Journal of The Institute of Electronics and Information Engineers Vol.57, NO.6, June 2020 https://doi.org/10.5573/ieie.2020.57.6.37
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2020-57-6-5

취약점 관리시스템을 이용한 주요정보통신기반시설 보안취약점 관리 방안

(Security Vulnerability Management Measures for Major Information and Communication Infrastructure using VMS)

최 재 현*, 이 후 진**

(Jaehyun Choi and Hoojin Lee©)

요 약

정부는 주요정보통신기반시설의 안전성 및 신뢰성을 확보하기 위하여 취약점 분석·평가를 실시하고 그 결과에 대해 필요한 보완조치 사항으로 이행계획을 수립 및 시행하여 기반시설에 대한 보안취약점을 점차 개선해 나가고 있다. 그러나 기반시설 취약점 분석·평가 시 활용하고 있는 취약점 분석·평가 상세가이드는 2017년 이후 업데이트가 진행되지 않고 있으며, 기반시설 담당자의 잦은 변경으로 인한 관리적인 문제도 빈번하게 발생하고 있다. 이에 대한 기반시설 정보보호 담당자의 고충을 파악하고 관리의 문제점을 도출하고자 하였으며, 본 논문에서 제시하는 취약점 관리시스템을 통해 주요정보통신기반시설의 기술 및 관리적 업무 개선방안을 제시하고자 한다. 수동으로 취약점 점검을 진행했었던 기존과 다르게 배치파일로 변환하여 점검을 수행함으로써 담당자의 업무가 감소된 효과가 있었다. 공공기관의 순환근무제 등으로 인한 잦은 담당자의 변경으로 업무연속성을 확보하기 힘들었으나, 취약점 관리시스템을 통하여 비전문가도 쉽게 업무 파악이 가능하도록 하였으며 업무감소와 연속성을 확보하여 기반시설의 관리 방안을 개선하고자 하였다.

Abstract

The government is gradually improving the security vulnerabilities of the infrastructure by conducting vulnerability analysis and evaluation in order to secure the safety and reliability of the major information and communication infrastructure and establishing and implementing an implementation plan with necessary supplementary measures for the results. However, the vulnerability analysis and evaluation detailed guide, which is being used to analyze and evaluate infrastructure vulnerabilities, has not been updated since 2017, and management problems have also frequently occurred due to frequent changes in infrastructure managers. In this regard, it was intended to grasp the grievances of the person in charge of infrastructure information protection and to draw up management problems, and to propose ways to improve the technical and managerial tasks of major information and communication infrastructure through the vulnerability management system (VMS) presented in this paper. Unlike the previous ones where the vulnerability check was carried out manually, the work of the person in charge was reduced by converting it to a batch file and performing the check. It was difficult to secure continuity of work due to frequent changes in the personnel in charge due to the circular work system of public institutions, etc., but non-experts were also able to easily identify their work through the vulnerability management system, and the plan was to improve the management of infrastructure by securing reduction of work and continuity.

Keywords : Security Vulnerability, Vulnerability Management System (VMS), Infrastructure, Business Continuity

* 정회원, ** 평생회원, 한성대학교 스마트융합컨설팅학과
(Department of Smart Convergence Consulting, Hansung University)
※ 본 연구는 한성대학교 교내학술연구비 지원과제임.
© Corresponding Author(E-mail : hjlee@hansung.ac.kr)
Received ; March 24, 2020 Revised ; April 20, 2020
Accepted ; April 26, 2020

Ⅰ. 서 론

인터넷의 발달은 사회 전 분야의 정보화를 촉진하고 우리 사회를 디지털 기반의 정보사회로 변화시켜주었다. 인터넷의 발전으로 사물인터넷, 빅데이터, 클라우드,

