Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 9 pp. 156-162, 2021

https://doi.org/10.5762/KAIS.2021.22.9.156
ISSN 1975-4701 / eISSN 2288-4688

개인정보보호를 위한 Azure 클라우드 보안 아키텍처 구성

박세준[1], 박연출[2*], 이용준[3]
[1]SK 정보보호담당, [2]LG 로봇선행연구소, [3]극동대학교 해킹보안학과

Configuration Method of Azure Cloud Security Architecture for Personal Information Protection

Se-Joon Park[1], Yeon-Chool Park[2*], Yong-Joon Lee[3]
[1]Information Security Group, SK
[2]Advanced Robotics LAB, LG
[3]Department of Hacking Security, Far East University

요 약 4차 산업혁명이 도래하여 각 산업에서는 클라우드 컴퓨팅, 인공지능, 빅데이터 등의 신기술을 도입 및 활용하고 있으며, 특히 클라우드 컴퓨팅은 다양한 특징과 장점들로 인하여 전 세계의 다양한 산업군에서 활용 가치가 커지고 있다. 그러나 클라우드 컴퓨팅 서비스 도입이 확산함에 따라 보안 취약성 또한 증대되고 있어 클라우드 컴퓨팅 서비스에서의 개인정보 유출에 대한 피해 규모도 증가할 것으로 전망되며, 개인정보 활용성 및 보안에 대한 딜레마 역시 더욱 심화할 것으로 전망되고 있다. 이에 본 연구에서는 최근 이용이 증가하고 있는 Azure 클라우드 서비스에서 개인정보보호를 위한 Azure 클라우드 기반 보안 아키텍처 구성방안을 제안한다. 제안하는 Azure 클라우드 보안 아키텍처는 Azure Well-Architected Framework 상의 보안 항목 및 개인정보보호를 위한 기술적 보안 요건을 고려한 Standard 보안 아키텍처 참조모델과 Azure 기반의 Native 보안 아키텍처 참조모델로 설계하였다. 본 연구에서 제안하는 Azure 보안 아키텍처는 개인정보를 활용하여 안전하고 신뢰성 높은 Azure 클라우드 시스템을 구성하는 많은 기업에 도움이 되기를 기대한다.

Abstract With the advent of the 4th industrial revolution, each industry is using new technology, and due to the many features and advantages of cloud computing, cloud services are being introduced to countless industries around the world at an unbelievably rapid pace. With the rapid increase in the introduction of cloud computing services, security vulnerabilities are increasing. The risk of personal information leakage from cloud computing services is also expected to increase, and the dilemma of personal information utilization and security is expected to intensify. Therefore, this study proposes an Azure cloud-based security architecture configuration method that can be applied to improve personal information security in Azure cloud services. The Azure cloud security architecture proposed in this study is expected to help many businesses and institutions that hope to establish a safe and reliable Azure cloud system.

Keywords : Azure Security, Architecture, Cloud Service, Security Threats, Personal Information Protection

*Corresponding Author : Yeon-Chool Park(LG)
email: yeonchool.park@gmail.com
Received June 14, 2021 Revised July 12, 2021
Accepted September 3, 2021 Published September 30, 2021

1. 서론

4차 산업혁명의 도래로 인하여 데이터 종류의 다양화와 데이터 규모의 확대는 빅데이터, 인공지능, 사물인터넷 등의 기술은 최근에 세계 각국에서 크게 성장하고 있는 기술이다. 4차 산업혁명 시대에는 이러한 방대한 데이터의 활용이 산업현장에서의 경쟁력으로 직결되므로 안전하고 신뢰받는 환경에서 데이터를 더욱 효과적으로 활용하는 기업일수록 특정 시장에 대한 지배력을 선점할 수 있는 환경으로 변화하고 있다. 최근 Digital Transformation이 가속화됨에 따라 국내/외 기업들의 클라우드 컴퓨팅의 전환이 급격하게 증가하고 있고 이에 따른 클라우드 컴퓨팅 책임공유모델에 따라 클라우드 컴퓨팅 환경 내 데이터 보안에 대하여 클라우드 사용자에게 책임과 보안의 필요성이 제고되고 있으며, 클라우드 Migration에 따른 비용과 보안에 대한 이슈도 증가하게 되었다. 클라우드 컴퓨팅 사용으로 인하여 Application에서 플랫폼 비즈니스로의 확대, SaaS 환경으로의 변화, 기존 On-Premise 자원에서 가상화 및 컨테이너 기반 인프라 환경으로의 구성, CI(Continuous Integration)/ CD (Continuous Delivery) 구성을 통한 DevOps 기반 운영 관리로의 변화가 발생하고 있다.

