情 報 保 護 學 會 誌
第22卷 第7號, 2012. 11

퍼블릭 클라우드 컴퓨팅 사용 기업이 고려해야 할 보안 위험과 대응 방안에 대한 小考

박 형 근*

요 약

클라우드 컴퓨팅의 보안 위험에 대한 여러 연구 결과들을 분석해 보고 퍼블릭 클라우드 컴퓨팅의 여러 비즈니스 모델의 특성을 기반으로 재분류를 통해 퍼블릭 클라우드 컴퓨팅 사용 기업이 고려해야 할 보안 위험과 대응에 대해 고찰하고자 한다.

Ⅰ. 서 론

2012년 올해 최고의 IT 화두는 클라우드 컴퓨팅, 빅 데이타, 그리고 모바일이다. 그 가운데 클라우드 컴퓨팅은 경제 불황과 맞물려 컴퓨팅 자원 활용의 극대화와 사용한 만큼만 비용을 지불하는 유틸리티 서비스 모델로 IT 운영 관리에 있어 현실적인 비용 절감 방안을 제시했다. 또한, 서비스 카탈로그의 간단한 선택으로 원하는 모든 서비스를 원하는 시간 내에 간편히 사용할 수 있는 편리성과 적시성은 사용자 관점에서도 매우 혁신적인 서비스였다. 그러나 인프라의 공유와 자산까지 모두 아웃소싱 되는 클라우드 컴퓨팅의 특성으로 인해 비용 절감과 편리성이라는 두 가지 이점에도 불구하고 클라우드 컴퓨팅의 확산을 막는 가장 큰 장애 중 하나는 바로 보안이었다. 이에 대해 가트너, CSA (Cloud Security Alliance), ENISA (European Network and Information Security Agency), NIST (National Institute of Standards and Technology) 등 수많은 조직에서 보안 위험에 대해 연구하고 분류하여 그 대응 방안을 발표하였다. 그러나 다양한 클라우드 컴퓨팅의 비즈니스 모델에 따른 특성의 이해와 분류가 모두 상이하였고, 특히 퍼블릭 클라우드 컴퓨팅을 이용하고자 하는 기업에 대해 정확한 정보를 제공하기에 미흡한 점이 많았다. 이에 본 소고에서는 그동안의 클라우드 컴퓨팅 보안 위험에 대한 연구 결과들을 분석해 보고 퍼블릭 클라우드 컴퓨팅의 여러 비즈니스 모델의 특성들을 기반으로 재분류하여 퍼블릭 클라우드 컴퓨팅 사용 기업이 고려해야 할 보안 위험과 대응 방안에 대해 고찰하고자 한다.

Ⅱ. 클라우드 컴퓨팅 보안 위험에 대한 기존 연구

클라우드 컴퓨팅의 보안 위험에 대해 연구한 여러 조직 중 본 소고에서 다루고자 하는 곳은 가트너, CSA, ENISA, 그리고 NIST의 네 가지 연구 결과에 대해 분석해 보고 퍼블릭 클라우드 컴퓨팅 사용 기업의 관점에서 다시 재해석 및 재분류하고자 한다.

2.1. 가트너 연구 결과 고찰

가트너에서의 클라우드 컴퓨팅의 보안 위험에 대한 연구 결과는 “Assessing the Security Risks of Cloud Computing(2008) [1] ”에서 살펴 볼 수 있다. 이 보고서에서 가트너는 여덟 가지의 클라우드 컴퓨팅 보안 위험에 대해 기술했다. 그 여덟 가지는 바로 Privileged User Access, Compliance, Data Location, Data Segregation, Availability, Recovery, Investigative Support, Viability 이다.

가트너가 첫 번째로 제시한 Privileged User Access의 의미는 민감한 기업 정보를 클라우드 컴퓨팅을 통해

* SecurityPlus 정보보안 커뮤니티, 한국 IBM (securityplus@securityplus.or.kr)

처리할 때, 그 데이터를 보호하기 위한 전통적인 보안 통제들도 클라우드 컴퓨팅 서비스를 제공하는 외부의 특권 관리자들에 의해 우회되어 접근 가능함을 경고한 것이다. 이것은 민감한 정보를 처리할 때 뿐만 아니라, 언제 어디서든 접근할 수 있는 클라우드 컴퓨팅 환경 속에서 오남용을 통한 불필요한 비용 발생과 악의적인 활동에 악용될 수 있는 가능성이 있다. 따라서 서비스 제공자의 특권 사용자와 함께 관리 권한 위임된 서비스 사용자의 특권 사용자 모두 특권 사용에 대한 통제 방안 강구와 모니터링이 필요하며 퍼블릭 클라우드의 모든 비즈니스 모델에 대해 적용 가능하다.

