클라우드 Shadow IT 위협 사례 분석을 통한 클라우드 리소스 스캐너 요구사항 도출

황혜경*, 이지원*, 백지은*, 성아영*, 최상훈[1], 박기웅†

, † 세종대학교 정보보호학과 (학부생, 교수†)
[1] 세종대학교 SysCore Lab. (연구 교수[1])

Deriving Requirements for a Cloud Resource Scanner through Analysis of Cloud Shadow IT Threat Cases

Hye-Kyung Hwang*, Ji-Won Lee*, Ji-Eun Baik*, A-Young Sung*, Sang-Hoon Choi[1], Ki-Woong Park†

, † Dept. of Computer and Information Security, Sejong University (Undergraduate Student, Professor†)
[1]SysCore Lab., Sejong University (Research Professor[1])

요 약

조사에 따르면, 2022년과 2023년에 전 세계 기업의 85%가 사이버 사고를 겪었으며 이 중 11%는 승인되지 않은 Shadow IT로 인해 발생한 것으로 나타났다 [1]. 복잡한 클라우드 환경에서는 가시성 문제가 자주 발생하며, 이에 따라 클라우드에서 Shadow IT 관련 보안 위협이 주요 포인트로 언급되고 있다. 따라서 본 논문에서는 클라우드 환경에서 나타나는 여러 보안 위협 중 'Shadow IT'에 집중한다. Shadow IT로 인해 발생하는 보안 위협 사례를 살펴본 후, 이를 CSA에서 제공하는 CCM (Cloud Controls Matrix) v4를 기준으로 분석하여 Shadow IT에 의한 클라우드 보안 사고를 최소화하기 위한 주요 관점을 제시한다.

I. 서론

클라우드 도입이 가속화됨에 따라 이를 노린 보안 위협도 증가하고 있다. 클라우드는 기존의 물리적 시스템이 아닌 논리적 시스템으로, 자산 식별 및 파악이 어렵다 [2]. 이에 따라 발생하는 Shadow IT는 복잡한 클라우드 환경의 가시성을 훼손해, 조직이 클라우드 서비스 사용이 안전한지 시각화하고 분석하는 것을 방해한다 [3].

본 논문에서는 클라우드 환경에서 Shadow IT로 인해 발생하는 보안 위협을 식별하고 이와 관련된 보안 프레임워크 내용을 분석하여, 조직이 Shadow IT로 인한 보안 위협을 완화할 수 있는 인사이트를 제공하고자 한다.

II. 배경지식

클라우드는 환경에서는 인가되지 않은 리소스가 발생하기 쉽고 이를 완전히 식별하는 데 한계가 있다. 이에 따라 시스템을 점검하고 인증하는 프레임워크를 기반으로 클라우드 환경에서의 Shadow IT에 관련된 점검 항목을 분석해 볼 필요가 있다.

여러 프레임워크 중 CCM v4 [4]는 클라우드 보안 통제 매트릭스로, 클라우드 환경에서 문제가 되는 영역들을 중점적으로 다루기 때문에 클라우드 자산 가시성과 통제 구조를 평가할 수 있다. 이에 따라 클라우드 환경에서의 Shadow IT에 대한 분석 및 대응에 적합하다고 판단하여 본 연구에서는 CCM v4를 기준으로 Shadow IT 관련 보안 항목을 분석하였다.

III. 사례 분석 및 고찰

3.1. C1: 클라우드 S3 취약점 사례

클라우드 환경에서 방치된 S3는 공격자의 의도대로 악용될 수 있다. 문제는 이러한 악용

사실조차 사용자가 인지하지 못하므로 더 큰 보안 위협을 초래한다.

