Microsoft Azure

클라우드 보안을 위한 5가지 모범 사례

클라우드 보안은 다양한 기업을 위한 기본적으로 새로운 환경입니다. 대부분의 보안 원칙은 사내 데이터센터(on-Premises)와 동일한 방식으로 유지되지만 구현은 전치만별입니다. 이 개요는 클라우드 보안을 위한 5가지 모범 사례(ID 및 액세스 제어, 보안 태세 관리, 앱 및 데이터 보안, 위협 보호와 네트워크 보안)에 대한 스냅샷을 제공합니다.

액세스 제어 강화 | 보안 태세 개선 | 앱 및 데이터 보호 | 위협 완화 | 네트워크 보호

01 액세스 제어 강화

기존의 보안 관행만으로는 최신 보안 공격을 방어할 수 없습니다. 따라서 최신 보안 관행은 공격자가 네트워크 경계를 침해한 것처럼 네트워크를 보호하는 "보안 침해 가정" 전략입니다. 오늘날 사용자는 다양한 위치에서 여러 디바이스와 앱을 통해 작업합니다. 유일한 상수가 사용자 ID이므로 사용자 ID가 새로운 보안 제어 평면입니다.

다단계 인증 구축

다음 인증 방법 중 두 가지 이상을 요구함으로써 다른 보안 계층을 제공합니다.

- 알고 있는 것(일반적으로 암호)
- 갖고 있는 것(전화처럼 쉽게 복제되지 않는 신뢰할 수 있는 디바이스)
- 신원을 나타내는 것(생체 인식)

조건부 액세스 활용

리소스가 액세스 제어 결정에 액세스되는 *방법*을 고려하여 보안과 생산성 간의 균형을 완벽하게 파악합니다. 조건을 기반으로 하는 클라우드 앱에 액세스하기 위한 자동 액세스 제어 결정을 구현합니다.

제로 트러스트 모델로 작업

액세스 권한을 부여하기 전에 인증 또는 접속하려는 모든 사람들의 ID를 확인합니다.

02 보안 태세 개선

더 많은 권장 사항과 보안 취약점이 확인되면 대응 분류 및 우선 순위 지정이 더 어려워집니다. 현재 환경 및 자산을 평가하고 잠재적인 보안 문제를 식별하는 데 필요한 도구가 있는지 확인하십시오.

현재 보안 태세 개선

Azure Security Center의 보안 점수와 같은 도구를 통해 모범 사례를 구현하여 보안 상태를 파악하고 개선할 수 있습니다.

이해 관계자 교육

이해 관계자와 보안 점수의 진행 상황을 공유하여 조직 보안을 개선할 경우 조직에 제공되는 가치를 증명할 수 있습니다.

정책에 있어 DevOps 팀과 협업

사후 대응 모드에서 벗어나려면 사전에 DevOps 팀과 협력하여 엔지니어링 주기 초기에 DevOps 보안으로서 핵심 보안 정책을 적용해야 합니다.

03 앱 및 데이터 보호

ID, 데이터, 호스트 및 네트워크에 걸쳐 계층화되고 심층적인 방어 전략을 통해 데이터, 앱 및 인프라를 보호합니다.

암호화

유휴 상태 및 전송 중인 데이터를 암호화합니다. 컨피덴셜 컴퓨팅 기술로 사용 중인 데이터를 암호화하는 것이 좋습니다.

보안 모범 사례 실행

오픈 소스 종속성에 취약성이 없는지 확인합니다. 또한 개발자는 보안 개발 수명 주기(SDL)와 같은 보안 모범 사례에 대해 교육을 받아야 합니다.

책임 공유

기업이 주로 사내 데이터센터(on-Premises)에서 운영되는 경우 전체 스택을 소유하고 자체 보안을 담당합니다. 클라우드 사용 방법에 따라 책임 사항이 변경되고 일부 책임은 클라우드 공급자에게 전가됩니다.

- IaaS: 가상 컴퓨터에서 응용 프로그램을 실행하는 경우 응용 프로그램과 OS가 모두 안전한지 확인하는 데 고객에게 더 많은 책임이 전가됩니다.
- PaaS: 클라우드 네이티브 PaaS로 전환되면 Microsoft와 같은 클라우드 공급자는 OS 단계에서 추가 보안 책임을 준수해야 합니다.
- SaaS: SaaS 단계에서는 고객이 요구하는 책임 사항이 더 많아집니다. 공동 책임 모델을 확인하십시오.

04 위협 완화

운영 보안 태세(보호, 탐지, 대응)는 우수한 보안 인텔리전스를 통해 빠르게 진화하는 위협을 조기에 식별하여 신속하게 대응할 수 있습니다.

모든 리소스 유형에 대한 탐지 활성화

가상 컴퓨터, 데이터베이스, 스토리지 및 IoT에 대한 위협 탐지가 활성화되었는지 확인합니다. Azure Security Center에는 모든 Azure 리소스 유형을 지원하는 기본 제공 위협 탐색이 있습니다.

위협 인텔리전스 통합

더욱 빠르고, 효율적이고, 사전 대응적인 결정을 내릴 수 있도록 필요한 컨텍스트, 관련성 및 우선 순위를 제공하면서 위협 인텔리전스를 통합하는 클라우드 공급자를 활용합니다.

보안 정보 및 이벤트 관리(SIEM) 현대화

요구에 따라 확장하고, AI를 사용하여 소음을 줄이고, 인프라가 필요하지 않은 클라우드 네이티브 SIEM을 고려해 보십시오.

05 네트워크 보호

우리는 끊임없이 혁신하는 네트워크 보안의 시대에 살고 있습니다. 환경이 변화함에 따라 보안 솔루션은 진화하는 위협 환경의 문제를 해결해야 하며, 공격자가 네트워크를 악용하는 것이 점점 더 어려워지고 있습니다.

강력한 방화벽 보호 유지

ID 및 액세스 관리에서도 방화벽 설정은 여전히 중요합니다. 경계를 보호하고, 적대적인 활동을 탐지하고, 대응을 구축하기 위한 제어 수단을 마련해야 합니다. 웹 응용 프로그램 방화벽(WAF)은 SQL 주입과 사이트 간 스크립팅과 같은 일반적인 악용으로부터 웹 앱을 보호합니다.

DDoS(Distributed Denial of Service) 보호 활성화

운영 비용을 제한하면서 가용성과 성능을 유지하기 위해 응용 프로그램 및 네트워크 계층을 대상으로 하는 악의적인 트래픽으로부터 웹 자산과 네트워크를 보호합니다.

초세분화된 네트워크 만들기

플랫 네트워크를 사용하면 공격자는 횡방향으로 손쉽게 이동할 수 있습니다. 가상 네트워킹, 서브넷 프로비저닝 및 IP 주소 지정 등과 같은 개념을 살펴보십시오. 초세분화를 사용하고 완전히 새로운 개념의 마이크로 경계를 수용하여 제로 트러스트 네트워킹을 지원합니다.

다음 단계는 무엇일까요?

Microsoft에게 문의하기

클라우드 워크로드의 보안을 강화하시겠습니까?

Azure 기반의 보안에 대해 자세히 알아보기