AWS에서 GDPR 규정 준수 탐색

*2018*년 *9*월

고지 사항

이 문서는 정보 제공 목적으로만 제공됩니다. 본 문서의 발행일 당시 AWS의 현재 제품 및 실행방법을 설명하며, 예고 없이 변경될 수 있습니다. 고객은 본 문서에 포함된 정보나 AWS 제품 또는 서비스의 사용을 독립적으로 평가할 책임이 있으며, 각 정보 및 제품은 명시적이든 묵시적이든 어떠한 종류의 보증 없이 "있는 그대로" 제공됩니다. 본 문서는 AWS 및 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 보증, 표현, 계약 약속, 조건 또는 보증을 구성하지 않습니다. 고객에 대한 AWS의 책임 및 의무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

목차

일반 데이터 보호 규정: 개요 1

GDPR이 EU에서 사업 활동을 하는 조직에 미치는 영향 1

GDPR을 위한 AWS의 준비 1

AWS 데이터 처리 부록(DPA) 2

GDPR 관련 AWS의 역할 2

CISPE 행동 강령 2

데이터 액세스 제어 3

모니터링 및 로깅 4

AWS에서 데이터 보호 6

암호화: AWS에서 데이터 암호화 6

강력한 규정 준수 프레임워크 및 보안 표준 12

공동 보안 책임 모델 12

AWS 규정 준수 프로그램 13

Cloud Computing Compliance Controls Catalog

(C5 – 독일 정부에서 지원하는 증명 체계) 14

문서 개정 15

요약

이 문서는 ‘AWS는 어떻게 고객이 GDPR(일반 데이터 보호 규정)을 준수하도록 지원합니까’와 같은 질문에 답변하기 위한 목적으로 작성되었습니다. Amazon Web Services(AWS)는 고객에게 자사의 비즈니스에 적용될 수 있는 GDPR 요구 사항을 준수하는 데 도움이 되는 서비스와 리소스를 제공합니다. 여기에는 AWS의 CISPE(Cloud Infrastructure Services Providers in Europe) 행동 강령 준수, 세분화된 데이터 액세스 제어, 모니터링 및 로깅 도구, 암호화, 키 관리, 감사 기능, IT 보안 표준 준수 및 AWS의 Cloud Computing Compliance Controls Catalog(C5) 증명이 포함됩니다.

일반 데이터 보호 규정: 개요

GDPR은 새로운 유럽 개인 정보 보호법입니다. GDPR은 각 회원국에 구속력이 있는 단일 데이터 보호법을 적용함으로써 유럽 연합(EU) 전체에 데이터 보호법을 포괄적으로 적용할 목적으로 제정되었습니다.
GDPR은 EU 거주자의 '개인 정보'를 처리할 때 EU 내에 설립되었거나 EU 내 개인에게 제품이나 서비스를 제공하는 모든 조직에 적용됩니다. 개인 정보는 식별된 또는 식별 가능한 자연인과 관련된 모든 정보를 말합니다.

GDPR이 EU에서 사업 활동을 하는 조직에 미치는 영향

GDPR의 핵심 중 하나는 EU 회원국 전체에서 개인 정보를 안전하게 처리, 사용 및 교환하는 방식에 대한 일관성이 생긴다는 것입니다. 조직은 강력한 기술 및 운영 조치와 규정 준수 정책을 구현하고 정기적으로 검토함으로써 자사에서 처리하는 데이터의 보안과 GDPR 규정 준수를 지속적으로 입증해야 합니다. 감독 기구는 최대 2,000만 EUR과 연간 전 세계 매출액의 4% 중 높은 금액의 벌금을 부과할 수 있습니다.

GDPR을 위한 AWS의 준비

AWS 규정 준수, 데이터 보호 및 보안 전문가가 전 세계 고객과 협력하면서 고객의 질문에 답하고, GDPR이 시행된 후 클라우드에서 워크로드를 실행할 준비를 하도록 지원하고 있습니다. 또한, 이러한 팀들은 AWS가 이미 GDPR 요구 사항을 준수하기 위해 수행하는 모든 것을 검토했습니다.

> **AWS는 AWS 서비스가 GDPR을 준수한다는 것을 확실히 말씀드릴 수 있습니다.**

제32조에 따라 컨트롤러 및 프로세서는 "처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적"을 고려하여 "적절한 기술적 및 조직적 조치를 이행"해야 합니다. GDPR은 다음과 같이 필요할 수 있는 보안 조치에 대한 구체적인 제안을 제공합니다.

- 개인 정보의 가명 처리 및 암호화.
- 처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성, 복원력을 보장할 수 있는 역량.
- 물리적 또는 기술적 사고가 발생하는 경우 개인 정보에 대한 가용성 및 열람을 시의 적절하게 복원할 수 있는 역량.
- 처리의 보안을 보장하는 기술적 및 조직적 조치의 효율성을 정기적으로 테스트 및 평가하기 위한 절차.

AWS 데이터 처리 부록(DPA)

AWS는 고객이 GDPR 계약상의 의무를 준수할 수 있도록 GDPR 규정 준수 데이터 처리 부록(GDPR DPA)을 제공합니다. AWS GDPR DPA는 AWS 서비스 약관에 통합되어 있으며 GDPR을 준수하기 위해 이를 필요로 하는 전 세계 모든 고객에게 자동으로 적용됩니다.

GDPR 관련 AWS의 역할

AWS는 GDPR에 따라 데이터 프로세서와 데이터 컨트롤러의 역할을 모두 수행합니다.

