금융 서비스를 위한 데이터 보호 및 보안

알아야 할 주요 사항

금융 서비스 기관이 클라우드로 옮기고 있습니다. 그 결과, 규제 기관은 특히 데이터와 관련하여 운영 중단에 적응하고 복구하는 기업의 능력을 조사하고 있습니다.

우려되는 주요 규제 개발에는 데이터 개인 정보 보호 및 사이버 보안과 관련된 규제와 유럽 금융 기관 내에서 또는 유럽 금융 기관과 비즈니스를 수행하는 기업을 위한 GDPR 및 Schrems II를 포함합니다.

데이터 프라이버시

금융 서비스 회사는 규제 기관으로부터 중요한 정보 자산과 이러한 자산이 의존하는 인프라를 식별하도록 요청받고 있습니다. 사이버 보안 행위는 은행의 중요한 운영에 대한 정보 자산의 중요도는 우선순위를 지정해야 합니다.

원격 액세스, 신속한 배포 및 대역폭 확장 고려 사항:

위험 완화: 기술 및/또는 애플리케이션에 대한 중단 또는 손상과 관련된 잠재적 위험을 사전에 계산합니다.

관리: 원격 자산 사용, 권한 있는 사용자 및 애플리케이션 개발을 포함하는 프로세스를 정의, 문서화 및 롤아웃합니다.

ICT 파트너십: 사이버 보안을 포함하여 ICT 팀을 정기적으로 업데이트하여 장기적인 원격 액세스를 수용할 수 있는 올바른 자세를 유지합니다.

사이버 이벤트 이후에 중요한 정보 무결성을 유지하기 위한 계획을 개발하고 중요한 정보 자산의 위협 프로필을 정기적으로 평가하는 것이 필수적입니다. 취약성을 정기적으로 테스트하고 ICT 관련 위험에 대한 복원력을 보장하는 것도 중요합니다.

사이버 보안

사이버 공격이 점점 더 정교해질 뿐만 아니라 디지털화, 상호 연결성 및 제3자에 대한 의존도가 높아져 개별 기관은 물론 전체 시장을 혼란에 빠뜨릴 가능성이 더 커졌습니다.

기업의 회복력을 유지하면서 개선하는 것은 조직이 고객 및 규제 기관과 신뢰를 구축하는 새로운 방법입니다.

금융 시장 인프라에 대한 유럽 중앙 은행의 기대 수준:

진화: 사이버 위험을 식별, 관리 및 완화하기 위해 설정, 진화 및 유지되는 필수 기능. 모니터링 및 관리되는 행위의 성과.

개선: 이전 수준 외에도 비즈니스 라인 전반에 걸쳐 통합되고 시간이 지남에 따라 개선되어 사이버 위험을 사전에 관리할 수 있는 고급 도구를 구현합니다.

혁신: 이전 수준에 추가하여 FMI와 더 넓은 생태계를 위한 인력, 프로세스 및 기술 혁신을 주도하여 사이버 위험을 관리하고 사이버 복원력을 강화합니다. 이를 위해서는 새로운 제어 및 도구 개발 또는 새로운 정보 공유 그룹 생성이 필요할 수도 있습니다.

기술 자산을 최신 상태로 유지하고 패치를 적용하여 신규 및 기존 사이버 위협과 지원되지 않는 기술을 완화해야 합니다. 기술 부채를 해결하기 위해 주요 변경 프로그램을 수립해야 할 수도 있습니다.

teradata.

Schrems II

이 판결은 주로 데이터 주권 및 식별가능한 정보(PII)의 보유/위치 제어에 관한 것입니다. 미국으로의 개인 데이터 전송과 관련하여 미국의 프라이버시 쉴드(Privacy Shield) 프레임워크를 인정하는 적절한 조치가 이루어졌습니다. 2020년 7월 유럽 사법 재판소에서 내린 이 판결로 인해 프라이버시 실드의 적절한 상태를 효과적으로 제거하여 미국과 EU 간의 데이터 전송에 불확실성이 발생합니다.

유럽 데이터 보호 위원회(European Data Protection Board)는 국경 간 이전 및 수입자의 제3국가를 평가하기 위한 6단계를 설정합니다.

- 자사의 이송을 알고 있는 수출업자
- 전송에 사용되는 전송 도구 확인
- 제3국의 법률 또는 관행이 귀하의 이전에 대한 보호 효과에 영향을 미칠 수 있는지 평가
- 데이터 보호 수준을 데이터 전송에 대한 필수적인 EU 기준으로 동등하게 준수하기 위한 조치를 알아보고 채택
- 이러한 추가 조치의 채택을 위한 공식적인 절차적 조치를 수행
- 적절한 간격으로 재평가하고 데이터 전송에 영향을 줄 수 있는 모든 개발 사항을 모니터링

Schrems II는 EU 외부에 있기 때문에 영국에 직접적인 영향을 미치지 않는 것처럼 보일 수 있지만 영국은 EU의 '골드 플레이트' 규제를 받는 경향이 있습니다. 이로 인해 EU 판결에 벗어나나길 원하지 않거나 EU 관행에서 벗어나는 것으로 보일 수 있습니다.

GDPR

이 EU 개인 데이터 법률은 전 세계 기업에 영향을 미치며 2018년에 발효되었습니다. GDPR은 기업이 개인 식별 정보(PII)로 할 수 있는 것과 할 수 없는 것을 조언합니다.

식별가능한 정보(PII)에는 다음이 포함됩니다(그러나 이에 국한되지는 않습니다).

이름	소셜미디어 사용
전화 번호	지역태그
주소	건강 기록
생일	인종
은행 계좌	종교적 신념
여권 번호	소속 정당

개인 데이터의 손실, 도난, 파괴 또는 변경으로 이어지는 모든 사고는 데이터 유출로 간주되며 최대 2천만 유로(2천3백만 달러) 또는 연간 글로벌 매출의 4%에 달하는 벌금이 부과될 수 있습니다.

어떤 조치를 취해야 합니까?

디지털 우선이 표준 운영 모델이 될 것이기 때문에 데이터 보호 및 보안은 미래의 글로벌 금융 서비스 기관의 주요 관심사입니다. 유연성은 미래의 성공을 위해 중요한 용소가 될 것이며 데이터 처리에 영향을 미치는 모든 새로운 규정이 최소한의 중단으로 충족될 수 있어야 합니다. 새로운 하이브리드 및 멀티 클라우드 인프라는 최고의 유연성을 제공합니다. 여러 클라우드 공급자 간에 데이터를 이동하고 워크로드를 이동할 수 있는 기능을 부여하고 필요한 경우 온프레미스로 되돌릴 수도 있습니다. 그리고 모든 데이터 이동은 최소한의 중단으로 신속하게 이루어집니다.

테라데이타 소개

테라데이타는 커넥티드 멀티 클라우드 데이터 플랫폼 기업입니다. 당사의 엔터프라이즈 분석은 시작에서 대규모 확장에 이르기까지 비즈니스 과제를 해결합니다. 오직 테라데이타만이 미래의 대규모 혼합 데이터 워크로드를 처리할 수 있는 유연성을 제공합니다. 테라데이타 Vantage 아키텍처는 클라우드 기반의 서비스형으로 제공되며, 개방형 에코시스템을 기반으로 구축됩니다. 이러한 설계 기능은 Vantage는 멀티 클라우드 환경에서 가격 성능을 최적화하는 이상적인 플랫폼으로 만들었습니다.
Teradata.com에서 자세히 알아보세요.

17095 Via Del Campo, San Diego, CA 92127 Teradata.com

teradata.