Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 8 pp. 509-515, 2024

https://doi.org/10.5762/KAIS.2024.25.8.509
ISSN 1975-4701 / eISSN 2288-4688

방산업체 취약점 관리 시스템 구축 방안

최지웅, 황도빈, 임준영, 김건태*
국방기술품질원

A Method of Building Vulnerability Management System in Defense Industry Companies

Jiung Choi, Dobin Hwang, Jun-Yeong Lim, Guntae Kim*
Defense Agency for Technology and Quality

요 약 본 논문은 방산업체의 취약점 진단 현황을 분석하고, 취약점 관리 시스템(Vulnerability Management System)의 필요성을 제시하는 것을 목표로 한다. 방산업체는 최근 북한 해킹 조직의 표적이 되어 심각한 보안 사고를 경험했으며, 이는 체계적인 취약점 분석과 평가의 필요성을 강조한다. 방산업체의 취약점 진단 현황을 분석한 결과, 정보보호 전문 역량 부족과 예산 부족 등의 이유로 인해 자체적인 취약점 분석과 평가가 어려운 점이 드러난다. 민간 분야에 비해 방산 분야는 망분리(Network Separation) 규제, 엄격한 보안 절차, 높은 비용 등의 문제로 인해 취약점 진단 시스템 도입이 어렵다. 이를 해결하기 위해 방산업체의 사이버 보안 강화를 위해 자동화된 취약점 관리 시스템의 도입이 필요하다. 하이브리드 진단 방식은 방산업체의 망분리 환경에 적합하며, 정기적인 보안 스캐닝과 실시간 모니터링을 통해 효율적인 취약점 진단을 수행할 수 있다. 또한, 중앙형 취약점 진단 시스템 구축과 관계 기관 간의 상호인정협정을 통해 방산업체의 업무 부담을 줄이고 보안 관리를 체계적으로 수행할 수 있다. 결론적으로, 방산업체의 사이버 보안을 강화하기 위해서는 자동화된 취약점 관리 시스템의 도입이 필요하다. 이를 통해, 방산업체는 전문 인력에 대한 의존도를 줄이고 효율적으로 보안 체계를 강화할 수 있다. 궁극적으로, 방산업체 취약점 진단 시스템 구축은 방산업체의 정보자산을 보호하고 국가 안보를 강화하는 데 중요한 역할을 할 것이다.

Abstract This study analyzed the current state of vulnerability assessment in defense industry companies to highlight the necessity of implementing a vulnerability management system. Recently, defense companies have experienced severe security incidents as they have become targets of North Korean hacking groups, underscoring the importance of systematic vulnerability analysis and assessment. An analysis of the current state of vulnerability assessments in defense companies reveals difficulties in conducting self-assessments and evaluations because of a lack of professional security expertise and insufficient budgets. Compared to the civilian sector, the defense sector faces challenges in adopting vulnerability assessment systems due to network segregation regulations, stringent security procedures, and high costs. Therefore, adopting an automated vulnerability management system is necessary to enhance cybersecurity in defense companies. A hybrid diagnostic approach, suitable for the segregated network environment of defense companies, can perform efficient vulnerability assessments through regular security scanning and real-time monitoring. In addition, establishing a central vulnerability assessment system and mutual recognition agreements between relevant agencies can reduce the workload and enable systematic security management. In conclusion, implementing an automated vulnerability management system is essential to strengthening the cybersecurity of defense companies. This will reduce the dependence on professional personnel and enhance security frameworks more efficiently. Establishing a vulnerability assessment system in defense companies will be crucial in protecting their information assets and strengthening national security.