- **데이터 프로세서로서의 AWS –** 고객 및 AWS 파트너 네트워크(APN) 파트너가 AWS 서비스를 사용하여 자사 콘텐츠의 개인 정보를 처리할 때 AWS는 데이터 프로세서의 역할을 합니다. 고객 및 APN 파트너는 개인 정보를 처리하기 위해 보안 구성 제어 기능을 비롯하여 AWS 서비스에서 제공하는 제어 기능을 사용할 수 있습니다. 이러한 경우, 고객 또는 APN 파트너는 데이터 컨트롤러 또는 데이터 프로세서의 역할을 하고 AWS는 데이터 프로세서 또는 하위 프로세서의 역할을 할 수 있습니다. AWS는 데이터 프로세서로서의 AWS의 책임이 포함되어 있는 GDPR 규정 준수 데이터 처리 부록(DPA)을 제공합니다.
- **데이터 컨트롤러로서의 AWS –** AWS가 개인 정보를 수집하고 해당 개인 정보를 처리하는 목적 및 방법을 결정하는 경우(예: AWS가 계정 등록, 관리, 서비스 액세스를 위해 계정 정보를 저장하거나 고객 지원 활동을 통해 지원을 제공하기 위해 AWS 계정의 연락처 정보를 저장하는 경우), AWS는 데이터 컨트롤러의 역할을 합니다.

CISPE 행동 강령

GDPR은 컨트롤러와 프로세서가 규정 준수 및 모범 사례를 입증하는 데 도움이 되도록 행동 강령 승인을 제공합니다. 공식 승인을 기다리고 있는 강령 중 하나는 클라우드 인프라 서비스 공급자를 위한 CISPE 행동 강령("강령")입니다. 이 강령은 고객에게 클라우드 공급자가 GDPR과 일치하는 적절한 데이터 보호 표준을 사용한다는 확신을 제공합니다.

이 강령의 몇 가지 주요 이점은 다음과 같습니다.

- 데이터 보호와 관련하여 누가 어떤 것에 대한 책임이 있는지 명확히 합니다. 이 행동 강령은 특히 클라우드 인프라 서비스의 맥락에서 GDPR에 따라 공급자 및 고객 양쪽의 역할을 설명합니다.
- 이 행동 강령은 공급자가 준수해야 하는 원칙을 명시합니다. 이 행동 강령은 고객이 GDPR을 준수하도록 지원하기 위해 공급자가 수행해야 하는 명확한 조치와 책임에 대한 GDPR의 주요 원칙을 명시합니다. 고객은 이러한 구체적인 이점을 자체 규정 준수 및 데이터 보호 전략에 활용할 수 있습니다.

- 이 행동 강령은 규정 준수에 대한 의사 결정을 하는 데 필요한 정보를 고객에게 제공합니다. 이 행동 강령은 공급자가 보안 책임을 다하기 위해 수행하는 조치를 투명하게 진행할 것을 요구합니다. 몇 가지 예를 들자면 이러한 조치에는 데이터 침해, 데이터 삭제, 제3자 하위 처리, 법 집행 및 정부 요청에 대한 알림을 제공하는 것이 포함됩니다. 고객은 이러한 정보를 사용하여 제공된 높은 수준의 보안을 충분히 이해할 수 있습니다.

2017년 2월 13일에 AWS는 Amazon EC2, Amazon Simple Storage Service(S3), Amazon Relational Database Service(RDS), AWS Identity and Access Management(IAM), AWS CloudTrail 및 Amazon Elastic Block Store(EBS)가 이 강령을 모두 준수한다고 공표했습니다(https://cispe.cloud/publicregister 참조). 이는 고객에게 AWS를 사용할 때 안전하고 보호되며 규정을 준수하는 환경에서 데이터를 완벽하게 제어할 수 있다는 추가적인 보증을 제공합니다. AWS는 이 행동 강령 외에도 ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS 레벨 1 등을 비롯하여 이미 국제적으로 인정을 받고 있는 다수의 인증 및 증명을 준수합니다.

데이터 액세스 제어

GDPR 제25조에서는 컨트롤러는 "기본적으로 각 특정 처리 목적에 필요한 개인 정보만 처리되도록 적절한 기술적 및 조직적 조치를 이행해야 한다"고 명시하고 있습니다. 다음 AWS 액세스 제어 메커니즘은 권한이 있는 관리자, 사용자 및 애플리케이션만 AWS 리소스 및 고객 데이터에 액세스하도록 허용하여 이러한 요구 사항을 준수하도록 지원합니다.

- **S3 버킷/SQS/SNS 등에 있는 AWS 객체에 대한 세분화된 액세스 –** 서로 다른 리소스에 대해 개개인에게 각기 다른 권한을 부여할 수 있습니다. 예를 들어 어떤 사용자에게는 Amazon Elastic Compute Cloud(EC2), Amazon Simple Storage Service(S3), Amazon DynamoDB, Amazon Redshift 및 기타 AWS 서비스에 대한 전체 액세스를 허용할 수 있습니다. 다른 사용자에게는 일부 S3 버킷에 대해 읽기 전용 액세스를 허용하거나, 일부 EC2 인스턴스를 관리할 수 있는 권한 또는 오직 청구 정보에만 액세스할 수 있는 권한을 허용할 수 있습니다.
- **Multi-Factor Authentication(MFA) –** 계정이나 개별 사용자에게 2팩터 인증을 추가하여 보안을 강화할 수 있습니다. MFA를 사용하면 귀사 또는 귀사의 사용자가 암호 또는 액세스 키뿐만 아니라 특별히 구성된 디바이스의 코드를 제공해야 계정에서 작업을 수행할 수 있습니다.
- **API 요청 인증 –** IAM 기능을 사용하여 EC2 인스턴스에서 실행되는 애플리케이션에 S3 버킷이나 RDS 또는 DynamoDB 데이터베이스와 같은 다른 AWS 리소스에 액세스하는 데 필요한 자격 증명을 안전하게 제공할 수 있습니다.
- **지리적 제한 –** 지리적 제한(지리적 차단이라고도 함)을 사용하여 특정 지리적 위치의 사용자가 CloudFront 웹 배포를 통해 배포하는 콘텐츠에

액세스하지 못하게 할 수 있습니다. 지리적 제한을 사용하려면 다음 두 가지 옵션 중에서 선택할 수 있습니다.

