

Microsoft 365의 데이터 안전을 위협하는 6가지 사각 지대와 해결 방법

Microsoft 365의 데이터 안전을 위협하는 6가지 데이터 보호의 구멍과 해결 방법

Microsoft 365를 사용하고 있다면 가용성이 매우 높은 애플리케이션에 안정적으로 액세스할 수 있습니다. Microsoft는 자체 클라우드 인프라를 갖추어 운영하는 것으로 높은 평판을 얻고 있지만 Microsoft 365 데이터 보호를 책임지지는 않습니다. 사실 Microsoft에서는 사용자가 직접 서드 파티 백업 앱이나 서비스를 디플로이하여 데이터를 보호할 것을 매우 명시적으로 권고합니다. 다음은 Microsoft 서비스 계약 내용의 일부입니다. “당사는 서비스가 지속적으로 운영되도록 최선을 다하지만 모든 온라인 서비스는 중단 및 정지가 발생하는 경우가 종종 있으며, Microsoft는 이로 인해 발생할 수 있는 모든 중단 또는 손실에 대해 책임을 지지 않습니다. 중단 발생 시, 저장한 **콘텐츠 또는 데이터를 검색하지 못할 수도 있습니다.** 서비스에 저장하거나 **서드 파티 앱 및 서비스를 사용하여 저장하는 방식으로 콘텐츠와 데이터를 정기적으로 백업할 것을 권장합니다.**”

이러한 내용이 있음에도 많은 비즈니스에서는 여전히 Microsoft가 Microsoft 365 데이터에 대해 완전한 보호와 장기적인 보존을 지원한다고 생각합니다. 그러나 Microsoft에서는 의도치 않은 데이터 삭제 및 맬웨어 공격 등 가장 일반적이면서도 중대한 데이터 손실 문제로부터 보호를 거의 지원하지 않습니다. 이러한 오해로 인해 많은 비즈니스에서는 불쾌하고 당황스러운 경험으로 이어질 수 있는 데이터 보호 격차가 발생합니다. IT 리더는 비즈니스의 Microsoft 365 데이터 보호 책임이 자신에게 있음을 인식해야 하며 일반적인 데이터 손실 원인으로부터 보호할 수 있는 포괄적인 백업 솔루션을 구현해야 합니다.

모든 비즈니스가 Microsoft 365 데이터에 대해 고려해야 하는 6가지 주요 데이터 보호 영역

1. 의도치 않은 데이터 삭제

데이터 보호 위험 요소: 일상적인 작업 과정에서 직원은 Microsoft 365 사용자 프로필, Exchange Online 이메일 및 첨부 파일, OneDrive for Business 파일, Teams 및 SharePoint Online 콘텐츠를 정기적으로 삭제합니다. 이러한 삭제는 우발적이거나 의도적일 수 있으며 나중에 후회하는 상황으로 이어질 수도 있습니다. 그러나 어느 경우이든 결과적으로 중요한 데이터 손실이 발생할 수 있습니다.

Microsoft 취약점: 이런 종류의 일상적인 리소스 삭제는 네트워크 전반에서 정기적으로 반복됩니다. 리소스의 수명도 문제를 악화시키는 요인입니다. 오래된 데이터일수록 영구 삭제되어 복구가 불가능할 수 있습니다. 최신 리소스를 비교적 최근에 삭제한 경우, 일시 삭제된 파일 및 이메일은 휴지통 또는 복구 가능한 항목 폴더에서 단기적으로 복구할 수 있으므로 문제가 그리 심각하지 않습니다.

2. 보존 정책 문제

데이터 보호 위험 요소: Microsoft 365 데이터 보존 정책에서 우선순위를 변경하거나 잘못 조정하면 데이터가 영구적으로 삭제될 수 있습니다. 이러한 위험의 경우 보존 정책의 정기적인 검토 및 업데이트를 통해서만 부분적으로 완화할 수 있습니다.

Microsoft 취약점: Microsoft 365 고객은 보존 정책을 관리할 책임이 있지만, 이유를 불문하고 기존 보존 정책이 만료되어 영구 삭제가 발생하면 Microsoft에서는 삭제된 리소스를 복구할 수 없습니다.

