Executive 시리즈

CIO를 위한 보안 필수 요소

클라우드 보호를 위한 필수 교육

주요 사항:

다른 위험들과 마찬가지로, 클라우드 컴퓨팅으로 인해 발생하는 교육, 우수 사례, 좋은 툴과 같은 것들은 다루기 힘든 문제가 아닙니다. IBM은 7가지 보안 필수 요소를 사용해 클라우드를 더욱 효과적으로 보호합니다.

CIO 대부분은 클라우드 컴퓨팅의 장단점에 대해 너무나도 잘 알고 있습니다. 클라우드의 유연성, 잠재적인 비용 절감, 사용의 용이성 때문에 이처럼 전문적으로 관리되는 원격 데이터 센터들은 전세계적으로 빠르게 확산되고 있습니다. 그러나 많은 잠재적인 고객들이 그럴 만한 이유로 인해 아직은 망설이고 있습니다. 미국과 유럽의 클라우드 서비스 제공업체들의 60% 이상이 조사 대상이었던 Ponemon 연구소의 최근 보고에 따르면 그들이 보유하고 있는 클라우드 애플리케이션이 충분히 안전을 보장받을 수 있는지 확신하지 못하는 것으로 조사되었습니다. 또한, 이러한 클라우드 제공업체 중 대다수가 클라우드 보호는 그들의 책임이 아니며, 고객에게 책임이 있다고 믿고 있었습니다.[1] 이러한 클라우드의 사용은 민감한 사안을 담고 있는 파일들이 다른 기업의 데이터와 섞이는 것은 아닌지 고객들로 하여금 의구심을 갖게 만듭니다. 따라서 고객은 데이터의 백업 방법이나 클라우드의 정전 상황 또는 클라우드 제공업체의 폐업 상황을 위한 대처 방안에 대해 질문할 수도 있습니다.

이러한 질문들이 중요하기도 하지만, 클라우드 업계의 CIO들이 직면하고 있는 주요 보안 문제들(예: 권한을 부여 받은 비 IT 전문가들의 증가)에 비하면 정말 사소한 것들입니다. 클라우드 컴퓨팅으로 인해 기업 전반에 걸쳐 수백 또는 수 천명의 선의의 사용자들이 지휘권을 가지게 되었습니다. 이것은 이전에는 기술을 오직 소비만 했던 사람들이 현재는 시스템을 구축할 수 있는 권한을 가지고 있음을 의미합니다. 그러나 이들은 기업 전체를 위험에 빠트릴 수도 있는 잠재적인 취약점들에 대해서는 이해하지 않고 있습니다. 기존에는 이러한 작업을 숙련된 전문가들(CIO의 고유 팀)이 처리해 왔습니다. 이 전문가들은 위험과 관련된 교육을 받고, 시스템 구성과 소프트웨어 유지보수 및 액세스 제어와 같은 문제에 있어 최상의 사례들을 따릅니다. 그러나 클라우드의 경우 이러한 핵심층은 자체적인 제어력의 대부분을 양도하게 됩니다. 이처럼 사용자에게 양도된 새로운 권한은 사용자 스스로가 자신이 구축하는 것이 무엇인지, 그리고 그것의 유지보수 방법에 대해 실제로 이해하지 않는 한 심각한 위험을 초래할 수도 있습니다.

종종 간과되기도 하는 중요한 해법 하나는 바로 교육입니다. 안전한 클라우드 환경을 구축하기 위해서는 모든 사람들에게 클라우드의 똑똑하고 주의 깊은 절차들에 관해 지시하는 광범위한 전사적 노력이 뒷받침되어야 합니다. 여기에는 위험 인식 문화를 만드는 것도 포함됩니다. 예를 들면, 다가올 고객 회의를 위해 호스팅 제품의 데모를 준비하는 영업 담당자는 적절한 절차에 따라 정보에 입각한 방법으로 위험 인식 문화를 창조해야 합니다. 클라우드가 제공하는 새로운 성능 검토 애플리케이션을 준비하는 인적 자원 관리자들도 마찬가지입니다. 인적 자원 관리자의 경우, 안전하지 못한 이미지 사용에서부터 비밀번호 공유 또는 용도 변경과 같은 규정을 준수하지 않는 행위들로 인해 외부로부터 공격을 받을 수 있으며, 잠재적으로는 기업을 위태롭게 만들 수 있음을 알아야 합니다. 클라우드 제공 서비스를 개발하는 모든 사람들은 사실상 IT 설계자가 됩니다. 따라서 이들 모두는 위험에 관해 이해하고, 적합한 교육을 받아야 하며, 책임을 가져야 합니다.