- CloudFront 지리적 제한 기능 사용. 이 옵션을 사용하면 배포와 관련된 모든 파일에 대한 액세스를 제한하고 국가 수준에서 액세스를 제한할 수 있습니다.
- 제3자 지리적 위치 서비스 사용. 이 옵션을 사용하면 배포와 관련된 파일의 하위 집합에 대한 액세스를 제한하거나 국가 수준보다 좀 더 세분화된 단위에 대한 액세스를 제한할 수 있습니다.

- **STS를 통한 임시 액세스 토큰 –** AWS Security Token Service(STS)를 사용하여 신뢰할 수 있는 사용자에게 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 생성 및 제공할 수 있습니다. 임시 보안 자격 증명은 IAM 사용자가 사용할 수 있는 장기 액세스 키 자격 증명과 거의 동일하게 작동하지만 다음과 같은 차이가 있습니다.
  - 이름에서 알 수 있듯이 임시 보안 자격 증명은 단기적입니다. 몇 분에서 몇 시간까지 지속되도록 구성할 수 있습니다. 자격 증명이 만료된 후 AWS에서는 해당 자격 증명을 인식하지 못하거나 해당 자격 증명으로 이루어진 API 요청의 어떠한 액세스도 더는 허용하지 않습니다.
  - 임시 보안 자격 증명은 사용자와 함께 저장되지 않지만, 요청 시 동적으로 생성되어 사용자에게 제공됩니다. 임시 보안 자격 증명이 만료되면(또는 그전에라도) 사용자가 새로운 자격 증명을 요청할 수 있습니다. 단, 사용자에게 여전히 이를 요청할 수 있는 권한이 있어야 합니다.

  이러한 차이로 인해 임시 자격 증명을 사용할 때 다음과 같은 이점이 발생합니다.
  - 애플리케이션에 장기 AWS 보안 자격 증명을 배포하거나 포함할 필요가 없습니다.
  - 사용자에 대한 AWS 자격 증명을 정의할 필요 없이 사용자에게 AWS 리소스에 대한 액세스 권한을 제공할 수 있습니다. 임시 자격 증명은 역할 및 자격 증명 연동의 기반이 됩니다.
  - 임시 보안 자격 증명은 수명이 제한되어 있으므로 이를 교체하거나, 필요가 없어졌을 때 명시적으로 취소할 필요가 없습니다. 임시 보안 자격 증명이 만료된 후에는 이를 다시 사용할 수 없습니다. 최대 한도 내에서 자격 증명의 유효 기간을 지정할 수 있습니다.

모니터링 및 로깅

GDPR은 "[각] 컨트롤러 및 해당하는 경우 컨트롤러의 대리인은 책임하에 처리 활동에 대한 기록을 유지해야 한다"고 규정하고 있습니다. 이 조항에는 기록해야 하는 정보의 세부 사항도 포함되어 있습니다. 즉, GDPR은 PII

데이터의 처리를 모니터링해야 한다고 규정하고 있습니다. 또한, 시의 적절한 침해 통지 의무에 따르면 사고를 거의 실시간으로 탐지해야 합니다. 고객이 이러한 의무를 준수하는 데 도움이 되도록 AWS에서는 다양한 모니터링 및 로깅 서비스를 제공합니다.

- **AWS Config를 사용한 자산 관리 및 구성 –** AWS Config는 AWS 계정 내 AWS 리소스 구성에 대한 상세 보기를 제공합니다. 여기에는 리소스가 서로 어떻게 관련되어 있고 과거에는 어떻게 구성되었는지가 포함되므로 시간 경과에 따른 구성 및 관계 변화를 확인할 수 있습니다.
  AWS 리소스는 Amazon Elastic Compute Cloud(EC2) 인스턴스, Amazon Elastic Block Store(EBS) 볼륨, 보안 그룹 또는 Amazon Virtual Private Cloud(VPC)와 같이 AWS에서 사용할 수 있는 엔터티입니다. AWS Config에서 지원하는 AWS 리소스 전체 목록은 지원되는 AWS 리소스 유형 페이지를 참조하십시오.
  AWS Config에서는 다음을 수행할 수 있습니다.
  - 원하는 설정에 대해 AWS 리소스 구성을 평가합니다.
  - AWS 계정과 연결된 지원되는 리소스의 현재 구성에 대한 스냅샷을 가져옵니다.
  - 계정에 있는 하나 이상의 리소스 구성을 검색합니다.
  - 하나 이상의 리소스에 대한 과거 구성을 검색합니다.
  - 리소스가 생성, 수정 또는 삭제될 때마다 알림을 수신합니다.
  - 리소스 간 관계를 확인합니다. 예를 들어 특정 보안 그룹을 사용하는 모든 리소스를 찾을 수 있습니다.
- **AWS CloudTrail을 사용한 규정 준수 감사 및 보안 분석 –** AWS CloudTrail을 사용하면 AWS Management Console, AWS SDK, 명령줄 도구 및 더 높은 수준의 AWS 서비스를 사용하여 수행한 API 호출을 비롯하여 계정에 대한 AWS API 호출 기록을 가져와서 클라우드 내 AWS 배포를 모니터링할 수 있습니다. 또한, CloudTrail을 지원하는 서비스에 대해 AWS API를 호출한 사용자 및 계정, 호출을 수행한 소스 IP 주소, 호출이 발생한 시점을 파악할 수 있습니다. API를 사용하여 CloudTrail을 애플리케이션에 통합하고, 조직을 위해 트레일 생성을 자동화하고, 트레일의 상태를 확인하고, 관리자가 CloudTrail 로깅을 활성화/비활성화하는 방법을 제어할 수 있습니다.
- **Trusted Advisor를 통한 구성 문제 식별 –** 로깅은 S3 버킷에 저장된 데이터에 대해 전달된 상세한 액세스 로그를 가져올 수 있는 방법을 제공합니다. 액세스 로그 레코드에는 요청 유형, 작업 요청에 지정된 리소스, 요청이 처리된 시간 및 날짜와 같이 요청에 대한 세부 정보가 들어 있습니다. 로그 콘텐츠에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서에서 서버 액세스 로그 형식 섹션을 참조하십시오.
- 서버 액세스 로그는 버킷 소유자에게 자신의 통제하에 있지 않은

