국내 클라우드 환경에서 데이터 노출 최소화를 위한 DSPM 모델 초안 설계

이서연[1], 정호심[2], 이승찬[3], 양진[4], 김세현[5], 양혁재[6]
[1]성균관대학교 일반대학원 과학수사학과 석사
[2]서울여자대학교 정보보호학과 학사
[3]건양대학교 스마트보안학과 학부생
[4]서울여자대학교 정보보호학과 학부생
[5]한성대학교 융합보안학과 학부생
[6]테이텀 시큐리티 대표
wlwkwn@g.skku.edu, grtff@swu.ac.kr, wnwo3964@daum.net, yjswu@swu.ac.kr,
semonehyeon@gmail.com, straod7777@gmail.com

Draft Design of a DSPM Model for Minimizing Data Exposure in the Domestic Cloud Environment

Seo-Yeon Lee[1], Ho-Sim Jeong[2], Seung-Chan Lee[3], Jin Yang[4],
Se-Hyeon Kim[5], Hyuk-Jae Yang[6]
[1]Dept. of Forensic Sciences, Sungkyunkwan University
[2]Dept. of Information Security, Seoul Women's University
[3]Dept. of Smart Security, Kon-Yang University
[4]Dept. of Information Security, Seoul Women's University
[5]Dept. of Convergence Security, Hansung University
[6]Tatum Security

요 약

현재 국내에서 클라우드를 사용하는 기업들은 고도화된 정보기술과 보안체계를 구축하여 다양한 서비스를 제공하고 있지만, 중요한 데이터의 노출을 막기 위한 데이터 보안 기술을 갖추고 있는 경우는 드물다. 이로 인해 데이터 유출 사고 발생 시 원인만을 파악할 뿐 실질적인 대안을 갖추지 않은 상황이다. 본 연구에서는 국내 클라우드 환경에서 데이터 노출을 최소화하기 위한 데이터 보안 관리 체계인 DSPM 모델의 초안을 제안한다.

1. 서론

클라우드 컴퓨팅 서비스는 4차 산업혁명과 인공지능 시대의 핵심 인프라로 자리 잡았으며 2023년 기준으로 국내 기업 중 69.5% 이상이 클라우드를 적용하고 있는 것으로 나타났다.[1] 그러나, 마이크로소프트와 같은 초국적 기업에서도 클라우드를 이용한 내부 데이터가 대량으로 노출되는 등의 사고가 빈번하게 발생하고 있다. 특히, 미국 대기업의 60%가 데이터 유출 피해를 입었고, 그 중 80% 이상이 클라우드에 저장된 데이터를 겨냥한 것으로 확인되었다.[2] 해외에서는 크리덴셜 등 내부 데이터 노출을 막을 수 있는 기술 중 하나로 DSPM(Data Security Posture Management) 솔루션의 개발과 도입을 추진하고 있지만, 국내에서는 해당 솔루션의 도입이 초기 단계에도 미치지 못하고 있다. DSPM은 클라우드 환경에서 데이터의 위치, 접근 권한, 사용 패턴을 실시간으로 모니터링하고 분석하여 민감한 데이터 노출 위험을 관리하고 예방하는 역할을 한다. 해외에서 적용하고 있는 다양한 산업의 규제와 데이터 보안 요구사항은 국내와 차이가 있어, 국내 기업들이 동일한 솔루션을 도입하여 적용하기에는 어려움이 있다. 따라서, 국내 클라우드 환경에 적합한 DSPM 모델을 설계하기 위해서는 국내 클라우드 환경 보안 요구사항 및 국내외 데이터 보호 규정 준수 요구사항 등이 고려되어야 한다.

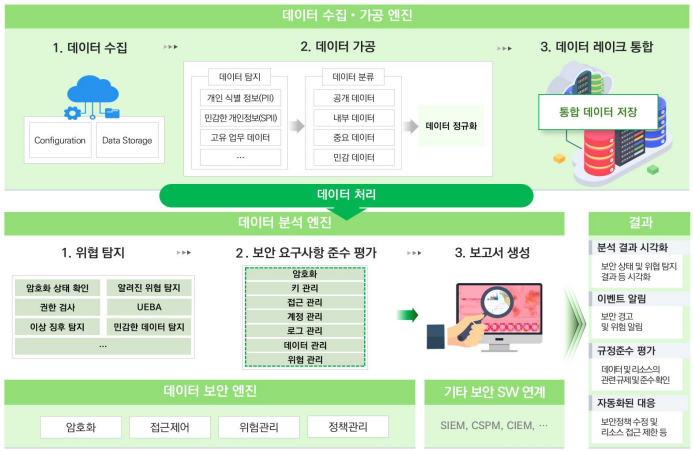
2. 국내 클라우드 환경에 적합한 DSPM 모델 초안 설계

2.1 DSPM 모델 개요

DSPM은 클라우드 환경에서 데이터에 대한 보안을 강화하기 위한 기술로, 민감도, 접근 권한, 저장 및 처리 방식에 따라 데이터 식별 및 위협을 평가하고 관리한다.