두 번째 항목인 Compliance의 의미는 클라우드 컴퓨팅 서비스 제공자가 서비스 사용자가 준수해야 하는 법규제사항에 대해 고려하지 않을 수 있는 위험에 대해 지적한 것이다. 컴플라이언스에 관한 이슈는 모든 클라우드와 관련된 비즈니스 모델에 대해 다 영향을 준다.

세 번째 항목인 Data Location은 데이터의 위치를 통제할 수 없음을 지적한 항목인데 일반적으로는 클라우드 컴퓨팅 서비스 사용자에게 있어 크게 중요한 사항은 아니다. 오히려 데이터의 위치와 관련된 문제는 두 번째 항목인 컴플라이언스, 즉 법 규제 사항 준수와 연관이 있다. 예를 들면 “정보통신망 이용촉진 및 정보보호 등에 관한 법률 제63조 국외 이전 개인정보의 보호”에 개인정보의 임의 국외 이전에 대해 법적으로 금하고 있어, 클라우드 컴퓨팅에 데이터를 적재하려는 서비스 사용자는 그 데이터가 만일 개인정보라면 저장되는 데이터 위치를 반드시 고려해야만 한다. 이 역시 모든 클라우드와 관련된 비즈니스 모델에 대해 다 영향을 준다.

네 번째 항목인 Data Segregation에 대해 가트너는 클라우드 컴퓨팅을 사용하는 중에는 트랜잭션이 SSL 혹은 SSH와 같은 암호화 통신을 사용하고 있기 때문에 대부분 안전하게 보호되고 있지만, 스토리지 상에서 데이터가 저장될 때에는 공유된 스토리지 공간 상에서 함께 존재하며, 데이터 분리를 하지 못할 위험에 대해 지적했다. 물론 이에 대해 분리해야 할 데이터 사이에는 서로 다른 키로 암호화하여 통제하지만, 특권 사용자는 이 서로 다른 키에 접근이 가능하므로 복호화 키에 접근을 통제하고 모니터링해야 함을 강조했다. 그러나 이 항목은 특권 사용자 접근 항목 내에 포괄될 수 있으며, 데이터 분리 운영의 책임이 가장 큰 SaaS 형태의 클라우드 컴퓨팅 서비스 제공자가 가장 큰 영향을 받는다. 반면 서비스 사용자가 직접 키 관리가 가능한 IaaS 형태의 클라우드 컴퓨팅 서비스 제공자나 사용자에게는 그 영향이 그리 크지 않을 수도 있다.

다섯 번째와 여섯 번째 항목인 Availability와 Recovery는 보안 관점의 가용성과 복구가 아니라, IT 관점의 가용성과 복구를 말하고 있어, 이 부분은 고찰의 범주에서 제외했다.

일곱 번째 항목인 Investigative Support는 각종 보안 사고에 대한 조사, 컴플라이언스와 감사 대응을 위한 조사와 증적 지원 등이 원활치 않을 수 있음을 지적했다. 이 역시 컴플라이언스 관점에서 고려될 수 있으며, 퍼블릭 클라우드의 모든 비즈니스 모델에 대해 적용 가능하다.

마지막으로 여덟 번째 항목인 Viability도 역시 보안 관점이라기 보다는 운영 관점에서 Lock-in 문제와 그 궤를 같이 하고 있는 이슈로 본 고찰의 범주에서는 제외했다.

지금까지 살펴본 가트너의 여덟 가지 보안 위험에 대해 그 분류 내용과 분류에 대해 보다 많은 영향을 받는 클라우드 컴퓨팅 비즈니스 모델(IaaS, PasS, SaaS)에 대해 사용자 관점으로 나눠 보면, “[표1] 가트너의 클라우드 컴퓨팅 보안 위험”과 같다.

〔표 1〕 가트너의 클라우드 컴퓨팅 보안 위험

보안 위험	사용자 관점 비즈니스 모델
Privileged User Access	모두 적용
Compliance	모두 적용
Data Location	모두 적용
Data Segregation	필요시, IaaS
Availability	해당 없음
Recovery	해당 없음
Investigative Support	모두 적용
Viability	해당 없음

가트너가 말한 여덟가지 클라우드 컴퓨팅 보안 위험은 크게 특권 사용자 접근과 컴플라이언스 이 두 가지로 요약할 수 있으며, 퍼블릭 클라우드 사용 기업에게 모두 적용될 수 있는 중요 보안 위험이다.