Keywords : Vulnerability Management System(VMS), Defense Industry, Vulnerability, CVSS, OWASP

*Corresponding Author : Guntae Kim(Defense Agency for Technology and Quality)
email: guntae_kim@dtaq.re.kr
Received July 4, 2024 Revised July 31, 2024
Accepted August 2, 2024 Published August 31, 2024

1. 서론

국가 안보와 직결된 방산업체는 사이버 보안의 중요성이 매우 크다. 2022년 말에는 북한 해킹조직이 해양·조선 기술을 연구하는 방산기관에 침투하기 위해 보안이 취약한 유지보수 업체를 먼저 해킹하였다. 우선 서버 계정정보를 탈취하였고, 이후 기관 서버에 등에 무단 침투하여 악성코드 유포를 시도 하였다[1]. 이어 2024년 4월에는 라자루스(Lazarus), 안다리엘(Andariel), 킴수키(Kimsuky) 등 북한 정부의 지원을 받는 주요 해킹 그룹들이 대한민국 방산업체들을 대상으로 전면적인 스파이 활동을 하였다. 이들은 일부 표적의 네트워크에 1년 넘게 잠복하여 방산업체들을 집중적으로 공격하기 위해 테스트 목적으로 열려있는 망 연계 시스템을 장악하였다. 개발팀 직원 컴퓨터 등 내부망의 중요자료를 수집하고 국외 클라우드 서버로 빼돌리는 수법을 통해 많은 방산업체들이 피해를 입었다[2]. 실제로 Fig. 1과 같이 북한 해킹 그룹의 소행으로 공개적으로 지목된 2009년 7월부터 2023년 5월까지의 사이버 공격 273건을 분석한 결과를 보면 북한의 사이버 전략은 정보수집과 같은 첩보 활동이 주 목적이며, 공격의 71.5%를 차지하고 있다[3].

이렇게 지속적인 북한의 해킹 공격을 분석한 결과, 공격자들은 기업의 Active Directory를 장악해 내부에 악성코드를 유포하는 대신 보안 소프트웨어의 제로데이 취약점을 악용하고 있다. 따라서 공격의 흐름을 전략·전술 관점에서 바라보고 적극적인 보안 대책이 필요하다. 개발 환경에서 보안 취약점을 최소화하고 취약점 발견 시 신속한 대응이 중요하며, 공격을 즉시 확인할 수 있는 가시성 확보가 필수적 요소로 대두되었다[4]. 이러한 상황 속에서 민간에서는 취약점 관리 시스템을 통한 주요정보통신기반시설 보안취약점 관리 방안에 대한 선행 연구가 진행되었다[5].

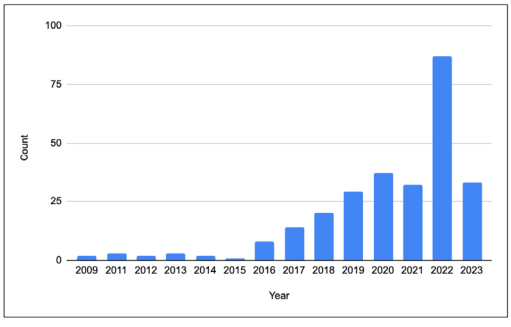

Fig. 1. Breakdown of cyberattacks attributed to North Korean state-sponsored actors by year (Recorded Future, North Korea's Cyber Strategy, June 2023)

이에 따라, 본 논문은 현재 방산업체 취약점 진단 현황을 분석함으로써 민간대비 방산분야 취약점 진단 시스템 도입의 한계를 식별하였으며, 식별한 한계점을 개선할 수 있는 방산업체 취약점 관리 시스템 구축을 위한 기술적, 제도적 방안을 제안한다.