인공지능 등 정보 기술의 발전이 매우 빠르게 진행되었으며, 정보화 기술 및 서비스에 대한 의존도가 꾸준히 증가하고 정보 기술의 발전과 함께 사이버 공격은 점차 더 잦아지고 있다. 이러한 사이버 공격은 개인과 기업 나아가 주요 기반시설을 겨냥한 사이버 공격과 테러로 변모하고 있어 사회적 혼란에 대한 우려가 높아지고 있다. 국내에서도 2013년 3.20 사이버 테러와 6.25 사이버 공격에 이어 2014년 한국수력원자력 정보 유출 등의 사건 및 사고에 대한 심각성에 대해 크게 화두가 된 바 있으며, 점차 고도화된 사이버 공격의 목표가 될 것으로 예상됨에 따라 국가적으로 대응하기 위한 체계적인 보호 대책이 필요하다. 이에 대한 국가적 대책으로 2001년 금융·통신·에너지 등 국가의 중요한 정보통신시설을 체계적으로 보호하기 위하여 정보통신기반보호법을 제정 및 공포하여 시행하고 있다[1]. 정보통신기반보호법에서는 해킹, 바이러스, 악성프로그램 유포 등의 전자적 침해행위의 수법이 점차 지능화되고 금전적 피해와 정신적 피해가 증가함에 따라 정보통신기반시설에 대한 체계적인 관리와 보호를 할 수 있도록 예방·대응·복구 등의 내용으로 규정하고 있다.

주요정보통신기반시설로 지정된 기관의 담당자는 전공자를 우선적으로 배정하고 있으나, 공공기관의 순환근무제 도입으로 공무원의 청렴성을 높이고 다양한 경험으로 전문가 양성에 도움이 되고자 하였지만 되려 기반시설 담당자에게는 불필요한 정책이 되었다. 순환근무제 등의 이유로 기반시설 담당자의 대부분이 2년이 되지 않은 채 다른 업무로 자리를 옮기고 있으며, 그 중 일부 기관은 비전문가가 주요정보통신기반시설의 업무를 담당하고 있는 실정이다. 더불어 소규모 기관의 경우 정보보호를 담당하는 부서나 전문 인력이 없는 기관도 다수 존재하고 기반시설 업무에 대한 경험과 지식이 전무한 담당자들은 업무에 대한 부담과 그로 인한 스트레스로 업무를 회피하게 되면서 더 잦은 기반시설 담당자의 변경이 발생하고 있다. 위에서 언급한 문제에 대한 개선방안의 일환으로 본 논문에서는 기반시설 정보보호 담당자들의 고충을 파악하고 기반시설 관리의 문제점을 효과적으로 도출하기 위한 취약점 관리시스템(Vulnerability Management System: VMS)이라는 새로운 시스템의 도입 및 적용을 제안함으로써 기존 주요정보통신기반시설 담당자들의 취약점 관리 문제(수동 취약점진단, 업무 비연속성, 담당자의 잦은 변경)에 대한 효율적인 관리 방법을 제시하고자 한다.

Ⅱ. 본 론

1. 주요정보통신기반시설

2001년부터 시행된 정보통신기반보호법은 전자적 침해행위로부터 주요정보통신기반시설의 보호에 관한 대책을 수립하고 시행하기 위해 제정되었다[2]. 국가 사회 전반적으로 주요 시설이 업무와 관련된 전자적 제어시스템과 관리시스템 그리고 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제1호에 의한 정보통신망을 정보통신 기반시설이라 한다. 이런 기반시설 중에서도 전자적인 해킹, 바이러스, 서비스 거부 등 외부 공격으로 인해 공격을 받았을 때 사회적으로 혼란을 불러올 수 있는 시설에 대해 국가적으로 보호하기 위해 지정한 정보통신 기반시설을 말한다[3].

주요정보통신기반시설로 지정된 관리기관은「정보통신기반 보호법」제9조에 따라, 주요정보통신기반시설로 신규 지정된 후 6개월 이내, 그리고 매년 취약점 분석·평가를 실시해야 한다[1]. 453개의 관리적·물리적·기술적 점검 항목에 대한 주요정보통신기반시설의 취약 여부를 점검하여 단기적으로는 발견된 취약점을 제거하고 장기적으로는 악성코드 유포, 해킹 등 사이버 위협 대응을 위한 종합적 개선 과정이라고 할 수 있다.

가. 주요정보통신기반시설 지정기준

2001년 4개 부처의 23개 시설에 대해 주요정보통신기반시설을 최초로 지정하였으며, 매년 주요정보통신기반시설을 추가로 지정하고, 2018년 1월 정보통신 등의 분야에서 231개 관리기관과 411개 기반시설로 지정하여 관리하고 있다[4]. 정보통신기반보호법의 주요정보통신기반시설은 표 1과 같은 사항을 고려하여 지정된다[5].

표 1. 주요정보통신기반시설 지정기준
Table1. Designation criteria for major information and communication infrastructure.