2.2. CSA 연구 결과 고찰

CSA (Cloud Security Alliance)에서 클라우드 컴퓨

팅 보안 위험에 대한 연구 결과는 “Top Threats to Cloud Computing Survey Results Update 2012 [2] ”에서 살펴 볼 수 있다. 이 보고서에서 제시한 클라우드 컴퓨팅의 가장 위험한 위협은 Data Loss/ Leakage, Insecure APIs, Malicious Insiders, Account/ Service & Traffic Hijacking, Abuse of Cloud Computing, Unknown Risk Profile, Shared Technology Vulnerabilities, DDoS으로 여덟 가지이다.

첫 번째인 Data Loss/ Leakage에 대한 위협은 모든 클라우드 컴퓨팅 비즈니스 모델에 해당 되는 보안 위험이다. 클라우드 컴퓨팅에 특화된 위험이라기 보다는 가장 일반적인 보안 위험이기 때문에 본 고찰의 범주에서 제외했다.

두 번째인 Insecure APIs에 대한 위협은 모든 서비스 모델에 해당 된다. 클라우드 컴퓨팅 서비스 제공자는 서비스 이용자의 기존 레거시 IT 인프라와의 연계 및 통합, 그리고 다양한 정보의 통신을 위해 여러 가지 서비스 인터페이스와 API를 공개하여 활용토록 하고 있다. 그러나 안전하지 않은 서비스 인터페이스와 API는 이와 연관된 클라우드 컴퓨팅과 기존 레거시 인프라 모두에 치명적인 보안 위협이 될 수 있다.

세 번째인 Malicious Insiders로 인한 위협은 역시 모든 서비스 모델에 해당된다. CSA가 지적한 Malicious Insiders는 클라우드 컴퓨팅 서비스 제공자의 내부 임직원에 의한 위협으로 가트너가 지적한 Privileged User Access 위험과 일맥상통한다. 그러나 CSA가 지적한 Malicious Insiders에 대한 사항은 서비스 사용자 보다는 서비스 제공자가 좀더 관심을 기울여야 한다.

네 번째인 Account/ Service & Traffic Hijacking의 전통적인 위협에 대해 CSA는 Identity Theft가 이러한 위협의 주된 원인이라고 주목했다. Identity Theft를 포함하여 Account/ Service & Traffic Hijacking은 모든 서비스 모델에 해당된다.

다섯 번째인 Abuse of Cloud Computing는 주로 IaaS와 PaaS에 해당되는 위협으로, 가트너에서 지적한 특권 사용자 이슈와 그 맥을 같이 하며, 악의적인 사용자에 의한 좀비 가상 서버와 같이 DDoS 공격에 악용되거나, 비즈니스 목적과 다른 용도로 클라우드 자원을 오남용하는 것을 뜻한다. 특히 서비스 사용자 관점에서도 관리 위임 받은 내부 직원에 의해 클라우드 자원이 비즈니스 목적과 다른 용도로 오남용되어 불필요한 비용이 발생되는 이슈는 가장 흔하게 발견되는 사례들이다.

여섯 번째인 Unknown Risk Profile는 클라우드 서비스 제공자의 제한된 정보 공유로 인해 파악되어야 하는 보안 위험들에 대해 미처 파악되지 못할 위험이 있다는 것으로 모든 클라우드 컴퓨팅 비즈니스 모델에 해당된다.

일곱 번째인 Shared Technology Vulnerabilities은 주로 공유된 자원과 가상화 인프라 상에서 야기되는 이슈로 IaaS 클라우드 컴퓨팅 비즈니스 모델에 해당되는 보안 위험이다. 특히 하이퍼바이저의 취약점이 전체 가상화 인프라에 악영향을 줄 수 있다.

여덟 번째인 Distributed Denial of Service는 다섯 번째인 Abuse of Cloud Computing 내 포함될 수 있는 내용으로 2008년 보고서에는 별도로 나눠서 다루지 않았으므로 본 고찰에서는 다루지 않는다.

지금까지 살펴본 CSA의 여덟 가지 보안 위험에 대해 그 분류 내용과 분류에 대해 보다 많은 영향을 받는 클라우드 컴퓨팅 비즈니스 모델(IaaS, PasS, SaaS)에 대해 사용자 관점으로 나눠 보면, “[표2] CSA의 클라우드 컴퓨팅 보안 위험”과 같다.