2. 이론적 배경

2.1 취약점 평가 및 분석방법론

2.1.1 CVSS (Common Vulnerability Scoring System)

CVSS는 보안 취약점을 객관적으로 평가하고 그 심각도를 측정하는 표준화된 방법론이다. CVSS는 2005년 미국 국토안보부(DHS) 산하의 국립 사이버 보안 부문(NCSD)에서 시작되었으며, 현재는 FIRST(Forum of Incident Response and Security Teams)에 의해 관리되고 있다. CVSS의 목적은 취약점의 심각도를 평가하는 일관되고 표준화된 접근 방식을 제공하여 조직이 다양한 취약점을 비교하고 정량적으로 평가할 수 있도록 하는 것이다. CVSS는 기본(Base), 시간적(Temporal), 환경적(Environmental) 메트릭으로 구성되어 있으며, 각각 취약점의 본질적인 특성, 현재 상태와 관련된 요소, 특정 조직의 환경에서의 영향을 평가한다. CVSS 점수는 심각도의 지표로 사용되며 보안 위험도를 직접적으로 나타내지는 않지만, 이러한 구조는 CVSS가 다양한 상황에서 취약점의 위험을 종합적으로 평가할 수 있도록 한다[6].

2.1.2 OWASP (Open Web Application Security Project)

OWASP는 2001년에 설립된 비영리 단체로, 웹 애플리케이션 보안을 강화하는 것을 목표로 한다[7]. OWASP는 전 세계 보안 전문가, 개발자, 연구자들이 참여하는 글로벌 커뮤니티로, 웹 보안 관련 자료, 도구, 문서, 표준 등을 무료로 제공한다. 주요 프로젝트 중 하나인 OWASP Top 10은 웹 애플리케이션에서 가장 흔하고 치명적인 보안 취약점 10가지를 정리한 목록으로, 보안 전문가와 개발자들에게 중요한 참고자료로 사용된다. OWASP는 보안 베스트 프랙티스를 공유하여, 개발자와 조직이 보다 안전한 소프트웨어를 개발할 수 있도록 지원하며, 이는 취약점 진단 시스템이 효과적으로 운영될 수 있도록

돕는다. OWASP의 가이드와 프레임워크는 보안 설계, 코딩, 테스트, 배포 등 소프트웨어 개발 라이프사이클 전반에 걸쳐 적용될 수 있다.

2.2 취약점 진단 기술

2.2.1 네트워크 기반 스캐닝

네트워크 기반 스캐닝은 네트워크 트래픽, 포트 상태, 서비스 버전 등을 분석하여 잠재적인 취약점을 탐지한다. 네트워크 상의 모든 장치와 시스템을 대상으로 하여 네트워크 토폴로지 전반에 걸쳐 취약점을 식별하며, 실시간으로 네트워크 환경을 모니터링하여 새로운 취약점을 빠르게 발견한다. 이를 통해 조직의 전체 네트워크 인프라를 종합적으로 평가할 수 있으며, 정기적인 스캐닝을 통해 보안 상태 변화를 추적하고, 새로운 취약점이 발생할 때마다 이를 신속히 탐지할 수 있다.

2.2.2 호스트 기반 스캐닝

호스트 기반 스캐닝은 개별 장치와 시스템 내부의 보안 취약점을 식별하고 평가한다. 각 호스트의 파일 시스템, 레지스트리, 구성 파일, 실행 중인 프로세스를 검사하여 내부적으로 존재하는 취약점을 탐지하며, 이를 통해 데이터베이스 설정과 접근 권한, 권한 상승 공격이나 데이터 유출 가능성을 확인할 수 있다. 또한, 실시간 감시 기능을 제공하여 즉각적인 보안 이벤트를 탐지하고 대응할 수 있게 한다. 예를 들어, 중요 파일이 비정상적으로 수정되거나 악성 소프트웨어가 실행되는 경우 이를 즉시 경고하고, 필요한 방어 조치를 자동으로 시행할 수 있다.

2.2.3 애플리케이션 기반 스캐닝

애플리케이션 스캐닝은 소스 코드 분석, 동적 분석, 정적 분석을 통해 애플리케이션 내의 취약점을 탐지한다. 개발 초기 단계부터 배포 후까지 지속적으로 수행되며, 소스 코드 분석을 통해 잠재적인 취약점을 식별하고 수정하며, 동적 분석을 통해 실제 운영 환경에서 발생할 수 있는 취약점을 탐지한다. 예를 들어, 웹 애플리케이션을 테스트 환경에서 실행시키면서, OWASP ZAP 같은 도구를 사용해 악의적인 입력 시도를 통해 보안 취약점을 탐지할 수 있다. 또한, 정기적인 스캔을 통해 새로운 취약점이나 업데이트로 인한 보안 결함을 빠르게 식별하고 대응할 수 있다.