Classification	Designation criteria
Major information communication infrastructure designation criteria	◦ The social importance of the work performed by the institution managing the infrastructure ◦ Dependence on the information and communication infrastructure of the work performed by the institution ◦ Interconnection with other infrastructure ◦ In the event of an infringement accident, the extent and extent of damage to national security and society ◦ The possibility of an infringement accident or the ease of recovery

주요정보통신기반시설의 지정 대상은 공공기관과 민간이 운영 및 관리하는 정보통신기반시설을 포함한다. 사이버 침해사고 발생 시 국가안보와 국민의 기본생활과 경제에 중대한 영향을 미치게 되는 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 시설을 말한다. 각 중앙행정기관의 장은 업무의 중요성, 의존도, 상호연계성, 피해규모 및 범위, 복구의 용이성을 기준으로 전자적 침해로부터 보호해야 할 필요가 있다고 인정되는 시설에 대하여 주요정보통신기반시설로 지정하고 있다[6, 7].

2. 기반시설 취약점 관리 문제점

취약점 분석·평가를 진단함에 있어 기술적 점검은 각 시스템에 대한 실제 설정값에 관한 것으로, 시스템에 대한 명령어(Command)와 메뉴 구성과 같은 기술적인 사항을 충분히 인지하고 있어야 가능하기에 주요정보통신기반시설 정보보호 담당자들의 어려움이 발생하고 있다[8]. 이에 대한 주요정보통신기반시설 정보보호 담당자들의 취약점 관리 문제로 세 가지를 언급하고자 한다.

첫째, 2017년 한국인터넷진흥원(KISA)에서 제작 및 배포한 가이드를 기준으로 컨설팅 전문업체가 수행하지 않는 경우 수동적 진단을 수행함으로써 취약점 점검 시 담당자의 수요 및 공수 증가로 인한 부담과 업무량이 증가하게 되었으며, 기반시설의 관리적·물리적·기술적 점검 항목은 표 2와 같다[2].

표 2. 기반시설 점검항목
Table2. Infrastructure checklist.

Classification		Diagnosis item			
		High	Medium	Low	Total
Administrative Part		39	35	40	114
Physical Part		7	8	11	26
Technical Part	UNIX Sever	43	18	12	73
	Windows Sever	45	34	3	82
	Security Equipment	16	9	1	26
	Network	14	21	3	38
	Control System	16	6	0	22
	PC	14	5	1	20
	DBMS	11	8	5	24
	WEB	28	0	0	28
Total		233	144	76	453

둘째, 기반시설 취약점 분석·평가 기준과 같이 취약점을 진단하는 기본 항목으로 크게 관리적·물리적·기술적 부문으로 분류되어 있다[8]. 그중 기술적 점검 항목은 유닉스서버, 윈도우서버, 보안장비, 네트워크, PC, DBMS, 웹, 제어시스템으로 분류가 되어 있으나, 기반시설로 지정된 시스템 중 위 범주에 들지 않는 시스템은 기반시설로 등재가 되어 있음에도 불구하고 제시된 진단 가이드가 없어 취약점 진단을 하지 못하고 있다. 마지막으로, 공공기관 업무 관례상 담당자의 잦은 변경이다. 이 문제는 다시 제도적인 문제와 관리적인 문제로 나뉘며, 제도적인 문제로는 순환근무제도로 인해 기반시설과 전혀 상관없는 비전문가가 기반시설 업무 담당자로 지정되어 업무를 수행하고 있다. 위와 같이 비전문가인 기반시설 정보보안 담당자들은 생소한 업무에 대한 업무 부담으로 잦은 변경이라는 악순환이 계속되고 있다. 관리적인 문제점으로 국가의 주요정보통신기반시설이라는 특수성과 중요성이 배제된 채 비전공자가 기반시설업무 담당자로 배치되어 업무 수행을 하고 있는 실정이다. 위에 언급한 문제로 인해 주요정보통신기반시설에 대한 업무처리의 전문성 결여, 취약점 진단에 대한 일회성 업무 인식 등 다양한 문제가 도출되고 있다.