2.3. ENISA 연구 결과 고찰

ENISA (European Network and Information Security Agency)에서 클라우드 컴퓨팅 보안 위험에 대한 연구 결과는 “Cloud Computing Security Risk Assessment(2009) [3] ”에서 살펴 볼 수 있다. 이 보고서에서 제시한 클라우드 컴퓨팅의 보안 위험은 Loss of

〔표 2〕 CSA의 클라우드 컴퓨팅 보안 위험

보안 위험	사용자 관점 비즈니스 모델
Data Loss/Leakage	모두 적용
Insecure APIs	모두 적용
Malicious Insiders	모두 적용
Account/Service & Traffic Hijacking	모두 적용
Abuse of Cloud Computing	IaaS, PaaS
Unknown Risk Profile	모두 적용
Investigative Support	모두 적용
Shared Technology Vulnerabilities	IaaS
DDoS	모두 적용

Governance, Lock-In, Isolation Failure, Compliance Risks, Management Interface Compromise, Data Protection, Insecure or Incomplete Data Deletion, Malicious Insider이다. 이 가운데, Data Protection, Compliance Risks와 Malicious Insider는 CSA에서 다뤘던 항목과 동일하므로 중복하여 다루지 않는다.

첫 번째 항목인 Loss of Governance은 클라우드 컴퓨팅 서비스 제공자에게 많은 통제와 권한을 위임해야 하나 SLA 계약에서는 많은 부분에 있어 확약을 하지 않으므로 보안에 있어 차이가 발생할 수 있다는 것으로 모든 클라우드 컴퓨팅 비즈니스 모델에서 적용된다.

두 번째 항목인 Lock-In 문제는 보안 이슈라기 보다는 공급망 관리 상의 이슈로 서로 다른 클라우드 컴퓨팅 인프라 간에 호환성을 보장할 수 있는 표준이 부재하기 때문에 하나의 클라우드 컴퓨팅 서비스 제공자로부터 다른 서비스 제공자로 이전하거나, 기존 Regacy 인프라로 이전하기 어려움을 의미한다.

세 번째 항목인 Isolation Failure은 멀티 테넌시(Tenancy)와 공유 자원 상에서 발생될 수 있는 이슈로 가트너에서 Data Segregation를 다뤘던 것과 유사하다. 이 역시 모든 클라우드 컴퓨팅 비즈니스 모델에서 적용되며 서비스 사용자 보다는 서비스 공급자가 좀더 고려해야 할 이슈이다.

네 번째 항목인 Management Interface Compromise는 클라우드 컴퓨팅 서비스 공급자가 서비스 사용자에게 제공하는 관리 권한을 위임한 관리 인터페이스로 보통 원격에서 웹을 통해 접근하게 된다. 서비스 사용자에게 할당된 클라우드 자원을 관리 운영할 수 있는 관리자 인터페이스로 침해 시 전체 인프라가 위험해 질 수 있고, 가트너에서 지적한 특권 권한 중 클라우드 컴퓨팅 서비스 사용자에게 위임된 특권이 해킹 등 외부의 위협에 의해 전체 인프라가 위험해질 수 있다. 전체 클라우드 컴퓨팅 비즈니스 모델에 전부 적용된다.

다섯 번째 항목인 Insecure or Incomplete Data Deletion은 공유된 스토리지 상에서 불완전하게 삭제된 데이터가 다시 재할당된 경우 포렌식 기술을 활용하여 복구가 가능함으로써 의도하지 않게 중요 정보가 다른 사람에게 전달될 가능성이 있어, Insecure or Incomplete Data Deletion 항목이 매우 중요하게 되었다. 주로 IaaS 클라우드 컴퓨팅 비즈니스 모델에 적용된다.

지금까지 살펴본 ENISA의 여덟 가지 보안 위험에 대해 그 분류 내용과 분류에 대해 보다 많은 영향을 받는 클라우드 컴퓨팅 비즈니스 모델(IaaS, PasS, SaaS)에 대해 사용자 관점으로 나눠 보면, "[표 3] ENISA의 클라우드 컴퓨팅 보안 위험"과 같다.

〔표 3〕 ENISA의 클라우드 컴퓨팅 보안 위험

보안 위험	사용자 관점 비즈니스 모델
Loss of Governance	모두 적용
Lock-In	해당 없음
Isolation Failure	모두 적용
Compliance Risks	모두 적용
Management Interface Compromise	모두 적용
Data Protection	모두 적용
Insecure or Incomplete Data Deletion	IaaS
Malicious Insider	모두 적용

Ⅲ. 퍼블릭 클라우드 컴퓨팅 서비스 사용자 관점의 보안 위험

앞서 살펴 본 가트너, CSA, 그리고 ENISA의 보안 위험들 가운데서 퍼블릭 클라우드 컴퓨팅 서비스 사용자와 직접적으로 연관성 있으며 대응 방안 수립이 가능한 위험들만 선별하고자 한다.

