20_데이터를 안전하게! 클라우드 운영보안의 핵심 - 2

#1
이번 시간에는 클라우드 컴퓨팅 운영보안에 대해 학습해 보겠습니다.
지난 시간에 이어 클라우드 컴퓨팅 운영보안에 고려해야 하는 내용을 살펴보겠습니다. 먼저, 준거성에 대해 알아보겠습니다.

#2
※ 준거성
클라우드 컴퓨팅 운영 보안에서 준거성은 국내에서 클라우드 인프라를 구축하고 운영하는 업체가 정보보호와 관련된 법적 요구 사항을 준수하는 것을 의미합니다. 이는「정보통신망법」,「개인정보보호법」, 클라우드 관련 법 및 정보보호 정책 등에서 확인할 수 있는 사항입니다.

#3
※ 준거성 확보 방안
준거성을 확보하기 위해서는 법적 요구 사항과 정보보호 정책을 내부 지침에 반영하고 준수해야 합니다. 또한, 정보시스템 보안감사를 통해 법적 요구 사항과 정보보호 정책 준수 여부를 확인하고 개선 조치를 해야 합니다. 이러한 감사 결과는 식별 가능한 형태로 기록하고 모니터링하며, 비인가된 접근 및 변조로부터 보호해야 합니다.

#4
※ AWS를 통한 준거성 확보 방안
AWS를 통해 준거성을 확보할 수 있습니다. AWS는 다양한 보안 및 규정 준수 서비스를 제공하고 있습니다. 예를 들어, AWS Config를 사용하여 구성 감사를 수행하고, AWS Inspector를 사용하여 보안 평가를 수행할 수 있습니다.
- AWS Config를 사용한 구성 감사: AWS Config는 AWS 리소스의 구성 상태를 지속적으로 모니터링하고 구성 변경 사항을 추적하여 관리하는 서비스입니다.
- AWS Inspector를 사용한 보안 평가: AWS Inspector는 자동화된 보안 평가 서비스로, AWS 리소스의 보안 취약점을 식별하고 보안 상태를 평가합니다.

#5
※ 가상화 및 서버 보안
클라우드 컴퓨팅에서는 가상화 기술을 활용하여 컴퓨팅 자원을 효율적으로 제공하고 관리합니다. 가상화는 자원의 통합과 재배치를 통해 운영비용 절감과 공간 절약을 이룰 수 있지만, 동시에 악성코드 전파나 하이퍼바이저 공격과 같은 새로운 보안 위협이 존재합니다.

#6
※ 가상화 및 서버 보안 강화 방안
- 주기적인 보안패치 및 점검: 클라우드 시스템에 대한 주기적인 보안패치 및 점검을 수행하여 가용성, 지속성, 악성코드 감염 예방을 보장합니다.
- 데이터의 무결성과 백업: 데이터를 안전하게 저장하고 관리하기 위해 주기적인 데이터의 무결성 점검과 백업을 수행합니다.

#7
※ AWS를 통한 가상화 및 서버 보안 방안
- AWS를 통해 가상화 및 서버 보안을 강화할 수 있습니다. 예를 들어, AWS는 AWS 보안 계정 및 권한 관리를 통해 사용자의 접근과 권한을 관리하여 데이터와 리소스에 대한 액세스를 제어합니다. 이를 통해 보안을 강화하고 필요한 최소한의 권한만 부여할 수 있습니다.
- AWS에서는 VPN을 설정하여 안전하고 암호화된 터널을 생성하여 서로 다른 네트워크 간에 안전한 통신을 제공합니다. VPN을 활용하여 사내 네트워크와 AWS 리소스 사이에 안전한 연결을 설정할 수 있습니다.

#8
※ 접근통제 보안
클라우드 서비스를 이용하는 사용자들의 자원 공유와 원격 접속의 증가로 인해 보안성을 강화한 사용자 인증과 접근 관리가 필요합니다. 클라우드 자원에 접근이 허가된 사용자만이 서비스에 접속할 수 있도록 보장하고, 부적절한 행위에 대한 모니터링과 차단을 위한 기술적인 정보보호 대책을 마련해야 합니다.

#9
질문자: 클라우드 환경에서의 접근통제 정책과 절차는 어떻게 구성되나요?

전문가:
1. 접근통제 정책 개발: 클라우드 환경에서의 사용자 접근 제어 규칙을 정의하고 보안 요구 사항을 고려하여 정책을 개발합니다.
2. 사용자 식별과 인증: 사용자를 식별하는 고유한 식별자와 인증 수단을 사용하여 사용자의 정체성을 확인합니다.
3. 권한 부여 및 역할 관리: 최소 권한 원칙에 따라 사용자에게 필요한 권한을 부여하고, 역할 기반의 접근 제어를 통해 권한을 관리합니다.
5. 접근제어 및 모니터링: 사용자의 접근을 제어하고, 접근한 활동을 모니터링하여 이상 동작이나 보안 위협을 식별하고 대응합니다.
6. 정기적인 점검과 갱신: 접근통제 정책과 절차를 주기적으로 검토하고 업데이트하여 보안 요구 사항을 충족시키며 최신화합니다.

#10
이어서 네트워크 보안과 데이터 보호 및 백업, 시스템 개발 및 도안 보안 방안에 대해 알아보겠습니다.