클라이언트가 수행한 요청의 성격에 대한 통찰력을 제공하므로 많은 애플리케이션에 유용합니다. 기본적으로 Amazon S3는 서비스 액세스 로그를 수집하지 않지만, 로깅을 활성화하면 Amazon S3가 시간 단위로 액세스 로그를 버킷에 전달합니다.

- S3 객체에 대한 세분화된 액세스 로깅
- VPC 흐름 로그를 통한 네트워크의 흐름에 대한 상세 정보
- AWS Config Rules를 사용한 규칙 기반 구성 확인 및 조치
- CloudFront에서 WAF 기능을 사용해 애플리케이션에 대한 HTTP 액세스를 필터링 및 모니터링

AWS에서 데이터 보호

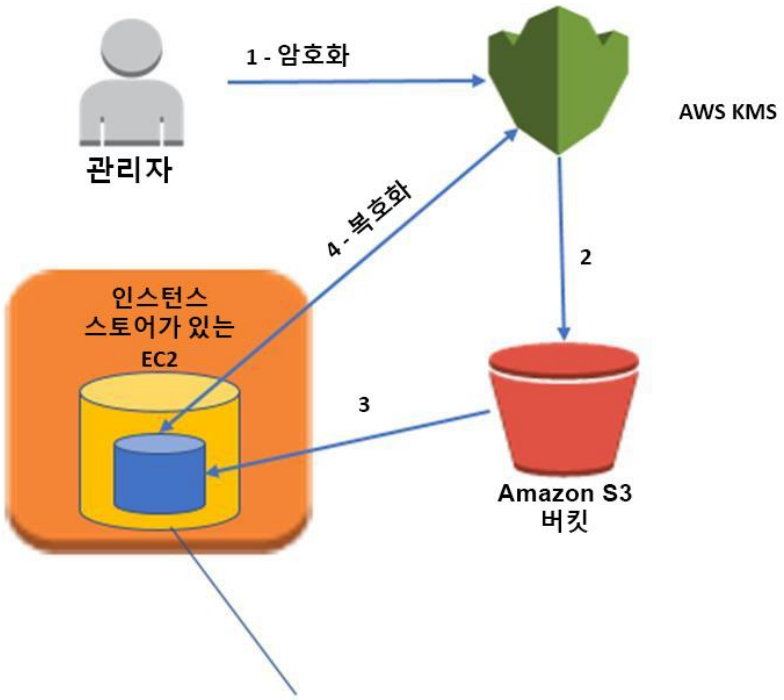
GDPR은 조직이 "(...) 개인 정보의 가명 처리 및 암호화(...)를 비롯하여 위험에 따라 적절한 보안 수준을 보장할 수 있는 적절한 기술적 및 관리적 조치를 이행"해야 한다고 규정하고 있습니다. 또한, 조직은 개인 정보의 무단 공개 또는 액세스를 차단해야 합니다. 마지막으로 개인 정보 침해가 발생하고 자연인의 권리와 자유에 큰 위험을 초래할 가능성이 있지만, 컨트롤러가 "암호화와 같이(...) 적절한 기술적 및 관리적 보호 조치"를 시행한 경우, 컨트롤러는 침해의 영향을 받는 정보 주체에게 통지할 필요가 없으므로 관리 비용과 평판 손상을 방지할 수 있습니다. AWS는 AWS에서 저장되고 처리되는 고객 데이터를 보호할 수 있도록 확장성이 뛰어나고 안전한 다양한 데이터 암호화 메커니즘을 제공합니다.

암호화: AWS에서 데이터 암호화

- **AES-256을 사용한 저장 데이터 암호화(EBS/S3/Glacier/RDS) –** 저장 데이터 암호화는 유효한 키 없이는 어떤 사용자 또는 애플리케이션도 디스크에 저장된 민감한 데이터를 읽을 수 없음을 보장하므로 규제 준수에 매우 중요합니다. AWS에서는 저장 데이터 옵션 및 키 관리를 제공하여 암호화 프로세스를 지원합니다. 예를 들어 AES-256 암호화를 사용하여 Amazon EBS 볼륨을 암호화하고 Amazon S3 버킷에 서버 측 암호화(SSE)를 구성할 수 있습니다. 또한, Amazon RDS는 TDE(Transparent Data Encryption)를 지원합니다.
  인스턴스 스토리지는 Amazon EC2 인스턴스에 임시 블록 수준 스토리지를 제공합니다. 이 스토리지는 호스트 컴퓨터에 물리적으로 연결된 디스크에 위치합니다. 인스턴스 스토리지는 버퍼, 캐시 및 스크래치 데이터와 같이 자주 변경되는 정보의 임시 스토리지에 적합합니다. 기본적으로 이러한 디스크에 저장된 파일은 암호화되지 않습니다. Linux EC2 인스턴스 스토어의 데이터를 암호화하는 방법은 Linux 내장 라이브러리를 사용하는 것입니다. 이 방법은 파일을 투명하게 암호화하여 기밀 데이터를 보호합니다. 따라서

데이터를 처리하는 애플리케이션은 디스크 수준의 암호화를 인식하지 못합니다.