3.1. 악의적인 특권 및 위임 특권

"악의적인 특권 및 위임 특권"은 가트너의 Privileged User Access, CSA/ ENISA의 Malicious Insiders에 상응한다. 여기서 특권이란 클라우드 컴퓨팅 서비스 제공자의 특권 사용자를 의미하며, 위임 특권이란 클라우드 컴퓨팅 서비스 사용자의 특권 사용자를 의미한다. 서비스 사용자 관점에 있어서는 클라우드 컴퓨팅 서비스 공급자의 악의적인 특권 사용자가 서비스 사용자의 중요 데이터에 대한 유출, 변조, 파괴가 가능하다는 사실을 인지하고 대응 방안을 마련하는 것이 필요하다.

또한, 클라우드 컴퓨팅 서비스 사용자의 위임 특권 사용자에 대한 접근 통제나 관리 역시 필요하다. 이러한 위임 특권 사용자의 악의적인 행위로 인해 서비스 사용자의 중요 데이터가 유출, 변조, 파괴되거나, 클라우드 서비스 내 할당된 공유 자원이 비즈니스 목적에 맞지 않게 오남용될 수 있다.

3.2. 취약한 인터페이스 연계 및 안전하지 않은 개발

“인터페이스 및 개발에 있어서의 취약점”은 CSA의 Insecure APIs"에 대응된다. 클라우드 컴퓨팅 인프라와 내부 기존 시스템을 연계하거나, 다른 클라우드 인프라와 정보를 주고 받는 등 외부 시스템과의 연계할 때, 인터페이스나 API를 활용하여 클라우드 컴퓨팅 서비스 사용자는 이 인터페이스를 사용하여 개발하게 된다. 공개된 인터페이스에 대한 보안 검토가 충분치 않았거나, 안전하지 않은 코딩을 했다면 그 소프트웨어 취약점을 통해 클라우드 컴퓨팅 인프라와 연계된 인프라 모두 외부 공격에 노출될 수 있다.

3.3. 취약한 인증 정보 관리

전통적인 IT 인프라 하에서도 인증 정보에 대한 라이프사이클 관리는 매우 중요한 보안 관리 중 하나이다. 그러나 클라우드 컴퓨팅 환경으로 관리 대상이 외부로 이전됨에 따라 엄격했던 인증 정보 관리가 느슨해지거나 아예 관리 대상에서 제외될 수도 있다. 특히 인터넷을 통해 언제 어디서든 접근 및 사용할 수 있다는 클라우드 컴퓨팅의 특성을 볼 때, 최초 인증 정보에 대한 안전한 전달과 주기적인 인증 정보의 라이프사이클 관리 역시 매우 중요하다. 암호화되지 않은 메일을 통해 최초 인증 정보를 주고 받는다든가, SSH Key나 패스워드를 서로 공유해서 사용한다든가, 주기적으로 변경하지 않고 지속 사용하는 등 취약한 인증 정보 관리는 클라우드 컴퓨팅 서비스의 탈취와 도난으로 중요 서비스에 대한 유출과 클라우드 컴퓨팅 서비스의 악용 등 여러 위협에 노출될 수 있다.

3.4. 클라우드 컴퓨팅 통한 중요 데이터 유출

언제 어디서든 인터넷을 통해 연결 가능한 클라우드 컴퓨팅 서비스는 편리함과 동시에 악의적인 내부 사용자에 의한 정보 유출의 중간 경로가 될 수 있다. 클라우드 컴퓨팅 서비스를 통해 내부의 중요 정보의 업로드와 외부에서 중요 정보의 다운로드가 가능하고, 게이트웨이로써 보안 체계를 우회하는 경유지로써의 활용이 가능함에 따라 기존 인프라에 구축된 내부 정보 유출 방지를 위한 보안 체계에 심각한 위협과 취약점이 될 수 있다.

3.5. 클라우드 컴퓨팅 내 중요 데이터 보호

가상화 기술을 기반으로 하는 클라우드 컴퓨팅 환경 내에서 가상화 기술 내 취약점에 대한 성공적인 공격, 가상화 인프라와 데이터에 대한 격리(Segmentation) 실패, 악성코드 등 다양한 이유로 인해 클라우드 컴퓨팅 내 데이터가 의도하지 않은 외부자에게 노출될 위협이 존재한다. 따라서, 클라우드 컴퓨팅 소비자는 클라우드 컴퓨팅 제공자의 보안 인프라에 부가하여 중요 데이터에 대한 위협에 대해 대응 방안 수립이 필요하다.

