클라우드 환경의 데이터 보호에 대해 반드시 알아야 할 사실

VERITAS™

스폰서 컨텐트

CIO

IDG 제공

클라우드 인프라스트럭처는 설정 및 관리가 용이하므로 클라우드가 "한 번으로 설정 완료"되는 것으로 오해하기 쉽습니다. 실제로 클라우드 제공업체는 로드 밸런싱, 인프라스트럭처 최적화, 루틴 시스템 관리와 같은 작업을 간소화하여 매우 우수한 서비스를 지원하면서 예측 가능한 성능과 무한에 가까운 확장성을 제공합니다. 게다가 자체 인프라스트럭처에 대해 강력한 보안도 유지합니다.

하지만 개별 고객 인스턴스 및 데이터 보호 관련 문제에 있어서는 상황이 조금 복잡해집니다. 대부분의 클라우드 제공업체는 고객이 직접 본인의 계정에 대한 액세스를 감시하고 스스로 데이터를 보호하도록 규정합니다. 고객은 클라우드 인프라스트럭처의 단순함에 매료되어 취약한 암호로 보호되는 클라우드 서버가 고객의 자체 데이터 센터에 있는 서버만큼이나 취약하다는 사실을 쉽게 잊어버리곤 합니다.

베리타스의 클라우드 솔루션 마케팅 담당 매니저인 Anthony Cusimano는 대부분의 경우 클라우드 인프라스트럭처와 로컬 인프라스트럭처의 유일한 차이점이 그저 '장소'라고 생각한다고 말합니다. 그는 "클라우드가 온프레미스 인프라스트럭처와 다르다는 생각은 옳지 않습니다. 규모와 위치가 다를 뿐 기본적으로 둘다 데이터 센터인 셈이죠. 다른 누군가의 인프라스트럭처에서 사용자의 자체 데이터 센터와 동일한 수준의 보안을 제공할 것으로 믿는 것은 위험한 생각입니다."라고 말합니다.

실제로 클라우드상의 보안 리스크가 더 클 수 있으며, 이는 종종 방화벽, VPN, 네트워크 세그먼트화, 기타 온프레미스 환경에서 일반적으로 수행되는 보호 기능으로 액세스가 보호되지 않기 때문입니다. Cusimano는 고객의 클라우드 설치 공간이 늘어남에 따라, "수백 명의 사람들이 중요한 정보에 액세스할 가능성이 있습니다. 사회 공학 기법 또는 랜섬웨어 공격의 경우, 단 하나만 손상되어도 문제가 됩니다."라고 말합니다.

데이터 보호에 관한 오해

클라우드 제공업체가 표준 서비스의 일부로 데이터 보호를 제공한다는 사실은 흔히 볼 수 있는 또 하나의 잘못된 상식입니다. 실제로는 그 어떤 주요 클라우드 제공업체도 핵심 서버 인스턴스에 백업 기능을 번들로 제공하지 않습니다. 단, 해당 서비스가 유료 옵션으로 제공될 수는 있습니다.

이에 관해 베리타스 수석 엔지니어인 Dave Little은 "클라우드 제공업체에서 여러분의 데이터를 보호하고 검증할 것이라는 기대는 하지 마십시오."라고 말합니다.

그럼에도 불구하고, 이러한 오해가 만연한 상황입니다. 최근 베리타스가 1,200명의 IT 및 비즈니스 의사 결정자를 대상으로 설문 조사를 실시한 결과, 응답자의 83%가 클라우드 제공업체에서 표준 서비스에 데이터 보호 기능을 번들로 제공한다고 생각하는 것으로 밝혀졌습니다.[1]

이러한 혼란이 발생한 이유로 클라우드 제공업체가 용량 관리 또는 로드 밸런싱 용도로 여러 데이터 센터 전반에서 데이터를 복제하는 관행을 들 수 있습니다. 하지만 그렇다고 보호가 보장되는 것은 아니며, 이는 고객이 기본적인 관리 프로세스가 무엇인지 제어할 수 없기 때문입니다. 더욱이 클라우드 제공업체는 법적 책임부터 보험료에 이르는 여러 다양한 이유로 고객 데이터의 무결성을 보장하지 않습니다. 다시 말해, 데이터 보호는 전적으로 고객의 책임입니다.

클라우드 데이터 보호에 대한 오해를 바로잡는 것이 특히 중요한 이유는 PC 및 서버의 데이터를 암호화하고 복호화 코드를 교환하는 조건으로 몸값 지불을 요구하는 새로운 형태의 치명적 악성 코드인 랜섬웨어의 등장과 관련되어 있습니다. Cybersecurity Ventures의 예측에 따르면, 2018년 한 해 동안 발생한 랜섬웨어 피해 비용이 총 80억 달러를 넘었으며, 올해는 14초에 한 번꼴로 랜섬웨어 공격이 발생할 것입니다.