3. 취약점 관리시스템

취약점 관리시스템은 주요정보통신기반시설의 기술적 취약점 분석 및 평가 방법 상세가이드를 기준으로 관리적·물리적·기술적 취약점 점검 항목을 바탕으로 구성된 시스템이다. 다양한 정보시스템(서버, 네트워크, 보안장비, PC 등) 취약점 점검을 자동과 수동 기능을 조합하여 담당자로 하여금 지속적으로 관리 및 개선을 하도록 도와주며, 발견된 취약점은 기반시설 관련자들에게 원스톱으로 관리할 수 있도록 도와주는 시스템을 말한다.

가. 취약점 관리시스템 주요 구성 항목

취약점 관리시스템의 주요 구성 항목으로는 설정관리, 프로젝트, 보고서, 이행관리, 통계로 구성되며 주요 항목은 표 3과 같다.

(1) 설정관리

설정관리 항목은 취약점 관리시스템에 대한 사용자, 운영자 권한 부여, 체크리스트 관리, 자산관리 등을 할 수 있는 메뉴로 구성이 되어 있다. 사용자 정보(운영자, 관리자 등)를 등록하거나 삭제하는 기능, 사용자별 권한 부여 기능, 기반시설 취약점 진단 체크리스트에 대한 관리, 기관에 존재하고 있는 모든 자산을 확인할 수

있는 기능으로 구성되어 있으며, 전자문서뿐만 아니라 웹 사용자 인터페이스(WEB UI)를 통해 쉽게 관리가 가능한 장점을 제공한다.

표 3. 주요 구성 항목
Table3. Major configuration items.

Main configuration	Explanation
Setting management	◦ User ◦ Operator authorization ◦ Diagnostic code management ◦ Threat assessment classification criteria management ◦ Checklist management ◦ Project management ◦ Asset management ◦ Script upload management
Project	◦ Provide security regulation template ◦ Customizing security regulations ◦ Check the progress of diagnosis ◦ Automatic and manual diagnostic selection
Report	◦ Detailed result report ◦ Risk analysis evaluation ◦ Detailed result report ◦ Risk analysis evaluation
Implementation management	◦ Implementation management bulletin ◦ Notice
Statistics	◦ Vulnerability diagnosis statistics ◦ Vulnerable host by item ◦ Vulnerability diagnostic statistics comparison

(2) 프로젝트

프로젝트 항목은 프로젝트 관리, 자산관리, 스크립트 등록의 메뉴로 구성이 되어 있다. 프로젝트 관리 메뉴는 매년 실시하는 취약점 점검 시 생성되는 페이지로 프로젝트명, 수행업체, 수행기간, 취약점 진단대상 등을 확인할 수 있다. 하위 메뉴로는 위험평가 기준, 위험분석평가방법, 위험수용수준(Degree of Assurance: DoA) 및 위험관리, 정보보호계획 수립기준에 대한 설정이 가능하다. 자산관리 메뉴는 프로젝트 자산에 대한 등록과 삭제를 할 수 있는 기능으로 자산에 대한 개별 등록과 일괄 등록이 가능하다. 스크립트 등록 메뉴는 다양한 시스템(서버, 네트워크, 보안장비, PC 등)에 맞는 스크립트 파일을 미리 등록하여 취약점 점검 시 시스템별로 스크립트를 매칭 하여 시스템에 대한 취약점 점검을 필요 시 수행할 수 있도록 지원해 준다.

(3) 보고서

보고서 항목은 다양한 보고서(상세결과보고서, 위험분석평가 보고서 등) 양식을 제공함으로써 취약점 진단 결과에 대한 다양한 보고서를 통해 진행했던 자산에 대한 취약점 진단통계를 항목별, 호스트별 등 다양한 관점에서 자산에 대한 취약점 확인이 가능하도록 기능을 제공한다. 더불어 상급자 보고 및 관련자와의 회의 시 다양한 상황에 맞는 보고서를 제공함으로써 담당자의 업무를 경감시켜준다.

(4) 이행관리

이행관리 항목은 게시판과 공지사항 기능을 제공함으로써 관리 및 운영 담당자간 업무협업이 가능하도록 도와주는 기능을 제공한다. 잔여 취약점에 대한 시스템 담당자들은 증적 자료를 업로드하여 처리되는 상황을 기반시설 담당자들에게 실시간으로 공유함으로써 진행에 대한 확인이 가능하도록 기능을 제공한다. 더불어 기반시설 업무 관련자에게 전달하고자 하는 내용은 공지사항 기능을 통해 간편하게 전달이 가능하며 담당자가 변경되더라도 해당 기능을 이용함으로써 기반시설의 이력관리가 가능하도록 도와준다.

