

Publication: ZDNet Korea

Date: 06/04/2011

Subject: The Security Issue as Cloud Conundrum, What is the Problem

[http://www.zdnet.co.kr/news/news\\_view.asp?article\\_id=20110406165046&type=xml](http://www.zdnet.co.kr/news/news_view.asp?article_id=20110406165046&type=xml)

클라우드의 난제 '보안', 무엇이 문제인가

경문희 기자 yomi@zdnet.co.kr 2011.04.06 / PM 05:21 클라우드, 넷이벤츠, 보안

[황카워(말레이시아)-경문희 기자] 클라우드를 언급할 때 빠지지 않는 이유는 보안이다. 기업이 IT자산을 내부에 가지고 있지 않다는 점이 정보 유출에 대한 불안감을 가중시키기 때문이다.

보안업계 역시 클라우드 보안에 주목하면서 적극적인 움직임을 보이지만 여전히 세간의 불안감을 지우기엔 역부족이다. 관련 정책 표준들도 이제 막 하나둘씩 수립되기 시작하는 과도기다. 클라우드의 주목도가 빠르게 높아지는 데 반해 보안 표준이 따라오지 못하는 상황인 셈이다.

클라우드 보안에서 가장 열된 토론이 벌어지는 주제는 보안의 책임 소재다. 명확한 규정이 정해져있지 않은 현상들이 논란을 더 키우고 있다.

대니 슈 트랜드미이크로 APAC 시니어디렉터는 6일 말레이시아 황카워에서 개최된 넷이벤츠 APAC 2011에서 "사실 클라우드는 표준이나 인증 측면에서는 많이 부족하다"며 "라 벤더들이 다른 표준을 채택하고 있는 상황"이라고 말했다.



▲ 팀 딜런 IDC AVP 리서치 담당

클라우드 보안의 책임소재는 계약에 따라 달라진다. 서비스수준협약(SLA)에 대한 이야기가 나오는 것도 그 때문이다. 팀 딜런 IDC 리서치 담당은 "향후 SLA 이슈가 강력하게 대두될 것"이라고 내다봤다.

필연적으로 클라우드를 도입하려는 입장에서는 체크해야할 점이 많다. 네트워크 보안, 퍼포먼스, 애플리케이션, 소셜미디어 등이 포함된다.

나타사 타마스카 켈렌드 제품마케팅 부사장은 클라우드 보안의 구체적인 방향을 모바일로 요약했다. 그는 "일드 디바이스들은 더욱 더 단순해지고 있다"며 "최근 확산되고 있는 스마트폰, 태블릿PC 등은 보안이 강화돼있지 않은 디바이스"라고 말했다. 네트워크 보안이 이슈로 떠오르는 이유를 설명한 것이다.

현재 클라우드를 이용하는 디바이스는 점점 더 해킹에 취약해지는 반면, 보안에 대한 요구는 더욱 높아지고 있다. 때문에 다수 업체가 새로운 서비스를 출시하는 방식으로 보안 책임을 추궁 받지 않기 위해서 노력하는 추세다.



▲ 대니 슈 트랜드미이크로 시니어디렉터, 진 강 스프린트 아시아 부사장, 나타사 타마스카 켈렌드 부사장(좌부터)

일일이 따질 경우 클라우드에서 보안을 민감하게 만드는 것은 해킹보다 내부 유출이다. 기존 보안 기술은 클라우드 환경에서도 적용되기 때문에 해킹 등 외부로부터의 침입에는 비교적 강력한 방어 시스템을 갖추 수 있다. 오히려 클라우드 사업자 직원이 고의적으로 정보를 유출하거나, 관리 부주의로 발생하는 정보유출이 더 우려된다.

슈 디렉터는 "정보는 해킹 프로그램에 감염된 USB를 사용하는 방법으로 간단하게 유출될 수 있다"며 "때문에 클라우드에 저장된 데이터를 암호화시키는 작업이 필요하다"고 설명했다.

그는 트랜드 미이크로의 시큐어 클라우드라는 제품을 소개했다. 그는 "이 제품은 퍼블릭 클라우드에 저장된 데이터를 암호화시켜 클라우드 사업자와 계약을 종료하더라도 데이터베이스 내에 저장된 정보는 안전하다"고 말했다.

클라우드 보안으로 인해 발생하는 서비스품질 저하도 우려되는 대목이다. 여러 보안 솔루션을 이것저것 복잡하게 클라우드 서비스에 적용하면 성능과 용량을 떨어뜨릴 수 있기 때문이다. 고객들이 클라우드 이 용자세를 고려하지 않게되는 우를 말하는 셈이다.

이에 대해 진 강 스프린트 아시아 부사장은 "최근 가상화 환경을 다룰 수 있는 새로운 형태의 보안 관련 애플리케이션이 나오고 있다"며 "이런 보안 제품들은 물리적 서버의 리소스를 줄여주면서도 고가용성을 제공한다"고 말했다.

최근 확산되고 있는 소셜미디어 보안에 대한 논의도 이뤄졌다. 악성코드가 실려진 링크가 확산되는 경우, 엄청난 정보 유출이 예상되기 때문이다. 토론은 소셜미디어를 통한 악성코드 링크 확산을 방지하는 방안은 현재까지는 완전방지 솔루션 별로 수립됐다.

슈 디렉터는 "소셜미디어로 연결된 링크가 악성 링크인지 파악할 수 있도록 하는 기술을 사용해 스캐닝해야 한다"며 "데이터센터와 이용자들이 악성 사이트에 접속하지 않도록 하는 것이 중요하다"고 말했다.