2.3 취약점 관리 시스템

취약점 관리 시스템은 정보 시스템 및 네트워크 인프라의 보안 취약점을 식별하고 평가하는 도구와 절차의 집합이다. 취약점 관리 시스템은 설정 관리, 프로젝트 관리, 보고서, 이행 관리, 통계의 다섯 가지 주요 구성 요소로 이루어져 있다[8]. 취약점 관리 시스템은 CVE(Common Vulnerabilities and Exposures) 데이터베이스를 참조하여 서버, 네트워크 장비, PC 등을 자동으로 스캔하고, CVSS(Common Vulnerability Scoring System) 척도를 이용해 취약점의 심각도와 영향을 평가한다. 대표적인 스캐닝 도구로는 Nessus, OpenVAS 등이 있으며, 이들 도구는 네트워크와 시스템 전반에 걸친 취약점을 탐지하고 분석한다. 정기적인 스캔을 통해 네트워크와 시스템의 보안 상태를 지속적으로 모니터링하며, 스캔 결과는 상세한 보고서로 제공되어 관리자에게 신속한 대응을 가능하게 한다. 보고서에는 취약점 세부 정보, 영향을 받는 시스템, 권장 조치 등이 포함되며, 이를 통해 관리자는 취약점의 우선순위를 정하고 필요한 보안 조치를 실행할 수 있다. 또한 자동 패치 기능을 통해 일부 취약점은 자동으로 수정할 수 있으며, 지속적인 모니터링과 주기적인 침투 테스트를 통해 새로운 취약점을 즉시 탐지하고 대응할 수 있다. 예를 들어, 네트워크 기반 스캐닝과 호스트 기반 스캐닝을 결합하여 네트워크 내부와 개별 시스템의 취약점을 모두 식별하고 대응할 수 있다. 또한, 애플리케이션 스캐닝을 통해 소스 코드 분석, 동적 분석, 정적 분석을 수행하여 애플리케이션 내의 취약점을 식별하고 수정할 수 있다. 이러한 방식은 개발 초기 단계부터 배포 후까지 지속적으로 애플리케이션의 보안 상태를 강화하는 데 효과적이다. 취약점 관리 시스템은 보안 규제 준수 여부를 평가하여 법적 요구사항을 충족하고, 조직의 보안 사고를 예방하며 시스템의 신뢰성을 유지하는 데 중대한 역할을 한다. 이를 통해 조직은 사이버 위협에 대한 전반적인 대응 능력을 향상시키고, 보안 체계를 강화할 수 있다. 결론적으로, 취약점 관리 시스템은 정보 시스템 및 네트워크 인프라의 지속적인 보안을 위해 필수적인 도구로 자리매김하고 있다.

3. 방산업체 취약점 진단 현황 분석

3.1 방산업체 취약점 진단

방산업체는 정보자산에 대한 취약점 분석과 평가를 반

기 1회 실시하고, 수시 자체 점검 결과를 기록하여 관리해야 한다[9]. 그러나 이러한 작업은 고도의 정보보호 전문 역량을 필요로 하며, 방산업체 자체적으로 이행하기에는 한계가 있다. 이러한 이유로 2021년 이후, 방위사업청 주관으로 사이버 보안 취약점 진단사업을 통해 매년 1회 취약점 점검을 지원하고 있다. 방위사업청은 방산업체 취약점 점검을 위해 2024년까지 약 80억 원이 투입하였고, 연도별 지원 금액은 Table 1과 같다[10].