본 연구에서의 DSPM 모델은 데이터의 수집, 가공, 통합과 함께 보안 위협을 사전에 식별하고 평가하여 개선하는 것을 목표로 한다. 데이터의 보안수

준에 따라 공개, 내부, 중요, 민감의 총 4가지로 분류하여 적절한 보안 조치를 적용하기 위한 체계를 구축하도록 한다.



(그림 1) 국내 클라우드 환경에서 데이터 노출 최소화를 위한 DSPM 모델

2.2 국내 클라우드 환경 보안 요구사항

국내 클라우드 보안 관련 요구사항으로는 「클라우드 컴퓨팅 서비스 보안 인증에 관한 고시」, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 등과 행정기관에서의 국가정보원 국가 클라우드 컴퓨팅 보안 가이드라인 등이 있다.

온프레미스 환경에서 클라우드 환경으로 전환됨에 따라, 기존의 ISMS-P 규정에서 요구하는 보안 요소들을 클라우드 네이티브 환경에 동일하게 접목시키는데 어려움이 발생하고 있다. 또한 다른 클라우드 보안 관련 요구사항들은 데이터 중요도 및 보안수준에 따라 보안 관리를 세분화하지 않는 한계가 있다. 클라우드 환경에 맞는 구체적인 데이터 보안 규정이 미비한 상황에서, DSPM을 통해 데이터 노출 없이 비즈니스 연속성을 유지하고 사고를 예방할 수 있을 것이다.

2.3 국내외 데이터 보호 규정 준수 요구사항

본 연구에서는 국내의 개인정보보호법, ISMS-P 및 해외의 GDPR, NIST 800-53 등을 기반으로 데이터를 보호하기 위한 요구사항을 분석 및 요약하였다. 기존의 법률 및 인증 체계에서 데이터 보안과 관련된 항목을 선별한 후, 그 중 공통된 요소들을 중심으로 보안 요구사항을 분류하였다. 도출된 보안 요구사항은 크게 암호화, 키 관리, 접근 관리, 계정 관리, 로그 관리, 데이터 관리, 위험 관리의 7가지 범주로 구분된다.

<표 1> 국내외 데이터 보호 규정에 따른 보안 요구사항 분류

분류	관련 규정	요구사항
암호화	ISMS-P	암호정책 적용
	GDPR	데이터 암호화
	NIST 800-53	암호화 보호
	…	
키 관리	ISMS-P	암호키 관리
	NIST 800-53	장치 식별 및 인증 등
	…	
접근 관리	ISMS-P	접근권한 검토
	GDPR	인증 및 권한 관리
	NIST 800-53	접근 통제 정책 및 절차 등
	개인정보보호법	개인정보 처리 시스템 접근 권한 관리 및 접근 통제
	…	
계정 관리	ISMS-P	사용자 계정 관리
	NIST 800-53	계정 관리 등
	개인정보보호법	개인정보 저장 또는 전송 시의 안전성 확보 조치
	…	
로그 관리	NIST 800-53	로그 기록 관리 등
	개인정보보호법	개인정보 처리 시스템 접속 기록 관리 등
	…	
데이터 관리	ISMS-P	정보자산 관리 등
	NIST 800-53	저장 정보 보호 등
	…	
위험 관리	GDPR	위험 관리 및 침해 대응 등
	개인정보보호법	악성 프로그램 방지 등
	…	

이러한 다양한 국내외 보안 요구사항을 바탕으로 DSPM 모델에 데이터를 자동으로 분류하고 민감도에 따라 적절한 보안 조치를 할당하는 기능을 포함하여 클라우드 환경에서의 데이터 보안을 강화할 수 있다.

3. 결론

국가정보원의 '다중계층보안(MLS)'이 도입된다면, 네트워크 중심 보안에서 데이터 중심 보안으로 전환될 것이다. 따라서 클라우드를 사용중인 기업들은 개별 데이터 보안수준의 평가와 관련 정책을 마련하기 위해 DSPM의 도입을 적극적으로 고려할 필요가 있다.

Acknowledgement

본 연구는 한국정보보호산업협회 제1기 ICT융합 보안크루의 지원을 받아 수행되었습니다.

참고문헌

[1] 과학기술정보통신부, 2023 정보화통계집, pp.2, 2024.

[2] 연합뉴스(2023.12.08. 보도), "전 세계 개인정보 유출, 재작년 11억 건→작년 15억 건", https://www.yna.co.kr/view/AKR20231208056500017(2024.09.11. 최종확인)