3.6. 미흡한 컴플라이언스 지원

국내외 각종 규제 및 감사에 대응하기 위해 클라우드 컴퓨팅 환경 하에서도 각종 로그에 대한 관리 및 감사 증적에 대한 수집 및 대응이 필요하다. 그러나, 클라우드 컴퓨팅 공급자의 적절한 지원이 없으면, 때에 따라선 컴플라이언스 지원 자체가 미흡할 위험이 존재한다. 다양한 클라우드 컴퓨팅 사용을 위한 부가적인 보안 통제를 구현하면서 이러한 미흡한 컴플라이언스 지원 역시 보완되어야 한다.

3.7. 계약과 SLA 내에 누락된 보안 요구사항

클라우드 컴퓨팅 사용자 관점에서 클라우드 컴퓨팅 공급자에게 보안 관련 요구사항을 반영할 수 있는 거의 유일한 기회는 계약과 서비스 수준 협약(SLA - Service Level Agreement)이다. 이때, 기업 내에서 필요한 보안 요구사항이 빠짐없이 검토되고, 각종 위험에 대한 클라우드 컴퓨팅 공급자의 대응 방안과 보안 관련 품질 제공 수준, 그리고 사고 발생 시 사후 책임 방안 등 다양한 보안 요구사항 항목에 대해 빠짐없이 검토되고 반영되어야 한다. 그러나 이때 검토가 부적합하다면 클라우드 컴퓨팅 제공자에 대해 사용자 기업의 보안 요구사항에 대한 통제 기회를 상실할 뿐만 아니라, 사후 사고 발생 시 책임과 배상에 관련 문제에 직면할 수도 있다. 따라서 클라우드 컴퓨팅 선택 시에도 많은 검토가 있어야 하겠지만, 계약과 SLA 내에서도 누락없이 모든 요구사항이 반영될 수 있도록 하는 방안이 강구되어야 한다.

Ⅳ. 퍼블릭 클라우드 컴퓨팅 서비스 사용자 관점의 보안 위험에 대한 대응 방안

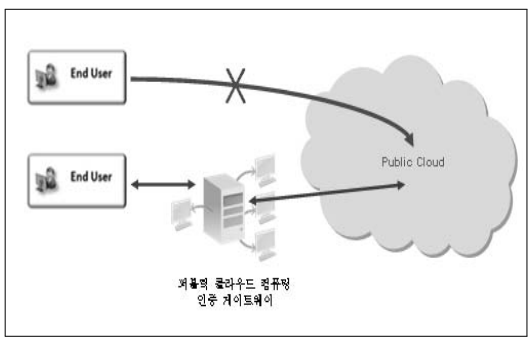
지금까지 퍼블릭 클라우드 컴퓨팅 서비스 사용자 관점의 보안 위험에 대해 살펴 보았다. 그럼, 이러한 보안 위협들에 대해서 클라우드 컴퓨팅 서비스 사용자는 어떤 대응 방안 적용이 가능한지 관련 기반 클라우드 보안 기술들을 토대로 알아본다.

4.1. 퍼블릭 클라우드 서비스 인증 게이트웨이

퍼블릭 클라우드 서비스 인증 게이트웨이는 프록시 및 게이트웨이 기술을 기반으로 계정 및 권한 관리 기술과 싱글 사인온 기술 등을 결합하여 개발 및 서비스를 제공한다. 클라우드 서비스 사용 기업 내 개별 사용자들이 퍼블릭 클라우드 컴퓨팅 인프라를 사용할 때에는 반드시 퍼블릭 클라우드 서비스 인증 게이트웨이를 통하지 않고는 서비스를 사용할 수 없도록 인증 관리 및 접근 통제 기술을 활용하여 강제화한다. 즉, 사용자는 퍼블릭 클라우드 서비스 인증 게이트웨이를 통하지 않고서는 인증 정보의 부재나 접근 권한 미흡으로 퍼블릭 클라우드 서비스를 활용할 수 없게 된다.

개별 사용자들이 퍼블릭 클라우드 서비스 인증 게이트웨이를 통해 인증을 할 때에는 2-factor 인증이나 다중 인증 기술들을 활용하여 인증 강화를 수행하며, 다양한 접속 조건(위치, 시간, 날짜, 디바이스 등)에 따라 위험 기반의 접속 통제를 강제화한다.