Table 1. Yearly vulnerability diagnosis budget

Year	'21	'22	'23	'24
Cost (KRW, Billion)	0.33	2.64	1.90	3.00

3.2 취약점 분석·평가의 문제

취약점 분석·평가 시 서버의 규모에 따라 점검해야 할 항목의 수가 급격히 증가한다. 과학기술정보통신부의 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드를 기준으로 한 대의 윈도우 서버만 운영할 경우 82개의 항목만 점검하면 되지만[11], 수십에서 수백 대의 시스템을 운영하는 기관은 점검 항목 수가 기하급수적으로 늘어난다. 윈도우 서버는 그래픽 환경으로 구성되어 있어 각 항목의 설정 값을 수동으로 확인해야 한다. 이로 인해 취약점 점검에는 상당한 시간이 소요되며, 각 기관의 규모와 서비스 종류에 따라 이러한 문제는 더욱 복잡해진다.

3.3 민간 대비 방산 분야 도입의 한계

취약점 진단 시스템은 민간 분야에서 널리 도입되어 효과적으로 운영되고 있지만, 방산 분야에서는 아래의 세 가지 주요 이유로 인해 적용이 어렵다. 첫 번째로 규제 문제이다. 방산업체는 국가 안보와 직결된 중요 정보를 다루기 때문에, 내부 업무망과 외부 인터넷망을 물리적으로 분리하는 망분리 규제를 준수해야 한다. 이로 인해 취약점 관리 시스템의 효율적인 운영이 제한된다. 취약점 관리 시스템은 주기적인 소프트웨어 업데이트와 취약점 데이터베이스와의 실시간 동기화가 필요하지만, 망분리 환경에서는 이러한 작업이 지연되거나 불가능하다. 외부 인터넷망에 접근할 수 없는 방산업체의 특성상 최신 보안 패치를 신속히 적용하기 어려워져, 알려진 취약점에 대해 지속적으로 노출될 가능성이 높아진다. 두 번째는 절차 문제이다. 방산업체는 민간 기업보다 엄격한 보안 절차를 따라야 하며, 이는 취약점 관리 시스템의 도입을 복잡하게 만든다. 방산업체의 보안 절차는 다단계의 승인 절차와 정밀한 감사 과정을 포함한다. 이러한 엄격한 보안 절차는 취약점 진단 시스템의 빠른 배포와 운영을 저해하며, 시스템의 실시간 대응 능력을 제한할 수 있다. 또한, 방산업체는 보안 취약점 데이터를 외부로 유출하지 않기 위해 내부적으로만 처리해야 하는 경우가 많아, 보안 취약점 시스템 도입 시 추가적인 보안 조치와 내부 절차를 마련해야 한다. 세 번째는 자원 문제이다. 취약점 진단 시스템을 효과적으로 운영하기 위해서는 상당한 초기 비용과 지속적인 유지 보수 비용이 필요하다. 방산업체는 망분리의 사유로 정보시스템에 이중으로 투자하여 운영하고 있기 때문에, 이러한 비용을 부담하는 데 어려움을 겪을 수 있다. 또한, 전문 인력을 확보하고 유지하는 것도 큰 도전 과제이다. 취약점 진단 시스템 운영에는 고도의 사이버 보안 전문 지식과 기술이 요구되므로, 방산업체는 이러한 전문 인력을 확보하는 데 어려움을 겪을 수 있다. 민간 분야에서는 시장 경쟁을 통해 보안 전문 인력을 쉽게 채용할 수 있지만, 방산 분야는 신원조회 등 보안 인력의 접근성과 공급이 제한적이다. 이와 같은 이유들로 인해, 방산 분야에서 취약점 관리 시스템의 도입은 민간 분야에 비해 복잡하고 어려운 과제로 남아 있다. 방산업체는 망분리 규제와 엄격한 보안 절차, 비용과 자원 문제를 해결하기 위한 별도의 전략이 필요하며, 이를 통해 취약점 진단 시스템의 효과적인 도입과 운영을 달성해야 할 것이다.