랜섬웨어 공격은 적절한 백업이 수행되지 않는 한 기업에 심각한 피해를 입힐 수 있습니다. 이 악성 코드 형식의 초기 버전은 주로 PC를 표적으로 했으며, 최근에는 서버와 스토리지 디바이스를 표적으로 삼은 보다 정교한 랜섬웨어의 변종이 등장했습니다. 더욱 우려되는 상황은 현재 수많은 변종이 자가 증식하면서, 일단 시스템 한 대가 감염되면 네트워크 전체에 확산되어 시스템 수백 대를 손상시킬 수 있다는 점입니다. 따라서 이러한 감염의 출처와 범위를 특정하기가 더욱 어려워집니다.

"악성 코드는 발견되지 않은 상태로 은밀하게 활동하면서 클라이언트 데이터와 리소스를 도용할 수 있습니다."라고 Cusimano는 말합니다.

대부분의 랜섬웨어는 사회 공학 기법을 통해 전파되는데, 특히 피싱 공격을 매개로 합니다. 사용자가 이메일에서 알 수 없는 링크를 누르면 부지불식간에 악성 코드가 설치되고 확산됩니다. 랜섬웨어 공격은 대상을 구분하지 않으므로 사용자가 클라우드 서비스에 로그인하면 감염이 클라우드 인스턴스로 전파되고 다른 가상 서버까지 감염시킬 수 있습니다.

의료 및 정부 기관은 특히 표적이 되기 쉬운데, 예산이 한정되어 장비에 최신 패치 프로그램을 업데이트하지 못할 가능성이 높기 때문입니다. 일례로 2019년 볼티모어시에 발생한 공격으로, 한 달 동안 주요 서비스가 중단되고 1,800만 달러 이상의 비용이 소요되었습니다. 2017년 FedEx는 랜섬웨어 공격으로 인해 3억 달러에 달하는 분기별 손실을 입기도 했습니다.

유일한 보호책은 백업입니다

현재 랜섬웨어를 완벽하게 차단할 수 있는 방법은 없습니다. 유일한 보호책은 중요 데이터를 자주 백업하여 공격을 당한 장비를 제거하고 데이터를 신속하게 복원하는 것입니다. 사용자는 로컬 및 클라우드의 여러 미디어에 대한 스냅샷 이미지와 백업을 포함하여 이전보다 다양한 옵션을 선택할 수 있습니다. 반면 이러한 옵션의 다양성으로 인해 복잡성이 증가하기도 합니다. 각각의 백업 옵션에는 나름의 장단점이 있습니다.

예를 들어 스냅샷은 복원 시간이 가장 짧다는 장점이 있는 반면, 성능이 저하되고 일부 스토리지 미디어에서는 작동하지 않으며 저장된 모든 데이터의 전체 이미지를 캡처하지 않는다는 단점이 있습니다. 테이프 백업의 경우 운영 비용이 상대적으로 저렴한 대신, 장비의 설치 및 유지 보수에 많은 비용이 들고 개별 파일에 대해 신속한 액세스를 허용하지 않는다는 단점이 있습니다. 디스크에 백업하면 액세스 문제는 해결되지만 비용이 많이 듭니다. 클라우드 백업은 대역폭의 제한이 있고 경우에 따라 규정에 의해 금지될 수 있습니다.

고가용성(HA) 서비스는 아무런 해결책이 되지 않습니다. HA는 미러링된 서버나 스토리지 디바이스로 데이터를 자동 복제하여 서버 장애 또는 가동 중단으로부터 보호하지만, 전체 백업을 대체하지는 못합니다. 또한 HA는 악성 코드와 데이터 삭제를 복제하면서 랜섬웨어 공격의 영향력을 가중시킬 수도 있습니다.

Little은 "HA 서비스는 클러스터링 또는 복사를 통해 애플리케이션의 가용성을 지원하여 다른 서버나 디스크가 대체할 수 있게 하지만, 동시에 데이터 삭제 또는 손상 시에도 그러한 현상이 빠르게 복제된다는 문제가 있습니다."라고 말합니다.

최적화된 백업 전략

최상의 해결책은 상황에 적합한 최선의 옵션을 선택할 수 있는 유연성을 제공하는 것입니다.

"복구할 수 있는 장소가 많고 사용 가능한 미디어 유형이 많을수록 데이터의 보안 및 복구 가능성 역시 높아집니다."라고 Cusimano는 말합니다.

많은 기업에서 이것은 라이프사이클의 서로 다른 지점에서 구축할 수 있는 백업 솔루션의 조합을 사용한다는 것을 의미합니다. 예를 들어, 어떤 기업이 두 대의 클라우드 서버와 한 개의 디스크에 중요 데이터를 백업하여 데이터 보호 및 복구 속도를 최적화하려 합니다. 하지만 일주일 후, 해당 데이터의 중요성이 낮아져 온프레미스 테이프와 한 개의 클라우드 아카이브로 옮겨질 수 있습니다.