개별 사용자들의 퍼블릭 클라우드 서비스 내에 다양한 활동들은 퍼블릭 클라우드 인증 게이트웨이를 통해 서비스 연결과 사용이 이뤄지므로, 필요한 감사 데이터를 효과적으로 수집할 수 있다. 또한 이 데이터에 대한 분석을 통해 클라우드 서비스 인프라에 대한 통합 보안 관제도 지원한다.



〔그림 1〕 퍼블릭 클라우드 컴퓨팅 인증 게이트웨이 개념도

전체 퍼블릭 클라우드 서비스에 대한 계정 및 권한, 그리고 인증 정보 관리는 계정 및 권한 관리 영역에서 지원한다.

이러한 기술을 통해 여러 접속 조건과 권한에 따라 위임 특권 권한(3.1)을 가진 사용자의 특권을 제어하고, 취약한 인증 정보(3.3)를 강화하며, 미흡한 컴플라이언스 지원(3.6)에 대한 대응 방안 수립 및 보완한다.

4.2. 클라우드 데이터 암호화와 키 라이프사이클 관리

클라우드 컴퓨팅 서비스 사용자를 위한 외부에서 클라우드 컴퓨팅 환경 내로 적용 가능한 데이터 암호화 기법은 주로 IaaS 상의 파일/ 데이터베이스나, PaaS 상의 데이터 입출력 시 암호화 함수를 지원하는 경우 구현이 가능하다. 아직 SaaS 상의 특화된 서비스에 대한 암호화 입출력은 아직 연구가 더 필요하다. 또한, 보다 빠른 암호화 지원이나 모바일 기반의 퍼블릭 클라우드 상의 암호화를 위한 경량 암호화 개발 등도 필요하다. 이러한 제한에도 불구하고, 클라우드 컴퓨팅 환경 하에서의 데이터 보호는 보안에 있어 마지막 수단이라 할만하다. 또한, 각 사용자나 조직 간에 데이터 분리를 위해서, 혹은 데이터 보안 자체를 강화하기 위해서는 데이터 보안의 마스터 키에 대한 엄격한 키 관리가 필요하다. 이러한 구현을 통해 클라우드 컴퓨팅 내 중요 데이터 보호(3.5)를 지원한다.

4.3. 클라우드 컴퓨팅을 위한 데이터 유출 방지

클라우드 컴퓨팅을 통한 개별 서비스 사용자들의 내부 정보 유출 방지를 위해서는 기업 내 정보 유출 방지 시스템과 연계하여 클라우드 컴퓨팅 상으로 데이터를 업로드하거나 다운로드할 때 정책 기반으로 통제하는 기술이 필요하다. 현재 기업에서 많이 활용되고 있는 DRM(Document Right Management)나 DLP (Data Loss Protection)이 관련 기술 개발에 대한 단초를 제공하고 있기는 하나, 퍼블릭 클라우드 컴퓨팅 환경과 연계하여 퍼블릭 클라우드 컴퓨팅 환경에서 데이터를 가공하고, 가공된 데이터의 다운로드나 업로드, 그리고 기업

내부의 데이터에 대해서는 퍼블릭 클라우드 컴퓨팅 환경으로의 업로드나 다운로드 모두 정책과 상황에 따라 전방위로 통제가 가능해야 한다. 이러한 기술 개발 및 구현을 통해 클라우드 컴퓨팅을 통한 중요 데이터 유출(3.4)을 방지할 수 있다.

4.4. 기존 보안 기술을 활용한 클라우드 컴퓨팅 보안

지금까지 살펴 본 새로운 클라우드 컴퓨팅 보안 기술 이외에도 기존 보안 기술들을 클라우드 컴퓨팅 영역에 활용하여 서비스 사용자들의 보안 관리를 지원하는 많은 기술 영역들이 존재한다. 이중 몇 가지를 살펴 보고자 한다.

첫 번째는 안티 바이러스 솔루션이다. IaaS 기반 클라우드 컴퓨팅 비즈니스 모델에서 활용 가능하며, 비활성화된 가상 서버 상의 바이러스 탐지 및 치료에 대한 숙제가 있긴 하나, 운영 중인 가상 서버에 대해서는 악성 코드에 대한 저항력을 제공한다. 악성 코드에 의해 클라우드 컴퓨팅 서비스에 대한 장애나, 이로 인한 중요 데이터에 대한 유출과 파괴(3.5) 등에 대한 저항력을 제공한다.