이처럼 증가하고 있는 클라우드 컴퓨팅 기반 시스템 구축으로 IT 환경들이 변화되고 있고 이에 따라 보안의 환경도 변화되고 있다. 클라우드 컴퓨팅 서비스에서의 개인정보보호 유출 역시 증가할 전망이다[1,2]. 클라우드 컴퓨팅 기술은 자원 공유, 가상화 등의 특성으로 인해 보안 위협들이 항상 내재하여 있고, 이러한 클라우드 컴퓨팅의 안전성 및 신뢰성 등에 대한 보안 문제로 인해 아직도 많은 기업이 클라우드 컴퓨팅 서비스 도입을 망설이고 있어 클라우드 산업의 활성화와 보안 문제에 따른 신뢰성 해결이 시급한 실정이다. 하지만, 기존 On-Premise 기반의 보안 아키텍처 구성만으로는 클라우드 컴퓨팅 환경으로의 변화에서 요구하는 보안에 대해서 한계가 있으므로 클라우드 컴퓨팅 기반 시스템 구축 시 적용할 수 있는 보안 아키텍처 구성이 요구되고 있다. CSP(Cloud Service Provider)에서 제시하는 참조 아키텍처 구성만으로는 개인정보 처리를 위한 국내 개인정보보호법 내 기술적 보호조치를 충족하기에는 부족한 부분이 있으므로 개인정보보호를 위한 보안 요건을 준수하며 CSP의 특화된 보안까지 고려한 보안 아키텍처 설계에 대한 필요성이 대두되고 있다.

이에 따라 본 연구에서는 클라우드 컴퓨팅 보안 위협과 개인정보 유출 사고 사례에 대해 살펴본 후 최근 많은 기관과 기업들이 이용하고 있는 Azure 클라우드 환경에서의 개인정보보호 처리를 고려한 보안 아키텍처 구성 및 활용방안을 제안한다.

2. 관련 연구

2.1 클라우드 컴퓨팅 책임공유 모델

클라우드 컴퓨팅 모델의 정의와 관련하여 가장 널리 사용되는 모델은 NIST(National Institute of Standards and Technology)에서 정의된 모델로서 클라우드 컴퓨팅을 최소한의 관리나 서비스 제공자의 상호 작용만으로도 컴퓨팅 시스템을 구성하는 자원들을 신속하고 편리하게 제공받을 수 있는 서비스로 정의한다[3]. 클라우드 서비스 모델은 일반적으로 서비스 유형에 따라서 IaaS (Infrastructure-as-a-Service), PaaS(Platform-as-a-Service), SaaS(Software-as-a-Service)로 분류할 수 있다[4,5].

클라우드 컴퓨팅 환경에서는 각각의 클라우드 컴퓨팅 모델 유형에 따라 클라우드 제공업체와 서비스 이용 고객인 기업이 보안에 대한 책임을 공유하는 책임공유모델을 기반으로 한다. 기존 On-Premise 환경에서는 물리적인 영역부터 Application, 데이터 영역까지도 모두 기업이 관리해야 하는 영역이었지만, 클라우드 컴퓨팅 환경에서는 IaaS와 같이 물리적인 영역, 하이퍼바이저 영역까지는 클라우드 제공업체가 관리하고 가상서버, Application 및 데이터 영역에 대해서는 기업이 관리해야 하는 영역으로 구분되어 있다. PaaS의 경우에는 미들웨어 부분까지는 클라우드 제공업체가 관리하고 Application 및 데이터 영역에 대해서 기업이 관리하는 영역으로 구분되어 있으며, SaaS의 경우에는 Application 영역까지 클라우드 제공업체가 관리하고 데이터 영역에 대해서만 기업이 관리하는 부분으로 구분되어 있다. 즉, 보안 관점에서도 클라우드 제공업체와 기업이 각각 관리하는 영역에 대한 보안을 책임지는 책임공유 모델 기반의 보안 관리가 필요하다.