(5) 통계

매년 진행하는 취약점 분석·평가 프로젝트별 점검 통계를 확인할 수 있으며 자산 현황, 점검결과, 점검대상별 이행률, 점검위험 분포도, 위험수용 현황 등을 확인할 수 있는 기능을 제공한다. 점검결과 메뉴에서 '자산별 차트'를 선택하면 Top 5 취약점이 도출되고, 진단대상 수량, 취약점 진단 평균, 도출된 취약점 개수가 출력된다. 점검대상별 이행률 메뉴에서는 그래프로 도식화되며, 그래프에서는 취약 항목, 이행개수, 잔여 취약점을 확인할 수 있다. 점검위험 분포도 메뉴에서는 취약점 진단 시 산정된 위험수용수준(DoA)에 대한 취약점 점검결과를 확인할 수 있는 기능을 제공한다.

나. 취약점 관리시스템 주요기능

취약점 관리시스템의 주요기능으로 자산관리, 취약점 진단관리, 취약점 이력관리, 보고서로 구성되어 있으며, 주요기능은 표 4와 같다.

표 4. 취약점 관리시스템의 주요기능
Table4. Major features of the vulnerability management system.

Main function	Explanation
Asset management	◦ User-friendly WEB UI ◦ Assignment and management of personnel for each asset ◦ Create asset management status document
Vulnerability diagnosis management	◦ Provision of security regulations template ◦ Customizing security regulations ◦ Check the progress of diagnosis ◦ Automatic and manual diagnostic selection
Vulnerability history management	◦ Diagnosis execution evidence inquiry and management ◦ Collaboration between management and operation personnel ◦ Vulnerability by asset
Report	◦ Provide detailed and risk analysis reports ◦ Provision of information protection plan ◦ Excel and Korean report form support

다. 취약점 관리시스템 사용자별 권한

취약점 관리시스템의 사용자별 권한은 컨설팅 권한, 관리자 권한, 장비담당자 권한으로 나뉘어져 있으며, 아래 그림 1과 같이 사용자별 권한을 분리한 이유는 주요정보통신기반시설의 모든 관련자 (시스템별 담당자, 정보보호 담당자 등)들과의 정보를 쉽게 공유하고자 하였으며, 보안업무 특성상 최소한의 권한을 부여함으로써 보안 사고의 위험성을 줄이고자 컨설팅 권한, 관리자 권한, 장비담당자 권한으로 구성을 하였다.

컨설팅 권한은 취약점 관리시스템의 모든 권한을 임시로 부여하는 권한으로 취약점 분석·평가 기간동안 취약점 관리시스템의 설치부터 구성까지 초기 설정(사용자, 운영자 권한 부여, 진단코드 관리 등)을 하며, 컨설팅 일정이 끝나게 되면 관리자 권한을 가진 담당자에게 모든 권한을 부여함으로써 관리자 권한에 귀속되는 임시 권한이다. 관리자 권한은 컨설팅 권한을 부여받음으로써 취약점 관리시스템의 모든 구성과 기능을 관리하는 최상위권한으로 기반시설 정보보호 관리자가 해당 권한을 부여받아 업무를 수행하는 권한이다. 장비담당자 권한은 각 시스템별(서버, 네트워크, 보안장비, DBMS, PC 등) 담당자가 자신이 담당하고 있는 시스템을 관리 할 수 있는 권한이다.

취약점 관리시스템에 등록된 자동 및 수동 진단스크립트를 통해 각각의 담당자들은 새롭게 도입된 시스템을 실시간으로 점검을 할 수 있으며, 취약점 분석·평가에서 발견된 취약점에 대해 취약점 관리시스템에서 제공하는 이행관리 게시판 기능을 이용하여 모든 시스템 담당자와 관련자가 취약점에 대한 정보를 공유할 수 있는 기능을 제공한다.

