중소기업 정보보호 강화를 위한 보안 취약점 점검 도구에 관한 연구

장윤정[1], 유헌창[2]
[1]고려대학교 컴퓨터정보통신대학원
[2]고려대학교 정보대학 컴퓨터학과
{yjems21, yuhc}@korea.ac.kr

A Study on Security Vulnerability Check Tool for Strengthening Information Protection of SMEs

Youn-Jung Jang[1], Heonchang Yu[2]
[1]Dept. of Software Security, Graduate School of Computer & Information Technology, Korea University
[2]Dept. of Computer Science and Engineering, Korea University

요 약

많은 기업에서 시스템 보안 침해사고가 증가함에 따라 국내에서는 보안성 강화를 위해 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 의무대상을 확대하고 있다. 이에 중소기업에서도 ISMS-P 인증을 받기 위한 준비가 필요해졌다. 그러나 ISMS-P 인증을 위한 시스템을 구축하기 위해 많은 비용과 인력이 필요하고 이를 중소기업에서 구축하기엔 현실적으로 어려운 부분이 있다. SCAP는 정보시스템의 취약점을 보안기준에 맞춰 자동 관리하는 프로토콜이다. 본 논문에서는 ISMS-P 인증 항목 중 시스템 자동관리가 가능한 부분을 도출하여 상용 소프트웨어와 동작 방식을 비교함으로써, 중소기업에 SCAP를 적용하여 시스템을 구축하는 것이 정보보호 강화에 도움이 될 수 있음을 검증하고자 한다.

1. 서론

과학기술정보통신부에 따르면 최근 4년간 국내 보안 침해사고 건수는 418건에서 1,045건으로 늘어났으며, 대표 침해사고 중 하나인 랜섬웨어의 경우에는 39건에서 303건으로 증가하였고 그 중 88.5%는 중소기업에서 발생하였다[1]. 이에 따라 정부는 비즈니스 안정성을 강화하고 정보보호 법적 준거성 확보 등의 이유로 “정보보호 및 개인정보보호 관리체계 인증제도(Personal Information Security Management System, ISMS-P)”를 시행하였고 1,000여개의 기업에서 인증서를 발급받아 운영되고 있다. ISMS-P 인증을 위해서 102개의 인증기준[2]을 통과하여야 하며 관련된 시스템을 구축하고 ISMS-P 인증수수료를 부담하는 등 기업에서는 최대 2억원의 비용이 발생하는 상황이다.

또한 한국정보보호산업협회에서 발표한 “2022 정보보호 실태조사”에 따르면 100인 미만의 중소기업의 정보보안 관련 종사자는 평균적으로 33%정도 이며, 기업 내 정보보호 기술개발 전담 부서를 운영하지 못하는 대표적인 이유는 ‘자금조달 및 기술개발 인력 확보 및 유치’로 조사되었다[3].

국내에는 이러한 중소기업의 ISMS-P 인증을 위한 제도를 검토하는 다양한 연구가 이뤄지고 있고 한국인터넷진흥원에서는 ISMS-P 구축 운영 교육 및 기술지원을 무료로 시행하고 있다. 하지만 중소기업을 위한 ISMS-P 인증에 관한 제도적인 관점에서의 연구는 많으나, 실질적으로 보안 취약성을 점검하기 위해 시스템 관점의 연구에는 현저히 적다. 한국인터넷진흥원의 기술지원의 경우 시간적으로 전체 참여 기업에 대한 지원이 불가능하여 일부를 선정하여 제공되고 있다. 현황에서 기업이 ISMS-P 인증을 검토하기 위해서는 관련 인력 고용 또는 사설업체를 통한 점검을 진행하여야 하는 상황이다.

본 논문에서는 중소기업에서 자체적으로 시스템 보안 취약성을 검토하고 나아가 ISMS-P 인증심사를 준비할 수 있도록 시스템 취약성 점검 도구(Security Contents Automation Protocol, SCAP)에 대해 소개하고 SCAP를 통한 취약성 모니터링의 자동화가 보안 관리를 위한 기능적, 비용적 측면에서 효과적임을 상용 보안 취약점 점검 도구인 SecuGuard SSE와 비교하여 증명하고자 한다.

2. 관련 연구

보안 취약점 점검 도구는 크게 호스트 기반의 점검 도구와 네트워크 기반의 점검 도구로 나눌 수 있다. 호스트 기반 점검 도구는 한 호스트 내에서 시스템 환경정보 등을 검사하는 것으로, 국내 대표 상용 보안 취약 점검도구는 나일소프트사의 SecuGuard SSE(System Security Explorer)[4], 지란지교에스앤씨사의 VADA 등이 있다. 오픈소스 보안취약점 점검 도구는 상용 도구와는 달리 전체 or 개인용 무료라는 특징을 가지고 있으며, 대표적인 오픈소스 보안 취약점 점검도구는 칼리 리눅스, 와이어샤크(Wireshark), SCAP 등이 있다. 하지만 국내 리눅스 시장은 Redhat, 우분투 등이 점유하고 있는 만큼 칼리 리눅스는 OS 종속성으로 인해 활용도가 떨어지며, 와이어샤크는 네트워크 트래픽을 분석하는 도구로써, 호스트 기반의 점검 도구를 사용하고자 하는 본 논문에는 맞지 않는 도구이기 때문에 SCAP에 대해 다루고자 한다.