2.2 클라우드 컴퓨팅 보안 위협

클라우드 보안 관련 국제연합조직인 Cloud Security Alliance에서는 매년 Cloud 환경에서의 보안 위협을 지속해서 발표하고 있다. 2010년 클라우드 컴퓨팅 7대 위

협부터 2016년 클라우드 컴퓨팅 12대 위협[6], 2019년 클라우드 컴퓨팅 11대 위협[7]과 같이 클라우드 서비스의 도입 및 이용이 활성화됨에 따라 클라우드 컴퓨팅 보안 위협도 관리적, 기술적 범위에서 점진적으로 증가하고 있으며, 보안 설정 오류, 보안 아키텍처/전략 미흡, 불충분한 권한관리에 대한 보안 위협은 기존 대비 클라우드 컴퓨팅 환경에서 새롭게 추가된 보안 위협으로써, 클라우드 컴퓨팅 사용자의 책임 영역 내에서 발생하는 보안 위협이다. 이는 클라우드 제공업체의 책임 영역이 아니므로 서비스 이용 고객인 기업이 책임 영역에 대한 명확한 인식을 통해 클라우드 컴퓨팅 환경 내 보안에 대한 활동이 중요하다는 것을 의미한다[8,9].

클라우드 보안 위협에 따른 사고 사례의 원인을 살펴보면 잘못된 인증/인가로 인한 데이터 유출 대응 미흡, 잘못 구성된 자원의 모니터링 자동화, 클라우드 컴퓨팅 기반 보안 아키텍처 수립 미흡, 최소권한 원칙에 따른 특수계정 인증 강화 미흡, 심층 방어기법 및 계정관리 미흡, 잘못된 접근권한에 대한 감사 및 주기적 교육 미흡, API 키 대상 보호 및 재사용 관리 미흡, 클라우드 컴퓨팅 적용 시 Managed 서비스 보안 설정 제어 미흡, 클라우드 컴퓨팅 환경에 대한 이상징후 모니터링 미흡 등으로 볼 수 있다. CSA의 가장 최근 발표 자료에 따르면 클라우드 보안 위협 요소는 시스템 취약성, 분산 서비스 공격 등 기술적 문제보다 내부자의 도덕적 해이, 불충분한 관리와 부주의 등 기술 외적인 문제와 관련된 것들이 매우 중요한 요소임을 지적하고 있다. 이는 곧 기술적 위협 대응책이 있어도 결국 내부 인력에 의한 의도된 위협은 막기 어렵고, 내부자들에 대한 보안 인식이 클라우드 서비스 보안을 위해 매우 중요한 요소임을 알 수 있다.

2.3 클라우드 서비스 개인정보유출 사고 사례

퍼블릭 클라우드 컴퓨팅의 경우 개인이나 기업의 민감한 데이터들이 외부 공간에 저장되어 있다는 점에서 신뢰성, 안정성 등의 보안 문제가 제기될 수 있다. Table 1에서와 같이 클라우드 환경에서의 개인정보 유출 사고에 관한 사례를 살펴보면, 개인정보 유출 사고 대부분은 기존의 보안 위협으로부터 발생하는 유형임을 볼 수 있다[10].