3.1.1 Bucket Monopoly 취약점 발견 [5]

Aqua의 Nautilus 팀은 사용자가 새로운 리전에서 CloudFormation 서비스를 처음 생성할 때, AWS가 자동으로 S3 버킷을 생성하는 것을 발견했다. 먼저 AWS가 생성하려는 버킷과 같은 이름의 버킷을 생성하는 "Bucket Monopoly" 공격을 수행하여 공격자가 버킷 이름을 선점하면, AWS는 공격자의 악성 버킷을 정상 버킷으로 신뢰한다. 사용자가 S3 버킷의 존재를 인지하지 못한다면, 버킷은 Shadow IT로써 공격자에 의해 악용될 수 있다.

3.1.2 관련 프레임워크 분석

CCM v4에서는 자산의 식별과 추적의 중요성을 강조한다. 데이터베이스 정보의 효과적 관리와 보호를 위해 물리 및 논리적 자산의 분류 및 추적을 요구한다. 제공자는 사용되는 모든 자산을 식별 및 목록화하여 관리해야 하며, 실시간 추적 체계를 유지해야 한다.

Bucket Monopoly 취약점 발견 사례와 CCM v4를 통해 시스템이 자동 생성하는 자산을 포함하여 모든 자산을 관리할 수 있어야 함을 알 수 있다. 또한, 시스템에 존재하는 리소스가 사용자의 승인을 받고 생성한 리소스가 맞는지 검증하는 절차도 필요하다.

3.2 C2: 클라우드 토큰 탈취 사례

조직의 승인을 받지 않은 IT 자원은 조직의 관리하에 있지 않으므로, 해당 자원이 조직 시스템에 접근하게 되면 예상치 못한 보안 위협을 야기할 수 있다.

3.2.1 Okta 해킹 사건 [6]

2023년, Okta는 공격자가 고객 지원 시스템에 무단 접근하여 민감 파일을 탈취하는 사건이 발생했다. 한 직원이 업무용 노트북에서 개인 Google 프로필에 로그인함에 따라 서비스 계정의 사용자 이름과 비밀번호가 직원의 개인 계정 또는 개인 장치가 침해되면서 서비스 계정의 자격 증명이 노출되었을 것으로 분석된다.

3.2.2 관련 프레임워크 분석

CSA CCM v4에서는 인적 자원에 의한 사고를 방지하기 위한 점검 사항을 제시한다. 자산의 사용에 있어 허용 범위를 명확히 정의해야 하고, 모바일 디바이스 및 엔드포인트에 대한 보안 통제를 강화해야 한다. 또한, MFA 도입을 통해 적절한 인증 과정을 거치도록 해야 한다.

Okta 사례와 CCM v4를 통해 개인 계정과 시스템 자산의 분리가 중요함을 알 수 있다. 시스템 내에서 허용 범위를 명확하게 정의하고, 사용자가 보안 정책을 준수할 수 있도록 적절한 보안 인식을 갖추도록 해야 한다. 또한, 시스템 혹은 계정 접근에 강력한 인증 과정을 도입하여 시스템상의 보안성을 확보해야 한다.

3.3 C3: 클라우드 서브 도메인 탈취 사례

클라우드 환경에서 조직의 서브 도메인 CNAME 레코드가 미사용 클라우드 서비스를 가리키는 상태로 방치되면, 이러한 상태는 잠재적인 보안 위협으로 공격에 악용될 수 있다.

3.3.1 서브 도메인 탈취 취약점 발견 [7]

Certitude Consulting은 주요 공공 기관의 서브 도메인 탈취 취약점을 발견했다. 이를 기반으로 그들은 WordPress.com에 호스팅된 호주 외교통상부, 영국 기상청, 미국 로드아일랜드주 보건국 등의 블로그를 점유했고, DNS 항목에 의해 참조되던 독일 보험 회사와 담배 제조업체의 AWS S3 버킷 또한 확보했다. 이를 통해 많은 조직의 서브 도메인이 탈취가 가능한 상태로 방치되어 있음을 보였다.

3.3.2 관련 프레임워크 분석

CSA CCM v4에서는 DNS를 포함한 클라우드 네트워크 환경의 보안을 강조한다. DNS를 포함한 네트워크 아키텍처에 대한 최신 문서를 유지해 구성과 데이터 흐름을 명확히 파악할 수 있어야 하며, DNS와 같은 네트워크 자산의 정기적 인벤토리를 갱신할 것을 권장한다.