- **디스크 및 파일 시스템 암호화 –** 2가지 방법을 사용하여 인스턴스 스토어의 파일을 암호화할 수 있습니다. 첫 번째 방법은 하나 이상의 암호화 키를 사용하여 전체 디스크 또는 디스크 내 블록을 암호화하는 디스크 암호화입니다. 디스크 암호화는 파일 시스템 수준 아래에서 작동하고, 운영 체계의 구애를 받지 않으며, 이름 및 크기와 같은 디렉터리 및 파일 정보를 숨깁니다. 예를 들어 Encrypting File System은 디스크 암호화를 제공하는 Windows NT 운영 체제의 NTFS(New Technology File System)에 대한 Microsoft 확장입니다.
  두 번째 방법은 파일 시스템 수준 암호화입니다. 파일 및 디렉터리는 암호화되지만, 전체 디스크 또는 파티션은 암호화되지 않습니다. 파일 시스템 수준 암호화는 파일 시스템 위에서 작동하며 운영 체제 전체에 걸쳐 이동할 수 있습니다.
- **Linux dm-crypt 인프라 –** Dm-crypt는 Linux 커널 수준 암호화 메커니즘으로, 사용자가 암호화된 파일 시스템을 탑재할 수 있도록 허용합니다. 파일 시스템 탑재는 파일 시스템을 디렉터리(탑재 지점)에 연결하여 운영 체제에서 사용할 수 있게 하는 프로세스입니다. 탑재한 후에는 추가 상호 작용 없이 애플리케이션에서 파일 시스템 내 모든 파일을 사용할 수 있으며, 이러한 파일은 디스크에 저장될 때 암호화됩니다.
  디바이스 매퍼는 블록 디바이스의 가상 계층을 만드는 일반적인 방법을 제공하는 Linux 2.6 및 3.x 커널의 인프라입니다. 디바이스 매퍼 암호화 대상은 커널 암호화 API를 사용하여 블록 디바이스의 투명한 암호화를 제공합니다. 이 문서의 솔루션은 LVM(Logical Volume Manager)이 논리적 볼륨에 매핑한 디스크 지원 파일 시스템과 함께 dm-crpt를 사용합니다. LVM은 Linux 커널에 대해 논리적 볼륨 관리를 제공합니다.
- **아키텍처 개요 –** 다음의 개략적인 아키텍처 다이어그램은 EC2 인스턴스 스토어 암호화를 활성화하기 위해 제안된 솔루션을 보여줍니다. 상세한 구현 계획은 다음 섹션에 이어집니다.



1. 관리자는 KMS를 사용하여 비밀 암호를 암호화합니다. 암호화된 비밀번호는 파일에 저장됩니다.
2. 관리자는 암호화된 비밀번호가 들어 있는 파일을 S3 버킷에 넣습니다.
3. 인스턴스 부팅 시 인스턴스가 암호화된 파일을 내부 디스크에 복사합니다.
4. 그런 다음 EC2 인스턴스가 KMS를 사용하여 파일을 복호화하고 평문 비밀번호를 검색합니다. 비밀번호는 LUKS를 통해 Linux 암호화된 파일 시스템을 구성하는 데 사용됩니다. 암호화된 파일 시스템에 기록된 모든 데이터는 디스크에 저장될 때 AES-256 암호화 알고리즘을 사용하여 암호화됩니다.

- **중앙 집중식(리전별로) 관리형 키 관리 –** AWS Key Management Service(KMS)는 데이터를 암호화하는 데 사용되는 암호화 키를 손쉽게 생성 및 제어할 수 있는 관리형 서비스이며, 하드웨어 보안 모듈(HSM)을 사용하여 키를 안전하게 보호합니다. AWS Key Management Service는 몇 가지 다른 AWS 서비스와 통합되어 이러한 서비스로 저장하는 데이터를 보호할 수 있습니다. 또한, AWS Key Management Service는 AWS CloudTrail과도 통합되어 모든 키 사용에 관한 로그를 제공함으로써 각종 규제 및 규정 준수 요구 사항을 충족할 수 있게 지원합니다.