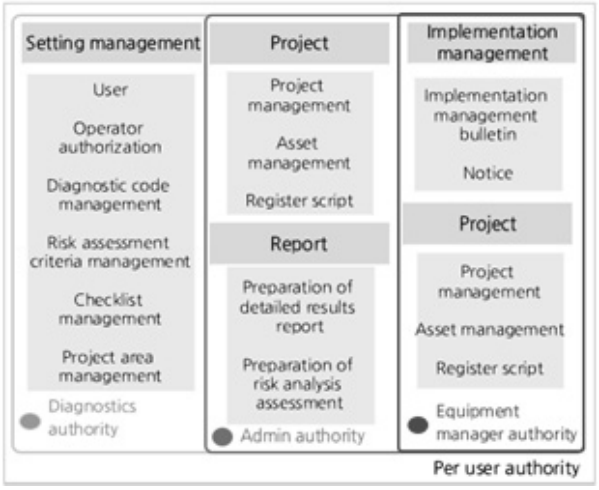

그림 1. 사용자별 권한
Fig. 1. Per user authority.

Ⅲ. 실 험

가. 취약점 분석·평가 문제점

행정안전부가 고시한 주요정보통신기반시설 취약점 분석평가 기준에 의하면 기반시설로 지정된 첫 해는 지정 후 6개월 이내에 취약점 분석·평가를 실시하고, 매년 정기적으로 취약점 분석·평가를 실시하도록 하고 있다[9]. 취약점 분석·평가 진행 시 운영 중인 서버의 규모에 따라 점검해야 할 취약점 항목의 숫자는 기하급수적으로 늘어난다. 한 대의 윈도우 서버만 운영 중일 경우 82개의 취약점 항목만 점검을 진행하면 되지만 각 기관의 규모와 서비스 종류에 따라 수십에서 수백대의 시스템을 운영할 경우 '취약점 항목 × 기반시설 지정 시스템 대수' 만큼 증가하게 된다. 특히, 윈도우 서버의 경우 사용자 편의를 위한 GUI환경으로 구성되어 있어 취약점 점검 항목에 대한 설정 값 확인을 위해 해당 항목에 대한 메뉴 설정 화면으로 들어가서 수동으로 확인을 해야 하기 때문에 상당한 시간이 소요되는 문제가 발생한다[7].

나. 서버 취약점 분석 배치파일 구현 필요성

사이버 공격이 지속적으로 증가하는 환경에서 취약점 분석·평가가 필수적이지만 기업의 업무환경은 턱없이 부족한 현실이며, 배치파일 구현의 이유로는 다음과 같다. 첫째, 기반시설로 지정된 시스템의 규모에 따라 기하급수적으로 증가하게 되어 점검시간이 매우 많이 소요

된다. 둘째, 취약들도 손쉽게 일괄적으로 관리할 수 있도록 취약점 분석평가를 지속적으로 관리하고 수행해야 하는 전담조직이 없거나, 소수의 IT 관련 담당자들이 겸직하고 있어 전문성이 결여되어 있다. 셋째, 기반시설 관리를 위한 시스템 등의 시설이 전무한 상태이다. 따라서 이러한 문제점을 해결하기 위해 기반시설 취약점 분석·평가 시 소요되는 업무량을 감소시키고, 전문성이 부족한 담당자점 관리시스템의 도입이 시급하며, 취약점 분석·평가 진단 항목의 배치파일을 적용한 결과는 그림 2와 같다.

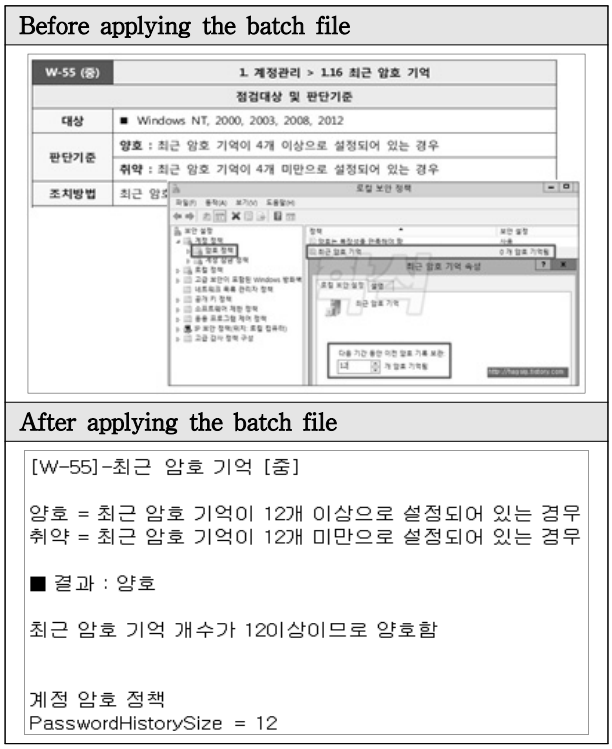

그림 2. 취약점 분석・평가 배치파일 적용 전후
Fig. 2. Vulnerability analysis evaluation before and after application of batch files.