서브 도메인 탈취 취약점 사례와 CCM v4를 통해 DNS 자산 및 서브 도메인에 대한 인벤토리 유지의 필요성을 알 수 있다. 자산 방치는 관리되지 않은 취약한 공격 표면을 만들 수 있으므로, 미사용 자산을 식별하고 즉시 제거 및 폐기해야 한다.

다음은 위에서 살펴본 Shadow IT로 인한 보안 위협 사례와 이에 기반한 CCM v4 내용을 요약하여 정리한 표이다.

<표 1> Shadow IT 사례별 프레임워크 정리

사례 번호	사례 요약	CSA CCM v4 분석
c1	- S3 버킷 자동 생성 기능 - Bucket Monopoly 공격으로 이어짐	- 자산 식별 및 추적의 중요성 강조 - 자동 생성되는 자산 식별에 대한 요구사항 필요
c2	- 업무용 기기에 개인 계정 로그인 - 개인 계정에 회사 계정 자격 증명이 저장됨	- 자산 사용 범위 정의 - MFA를 사용한 인증 필요
c3	- 많은 조직의 서브 도메인이 탈취 가능한 상태로 방치	- 네트워크 아키텍처 인벤토리 유지 - 사용하지 않는 자산 즉시 제거

IV.결론

본 논문에서는 클라우드 환경에서 Shadow IT로 인해 발생했던 취약점 및 보안 사고 사례를 식별했고, 이러한 취약점에 연관된 CSA CCM v4의 보안 항목을 분석했다.

클라우드 환경에서의 Shadow IT으로 인한 보안 위협에 대응하기 위해, Shadow IT 식별에 활용할 수 있는 도구들을 사용할 수 있다. AWS CloudTrail는 사용자, 역할, AWS 서비스가 수행한 모든 작업이 이벤트로 기록한다. 이 도구는 리소스 생성자를 추적하기 위해 로그를 확인하는 데 사용될 수 있다. Cloud-Nuke는 계정에서 더 이상 사용하지 않는 리소스를 일괄 삭제한다. 이러한 도구는 리소스 방치를 식별 및 방지하고, 리소스의 진위성을 판별하는 데 사용될 수 있다. FindMyTakeover는 멀리 클라우드 환경에서 더 이상 존재하지 않는 인프라를 참조하고 있는 DNS record를 찾아내고, 이를 통해 잠재적인 서브 도메인 탈취 가능성을 쉽게 탐지할 수 있다.

그러나 목적이나 탐지 범위가 다른 도구들을 적소에 사용하는 데에는 전문적인 지식과 많은 시간이 필요하며, 점검 항목이 많아질수록 누락되는 부분이 생기기 마련이다. 향후 연구에서는 스캐닝 도구를 자동 실행하고 스캔 정보를 아카이빙 및 종합적으로 제공함으로써 클라우드 환경의 가시성 및 보안성을 높일 수 있는 시스템에 대한 연구가 필요하다.

[참고문헌]

[1] Alessandro Mascellino, “New Report: 85% Firms Face Cyber Incidents, 11% From Shadow IT”, 2023.12.

[2] Thomas,E., Zaigham,M., andRicardo,P., Cloud computing: Concepts, technology & architecture

[3] Cloud Security Alliance, “Top Threats to Cloud Computing 2024”, 2024.08.

[4] Cloud Security Alliance, “CCM v4.0 Implementation Guidelines”, 2024.06.

[5] Yakir Kadkoda, Ofek Itach, Michael Katchinskiy, “Bucket Monopoly: Breaching AWS Accounts Through Shadow Resources”, Aqua Security, 2024.09.

[6] Alex Scroxton, “Shadow IT use at Okta behind series of damaging breaches”, Computer Weekly, 2023.11.

[7] Florian Schweitzer, “Thousands of Organizations Vulnerable to Subdomain Hijacking”, Certitude Consulting, 2023.08.