Table 1. Personal Information Leakage Incident

Cloud Vendor	Leakage Incident Case
AWS('19.07)	Hacking using F/W vulnerability
Apple('14)	Leakage due to capture authority
ZenDesk('13.02)	Hacking using SW vulnerability
Google('11.02)	Deletion message using S/W error
MS('10)	Leakage due to resource sharing

AWS는 미국의 대형은행에서 관리 실수로 방화벽 취약점을 이용하여 개인정보가 해킹된 사고가 있었고, Apple은 권한 탈취를 통하여 유명 배우들의 사진이 유출되는 사고가 있었으며, ZenDesk는 S/W 취약점을 이용한 해킹을 통하여 개인정보가 유출되는 사고 사례를 확인할 수 있다. Google에서는 S/W 구현 오류로 사용자의 주소록 및 메시지가 삭제되는 사고가 있었고, MS에서는 클라우드 서비스 환경설정 오류로 인하여 클라우드 서비스를 사용하는 기업정보가 타인에게 유출되는 사고 사례를 확인할 수 있다. 이처럼 기존과 같은 보안 위협으로부터 혹은 클라우드의 가상화 기술 및 Multi-Tenancy 기술로 인한 공유자원 문제로부터 개인정보 유출 사고가 발생하고 있음을 알 수 있다.

3. Azure 보안 아키텍처

3.1 Azure Well-Architected Framework

Azure 보안 아키텍처는 Azure Well-Architected Framework 및 개인정보의 기술적 보호조치 보안 요건이 반영된 참조 아키텍처 모델을 제시한다. Azure Well-Architected Framework에서는 '비용 최적화', '운영 효율성', '성능 효율성', '안정성', '보안'의 5개 영역을 제시하고 있으며, Table 2와 같이 보안영역에서는 '조직 위험 감소', '거버넌스/위험 및 규정 준수', 'ID 및 접근관리', '네트워크 및 인프라 보호', '데이터 보호', 'Application/서비스', '관리', '보안 운영'과 같이 총 8개의 보안 항목으로 구성된다.

Table 2. Security in Azure Well-Architected Framework

Security Area	Azure Service
[1] Organization Risk Reduction	Site Recovery
[2] Conform Governance/Regulation	Policy, Advisor
[3] ID&Access Management	AD, Activity Logs
[4] N/W, Infra Protection	NSG, VPN, WAF
[5] Data Protection	Key Vault, ASC
[6] Application, Service	DevOps
[7] Management	Just-In-Time
[8] Security Operation	Sentinel, SC

'조직 위험 감소'에서는 Azure 내 서비스의 가용성 확보를 위하여 Pared-Region을 활용한 Site Recovery를 통해 백업을 구성하도록 제시하고 있으며, '거버넌스/위험 및 규정 준수'에서는 Azure Policy를 통해 조직이 준수해야 하는 규칙 등 거버넌스를 수립하고 'ID 및 접근관리'에서는 Azure AD를 통해 자원에 대한 역할 기반 접근통제를 구현함으로써 Activity Logs를 통해 Azure AD 사용자 행위에 대한 로깅과 책임 추적성 확보를 제시하고 있다. '네트워크 및 인프라 보호'에서는 Network Security Group, Azure Firewall을 통해 자원에 대한 접근통제와 DDoS Protection을 통한 네트워크에 대한 보호를 제시하고 있으며, '데이터 보호'에서는 Key Vault를 통해 Storage Account, SQL DB 등 자원에 대한 암호화와 App Service Certificate의 전송구간 암호화를 통해 데이터의 안전한 보호를 제시하고 있다. 'Application/서비스'에서는 App Service를 통해 웹서버의 환경변수를 Azure 상에 안전하게 보호하는 방안을 제시하고 '관리'에서는 Azure AD의 자원 접근권한이 상시 부여되지 않고 필요할 때 승인 절차에 의해 부여될 수 있도록 Just-in-time 활용방안을 제시하며, 마지막으로 '보안 운영'에서는 Sentinel을 통해 Azure 상의 보안 위협을 모니터링하고 Security Center를 통해 Azure Policy에서 정의한 조직 거버넌스에 대한 준수 여부와 ISO, CIS 등 글로벌 표준 준수율의 지속적인 관리방안을 제시하고 있음을 볼 수 있다.