- **중앙 집중식 키 관리 –** AWS Key Management Service는 암호화 키에 대한 중앙 집중식 제어를 제공합니다. AWS Management Console, AWS SDK 또는 CLI를 사용하여 손쉽게 키를 생성하고 가져오고 교체할 수 있을 뿐 아니라 사용 정책을 정의하고 사용을 감사할 수도 있습니다. KMS의 마스터 키는 사용자가 가져왔든 KMS가 생성했든 관계없이 암호화된 형식으로 내구력이 매우 뛰어난 스토리지에 저장되므로 필요할 때 검색할 수 있습니다. 마스터 키로 이미 암호화된 데이터를 다시 암호화할 필요 없이 KMS가 KMS에 생성된 마스터 키를 1년에 한 번 자동으로 교체하도록 선택할 수 있습니다. 이전에 암호화된 데이터를 복호화할 수 있도록 KMS가 마스터 키의 이전 버전을 유지하므로 사용자는 이를 추적할 필요가 없습니다. 새로운 마스터 키를 생성하고, 이러한 키에 액세스할 수 있는 사용자 및 원할 때 사용할 수 있는 서비스를 제어할 수 있습니다. 또한, 자체 키 관리 인프라에서 키를 가져와 KMS에서 사용할 수 있습니다.
- **AWS 서비스 통합 –** AWS Key Management Service는 몇 가지 다른 AWS 서비스와 원활하게 통합됩니다. 이러한 통합은 손쉽게 AWS KMS 마스터 키를 사용하여 이러한 서비스로 저장하는 데이터를 암호화할 수 있다는 의미입니다. 자동으로 생성되고 통합된 서비스에서만 사용할 수 있는 기본 마스터 키를 사용하거나, KMS에서 생성했거나 자체 키 관리 인프라에서 가져왔고 사용할 권한이 있는 사용자 지정 마스터 키를 선택할 수 있습니다.
- **감사 역량 –** AWS 계정에 AWS CloudTrail을 활성화한 경우, KMS에 저장하는 키의 각 사용은 로그 파일에 기록되며 이 파일은 AWS CloudTrail을 활성화할 때 지정한 Amazon S3 버킷에 전달됩니다. 기록된 정보에는 사용자, 시간, 날짜 및 사용된 키에 대한 세부 정보가 포함됩니다.
- **확장성, 내구성 및 고가용성 –** AWS Key Management Service는 관리형 서비스입니다. AWS KMS 암호화 키 사용량이 증가해도 추가적인 키 관리 인프라를 구입할 필요가 없습니다. AWS KMS는 암호화 키 요구 사항에 맞춰 자동으로 확장됩니다.
  AWS KMS가 사용자 대신 생성한 마스터 키 또는 사용자가 가져온 마스터 키는 서비스에서 내보낼 수 없습니다. AWS KMS는 99.999999999%의 내구성을 제공하도록 설계된 시스템에 암호화된 버전의 키 복사본을 여러 개 저장하여 액세스해야 할 때 키를 사용할 수 있도록 보장합니다. 키를 KMS로 가져오는 경우 언제든 키를 다시 가져올 수 있도록 키 사본을 안전하게 유지 관리해야 합니다.
  AWS KMS는 AWS 리전 내 여러 가용 영역에 배포되어 암호화 키에 대한 뛰어난 가용성을 제공합니다.

  - **보안 –** AWS KMS는 마스터 키에 다른 누구도 액세스할 수 없도록 설계되었습니다. 이 서비스는 디스크에 평문 마스터 키를 저장하지 않고, 메모리에 보관하지 않으며, 키를 사용하는 호스트에 액세스할 수 있는 시스템을 제한하는 등 포괄적인 강화 기법으로 마스터 키를 보호하도록 설계된 시스템을 기반으로 합니다. 서비스의 소프트웨어를 업데이트하기 위한 모든 액세스는 Amazon 내 독립적인 그룹에서 감사 및 검토하는 다자간 액세스 제어에 의해 제어됩니다.
    AWS KMS 작동 방식에 대한 자세한 내용은 AWS Key Management Service 백서를 참조하십시오.

- **VPN 게이트웨이를 통해 AWS로 IPsec 터널링 –** Amazon VPC를 사용하면 Amazon Web Services(AWS)의 논리적으로 격리된 섹션을 프로비저닝하여 사용자가 정의하는 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. 사용자는 자체 IP 주소 범위 선택, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성을 비롯하여 가상 네트워킹 환경을 완벽하게 제어할 수 있습니다. 또한, 기업 데이터 센터와 VPC 간에 하드웨어 VPN(Virtual Private Network) 연결을 생성하고 AWS 클라우드를 기업 데이터 센터의 확장으로 활용할 수 있습니다.
  Amazon VPC의 네트워크 구성을 손쉽게 사용자 지정할 수 있습니다. 예를 들어 웹 서버를 위해서는 인터넷에 액세스할 수 있는 퍼블릭 서브넷을 생성하고 데이터베이스 또는 애플리케이션 서버와 같은 백엔드 시스템은 인터넷에 액세스할 수 없는 프라이빗 서브넷에 배치할 수 있습니다. 보안 그룹 및 네트워크 액세스 제어 목록을 비롯한 여러 보안 계층을 활용하여 각 서브넷의 Amazon EC2 인스턴스에 대한 액세스를 제어할 수 있습니다.

- **CloudHSM을 사용한 클라우드의 전용 HSM 모듈 –** AWS CloudHSM 서비스는 AWS 클라우드에서 전용 하드웨어 보안 모듈(HSM) 어플라이언스를 사용하여 데이터 보안에 대한 기업, 계약 및 규제 준수 요구 사항을 충족하도록 지원합니다. CloudHSM을 사용하면 HSM에서 수행하는 암호화 작업 및 암호화 키를 제어할 수 있습니다.
  AWS 및 AWS Marketplace 파트너는 AWS 플랫폼 내 민감한 데이터를 보호하는 다양한 솔루션을 제공하지만, 암호화 키 관리에 대한 엄격한 계약 또는 규제 요구 사항의 적용을 받는 애플리케이션 및 데이터의 경우 추가적인 보안이 필요할 때가 있습니다. 지금까지는 민감한 데이터(또는 민감한 데이터를 보호하는 암호화 키)를 온프레미스 데이터 센터에 저장하는 것이 유일한 옵션이었습니다. 유감스럽게도 이로 인해 이러한 애플리케이션을 클라우드로 마이그레이션하지 못하거나 성능이 현격히 저하되었습니다. AWS CloudHSM 서비스를 사용하면 안전한 키 관리를 위한

정부 표준에 맞춰 설계되고 검증된 HSM 내에서 암호화 키를 보호할 수 있습니다. 본인만 액세스할 수 있도록 하는 등 데이터 암호화에 사용되는 암호화 키를 안전하게 생성, 저장 및 관리할 수 있습니다. AWS CloudHSM은 애플리케이션 성능을 저하하지 않고 엄격한 키 관리 요구 사항을 준수하는 데 도움이 됩니다.