3.4 방산업체 취약점 관리 시스템

앞서 분석한 민간대비 방산분야 도입의 한계를 개선하기 위해 자동화된 취약점 관리 시스템의 도입이 필요하다. 현재의 취약점 분석평가는 점검 정책의 일관성 부족, 다수의 점검 대상 관리의 어려움, 정보 시스템 전체를 대상으로 한 점검의 어려움 등 여러 문제점을 안고 있다. 취약점 관리 시스템은 자동화된 도구를 통해 지속적인 취약점 스캐닝, 평가 및 관리 기능을 제공하여, 시공간 제약 없이 실시간으로 보안 상태를 모니터링하고 취약점에 신속히 대응할 수 있게 한다. 이를 통해 방산업체는 전문 인력 의존도를 줄이고 보다 효율적으로 사이버 보안 체계를 강화할 수 있다. 취약점 관리 시스템은 네트워크, 서버, 애플리케이션 등의 취약점을 지속적으로 모니터링하고 자동으로 패치를 적용하여 보안 상태를 유지할 수 있다. 이는 초기 보안 취약점을 사전에 차단하고, 관리자의 기술력 부족으로 인한 문제를 보완할 수 있게 한

다. 또한, 일관된 보안 점검 정책을 수립하고, 점검 결과를 체계적으로 비교 분석할 수 있어 전체적인 보안 수준을 향상시키는 데 기여할 수 있다. 방산업체의 정보자산을 보호하고, 국가 안보를 강화하기 위해서는 취약점 관리 시스템의 도입이 필수적이다.

4. 방산업체 취약점 관리 시스템 구현 방안

앞서 방산업체의 사이버 보안 현황을 분석하고, 취약점 관리 시스템 구축의 필요성을 확인하였다. 이를 위해 관계기관 전체의 노력이 필요하며, 이에 따라 기술적 방안과 제도적 방안을 두 축으로 방산업체 취약점 관리 시스템 구축 방안을 제시하고자 한다.

4.1 기술적 방안

취약점 진단 방식은 기술적으로 크게 에이전트 기반(Agent-based) 진단 방식, 에이전트리스(Agentless) 진단 방식, 수동 진단(Manual Diagnostic) 방식, 하이브리드(Hybrid) 진단 방식으로 나눌 수 있다. 에이전트 방식은 점검 서버를 통하여 일괄 배포 및 점검 수행이 가능하여, 상시 점검을 통한 대상 장비의 상태를 실시간 모니터링 가능하다는 장점이 있다. 에이전트리스 방식은 네트워크 장비 및 보안 장비와 같이 에이전트 설치가 불가능하나 스크립트 실행이 가능한 시스템일 경우 활용 가능하다. 수동 진단 방식은 네트워크 연결이 불가한 폐쇄망에서 사용하는 방식으로 점검자가 직접 점검한다는 점에서 에이전트리스 진단 방식과 구분된다. 하이브리드 진단 방식은 앞서 언급한 세 가지의 진단 방식을 통합하여, 기관 환경에 맞게 유동적으로 적용하여 진단을 수행한다. 이에 대한 내용을 Table 2에 정리하였다.

Table 2. Vulnerability Diagnosis Method

Method	Explanation
Agent-Based Diagnostic Method	- Install the Agent on the inspection target to perform batch distribution and inspection using a distribution system, etc
Agentless Diagnostic Method	- Used when it is not possible to install and run an agent on the target system.
Manual Diagnostic Method	- Inspectors perform diagnostics directly without the use of vulnerability check tools
Hybrid Diagnostic Method	- Integrate agent, agentless, and manual assessment methods to be applied according to the institution's environment.