3.2 Azure 보안 아키텍처 구성방안

Well-Architected Framework 기반으로 Azure에서 제시하고 있는 보안 아키텍처는 기본적인 Native 서비스 구성만으로 제시되어 있어, 개인정보 처리 시 개인정보보호를 위한 기술적 보호조치 요건을 충족하기 위해서는 Azure 보안 Native 서비스 추가 반영 및 3rd-Party 적용에 대한 고려가 필요하다. 이와 함께 3rd-Party 적용 영역에 대해서 Azure Native 서비스로의 대체 가능성 및 한계점을 검토하여 비용 효율화 관점에 대해서도 고려할 필요성이 있다. 이를 위하여 Table 3에서와 같이 Standard 보안 아키텍처 참조모델과 Native 보안 아키텍처 참조모델을 제시한다.

Standard 보안 아키텍처 참조모델은 개인정보보호를 위하여 요구되는 기술적 보호조치 요건 및 추가 보안 강화를 위한 구성방안을 제시하고, Native 보안 아키텍처 참조모델은 Azure Native 서비스 중심으로 구성하여 보안 비용 효율화 관점을 고려한 구성방안을 제시한다.

Table 3. Security Architecture Reference Model

Type	Description
Standard	Regulation based architecture
Native	Native Service based architecture

4. Azure 보안 아키텍처 구성방안

4.1 Standard 보안 아키텍처 구성

Standard 보안 아키텍처 참조모델은 Azure Well-Architected Framework 상의 보안 항목에서 기본적으로 제시되고 있는 Azure Native 서비스를 포함하고 개인정보보호를 위한 기술적 보호조치 요건 준수 및 추가 보안 강화를 위하여 DDoS Protection Standard, Key Vault Premium, Security Center Standard, Azure AD PIM, Azure AD 조건부 액세스, Azure AD Identity Protection, Purview 서비스를 추가로 고려하여 Fig. 1과 같이 구성하였다.

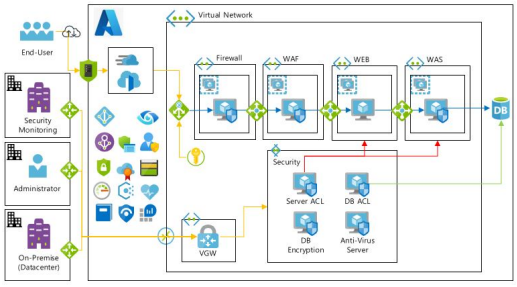


Fig. 1. Standard Security Architecture

Standard 보안 아키텍처 참조모델은 Azure Well-Architected Framework에서 제시하는 8가지 보안 항목 기반으로 법규/규제에서 요구하는 수준을 충족할 수 있도록 다음과 같이 설계하여 제시하였다.

조직 위험 감소 영역에서는 Application에 대한 복원력 설정을 위하여 Snap Shot, Paired-Region을 활용한 Site Recovery를 통해 가용성을 확보하도록 구성한다. 거버넌스/위험 및 규정 준수 영역에서는 Azure 환경 내에서 IT 및 보안 거버넌스를 정의할 수 있는 Azure Policy를 통해서 Azure 환경 내에서 조직이 준수해야 할 보안 정책들을 정의하고 Security Center(Standard)를 통해 Policy에 사전에 정의된 규칙의 위반 사항들을 모니터링 가능하도록 구성한다. ID 및 접근관리 영역에서는 Azure AD를 통해 업무 역할별 적정한 권한을 부여하

고, Activity Log를 통해 모든 자원의 접근과 변경사항에 대해서 로그를 개인정보보호를 위한 기술적 보호조치에서 요구하는 기간을 보존하고 주기적으로 적정성 검토를 수행하며 Azure AD PIM, Azure AD 조건부 액세스, Azure AD Identity Protection 기능을 통해 특정 국가와 IP, 장치에서만 접근할 수 있도록 추가적인 보안을 강화한다. 네트워크 및 인프라 보호 영역에서는 웹 서비스에 접근하는 트래픽에 대해서 Front Door의 Geo-Blocking 기능 활성화를 통해 불필요한 해외 트래픽을 차단하여 보안 위협을 최소화하고, DDoS Protection(Standard)을 통해 DDoS 공격에 대한 방어체계를 구성하고 침입탐지시스템과 웹 방화벽을 통해 유해 트래픽과 웹 취약점에 대한 공격을 방어하도록 구성한다. Virtual Network 내의 Virtual Machine, Azure SQL과 같은 중요 자원 대상의 원격 접속은 인터넷망을 통해 접근이 불가하도록 Network Security Group을 설정하고 Azure VPN Connection을 통해 Virtual Network 내에 있는 서버 접근통제, DB 접근통제 솔루션을 거쳐 Virtual Machine과 Azure SQL 등에 접속할 수 있도록 접근통제와 권한관리를 적용하고 작업 이력은 모두 보존하도록 구성한다.