이와 같이 니즈는 새로운 기술 옵션의 등장, 가격 변경, 규제 요건 강화, 도입, 기타 여러 요인으로 인해 시간이 지나면서 계속 바뀔 수 있습니다. 또한 고객이 백업 전략을 세밀하게 조정하여 테이프 및 기타 아카이브 스토리지 기술과 같이 계층화된 옵션의 장점을 활용하려 할 수 있습니다. 이때 단일 백업 솔루션으로 이러한 전환을 유연하고 자동화된 방식으로 수행할 수 있습니다.

Little은 백업이 강력한 데이터 보호 훈련의 일환으로 고객이 어떤 데이터를 보유했는지, 어떤 수준의 백업 보호를 제공할지, 복구 요건은 무엇인지 등을 파악하는 것부터 시작된다고 설명합니다.

그는 "항상 복구 요건을 중심으로 전체 백업 솔루션을 설계해야 한다"고 합니다. 이러한 니즈를 파악하는 것은 데이터 보호는 물론, 비용 절감에도 도움이 됩니다. "대부분의 사람들이 데이터를 너무 오래 너무 많이 보관합니다."라고 Little은 덧붙입니다. 예를 들어, 더 적은 비용으로 데이터를 안전하게 아카이빙할 수 있음에도 백업 서버에 오래된 데이터를 계속 유지하는 경우가 있습니다.

Cusimano의 백업 제안

가능한 자주, 더 많이 백업하십시오. 최적의 일정은 고객의 비즈니스에 따라 다르며 분 단위에서 일 단위까지 다양합니다. 좋은 전략은 다운타임 비용과 백업 비용을 비교하여 둘 사이의 균형을 맞추는 것입니다.

여러 위치와 클라우스에 백업하십시오. 백업 옵션을 다양하게 사용할수록 데이터 유출 리스크가 줄어듭니다. 제어용으로 온프레미스 인프라스트럭처를 활용하고 편의를 위해 클라우드 백업을 사용합니다. 네트워크에 연결되지 않고 "에어 갭(air gap)"된 서버에 특히 중요한 데이터를 백업할 수도 있습니다.

복구 시간 목표를 명확하게 설정하고 그에 대한 테스트를 시행하십시오. 테스트는 매우 중요합니다. 예기치 않은 사고는 피할 수 없으며 테스트를 자주 수행하여 예측 능력을 높일 수 있기 때문입니다. 미디어 장애에 대한 좋은 대비책이기도 합니다.

랜섬웨어 공격을 구체적으로 테스트하십시오. 최신 패치 프로그램과 안티바이러스 정의를 확보하는 것은 늘 권장되지만, 이것만으로 랜섬웨어를 완벽하게 차단할 수는 없습니다. 대량의 데이터가 갑자기 잠금 상태가 되는 시나리오를 테스트하면서 신속한 복구 계획을 개발합니다.

우수한 보안 프랙티스를 사용하십시오. 로그인 인증 정보를 자주 변경하고 액세스 디렉토리도 정기적으로 검토해야 합니다. 백업 인프라스트럭처에는 자체적으로 구성한 액세스 제어 및 정책 세트를 갖추고 기본 IT 네트워크를 침해한 공격자들이 백업 데이터를 손상시키지 못하도록 합니다.

가상 머신 레벨에서 백업을 수행하여 시스템 상태를 신속하게 복구하십시오. 통합적인 데이터 백업을 대체할 수는 없지만 총 다운타임 시간을 대폭 줄일 수 있습니다.

클라우드는 기업의 민첩성과 속도를 향상시키는 우수한 툴이지만, 클라우드 서비스가 제공하는 데이터 보호의 한계를 인식하고 그에 맞춰 적절하게 계획을 수립해야 합니다. 효율적인 백업 및 복구 인프라스트럭처를 구현하면 랜섬웨어 같은 새로운 보안 위협에 대비하면서 운영 비용을 절감하고 유연성을 향상시킬 수 있습니다.

Veritas NetBackup의 통합 데이터 보호는 소프트웨어를 기반으로 하는 벤더 중립적인 플랫폼으로, 기반 환경보다 정보의 가치에 중점을 두고 있습니다. 규모에 관계없이 모든 워크로드를 보호하고 여러 포인트 제품 간에 고민할 필요가 없습니다. NetBackup은 어디서든 레질리언스 및 온디맨드 액세스를 보장하며 세계 각처에서 갈수록 증가하는 데이터 저장 관련 리스크 및 비용을 줄일 수 있게 도와줍니다.

자세한 내용은 www.veritas.com/ko/kr/solution/cloud에서 확인하십시오.

[1] "Truth in Cloud Report," Veritas Technologies, 2017년