3. 내부자 보안 위험

데이터 보호 위험 요소: 일상적이고 악의적이지 않은 삭제 위험 이외에도, 양심을 품거나 계약이 종료된 직원, 계약자 또는 파트너가 데이터를 악의적으로 변경하거나 파괴하지 않도록 Microsoft 365 데이터 및 리소스를 안전하게 보호해야 합니다.

Microsoft 취약점: 비교적 최신 리소스가 삭제되는 경우를 제외하고, Microsoft는 내부자가 Microsoft 365 데이터를 악의적으로 파괴하거나 변경하지 못하도록 보호하지 않습니다.

4. 외부 보안 위험

데이터 보호 위험 요소: Microsoft 365 데이터는 다양한 맬웨어 위협, 특히 온라인으로 금전적 대가를 받을 때까지 사용자 데이터를 암호화하고 인질로 삼는 랜섬웨어에 의한 파괴 또는 변경에 취약할 수 있습니다.

Microsoft 취약점: Microsoft는 랜섬웨어와 같은 맬웨어 공격에 대해 매우 제한적인 보호만을 제공하며, 맬웨어에 의해 암호화되거나 변경된 파일을 공격받기 이전 상태로 복원하는 기능을 매우 한정적으로 지원합니다.

5. 온프레미스 기반 Microsoft Office에서 마이그레이션

데이터 보호 위험 요소: 비즈니스에서 기존 프리미엄 기반 Microsoft Office 애플리케이션 제품군을 클라우드 기반 Microsoft 365 서비스로 마이그레이션하려면, 일반적으로 레거시 데이터 보호 솔루션에서 클라우드 기능이 있는 새로운 솔루션으로 전환해야 합니다. 대부분의 경우 2가지 백업 솔루션이 호환되지 않아 레거시 데이터를 새로운 환경에서 복원할 수 없습니다.

Microsoft 취약점: Microsoft는 Office에서 Microsoft 365로 마이그레이션하는 과정에 데이터 손실 문제를 해결하는 솔루션을 제공하지 않습니다. Office 및 Microsoft 365에 백업 기능을 통합하는 서드 파티 데이터 보호 솔루션은 거의 없으며 아쉽게도 보통 Office 또는 Microsoft 365 둘 중 하나만을 지원합니다.

6. 법률 및 규정 준수 문제

데이터 보호 위험 요소: 위에서 설명한 보호되지 않는 데이터 손실 상황에서 규정 준수 요구 사항 및 법적 문제로 인해 비즈니스 비용 지출이 더욱 커질 수 있습니다. 복구할 수 없는 Microsoft 365 데이터 손실은 비즈니스에 정부 또는 산업별 규제 벌금, 법적 처벌, 수익 및 주가 손실, 고객 신뢰 저하, 회사의 브랜드 손상을 초래할 수 있습니다.

Microsoft 취약점: 위에서 언급한 모든 관련 데이터 손실 위험에 대하여, Microsoft가 다양한 규정 준수 및 법적 문제로부터 Microsoft 365를 사용하는 조직을 보호하기 위해 할 수 있는 일은 거의 없습니다. 예를 들어, SharePoint Online에 EU 기반 고객 개인 데이터를 저장하는 비즈니스는 랜섬웨어 공격을 받은 후 해당 데이터에 대한 사본을 요청할 수 없어 GDPR 요구 사항을 위반하게 될 수 있습니다.

Microsoft 365 데이터 보호

Microsoft 365를 사용하고 있다면 가장 안정적이고 사용이 간편한 백업 솔루션인 Acronis Cyber Protect를 사용하여 Microsoft의 기초적인 데이터 보호 기능을 보완해야 합니다. 빠른 백업, 안정적인 지정 시간 복구, 유연한 복원, 클라우드 스토리지 옵션은 물론 빠른 검색 기능까지 갖춘 Acronis Cyber Protect를 사용하여 끊임없이 진화하는 위협 환경에서 비즈니스의 중요한 Microsoft 365 데이터를 보호할 수 있습니다.

Microsoft는 자체 클라우드 인프라의 탄력성을 보장하지만 데이터 보호는 사용자의 책임입니다. 전 세계의 비즈니스 및 기술 리더는 Acronis Cyber Protect를 사용하여 Microsoft 365 데이터를 보호하고 비즈니스를 원활하게 운영하고 있습니다.

**Acronis Cyber Protect에 대해
자세히 알아보려면 지금 바로 30일 무료
평가판을 시작하세요.**

시작