데이터 보호 영역에서는 전송 시 암호화와 저장 시 암호화 적용이 필요하며, 전송 시 암호화는 End-User와 웹 서버 간의 인터넷망 통신 구간을 암호화하는 것으로 App Service Certificate를 통해 SSL 인증서를 Application Gateway 혹은 웹 서버에 적용하여 구성하고, 저장 시 암호화는 중요한 데이터가 보관되는 Storage Account, Azure SQL 등 데이터 저장소에 Key Vault(Premium)의 암호화 키를 통해 저장소 내 데이터를 암호화하도록 구성한다. Application/서비스 영역에서는 App Service를 통하여 환경변수가 안전하게 관리되도록 구성하고, 관리 영역에서는 필요시에만 Azure AD 접근권한 부여를 위한 Just-in-Time 서비스를 구성하며, 보안 운영 영역에서는 Log, Azure Activity Log를 기반으로 Azure 환경 내에서의 위협을 탐지하는 지능형 탐지 서비스인 Azure Sentinel을 활용하여 Azure 환경 내 보안 위협을 탐지하고 분석할 수 있는 체계를 구성하며 Security Center(Standard)를 통해 Azure 환경 내 보안 설정에 대한 자동화된 스코어링을 통해 보안 수준 관리가 가능하도록 구성한다. 또한 Purview 서비스를 통하여 Azure SQL, Storage Account 내 저장된 개인정보 등에 대한 현황을 주기적으로 점검할 수 있도록 구성한다. 이처럼 8가지 보안 항목 기준으로 추가 구성이 필요한 Native 서비스까지 고려한 보안 아키텍처를 구성한 후에는 개인정보보호를 위한 기술적 보호조치 충족을 위하여 Table 4에서와 같이 영역별 보안솔루션 적용이 필요하며, Figure 1에서와 같이 DDoS, Firewall, SSL-VPN, 전송구간 암호화 영역 외에는 일반적으로 3rd-Party 보안솔루션이 많이 활용되고 있다.

Table 4. Security Domain & Area

Domain	Security Area	Solution
N/W	DDoS	Native
	Firewall	Native
	IDPS	3rd-Party
	SSL-VPN	Native
DB/Storage	DB Access Control	3rd-Party
	Data Encryption	3rd-Party
Server	Server Access Control	3rd-Party
	Anti-Virus	3rd-Party
Application	Web Firewall	3rd-Party
	Transmission Encryption	Native

4.2 Native 보안 아키텍처 구성

Native 보안 아키텍처 참조모델은 Fig. 2와 같이 Standard 보안 아키텍처 참조모델 상의 3rd-Party 보안솔루션을 Azure Native 서비스로 대체 구성하여 설계하여 제시하였다.

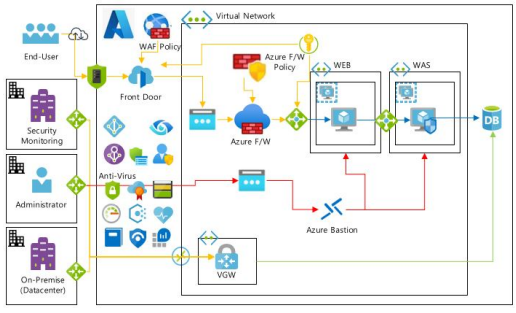


Fig. 2. Native Security Architecture

Table. 5는 N/W, DB/Storage, Server, Application 각각의 영역 기준으로 제시하고 있는 Azure Native 서비스 대상으로 개인정보보호를 위한 기술적 보호조치 충족 여부에 대한 검토 결과를 나타낸 것이다.