방산업체는 중요 정보를 다루기 때문에 망분리 환경을 필수적으로 유지하고 있다. 이러한 환경에서는 전통적인 취약점 진단 방식이 효과적으로 작동하지 않을 수 있다. 이를 해결하기 위해 하이브리드 진단 방식을 도입하는 것이 필요하다. 하이브리드 진단 방식은 에이전트 기반 진단 방식과 에이전트리스 진단 방식 및 수동 진단 방식을 결합하여 망분리 환경에 적합한 취약점 진단을 수행한다. 외부 인터넷 환경에 노출된 서버 등에는 에이전트를 설치하여 세부적인 취약점을 분석하고, 에이전트 설치가 불가능한 네트워크 장비 및 보안장비에는 에이전트리스 진단 방식을 통해 네트워크 트래픽과 포트 상태 등을 분석하여 외부 침입 경로를 식별한다. 더불어 보안 등의 이유로 도구를 사용할 수 없는 폐쇄망 환경에서는 점검자가 수동 진단 방식을 통해 망분리 환경에서도 효율적인 취약점 진단이 가능해진다. 이에 대한 하이브리드 취약점 진단 방안을 Fig. 2에 작성하였으며, 폐쇄망 내에서 수동 진단이 아닌 취약점 관리 시스템을 별도 구축 할 수 있다.

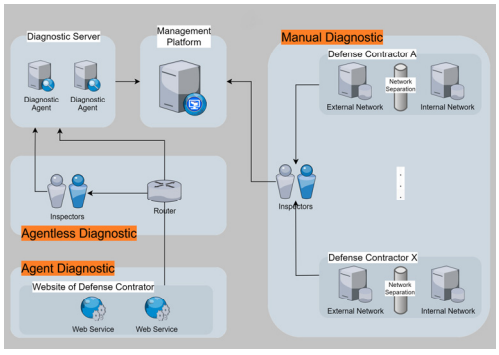

Fig. 2. Hybrid diagnostic method

4.2 제도적 방안

방산업체의 사이버 보안 강화를 위해 다양한 제도가 운영되고 있으나, 각 제도를 주관하는 기관이 다르고, 이에 따른 업무 피로도가 누적되고 있다. 이러한 문제를 해결하기 위해 중앙형 취약점 진단 시스템을 구축하는 방안을 제안한다. 중앙형 시스템은 각 기관의 취약점 진단 결과를 통합하여 중앙에서 관리하고, 이를 기반으로 효율적인 보안 대책을 수립할 수 있도록 한다.

또한, 보안감사, 실태조사, K-RMF(Korea Risk Management Framework), CMMC(Cybersecurity Maturity Model Certification) 등 다양한 제도가 방위력 개선을 위해 운영되고 있으나, 각 기관의 긴밀한 소통

과 연구를 통해 보안 요구 사항을 통합하고 일관된 보안 점검 기준을 마련한다면 방산업체가 보다 체계적으로 보안 관리를 수행할 수 있도록 도울 수 있을 것이다.

5. 결론

본 논문은 방산업체의 사이버 보안 현황을 분석하고, 기술적 및 제도적 측면에서 취약점 진단 시스템 구축 방안을 제시하였다. 방산업체는 국가 안보와 직결된 중요 정보를 다루고 있어 사이버 보안의 중요성이 매우 크다. 그러나 최근에는 지능화된 해킹 공격으로 인해 보안 사고가 빈번히 발생하고 있으며, 이는 주로 홈페이지 설계 오류와 관리자의 보안 의식 및 기술력 부족에서 기인한다. 이러한 문제를 해결하기 위해서는 자동화된 취약점 관리 시스템의 도입이 필수적이나, 규제, 절차, 자원 부분에서의 한계가 있다.

해당 한계를 해결하기 위해 본 논문에서는 기술적, 제도적 방안을 제안하였다. 기술적 방안으로는 하이브리드 진단 방식을 도입하여 망분리 환경에 적합한 정기적인 보안 스캐닝과 실시간 모니터링을 통한 효율적인 취약점 진단을 수행할 수 있다. 제도적 방안으로는 중앙형 취약점 진단 시스템 구축과 관계 기관 간의 상호인정협정을 통해 방산업체의 업무 부담을 줄이고 보안 관리를 체계적으로 수행할 수 있다. 이를 통해 방산업체는 전문 인력 의존도를 줄이고, 보다 효율적으로 사이버 보안 체계를 강화할 수 있으며, 일관된 보안 점검 정책을 수립하고 점검 결과를 체계적으로 비교 분석할 수 있어 전체적인 보안 수준을 향상시키는 데 기여할 수 있다. 다만, 망분리 규제와 같은 환경적 한계가 존재하기 때문에 이를 극복하기 위한 추가 연구가 필요하다.