한국의 주요 기반시설 식별 및 지정제도를 분석해 보았을 때, 관련 법령 등에 따라 소관 부처 또는 위원회 등을 통해 분야별 주요 기반시설을 지정하여 그 목록을 직접 관리한다. 또한, 해당기관의 정보통신시스템에 대한 인증이 아니라 보안관리 체계가 제대로 구축, 운영되고 있는지 확인하고 미흡한 부분은 보완 및 보안대책을 지원하는 방식으로 운영되고 있는데, 이는 미국의 정보 보안 연방 법률인 FISMA(Federal Information Security Management Act)와 유사한 방식이다.

SCAP는 자동화된 취약성을 관리, 측정 및 FISMA 준수를 포함하여 기업에 배포된 시스템의 정책 준수 평가를 가능하게 하는 도구로서, 보안 소프트웨어 제품을 식별하고 소프트웨어의 보안 구성에 대한 정보를 전달하는 형식과 명명법을 표준화하는 규격이다. 그리고 미국 NIST(National Institute of Standards and Technology)에서 보안 점검 목록을 작성하고 보안취약점 점검을 위해 각종 구성 요소를 지원한다[5]. SCAP를 이용하여 시스템 패치 여부를 자동으로 확인하고 보안 구성 설정을 검사하여 시스템의 이상 징후를 확인함으로써 시스템의 보안을 모니터링 하는데 사용할 수 있다[6].

SCAP 표준을 구현하고 시행하기 위한 오픈소스 도구 모음은 OpenSCAP사의 SCAP Workbench와 Nessus사의 Nessus가 있는데, 본 논문에서는 오픈소스인 SCAP Workbench를 통해 실험을 진행하였다. SCAP Workbench는 Linux OS에서 패키지 설치를 통해서 구축 가능하며, 시스템 취약성 점검을 위한 소스 데이터를 제공해 주고 있다.

3. 중소기업 정보보호 관리를 위한 시스템 평가 항목

SCAP를 통한 보안 취약점 점검을 진행하기 위해서는 첫째, 검증 기준이 구체적이어야 하고, 둘째 명시된 기준을 검증할 수 있는 검증 방안의 개발이 선행되어야 하며, 마지막으로 검증방안에 대해 SCAP를 구동하는 언어(OVAL)를 통해 표현함으로써 자동화할 수 있어야 한다. 국내에서 ISMS-P 인증을 받기 위해서는 기술적인 영역뿐만 아니라 관리적 영역을 충족시켜야 하며, 관리적 영역의 경우 정책 및 업무 수행에 관련된 항목이 대부분으로 각 기업별로 통일시켜 점검하는 것이 어렵고, 서류 및 인터뷰를 통해 관리적인 조치를 판단하기 때문에 자동화가 어려운 영역이다. 따라서 본 논문에서는 ISMS-P 평가 항목 중 정보시스템의 환경설정, 소스코드 분석, 취약점 평가와 같이 기술적 검증이 가능한 영역을 선별하고자 한다.

ISMS-P의 102개의 인증 기준[2] 중 '1.관리체계 수립 및 운영'의 16개 항목과 '2.보호대책 요구사항'의 64개 항목 중 42개 항목, '3.개인정보 처리 단계별 요구사항'의 22개 항목은 <표 1>과 같은 각각의 사유로 인해 실험 대상 항목에서 제외하였고, 최종적으로 본 논문에서 다루고자 하는 서버(Server) 관련 자동화가 가능한 ISMS-P 인증 항목 13개를 도출하였다(그림 1).

<표 1> ISMS-P 인증 항목 선정 사유

실험 대상 선정/제외 사유	ISMS-P 인증 항목(항목 수)	총 항목수
보고서 제출 및 인터뷰를 통한 인증 획득	1. 관리체계 수립 및 운영(16)	58
	2. 보호대책 요구사항(42)	
개별 Database 접근 권한 관리	3. 개인정보 처리 단계별 요구사항(22)	22
서버(Server) 외 시스템 항목	2. 보호대책 요구사항(9)	9
본 논문의 실험 범위 선정	2. 보호대책 요구사항(13)	13

구분	ISMS-P 항목명	구분	ISMS-P 항목명
2.5.2	사용자 식별	2.9.4	로그 및 접속기록 관리
2.5.3	사용자 인증	2.9.6	시간 동기화
2.5.4	비밀번호 관리	2.10.3	공개서버 보안
2.6.2	정보시스템 접근	2.10.8	패치 관리
2.6.6	원격접근 통제	2.11.2	취약점 점검 및 조치
2.7.1	암호정책 적용	2.11.3	이상행위 분석 및 모니터링
2.8.5	소스프로그램 관리		