조사 대상인 미국과 유럽의 클라우드 서비스 제공업체 중 60% 이상이 그들이 보유한 클라우드 애플리케이션의 안전이 충분히 보장되는지에 대해 확신하지 못한다고 답했습니다.[1]

출처: Ponemon 연구소

클라우드 사용 경험은 의심하지 않는 사용자를 안심시켜 보안을 허술하도록 만들 수 있기 때문에 이러한 노력은 특히 중요합니다. 클라우드가 사용자에게는 그들의 스마트폰과 태블릿을 위한 앱스토어처럼 편안하고 친근한 상용 서비스처럼 느껴질 수 있습니다. 하지만 고객들은 클라우드를 마치 각자의 집을 차지하고 있는 외딴 마을 정도로 생각해야 합니다. 이 마을에는 합리적인 법률과 근면한 경찰서가 있을 수 있지만 그들의 문을 잠그고, 모션 감지기를 설치하며, 그들의 열쇠를 아이들에게 무조건 빌려주지 않는 것은 집 주인에게 달려 있습니다. 비록 대부분의 클라우드가 숙련된 전문가들에 의해 실행되며 보안 서비스들을 제공하지만, 사용자들의 경계심과 상식도 필요합니다.

[1] "클라우드 컴퓨팅 제공업체들의 보안 연구", Ponemon 연구소: 2011년 4월 연구 보고서(http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf)

고객들은 클라우드를 마치 각자의 집을 차지하고 있는 외딴 마을 정도로 생각해야 합니다. 이 마을에는 합리적인 법률과 근면한 경찰서가 있을 수 있지만 그들의 문을 잠그고, 모션 감지기를 설치하며, 그들의 열쇠를 아이들에게 무조건 빌려주지 않는 것은 집 주인에게 달려 있습니다.

일단 안전한 환경이 마련되면 그것을 유지하는 것은 다음 문제입니다. 환경은 변하기 마련입니다. 클라우드 사용자는 "보안 드리프트"를 경계해야 합니다. 예를 들면, 제품 데모를 위해 클라우드를 사용하는 영업 담당자는 시스템을 위해 중요한 보안 패치를 포함하는 소프트웨어의 최신 업데이트를 다운로드하고 설치하는 것을 게을리 할 수도 있습니다. 이것이 고객에게 제품을 제공해야 하는 즉각적인 필요에 영향을 주지 않을 수도 있지만, 클라우드 기반의 다른 환경에 위험을 초래할 수도 있습니다.

다른 위험들과 마찬가지로, 클라우드 컴퓨팅으로 인해 발생하는 교육, 우수 사례, 좋은 툴과 같은 것들은 다루기 힘든 문제가 아닙니다. IBM은 7가지 보안 필수 요소를 사용해 클라우드를 더욱 효과적으로 보호합니다.

클라우드 컴퓨팅을 위한 보안 필수 요소

1. 교육

클라우드는 대부분의 사용자들이 그들이 사용하는 이미지를 액세스하고 커스터마이즈 할 수 있도록 하면서 IT 인력의 기존 업무 대부분을 분배합니다. 사용자는 시작하기 전에 먼저 위험과 책임에 대해 이해해야 하며, 사용자가 이해하고 존중하는 우수 사례들을 따라야 합니다. 위험 인식 문화를 창조하는 것은 보안을 위해 매우 중요하며, 특히 클라우드 컴퓨팅에 있어 더욱 중요합니다.