두 번째는 서버 보안 솔루션이다. 이 역시 IaaS 기반 클라우드 컴퓨팅 비즈니스 모델에서 활용 가능하며, 운영 중인 가상 서버 내에서 root를 포함한 사용자의 파일 시스템에 대한 접근, 변조, 삭제, 실행, 실행 정지 등을 통제할 수 있으며, 서버 내 사용자 행위에 대한 감사 데이터를 제공한다. 서버 보안 솔루션의 경우, 취약한 인증 정보 관리(3.3)와 이로 인해 서버가 탈취됨으로 클라우드 컴퓨팅을 통해 중요 데이터가 유출(3.4)되지 않도록 지원한다. 또한, 사용자 행위에 대한 상세한 감사 데이터 제공을 통해 미흡한 컴플라이언스 지원(3.6)을 보완한다.

세 번째는 취약점 진단 솔루션이다. 모든 클라우드 컴퓨팅 비즈니스 모델에서 사용 가능하며, 가상 서버와 클라우드 컴퓨팅 상에서 개발된 애플리케이션 등에 대해서 취약점을 탐지하고 알려 주며, 수정할 수 있도록 가이드를 제공한다. 이를 통해 취약한 인터페이스 연계와 안전하지 않은 개발(3.2)을 하지 않도록 지원한다.

네 번째는 패치 관리 솔루션이다. 이 솔루션 영역은 IaaS 기반 클라우드 컴퓨팅 비즈니스 모델에 적용되며, 가상 서버에서 운영되고 있는 서버, 데이터베이스, 애플리케이션에 대한 새로운 픽스팩이나 보안 패치들을 일괄 적용할 수 있다. 이를 통해 클라우드 컴퓨팅 내 중요 데이터를 보호(3.5)를 지원한다.

마지막 다섯 번째로 통합 보안 관제이다. 기존 통합 관제 영역을 확대하여 로그 수집, 관리 및 검색과 외부로부터의 보안 위협, 내부로부터의 정보 유출 등 다양한 정보 위협 상황을 모니터링하여 대응할 수 있도록 해주며, 기존 통합 보안 관제 솔루션에 빅데이터 기술이 채택되면서 이러한 영역으로의 확대 적용이 가능하게 되었다. 이를 통해 미흡한 컴플라이언스 지원(3.6)부터 퍼블릭 클라우드 컴퓨팅을 사용하면서 발생되는 위협에 대해 보다 앞서 인지하고 대응할 수 있도록 해 준다.

Ⅴ. 결 론

지금까지 그동안의 클라우드 컴퓨팅 하에서의 보안 위협과 위험에 대해 분석 및 고찰해 보았다. 또한, 그 연구들을 바탕으로 퍼블릭 클라우드 컴퓨팅 서비스 사용자 관점에서 고려해야 할 보안 위협에 대해 도출하고, 그에 대해 다양한 퍼블릭 클라우드 컴퓨팅 보안 기술 소개를 통해 대응 방안에 대해 알아 보았다. 분명 클라우드 컴퓨팅 서비스 제공자가 고려해야 할 보안 위험과 클라우드 컴퓨팅 서비스 사용자가 고려해야 할 보안 위험은 다르다. 또한, 각 퍼블릭 클라우드 컴퓨팅 서비스 모델마다 적용할 수 있는 보안 기술의 한계와 대응할 수 있는 보안 위험도 달랐다. 본 소고를 시작으로 하여, 다양한 클라우드 컴퓨팅 비즈니스 모델과 서비스 형태에 따라, 그리고 서비스 제공자와 사용자를 위한 특화된 보안 가이드라인과 보안 기술들이 나오길 바라며, 본, 기고의 끝을 맺는다.

참고문헌

[1] Jay Heiser, Mark Nicolett, “Assessing the Security Risks of Cloud Computing”, Gartner, pp. 2-4, 2008.

[2] “Top Threats to Cloud Computing Survey Results Update 2012”, CSA, 2012.

[3] “Cloud Computing Security Risk Assessment”, ENISA, 2009.

[4] “Cloud Computing Synopsis and Recommendations, Special Publication 800-146”, NIST, 2012

〈著者紹介〉

박 형 근 (Hyungkeun Park)
2000년 7월 : 고려대학교 화학공학과 졸업
2000년 10월 ~ 현재 : 한국 IBM 보안 솔루션 사업부 기술팀 리더, 現 방송통신위원회 미래전략 IT 자문 위원 - 클라우드 컴퓨팅 보안 분야, 現 국제 ITI Korean Cyber Security Group 리더, 現 정보보안 전문 커뮤니티 시큐리티플러스 대표 운영자, 現 국제 정보보안 포럼, Open Group, OASIS, TCG, ISC2, ISACA 정회원, CISSP, CISA, CGEIT
<관심분야> 정보보호