Table 5. Azure Native Service Verification

Domain	Security Area	Azure Native	Verification
N/W	DDoS	DDoS Protection	O
	Firewall	NSC/ Azure F/W	O
	IDPS	Azure F/W IDPS	△
	SSL-VPN	VPN Gateway	△
DB/ Storage	DB Access Control	-	△
	Data Encryption	Key Vault	O
Server	Server Access Control	Bastion	△
	Anti-Virus	MS Defender	O
Appl.	Web Firewall	WAF Policy	△
	Transmission Encryption	Front Door/ Key Vault	O

Azure Native 서비스 중에서 DDoS Protection, NSG/ Azure F/W, Key Vault, MS Defender, 전송구간 암호화 서비스는 별도 고려사항 없이 보안 아키텍처 구성이 가능하다. Azure SQL Database, SQL Database Managed DB 대상으로는 필드 암호화 기능도 제공하고 있으며, 최근 Windows 및 Linux 대상으로 MS Defender for Endpoint 서비스가 출시되어 Anti-Virus 영역까지 Native 보안 아키텍처 구성이 가능하다. Azure F/W IDPS, VPN Gateway, DB 접근통제, Azure Bastion, WAF 구성 시에는 다음과 같은 사항을 고려하여야 한다. Azure F/W IDPS 서비스와 WAF Policy 서비스는 기본적으로 Managed Rule-set을 제공하고 있지만, 국내 보안관제 수행 사례가 없어 자체 모니터링 체계 구축이 필요하다. VPN Gateway 서비스는 SSL-VPN 접속, MFA를 제공하지만, 사용자별 Destination IP 접근제어가 어려운 한계점이 존재하여 VPN Gateway 기반의 DB 접근통제 구성 시에는 DB 접속을 위해 Azure AD에 토큰을 요청하는 단계에서 DB 접근권한을 Resource Group 단위로 제어할 수 있도록 추가적인 구성이 필요하다. DB 접근통제 구성 시에는 개인정보보호 기술적 보호조치 요건에서 요구하는 로깅을 위해서는 DB 엔진을 통한 로깅 구성이 필요하며 이 경우 DB 자체에 성능저하를 유발할 수 있으므로 이를 사전에 고려하여 DB Spec. 구성이 필요하다. Azure Bastion 서비스는 Azure AD를 통해 사용자별 Bastion에 대한 접근통제를 구성할 수는 있으나, Bastion에서 VM에 대한 접근권한을 관리할 수 없으므로 사용자 그룹별 Bastion을 별도로 구성하는 보안 아키텍처 구성이 필요하다.

5. 결론

최근 클라우드 컴퓨팅 서비스 활성화가 가속화됨에 따라 클라우드 환경에서의 개인정보보호는 기존 보안 취약점뿐만 아니라 가상환경, Multi-Tenancy 등 기술적 환경 기반의 보안 취약점에 대한 고려가 필요하다. 이를 위해 우선 관련 연구로서 클라우드 서비스 모델 및 책임공유 모델을 살펴보았고, 클라우드 컴퓨팅 보안 위협에 대해 정리하였으며, 클라우드 서비스 내 개인정보 유출 사고 사례를 분석하였다. 이후 관련 연구를 참조하여 Azure Well-Architected Framework 상의 보안을 고려한 Azure 보안 아키텍처 참조모델을 구성하여 제안하였다.

Azure Well-Architected Framework 내 8가지 보안 요건을 고려하여 2가지 유형의 Azure 보안 아키텍처 참조모델을 제시하였다. Azure 클라우드에서 가용한 모든 보안을 구성함으로써 개인정보보호를 위한 기술적 보호조치 요건을 충족하는 수준의 Standard 보안 아키텍처 참조모델을 제시하였고, Standard 보안 아키텍처 참조모델 상의 3rd-Party 보안솔루션을 Azure Native 서비스로 대체한 Native 보안 아키텍처 참조모델을 제시하였다.