AWS CloudHSM 서비스는 Amazon Virtual Private Cloud(VPC)와 연동됩니다. CloudHSM 인스턴스는 사용자가 지정하는 IP 주소로 VPC 내에 프로비저닝되므로 Amazon Elastic Compute Cloud(EC2) 인스턴스에 대한 간단한 비공개 네트워크 연결을 제공합니다. CloudHSM 인스턴스를 EC2 인스턴스 근처에 배치하면 네트워크 지연 시간이 줄어들어 애플리케이션 성능이 향상될 수 있습니다. AWS는 CloudHSM 인스턴스에 다른 AWS 고객으로부터 격리된 전용 및 독점(단일 테넌트) 액세스를 제공합니다. 여러 리전 및 가용 영역(AZ)에서 사용할 수 있는 AWS CloudHSM을 통해 애플리케이션에 안전하고 내구력 있는 키 스토리지를 추가할 수 있습니다.

- **통합 –** CloudHSM을 Amazon Redshift 또는 Amazon Relational Database Service(RDS) Oracle과 함께 사용하거나, 신뢰할 수 있는 루트 역할을 하는 SafeNet Virtual KeySecure, Apache(SSL 종료) 또는 Microsoft SQL Server(투명한 데이터 암호화)와 같은 타사 애플리케이션과 함께 사용할 수 있습니다. 또한, 자체 애플리케이션을 작성할 때 CloudHSM을 사용하고 PKCS#11, Java JCA/JCE, Microsoft CAPI 및 CNG를 비롯하여 익숙한 표준 암호화 라이브러리를 계속 사용할 수 있습니다.
- **감사 가능 –** 보안 및 규정 준수를 목적으로 리소스 변경을 추적하거나 활동을 감사해야 하는 경우, CloudTrail을 통해 계정에서 이루어진 모든 CloudHSM API 호출을 검토할 수 있습니다. 또한, syslog를 사용하여 HSM 어플라이언스의 작업을 감사하거나 syslog 로그 메시지를 자체 수집기로 전송할 수 있습니다.

강력한 규정 준수 프레임워크 및 보안 표준

GDPR에 따라 "처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장할 수 있는 역량"과 더불어 안정적인 복원, 테스트 및 전반적인 위험 관리 프로세스를 적절한 기술적 및 관리적 조치에 포함해야 할 수 있습니다. AWS는 강력한 규정 준수 프레임워크 및 고급 보안 표준을 제공합니다.

공동 보안 책임 모델

AWS가 데이터를 보호하는 방법을 자세히 살펴보기 전에 클라우드에서의 보안이 온프레미스 데이터 센터에서의 보안과 약간 다른 점에 대해 설명하겠습니다. 컴퓨터 시스템 및 데이터를 클라우드로 이전하면 보안 책임은 고객과 클라우드 서비스 공급자 간 공동 책임이 됩니다. 이 경우 AWS는 클라우드를 지원하는 기본 인프라를 보호할 책임이 있으며, 고객은 클라우드에 저장하거나 클라우드로 연결하는 모든 것에 대한 책임이 있습니다. 이 공동 보안 책임 모델은 많은 경우에 고객의 운영 부담을 줄여주고 일부 경우에는 고객의 추가적인 조치 없이 기본 보안 상태를 개선할 수도 있습니다.

AWS의 보안 책임

Amazon Web Services는 AWS 클라우드에서 제공하는 모든 서비스가 실행되는 글로벌 인프라를 보호할 책임이 있습니다. 이 인프라는 AWS 서비스를 실행하는 하드웨어, 소프트웨어, 네트워킹 및 시설로 구성됩니다. 이러한 인프라를 보호하는 것이 AWS의 최우선 과제이며 이러한 보호를 직접 확인하기 위해 고객이 AWS 데이터 센터 또는 사무실을 방문할 수는 없지만 AWS에서는 AWS가 다양한 컴퓨터 보안 표준 및 규정을 준수함을 확인한 제3자 감사자의 여러 보고서를 제공합니다(자세한 내용은 aws.amazon.com/compliance 참조). 이러한 글로벌 인프라를 보호하는 것 외에도 AWS는 관리형 서비스로 간주되는 제품의 보안 구성에 대한 책임이 있습니다. 이러한 유형의 서비스에는 Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces 및 기타 여러 서비스가 있습니다. 이러한 서비스는 클라우드 기반 리소스의 확장성 및 유연성과 더불어 관리형이라는 추가적인 이점을 제공합니다. 이러한 서비스의 경우 AWS에서 게스트 운영 체제(OS) 및 데이터베이스 패치, 방화벽 구성 및 재해 복구와 같은 기본적인 보안 작업을 처리합니다. 이러한 대부분의 관리형 서비스의 경우 고객은 리소스에 대한 논리적 액세스 제어를 구성하고 계정 자격 증명을 보호하기만 하면 됩니다. 일부 서비스의 경우 데이터베이스 사용자 계정 설정과 같은 추가 작업이 필요할 수도 있지만 전반적인 보안 구성 작업은 서비스에서 수행합니다.