다. 분야별 취약점 점검 항목 개선

정보통신기반보호법 제9조(취약점의 분석・평가)에 의해 시행되는 취약점 분석·평가는 주요정보통신기반시설로 지정된 시스템에 대해 공통적으로 실시하는 필수 항목과 기관의 사정에 따라 선택적으로 실시하는 선택 항목으로 구분하여 취약점을 분석한다. 그러나 주요정보통신기반시설은 다양한 기반시설의 중요도에 따라 지정하고 지속적으로 지정 대상이 확대되고 있기에 필수 항목 점검의 수행으로 공통된 위협에 대응해야 할 뿐만 아니라, 산업 분야별로 고려해야 할 항목의 추가 점검 항목에 대한 개발이 된다면 주요정보통신기반시설의 취약점 분석평가의 실효성이 증대 될 것으로 보인다. 그림 3은 필수 점검 항목에 대한 문서 형식의 보고서로 점검을 진행했었던 기존과 달리 취약점 관리시스템 도입 시 WEB UI를 통해 기반시설의 모든 관련자들은 부여된 권한을 통해 시스템에 대해 관리하고 현황 파악 등을 할 수 있도록 도와준다.

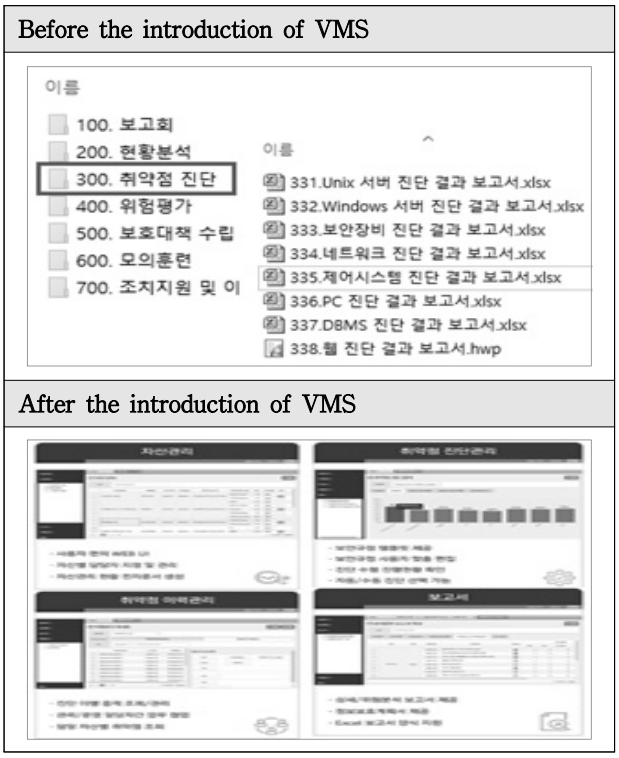

그림 3. 취약점 관리시스템 도입 전후
Fig. 3. Before and after the introduction of the vulnerability management system.

Ⅳ. 결 론

지속적인 사이버 위협의 증가로 인해 국민에 편의를 제공하는 주요정보통신기반시설에 대한 취약점 분석·평가는 이제 필수적인 사항이 되었다. 본 논문에서는 기반시설의 관리적인 문제점을 도출하여 개선의 필요성과 취약점 관리 문제에 대한 효율적인 방안을 모색해 보았다. 즉, 취약점 관리시스템을 도입·활용하여 주요정보통신기반시설 담당자들의 문제점에 대한 효율적인 관리방법을 도출할 수 있었다. 첫째, 기존 수동 진단으로 인한 기반시설 담당자의 업무 증가는 취약점 관리시스템을 활용하여 반자동으로 취약점 점검을 함으로써 담당자의 업무가 감소되는 효과가 있었다. 둘째, 기반시설 담당자의 잦은 보직 변경으로 인한 업무 연속성을 확보하기 위해 취약점 관리시스

템의 기능을 통해 기존 관리적인 문제를 해결할 수 있게 되었다. 마지막으로, 이전에는 기술적 취약 항목에 대한 정형화된 가이드로 인해 적절한 진단을 하지 못했으나 일반적인 기반시설에 대한 점검기준과는 다른 특화된 점검기준을 취약점 관리시스템의 컨설팅 권한을 가진 외부 컨설팅 전문기관을 통해 시스템별 특징에 맞는 점검 항목을 새롭게 만듦으로서 최소한의 보안취약점 분석·평가에 대한 진단이 가능할 것으로 예상되었다.

