트 메타데이터 API를 타깃으로 한 공격**
클라우드 서비스(AWS, Azure 등)에서 제공하는 인스턴트 메타데이터 API는 사이버 공격을 방어할 수 있는 기능이나 따로 모니터링하는 경우가 거의 없어 각종 공격에 매우 취약하다. 특히 리버스 프록시 등을 이용한 공격에 쉽게 노출되는 경향이 있다.

5) **오케스트레이션 공격(Orchestration Attack)**
컨테이너 관리를 위해 서버의 활성화, 자원 할당, 네트워크 처리, 이미지의 생성 등 여러 가지 업무를 수행할 때 사용되는 기술을 오케스트레이션이라 한다. 오케스트레이션 공격은 이러한 작업을 수행할 때 사용되는 계정 정보나 암호화 키를 훔쳐 여러 업무에 직접 접근하고 공유 자원을 악용할 수 있다.

클라우드 보안 대응 방안

지금까지 클라우드 보안 위협과 환경 변화, 보안 사고, 공격 유형 등을 살펴보았다. 국내/외 기업들의 클라우드 서비스 전환이 활발하게 이뤄지는 상황에서 보안의 위험성을 최소화하기 위한 대책 수립은 선택이 아닌 필수이다.
안전한 클라우드 환경 조성을 위해서는 제도를 효율적으로 활용해야 하며, 이를 기반으로 각 기업들의 특성을 고려한 체계를 만들어야 한다.

국가	인증명	인증기준	인증기관	평가기관	비고
미국	FedRAMP	NST SP 800-53	FedRAMP PMO (운영사무국)	공인기관 (총 38 개 기관)	-연방 정부에 도입되는 민간 클라우드 서비스 -국가 인정 공인기관에서 평가
일본	JCISPA	클라우드 정보보안 기준	JASA (일본 정보 보안감사협회)	JASA (인증심사위원회)	-퍼블릭 클라우드 서비스 대상 -민간 협회에서 운영

	ASP, SaaS 인증 Iaas, PaaS 인증 데이터센터 인증	클라우드서비스 안전성에 관한 정보공개지침	ASPIC (일본ASP 산업협회)	ASPIC (인증심사위원회)	-국가에서 인정한 협회에서 수행
싱가포르	MTCS-SS	ISO/IEC 27001 +자체규정	ITSC (정보기술 표준위원회)	공인기관 (총 7 개 기관)	-국가 인정 공인기관에서 평가
영국	UK G- Cloud	ISO/IEC 27001 +자체규정	CESG (국가정보 보증기술국)	-	-국가 인정 공인기관에서 평가
호주	ASD CCSL	ISO/IEC 27001 +자체규정	ASD (호주 신호국)	IRAP (인증심사위원회)	-독립적 보안 등록 평가자가 수행한 종합적인 평가를 승인

[해외 클라우드 보안인증 운영 현황 비교]
출처: 한국인터넷진흥원(KISA)

클라우드가 활성화된 미국의 경우 2010년부터 공공부문의 클라우드 우선 도입 정책을 추진하고 있다. 그리고 안전한 클라우드 환경 조성을 위한 보안 정책인 패드램프(FedRAMP)를 통해 공공부문의 민간 클라우드 이용 활성화를 이끌고 있다. 이 패드램프는 클라우드 서비스의 보안 평가 인증 관련 모든 사항을 통합하고 있으며, 연방정부의 민간 클라우드 도입을 위한 보안성 평가 항목 등을 규정하고 있다. 미 연방정부의 '정보시스템 및 개인정보 보안 지침'인 'NIST SP 800-53'을 기반으로 클라우드 서비스에 특화된 사항을 추가해 총 17개 분야 325개의 보안 통제 기준을 제시하고 있다.

구분	주요 내용
관리적 조치	정보보호 정책 및 조직, 인적 보안, 자산관리, 서비스 공급망 관리, 침해사고 관리, 서비스 연속성 관리, 준거성
물리적 조치	물리적 보호구역 지정 및 보호, 정보처리 시설 및 장비 보호
기술적 조치	가상화 보안, 접근통제, 네트워크 보안, 데이터 보호 및 암호화, 시스템 개발 및 도입 보안
공공기관추가 조치사항	서비스 수준 협약, 도입전신장비 안전성, 물리적 분리, 이중화 및 백업 체계 구축, 암호화 기술 제공, 보안관제 제반 환경 지원

[클라우드 정보보호 기준(안)]
출처: 과학기술정보통신부

우리나라도 클라우드컴퓨팅법 제23조에 따른 정보보호 기준을 제시해 이용자 신뢰도 향상 및 서비스 제공자의 보안 수준을 제고하고자 '정보보호에 관한 기준 고시'를 제정하고 있다. 특히 개인정보나 기밀 사항

등 민감한 정보를 다루는 공공부문은 보다 높은 수준의 보안성 및 심도 있는 검증이 요구되기 때문에 공공기관이 안전하게 민간 클라우드 이용을 할 수 있도록 보장하는 제도적 장치를 마련한 것이다.

고시에는 국제표준(ISO27001)과 '클라우드컴퓨팅법'에서 규정한 정보보호 조치사항 등을 핵심 요소로 삼아 관리/물리/기술적 보호조치 및 공공기관용 추가 보호조치 등 총 14개 부문에 118개 통제 항목을 마련했다. 미국과 비교했을 때 사업자의 부담을 낮추기 위해 통제 항목 수를 줄이고, 서비스 안전성 및 신뢰성을 담보하기 위한 핵심 항목을 추가/강화한 것이 특징이다. 그리고 클라우드 서비스 제공자가 정보보호 기준 준수 여부를 과기부에 확인을 요청할 경우, 전문기관(KISA)을 통해 시험·평가를 실시할 수 있도록 했다.

클라우드 정보보호를 위한 고시가 제정됐지만, 다양한 클라우드/컨테이너 플랫폼 환경에 맞는 구체적이고 현실성 있는 보안 대책으로 활용되기에 다소 아쉬움이 있는 부분이 있다. 이를 보완하려면 각 기업은 클라우드/컨테이너 플랫폼별로 계정 보안, 네트워크 보안, 접근 제어, DB 보안, 데이터 보안, 오케스트레이션 관리 등을 고려한 세부 보안 체계를 수립해야 한다.

제도적 기반으로 클라우드 활용에 대한 전체적인 보안 기준을 세우고, 플랫폼별로 기술적/관리적 지침을 적용하여 보안에 대한 우려 사항을 최소화한다면, 클라우드 서비스의 활성화는 더욱더 빠르게 진행될 것이라 예상된다.