2. 데이터 보호

데이터를 암호화해야 합니다. 데이터에 액세스할 수 있는 개인을 식별하고, 개인별 업무상 필요한 것에만 각각의 액세스를 제공합니다. IT 팀은 권한이 없는 개인 또는 외부인이 백 채널(back channel)을 통해 액세스할 수 없도록 이러한 활동을 적절히 감시해야 합니다.

3. 보안 환경 유지

특히 대규모 클라우드 환경에서는 이미지를 사용하기 쉽고, 위험하게도 이러한 이미지의 통제권을 쉽게 잃을 수도 있습니다. 따라서 이러한 경우 보안 패치에 뒤쳐지는 위험을 감수하게 됩니다. 패치되지 않은 소프트웨어는 악성 코드 감염 및 데이터 유출의 위험을 증가시킬 수 있으므로 각 이미지에 대한 상세 기록을 보유하며, 안전하게 구성된 최신 필수 데이터에 대한 접근 인원을 제한하는 것이 중요합니다.

4. 지속적인 테스트 수행

컴퓨팅 툴과 환경은 배치 이전과 이후 모두 테스트해야 합니다. 취약점들은 장시간 개방되는 경향이 있으므로 검증과 평가가 상당히 중요합니다. 이러한 검증과 평가에는 초기 비밀번호가 사용되지 않는다는 것과 네트워크 인터페이스가 출입구나 창문을 개방하지 않는다는 것을 확인하는 테스트가 포함되어야 합니다.

5. 벤더 검증

클라우드 벤더를 잘 알고 신뢰하십니까? 그리고 이 벤더가 보안 요건을 포함한 귀하의 비즈니스 요건과 요구사항을 이해하고, 충족하며, 준수하고 있습니까? 위의 질문들에 대한 답은 모두 '예'이어야 합니다. 만약 귀하가 벤더와 각자 다른 길을 간다면 데이터는 어떻게 될까요? 따라서 이러한 사항은 종료 시점이 아닌 시작할 때 파악해야 합니다.

6. 거버넌스 강화

심지어 10,000 마일 떨어져 있는 데이터라 하더라고 끊임없이 변화하는 거버넌스를 준수해야 합니다. 각 기업은 데이터에 대한 정기적인 감사를 수행할 수 있어야 하며, 준수 보고서를 만들어야 합니다. 또한 조정이 필요한 경우 데이터가 현장에 보관되어 있는 것처럼 자유롭게 조정할 수 있어야 합니다.

7. 지역 고려

데이터 센터의 위치는 상당한 차이를 만들 수 있습니다. 일부 지역에서는 국경 내에 위치한 데이터에 대한 권리를 정부가 가지고 있습니다. 어떤 장소에서는 정치적 불안 또는 정전으로 인해 데이터 센터 운용에 지장이 생길 수도 있습니다. 따라서 귀하는 클라우드 제공업체뿐 아니라 지역에도 투자를 하고 있는 것입니다.

CIO를 위한 보안 필수 요소

IBM에서는 위험을 제어하기 위한 혁신과 필요성 사이에 균형을 찾는 접근법에 필수적인 훈련들이 포함되어 있습니다. 이러한 훈련들은 지금처럼 끊임없이 연결되는 시대에서 보안 정보로 가는 길을 제공합니다.

클라우드를 안전하게 이용하려면 어떻게 해야 할까요?

액세스 및 교육의 균형 유지

대화 참여

추가 기사나 CIO를 위한 보안 필수 요소에 대한 자세한 정보가 필요하거나, 다른 보안 리더들과 생각을 공유하길 원하실 경우, www.ibm.com/smarter/cai/security에 가입하시기 바랍니다.

저자 소개

Kristin Lovejoy, IBM Office of the CIO의 IT Risk 부사장

연락처: klovejoy@us.ibm.com

IBM Center for Applied Insights 정보

IBM Center for Applied Insights는 고객에게 새로운 가치로 나아가는 길을 안내하기 위해 폭넓은 컨텐츠와 분석적 전문 기술을 통합합니다. 본 센터에서는 기업의 행동을 촉구하고자 연구를 실시하고, 실용적인 지침과 함께 자산 및 툴을 구축하고 있습니다.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
March 2012

WGW03004-USEN-00