#11
※ 네트워크 보안
클라우드 환경은 온프레미스 환경과는 달리 논리적으로 네트워크 및 서버를 구성하고 운영할 수 있게 해줍니다. 불법적인 접근이 허용되면 네트워크와 서버를 훼손하여 가용성을 저하시키거나, 정보 유출이나 악의적인 목적으로 악용될 수 있는 서버를 생성하는 등의 위협이 발생할 수 있습니다.
이러한 위협을 방지하기 위해서는 정교한 접근통제 정책을 수립하여 적용해야 합니다. 접근통제 정책은 아키텍처 설계 단계에서 검토되어야 하며, 아키텍처 구축 과정에서 반영되고 모니터링되어야 합니다.

#12
※ 가상 네트워크 보안
- 가상 네트워크는 클라우드 환경에서 논리적으로 구성된 네트워크로, 가상 서버, 가상 서브넷, 가상 라우터 등이 포함됩니다.
- 클라우드 서비스 제공자인 AWS에서는 Amazon Virtual Private Cloud (VPC)를 제공하여 가상 네트워크를 구성할 수 있습니다.
- VPC에서는 서브넷을 정의하고 보안 그룹과 네트워크 ACL을 설정하여 네트워크 트래픽을 제어할 수 있습니다.

- 추가적으로 가상 사설망(VPN)을 설정하여 안전하고 암호화된 통신을 구축할 수 있습니다.

#13
※ 물리적 네트워크 보안
- 물리적 네트워크 보안은 클라우드 인프라를 구성하는 물리적 요소에 대한 보안을 강화하는 방안을 의미합니다.
- 이는 데이터 센터의 물리적 접근 제어, 네트워크 장비의 보안 설정, 네트워크 감시 및 침입 탐지 시스템 등을 포함합니다.
- AWS는 데이터 센터에 대한 물리적 보안을 강화하기 위해 엄격한 출입 제어 및 감시 시스템을 운영하고 있습니다.
- 또한, 네트워크 장비인 가상 프라이빗 게이트웨이(VPG)를 통해 가상 네트워크와 온프레미스 네트워크 간의 안전한 연결을 제공합니다.

#14
※ 데이터 보호 및 백업
클라우드 서비스를 이용할 때는 이용자의 대용량 정보나 기업의 중요 기밀 정보와 같은 데이터를 다른 이용자와 공유하는 스토리지에 저장하게 됩니다. 또한, 데이터 전송 중에도 데이터 유출의 위험이 존재하기 때문에 데이터의 암호화된 전송이 필요합니다.

클라우드의 특성상 가상화로 구현된 인프라와 관련된 데이터는 백업이 불가능한 경우가 있습니다. 이를 위해 내부의 백업 정책을 수립하고, 이용자 데이터의 백업을 주기적으로 수행하며 백업 시스템을 테스트하고 점검하는 것이 필요합니다.

#15
※ AWS를 활용한 데이터 보호
- AWS에서는 데이터의 기밀성과 무결성을 보호하기 위해 다양한 암호화 기술을 지원합니다. S3와 EBS 등의 스토리지 서비스에서는 데이터 암호화를 제공하여 저장된 데이터를 보호할 수 있습니다.
- AWS Key Management Service(KMS)를 사용하여 데이터의 암호화 키를 관리하고, 데이터 암호화에 사용할 수 있습니다. KMS는 안전한 키 관리를 제공하여 데이터 보호를 강화합니다.

- 또한, AWS에서는 네트워크 트래픽의 암호화를 위해 가상 사설망(VPN) 및 SSL/TLS를 지원합니다. 이를 통해 데이터의 안전한 전송을 보장할 수 있습니다.

#16
※ AWS를 활용한 데이터 백업
- AWS는 데이터의 백업을 위한 다양한 서비스를 제공합니다. Amazon S3를 사용하여 데이터의 안정적인 저장과 백업을 수행할 수 있습니다. S3는 내구성이 높고 데이터 손실 가능성이 낮은 스토리지 서비스입니다.
- AWS Backup은 자동화된 데이터 백업 서비스로, 다양한 AWS 리소스의 백업을 관리하고 복구를 지원합니다. 이를 통해 데이터의 안전한 보존과 복구가 가능합니다.
- 또한, Amazon RDS와 Amazon DynamoDB 같은 관리형 데이터베이스 서비스는 자체적인 백업 및 복구 기능을 제공하여 데이터의 안정성을 확보합니다.

#17
※ 시스템 개발 및 도입 보안
시스템 개발 및 도입 보안은 클라우드 시스템을 신규로 개발하거나 기존 시스템을 변경 또는 도입하는 경우 중요한 보안 사항입니다. 이 단계에서는 안전하지 않은 코딩 방법을 사용하지 않고, 소스 코드에 악성 코드가 심어지지 않도록 해야 합니다. 이를 위해 분석 및 설계 과정에서 도출된 보안 요구 사항을 적용하고, 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제 절차를 수립하는 것이 중요합니다.

#18
질문자: 신규 클라우드 시스템 개발이나 기존 시스템 변경 시에 보안 요구 사항을 정의하기 위해 어떤 과정을 거쳐야 하나요?
전문가: 신규 클라우드 시스템 개발이나 기존 시스템 변경 시에는 정보 영향 평가 결과, 정보보호 기본 요소, 최신 보안 취약점 등을 고려하여 보안 요구 사항을 정의해야 합니다. 이를 통해 시스템의 보안성을 강화하고 안정적인 운영을 보장할 수 있습니다. 보안 요구 사항은 개발자와 시스템 설계자가 함께 고려해야 하며, 개발 및 도입 과정에서 지속적인 보안 검토와 평가가 이루어져야 합니다.