Azure 클라우드 보안 아키텍처 구성을 통하여 Azure AD 기반의 사용자 계정 생성, 역할 정의와 자원에 대한 액세스를 통합적으로 관리할 수 있고 Sentinel을 통하여 Azure 내 보안 위협 모니터링 외에도 타 CSP의 보안 위협을 통합적으로 모니터링이 가능하므로 추후 멀티클라우드 환경 기반의 보안 아키텍처 구성에 대한 부분도 고려가 필요한 부분으로 판단된다.

본 연구에서 제안한 Azure 클라우드 보안 아키텍처 참조모델이 앞으로 안전하고 신뢰성 높은 Azure 클라우드 시스템을 구축하고자 하는 기업에 도움이 되기를 기대한다.

References

[1] Wang, T., Zhou, J., Huang, M., Bhuiyan, M. Z. A., Liu, A., Xu, W., & Xie, M., "Fog-based storage technology to fight with cyber threat", *Future Generation Computer Systems*, 83, 208-218, 2018. DOI: https://doi.org/10.1016/j.future.2017.12.036

[2] KIM, M.K., *The Improvement of domestic cloud security certification system through the comparative analysis with the CSA*, Master's Theses, Graduate

School of Soon Chun Hyang University, pp.3-9, 2019.

[3] Peter Mell, and Tim Grace, "The NIST Definition of Cloud Computing", *National Institute of Standards and Technology, U.S. Department of Commerce*, Version 15, Oct 2011.
DOI: https://doi.org/10.6028/NIST.SP.800-145

[4] ENSI-MARIA, IaaS, PaaS, SaaS – What do they mean?, Cloud on move, 2017,

[5] Multi-Cloud Blog, SaaS vs PaaS vs IaaS: What's The Difference and How To Choose, https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose (accessed Aug. 24, 2020)

[6] Cloud Security Alliance, The Trecherous 12, Cloud Computing Top Threats in 2016, 2016.

[7] Cloud Security Alliance, Top Threats to Cloud Computing in 2019, The Egregious 9, 2019.

[8] LA, Y.S., *Cloud Computing Service Security Assurance Programs Comparison Analysis and Improvement Suggestions*, Graduate School of Nam Seoul University, pp.1-6, 2016.

[9] Lee, C.J., A *Study on security requirements for privacy in a home cloud environment*, Graduate School of Soon Chun Hyang University, pp.8-14, 2017.

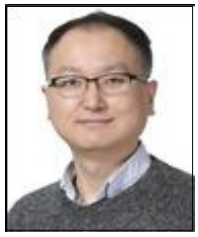
[10] LIM, S.Y., *A Study on the Management System for Domestic Personal Information Protection in the Cloud Environment*, Graduate School of KONKUK University, pp.1-19, 2020.

박 세 준(Se-Joon Park) [정회원]

- 1996년 2월 : 숭실대학교 수학과 (이학사)
- 1998년 2월 : 숭실대학교 컴퓨터 공학과 (공학석사)
- 2004년 8월 : 숭실대학교 컴퓨터 공학과 (공학박사)
- 2006년 1월 ~ 현재 : SK 정보보호 담당 수석연구원

〈관심분야〉
개인정보보호, 인공지능보안, 정보보호

박 연 출(Yeon-Chool Park) [정회원]



- 2004년 2월 : 숭실대학교 컴퓨터 학과 (공학박사)
- 2005년 4월 ~ 2009년 3월 : 성균관 대학교 ISRI 연구교수
- 2009년 5월 ~ 2010년 6월 : 스웨덴 Umea Univ. Post-Doc.
- 2011년 4월 ~ 2013년 2월 : 프랑스 Pascal Institute Post-Doc.
- 2013년 9월 ~ 현재 : LG전자 CTO 책임연구원

〈관심분야〉
컴퓨터비전, 로봇비전, 인공지능

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터 학과 (공학박사)
- 2010년 2월 ~ 2016년 3월 : 한국 인터넷진흥원 수석연구위원
- 2016년 4월 ~ 2020년 3월 : 국방 보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
인공지능보안, 국방보안, 해킹보안