주요정보통신기반시설을 관리할 책임이 있는 관계 기관의 담당자들은 본 논문에서 제안하는 방안을 활용하여 업무량 감소, 기관별 특성을 반영한 점검 항목 개선, 담당자의 잦은 변경 등의 기반시설 취약점 관리 문제점을 개선함으로써 해당 시설에 적합한 취약점 분석·평가를 수행하고 주요정보통신기반시설 관리상에서 발견된 보안취약점에 대한 개선이 될 것이다. 사이버테러 위협 등 새로운 유형의 침해사고에 대해서 국가 차원의 체계적인 보호대책 마련과 도출된 취약점에 대한 지속적인 조치와 개선계획을 수립하여 관리해야 할 필요가 있으며, 기반시설 시스템의 특수성과 중요성을 인지하고 정보보호 활동에 많은 관심과 지원이 필요하다고 하겠다. 따라서 향후 제안된 취약점 관리시스템을 구현하여 기반시설 관리 문제점에 대한 개선방안의 실효성을 검증하고 객관적 비교 입증 과정을 거쳐 현실적이고 체계적인 관리 기반 체계를 마련하도록 할 예정이다.

REFERENCES

[1] S. T. Park, et al., “A study on the vulnerability analysis and assessment management for the protection of major information and communication infrastructures,” Journal of KIISC, vol. 19, no. 6, pp. 32-40, Dec. 2009.
[2] Korea Information Security Agency, Establishment of improvement scheme for information security consulting company designation system, KISA, pp. 59, 2008
[3] Ministry of Legislation, “Information and Communication Infrastructure Protection Act,” Seoul, Korea, 2019.
[4] J. I. Kim, et al., “Strengthening protection of information and communication infrastructure. [Online],” Feb. 2018.
[5] S. Y. Min, et al., “Design of comprehensive security vulnerability analysis system through efficient inspection method according to necessity of upgrading system vulnerability,” Journal of KAIS, vol. 18, no. 7, pp. 1-8, Jul. 2017.
[6] NIS, et al., “2019 national information protection white paper,” Seoul, Korea, Jun. 2019.
[7] D. H. Jang, “A research on quality improvement methods for the scan items of WINDOWS security vulnerability in critical IT infrastructure,” Master dissertation, Sungkyunkwan University, Seoul, Korea, Jan. 2018.
[8] MSIT and KISA, “Detailed guide on the analysis and evaluation of technical vulnerabilities in major information and communication infrastructure,” Seoul, Korea, Dec. 2017.
[9] H. K. Noh, “(A) study on the improvement of the vulnerability management system in the information and communications infrastructure: vulnerability analysis and evaluation for major information and communications infrastructure,” Master dissertation, Soongsil University, Seoul, Korea, Feb. 2013.
[10] P. S. Kim. “Measures to Improve Civil Service Circulation [Online],” May 2018.
[11] MOIS, “Criteria for analyzing and evaluating vulnerabilities in major information and communications infrastructure,” Seoul, Korea, Dec. 2012.

저 자 소 개

최 재 현(정회원)
1996년 한국방송통신대학교 컴퓨터과학과 학사 졸업.
2013년 한국방송통신대학교 정보과학과 석사 졸업.
2020년 한성대학교 스마트융합컨설팅학과 박사 과정 수료.
<주관심분야 : 정보보안, 인공지능, 빅데이터, 보안취약점 관리>

이 후 진(평생회원)
1997년 서울대학교 전기공학부 학사 졸업.
2002년 The University of Texas at Austin ECE 석사 졸업.
2007년 The University of Texas at Austin ECE 박사 졸업.
2009년~현재 한성대학교 IT융합공학부 및 스마트융합컨설팅학과 교수
<주관심분야 : 통신 및 네트워크, 멀티미디어 신호처리, 사이버보안>