AWS 클라우드 보안 실습

클라우드 시대, 우리는 무엇을 어떻게 지켜야 하는가?

SECURIOUS(시큐리어스) Team Defense & Cloud 2-A Part 2

클라우드, 빌려 쓰면 다 해결되는 것 아닐까?

> **신입생의 흔한 오해:**
>
> "대기업인 AWS가 알아서 다 지켜주는 거 아냐? 우리가 신경 쓸 게 있나?"

현실: 클라우드는 '도구'일 뿐, 어떻게 쓰느냐에 따라 보안의 성패가 갈립니다.

오늘 우리가 반드시 이해해야 할 핵심 개념:

공동 책임 모델 (Shared Responsibility Model)

AWS가 책임지는 영역: "클라우드 자체의 보안"

물리적 인프라

데이터 센터 보안, 출입 통제, 환경 제어 (냉각, 전력) 등 물리적 보호

하드웨어

서버, 스토리지 장비, 컴퓨팅 리소스의 무결성 및 하이퍼바이저 보안 관리

글로벌 네트워크

리전, 가용 영역(AZ), 엣지 로케이션 간의 안전한 연결 및 네트워크 인프라 보호

"자물쇠(보안 도구)는 AWS가 완벽하게 준비해서 제공합니다."

Shared Responsibility Model: Security OF the Cloud

우리가 책임지는 영역: "클라우드 내에서의 보안"

설정 및 권한

누가 어떤 자원에 접근할 수 있는지(IAM), 보안 그룹 설정, 네트워크 ACL 구성

데이터 암호화

저장된 데이터와 전송 중인 데이터의 암호화 및 키 관리

운영체제 및 패치

EC2 인스턴스 내 OS 업데이트, 애플리케이션 취약점 패치, 런타임 보안 관리

"자물쇠를 잠그는 것은 사용자의 몫입니다."

Shared Responsibility Model: Security IN the Cloud

사례 1: SKT 유심 정보 유출 (2025.4)

ACTUAL INCIDENT 2025

"기본적인 패치 관리의 부재가 불러온 대참사"

사고 규모

약 2,600만 건의 고객 정보 유출

주요 원인

8년 넘게 방치된 리눅스 취약점 + 내부 네트워크 분리 실패

관련 기사

- https://m.boannews.com/html/detail.html?idx=138964
- https://sslc.kr/board/news/1014

핵심 교훈

아무리 거대한 인프라와 자본을 가진 기업이라도, **보안의 기본(패치 관리)**이 지켜지지 않으면 규모는 아무런 방패가 되지 못합니다.

출처: 개인정보보호위원회 / 데일리시큐

사례 2: 쿠팡 고객 데이터 탈취 (2025.11)

약 3,370만 고객 계정 정보 유출

대한민국 인구의 약 2/3에 해당하는 규모의 대형 사고

사고 원인

퇴사한 직원이 기존의 접근 권한을 그대로 보유하고 있었으며, 이를 이용해 내부 인증 키를 탈취, 고객 토큰을 위조하여 데이터에 접근함

핵심 교훈

인력 변동 시 즉각적인 권한 회수가 필수적이며, 모든 사용자에게 업무에 필요한 최소한의 권한만 부여하는 원칙이 지켜져야 함

최소 권한 원칙 (Principle of Least Privilege)

"권한은 주는 것보다 뺏는 것이 더 중요합니다." - IAM 관리의 핵심

출처: NordVPN / 엔키화이트햇 | AWS Cloud Security Training

관련 기사: https://www.chosun.com/economy/tech_it/2026/02/10/PF6WP7M5WVHW7JNGV4EKJRIKDM/

사례 3: 오라클 클라우드 구형 서버 해킹 (2025.1)

사고 규모	약 600만 건의 로그인 정보(SSO, LDAP 비밀번호) 유출 주장
발생 원인	2017년 이후 사용되지 않은 구형 서버가 방치된 채 외부 접근이 가능한 상태로 유지됨

핵심 교훈: "CSP라고 예외는 없다"

클라우드 환경에서도 사용하지 않는 자원을 방치하거나 설정을 관리하지 않으면 반드시 뚫립니다.
클라우드 서비스 제공사(CSP)의 인프라 보안과는 별개의 문제입니다.

출처: 요즘IT

관련 기사: https://m.boannews.com/html/detail.html?idx=136696

데이터로 보는 클라우드 보안의 현실

핵심 사고 원인

Misconfig

클라우드 구성 오류는 여전히 데이터 유출의 핵심 원인 (Fidelis Security)

공공기관 위협

1.6만 건

국내 공공기관 대상 일일 해킹 시도 횟수.
약 80%가 북한 소행 추정 (Mordor Intelligence)

도입 망설임 이유

44%

기업이 클라우드 도입을 주저하는 이유 1위:
외부 저장에 대한 보안 우려 (삼성SDS)

Source: Fidelis Security, Mordor Intelligence, Samsung SDS (2025)

설정 하나가 보안 사고의 시작입니다

클라우드 보안은 이론이 아닌 실제 상황입니다

2025년의 실제 사례들이 증명하듯, 보안 사고는 먼 나라 이야기가 아닙니다.