고객의 보안 책임

AWS 클라우드를 사용하면 몇 주가 아니라 몇 분 만에 가상 서버, 스토리지, 데이터베이스 및 데스크톱을 프로비저닝할 수 있습니다. 또한, 클라우드 기반 분석 및 워크플로 도구를 사용하여 필요에 따라 데이터를 처리한 후 자체 데이터 센터 또는 클라우드에 저장할 수 있습니다. 어떤 AWS 서비스를 사용하느냐에 따라 고객 보안 책임의 일부로 고객이 수행해야 하는 구성 작업의 양이 결정됩니다.

Amazon EC2, Amazon VPC 및 Amazon S3와 같이 잘 알려진 Infrastructure as a Service(IaaS) 카테고리에 해당하는 AWS 제품은 고객이 전적으로 제어하며, 필요한 보안 구성 및 관리 작업도 모두 고객이 수행해야 합니다. 예를 들어 EC2 인스턴스의 경우 게스트 OS 관리(업데이트 및 보안 패치 포함), 인스턴스에 설치하는 모든 애플리케이션 소프트웨어 또는 유틸리티, 각 인스턴스에 AWS에서 제공하는 방화벽 구성(보안 그룹이라고 함)에 대한 책임이 고객에게 있습니다. 이는 기본적으로 서버가 어디에 있든 관계없이 고객이 수행해오던 것과 동일한 보안 작업입니다.

Amazon Relational Database Service(RDS) 또는 Amazon Redshift와 같은 AWS 관리형 서비스에서는 특정 작업을 수행하는 데 필요한 모든 리소스를 제공하지만 이에 따라오는 구성 작업은 제공하지 않습니다. 관리형 서비스에서는 인스턴스 시작 및 유지 관리, 게스트 OS 또는 데이터베이스 패치, 데이터베이스 복제에 대해 걱정할 필요가 없습니다. AWS에서 고객 대신 이를 처리합니다. 하지만 모든 서비스와 마찬가지로 고객은 AWS 계정 자격 증명을 보호해야 하며, 각 사용자가 고유한 자격 증명을 보유하고 고객이 직무 분리를 구현할 수 있도록 Amazon Identity and Access Management(IAM)로 개별 사용자 계정을 설정해야 합니다. 또한, 각 계정에 Multi-Factor Authentication(MFA)을 사용하고, SSL/TLS를 사용해 AWS 리소스와 통신하고, AWS CloudTrail을 사용해 API/사용자 활동 로깅을 설정하는 것이 좋습니다. 취할 수 있는 추가 조치에 대한 자세한 내용은 AWS 보안 리소스 웹 페이지에서 AWS 보안 모범 사례 백서와 추천 자료를 참조하십시오.

AWS 규정 준수 프로그램

Amazon Web Services 규정 준수는 고객이 클라우드에서 보안 및 데이터 보호를 유지 관리하도록 AWS에 구현된 강력한 제어 기능을 이해하는 데 도움이 됩니다. 시스템이 AWS 클라우드 인프라상에 구축됨에 따라 규정 준수는 공동의 책임입니다. 거버넌스 중심의 감사 친화적인 서비스 기능을 적용 가능한 규정 준수 또는 감사 표준과 결합함으로써 AWS 규정 준수 인에이블러는 기존 프로그램을 기반으로 하여 AWS 보안 제어 환경을 구축 및 운영하도록 지원합니다. AWS에서 고객에게 제공하는 IT 인프라는 보안 모범 사례 및 다음과 같은 다양한 IT 보안 표준에 따라 설계 및 관리됩니다.

- SOC 1/SSAE 16/ISAE 3402(이전 명칭 SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP 및 FedRAMP
- DoD SRG
- PCI DSS 레벨 1
- ISO 9001/ISO 27001
- ITAR
- FIPS 140-2
- MTCS 티어 3

또한, AWS 플랫폼이 제공하는 유연성 및 제어를 통해 고객은 다음과 같은 여러 산업별 표준을 충족하는 솔루션을 배포할 수 있습니다.

- Criminal Justice Information Services(CJIS)
- Cloud Security Alliance(CSA)
- Family Educational Rights and Privacy Act(FERPA)
- 미국 의료 정보 보호법(HIPAA)
- Motion Picture Association of America(MPAA)

AWS에서는 백서, 보고서, 인증, 인가 및 기타 타사 증명을 통해 IT 제어 환경에 대한 다양한 정보를 고객에게 제공합니다. 자세한 내용은 위험 및 규정 준수 백서를 참조하십시오.

Cloud Computing Compliance Controls Catalog (C5 – 독일 정부에서 지원하는 증명 체계)

Cloud Computing Compliance Controls Catalog(C5)는 독일 연방 정보 보안실(BSI)에서 독일에 도입하고 독일 정부에서 지원하는 증명 체계로서, 독일 정부의 "클라우드 공급자를 위한 보안 권장 사항"과 관련하여 조직이 일반적인 사이버 공격에 대한 운영 보안을 입증하는 데 도움이 됩니다.
C5 증명은 워크로드를 클라우드로 이전할 때 AWS 고객과 해당 규정 준수 고문이 AWS에서 제공하는 IT 보안 보증 서비스의 범위를 이해하는 데 사용할 수 있습니다. C5는 클라우드 관련 제어 기능뿐만 아니라 IT-Grundschutz와 동등한 규제 기관에서 정의한 IT 보안 수준을 포함합니다.
C5는 데이터 위치, 서비스 포지셔닝, 관할 지역, 기존 인증, 정보 공개 의무 및 전체 서비스 설명과 관련된 정보를 제공하는 추가 제어 기능을 포함합니다. 고객은 이 정보를 사용하여 자사의 클라우드 컴퓨팅 서비스 사용과 관련된 법적 규정(예: 데이터 프라이버시), 자체 정책 또는 위협 환경을 평가할 수 있습니다.

문서 개정

날짜	설명
2018년 9월	마이너 업데이트.
2017년 11월	초판