References

[1] Eunjoo Park, South Korean and German Intelligence Agencies Warn of North Korean Cyber Threats to Defense Technology, boannews(Feburary 20, 2024), www.boannews.com

[2] Scott Ikeda, State-Sponsored North Korean Hackers Penetrated South Korean Defense Companies, Stole Sensitive Technical Data, CPO Magazine(MAY 3, 2024), www.cpomagazine.com

[3] Recorded Future, North Korea's Cyber Strategy, Report, June 2023.

[4] Jaehyun Choi, Hoojin Lee, " Security Vulnerability Management Measures for Major Information and Communication Infrastructure using VMS", *Journal of The Institute of Electronics and Information Engineers*, Vol.57, NO.6, June 2020.
DOI: https://doi.org/10.5573/ieie.2020.57.6.37

[5] MSIT, KISA, Cyber Threat Trends Report for the First Half of 2023, Report, p.20.

[6] Haerin Kim, Seungwoon Lee, Su-Youn Hong, "A Quantitative Security Metric Based on MITRE ATT&CK for Risk Manageme", *Journal of The Korea Institute of Information Security & Cryptology*, VOL.34, NO.1, Feb 2024.
DOI: https://doi.org/10.13089/JKIISC.2024.34.1.53

[7] OWASP, "The Open Web Application Security Project (OWASP)", owasp.org/about, June 2024.

[8] Jaehyun Choi, Hoojin Lee, "Security Vulnerability Management Measures for Major Information and Communication Infrastructure using VMS", *Journal of The Institute of Electronics and Information Engineers* Vol.57, NO.6, June 2020.
DOI: https://doi.org/10.5573/ieie.2020.57.6.37

[9] DAPA, Defense Industry Technology Protection Guidelines, Korea, MAY 16, 2024

[10] DAPA, Cybersecurity Vulnerability Diagnosis Project, RFP, Korea, 2021-2024.

[11] MSIT, KISA, Detailed Guide on the Technological Vulnerability Analysis and Evaluation Method of Major Information and Communication Infrastructure, Korea, 2021.

최 지 웅(Jiung Choi) [정회원]

- 2014년 2월 : 금오공과대학교 컴퓨터공학부 졸업 (공학학사)
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방무기체계, 정보보호, 네트워크

황 도 빈(Dobin Hwang) [정회원]

- 2014년 2월 : 공군사관학교 시스템공학과(시스템공학학사)
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방보안, 방위산업보안, 개인정보보호, 인공지능

임 준 영(Jun-Yeong Lim) [정회원]

- 2016년 8월 : 부산대학교 정보컴퓨터공학부 졸업 (학사)
- 2018년 8월 : 부산대학교 전기전자컴퓨터공학과 졸업 (석사)
- 2018년 9월 ~ 2019년 2월 : 부산대학교 산학협력단 연구원
- 2020년 1월 ~ 2023년 7월 : 부산은행 정보개발부 대리
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방무기체계, 국방무기SW, 인공지능, 빅데이터, 사물인터넷

김 건 태(Guntae Kim) [정회원]

- 2013년 2월 : 부산대학교 기계공학부 졸업 (학사)
- 2015년 2월 : 한국과학기술원 기계항공시스템학부 졸업 (석사)
- 2015년 2월 ~ 2015년 9월 : LG전자 CTO부문 연구원
- 2015년 9월 ~ 현재 : 국방기술품질원 기술침해분석팀 선임연구원

〈관심분야〉
국방무기체계, 정보보호