기술보다 중요한 것은 올바른 관리입니다

최첨단 클라우드 기술을 사용하더라도, 기본적인 설정과 권한 관리가 핵심입니다.

공동 책임 모델을 잊지 마세요

AWS는 인프라를 지키고, 그 안의 데이터를 지키는 것은 우리의 몫입니다.

"설정 하나가 보안 사고로 이어집니다"

그리고 이건 이론이 아니라 2025년에 실제로 일어난 일입니다.

IAM: "누가 무엇을 할 수 있는가?" (인증과 인가)

인증 (Authentication)

"당신은 누구인가?"

ID/PW, MFA(다요소 인증) 등을 통해

사용자의 신원을 확인하는 과정

인가 (Authorization)

"당신은 무엇을 할 수 있는가?"

확인된 사용자에게 특정 자원에 대한

접근 권한(Policy)을 부여하는 과정

쿠팡 사례 복습: 퇴사한 직원의 권한이 회수되지 않아 발생한 사고는 전형적인 IAM 관리 실패의 결과입니다. 클라우드 보안의 첫 번째 방어선은 철저한 계정 관리에서 시작됩니다.

관련 자료: https://medium.com/awesome-cloud/aws-iam-overview-what-is-aws-iam-user-role-group-policy-introduction-features-use-cases-benefits-security-d27c0e18e7ab

최소 권한 원칙: "편리함보다 안전함이 우선입니다"

위험한 생각: "관리자(Admin) 권한 하나면 일하기 편하잖아?"

편리함은 보안의 가장 큰 적입니다. 모든 권한을 가진 계정은 해커에게 가장 매력적인 타겟입니다.

아파트 마스터키 비유

아파트의 모든 문을 열 수 있는 마스터키를 전 주민에게 나눠준다면?

단 한 명만 키를 분실해도 아파트 전체가 위험에 빠집니다.

실천: 최소 권한 부여

각 사용자에게 업무 수행에 꼭 필요한 '최소한의 권한'만 부여해야 합니다.

권한은 필요할 때만 일시적으로 확장하는 것이 정석입니다.

네트워크 접근 통제: "보이지 않는 벽을 세우는 법"

Security Group (보안 그룹)

인스턴스 단위의 가상 방화벽

허용(Allow) 규칙만 설정 가능하며, 요청에 대한 응답을 자동으로 허용하는 Stateful 방식

Network ACL (네트워크 ACL)

서브넷 단위의 방화벽

허용과 거부(Deny) 규칙 모두 설정 가능하며,

인바운드/아웃바운드를 각각 제어하는 Stateless 방식

SKT 사례 복습: 내부 네트워크 분리 실패는 적절한 네트워크 통제 설정이 없었기 때문입니다.
서비스 간의 불필요한 통신을 차단하는 것이 보안의 기본입니다.

관련 자료: https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-security-groups.html

자, 개념은 여기까지.

이제 실제로 AWS 콘솔이 어떻게 생겼는지 볼까요?

HANDS-ON LAB

AWS Skill Builders - Console 접속 및 실습

"백문이 불여일견, 직접 설정해보며 보안의 무게를 느껴봅시다."

💡 이번 실습이 흥미롭다면, SCS 자격증의 KEK, Envelope Encryption 등 심화 주제도 Phase 2에서 함께 도전해 봐요!

Skill Builers 실습 전 필수 개념 가이드

사용자 & 그룹

사용자는 반드시 그룹에 속해야 합니다. 그룹별로 수행 가능한 권한이 다르기 때문입니다.

"임원은 중요 문서 열람 가능, 직원은 승인 후 열람 가능, 인턴은 열람 불가"처럼 역할에 따라 그룹을 나눕니다.

정책 & JSON

그룹이 할 수 있는 일을 정의한 문서를 '정책'이라고 하며, 이는 JSON 형식으로 작성됩니다.

"Effect": "Allow"와 같이 '키:값' 형태로 구성된 글을 써서 저장하면 즉시 적용됩니다.

EC2 & S3의 관계

EC2는 업무를 처리하는 '사람', S3는 파일을 보관하는 '책장'과 같습니다.

사람이 책장에서 자료를 꺼내어 일을 하듯, EC2는 S3에 데이터를 넣거나 가져와서 처리합니다.

콘솔은 눈에 익으셨나요?

이제 퀴즈로 지금까지 배운 내용을 확인해 봅시다!

REVIEW

공동 책임 모델 | 클라우드 기본 보안 조치 | IAM 기초

"개념과 화면을 연결해 보는 시간입니다. 가벼운 마음으로 참여해 주세요!"

퀴즈 세션 시작

[Quiz 1] 공동 책임 모델의 이해

다음 중 '공동 책임 모델'에서 사용자가 직접 관리해야 하는 보안 영역은 무엇인가요?

01 데이터 센터의 물리적 출입 통제

02 서버 하드웨어의 무결성 관리

03 S3 버킷의 접근 권한 및 암호화 설정

04 글로벌 네트워크 인프라의 가용성 보장

[Quiz 1] 공동 책임 모델의 이해

다음 중 '공동 책임 모델'에서 사용자가 직접 관리해야 하는 보안 영역은 무엇인가요?

01 데이터 센터의 물리적 출입 통제

02 서버 하드웨어의 무결성 관리

03 S3 버킷의 접근 권한 및 암호화 설정

04 글로벌 네트워크 인프라의 가용성 보장

[Quiz 2] 주요 보안 조치의 이해

다음 보안 조치에 대한 설명 중 틀린 것은 무엇인가요?

01 IAM: '누가 무엇을 할 수 있는가'를 정의하는 인증 및 인가 서비스이다.

02 최소 권한 원칙: 모든 사용자에게 관리자(Admin) 권한을 주어 업무 효율을 높이는 원칙이다.

03 Security Group: 인스턴스 레벨에서 작동하는 상태 저장(Stateful) 방화벽이다.

04 NACL: 서브넷 레벨에서 작동하는 상태 비저장(Stateless) 방화벽이다.

[Quiz 2] 주요 보안 조치의 이해

다음 보안 조치에 대한 설명 중 틀린 것은 무엇인가요?

01 IAM: '누가 무엇을 할 수 있는가'를 정의하는 인증 및 인가 서비스이다.

02 최소 권한 원칙: 모든 사용자에게 관리자(Admin) 권한을 주어 업무 효율을 높이는 원칙이다.

03 Security Group: 인스턴스 레벨에서 작동하는 상태 저장(Stateful) 방화벽이다.

04 NACL: 서브넷 레벨에서 작동하는 상태 비저장(Stateless) 방화벽이다.

[Quiz 3] IAM 정책 JSON 분석

```
"Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ReadAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
],
   "Resource": "*"
}
 ]
```

이것은 어떤 IAM 정책 JSON의 일부입니다.

여기에 나타난 보안상 가장 큰 문제점을 고르세요.

- **A** Action이 너무 적다
- **B** Resource 범위가 너무 넓다 (모든 버킷 접근)
- **C** JSON 구조가 잘못됐다
- **D** S3는 접근하면 안 된다

[Quiz 3] IAM 정책 JSON 분석

```
"Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ReadAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
],
   "Resource": "*"
}
 ]
```

이것은 어떤 IAM 정책 JSON의 일부입니다.

여기에 나타난 보안상 가장 큰 문제점을 고르세요.

- **A** Action이 너무 적다
- **B** Resource 범위가 너무 넓다 (모든 버킷 접근)
- **C** JSON 구조가 잘못됐다
- **D** S3는 접근하면 안 된다

오늘 교육의 핵심 3줄 요약

01

클라우드 보안은 내 책임

남의 컴퓨터를 빌려 쓰는 것이지만,
그 안의 데이터와 설정은
전적으로 사용자의 몫입니다.

02

설정 하나가 사고의 시작

2025년의 실제 사례들이 증명하듯,
사소한 설정 오류가
대형 사고로 이어집니다.

03

IAM이 보안의 출발점

'누가 무엇을 할 수 있는가'를 정의하는
IAM 관리가 클라우드 보안의
첫 단추입니다.

Q & A

질의응답

오늘 배운 내용 중 궁금한 점이 있나요?

클라우드 보안, 사고 사례, 혹은 앞으로의 실습에 대해 자유롭게 질문해 주세요.

다음 시간 예고: "이제 직접 설정해 봅시다!"

이론은 여기까지, 다음 주에는 진짜 클라우드 보안 전문가가 되어 봅시다.

S3 보안 실습

직접 S3 버킷을 생성하고, 퍼블릭 액세스 차단 설정을 변경하며 데이터 노출을 막는 방법을 익힙니다.

IAM 권한 실습

사용자에게 최소 권한만 부여하는 정책을 직접 작성하고, 권한이 없을 때 발생하는 오류를 확인해 봅니다.

🚀 **2-B 팀이 준비한 흥미진진한 실습 시나리오를 기대해 주세요!**

다음 시간 사전 준비 안내

AWS 계정 생성

아직 계정이 없다면 다음 시간 전까지 반드시 생성해 주세요. (해외 결제 가능 카드 필요)

접속 테스트

AWS 콘솔에 정상적으로 로그인이 되는지 미리 확인해 주세요. (IAM 사용자 로그인 권장)

실습 가이드 확인

공유될 '2회차 실습 가이드'를 미리 읽어오시면 실습 진행이 훨씬 수월해집니다.

"준비된 자만이 안전한 클라우드를 만들 수 있습니다. 다음 주에 만나요!"