(그림 1) 자동화가 가능한 ISMS-P 인증 항목

4. SCAP 적용 가능성 실험

SCAP Workbench는 SCAP Master 시스템에서 SSH 통신을 통해 취약점 점검 대상 시스템에 원격

접속하여 OVAL로 구성된 스크립트를 실행하는 순서로 구동되며, 앞서 도출한 인증항목을 검증하기 위해 Master 시스템 1대와 취약점 점검 대상 시스템 1대를 구성하였다.

본 논문에서 도출한 13개의 ISMS-P 인증 항목 중 “사용자 인증”과 “취약점 점검 및 조치” 항목을 통해서 SCAP 실험 진행 및 결과를 보이고자 하며, 해당 항목들을 인증받기 위한 여러 설정 값 중에서 SSH를 통해 접속 시, Password가 5회 이상 틀리면 계정을 잠그도록 설정하는 항목을 통해 실험을 진행하였다. (그림 2)는 SCAP Workbench를 이용하여 실험한 결과로서, “Set SSH authentication attempt limit” 라는 항목이고, (그림 3)은 SSE를 통해서 나온 결과로 “[SRV-127] 계정 잠금 임계값 설정”이라는 항목이다. 해당 설정은 /etc/ssh/sshd_config 라는 파일에 MaxAuthTries 라는 설정을 통해서 5회를 넘지 않도록 설정하면 Pass(조치), 해당 설정 자체가 존재하지 않거나 5회 이상으로 설정하면 Fail(미조치)로 표기하게 된다.

(그림 2) SCAP Workbench 실험 결과

(그림 3) SSE 구동 결과

해당 내용을 통해서 두 취약점 분석 도구를 다음과 같이 비교해보고자 한다. 우선, 시스템 구성 방법을 비교했을 때, SCAP와 SSE 모두 취약점을 점검할 Master 서버 1대를 구성하며, SCAP는 OS 패키지 설치를 통해서 구성하고 SSE는 업체가 전달해준 exe 파일을 통해서 구성하게 된다. 또한 취약점을 점검받을 Client 서버에는 각각 SCAP 패키지와 SSE Client 설치 파일을 설치함으로써 취약점 점검을 진행하는 것을 가능하게 한다. 또한 두 도구 모두 SSH를 통한 점검을 진행하게 되며, 각각의 스크립트를 통해 취약성을 점검하게 된다. 이렇게 시스템 구성 방안은 매우 흡사함을 알 수 있다.

다음으로 도구 사용 편의성에 대해서 비교해보면, SCAP Workbench는 OpenSCAP에서 주어진 스크립트로, SSE는 업체에서 수작업을 통해 만들어진 스크립트로 원하는 Client 서버를 설정하여 점검을 진행한다. 이 과정은 마우스 클릭을 통해서 이뤄지게 되고 점검 결과는 각각 SCAP Workbench와 SSE 관리자 툴을 통해 바로 확인 가능하며 Html 파일을 통해 웹페이지에서 상세 내용을 확인 가능하다.

5. 결론

ISMS-P 인증 심사 준비를 위한 항목 중 자동화가 가능한 항목에 대해서 SCAP Workbench를 이용한 보안 취약성 점검과 상용 소프트웨어를 통한 점검이 기능적으로 큰 차이가 없고, 사용 편이성에 대한 이점도 확인하였다. 이를 통해 시스템 구축 및 운영관리에 따라 비용이 발생되는 상용 소프트웨어 대신 무료로 사용 가능한 SCAP Workbench가 중소기업에서 ISMS-P 인증 심사를 준비하는데 도움이 될 수 있음을 알 수 있다. 이번 연구를 통해서 ISMS-P 인증 항목 중 하나의 항목에 대해서 SCAP가 상용 소프트웨어와 성능 및 사용 편이성을 비교했을 때, SCAP가 이점이 있음을 발견할 수 있었다. 향후 연구에는 모든 항목에 대해서 비교하여 주장하는 바에 대해 근거를 체계화 하고자 한다.

참고문헌

[1] 과학기술정보통신부, “2023 사이버 보안 위협 전망 보고서”, 2022.

[2] 한국인터넷진흥원(KISA),“ISMS-P 인증기준 안내서 (2022.04)”, 2022.

[3] 한국정보보호산업협회(KISIA), “2022 정보보호산업 실태조사”, 2022.

[4] 나일 소프트, SecuGuard SSE, http://www.nilesoft.co.kr, 2023.

[5] Radack, S. and Kuhn, D., “Managing Security: The Security Content Automation Protocol,” IT Professional, IEEE, Vol.13, No.1, pp.9-11, 2011.

[6] D. Waltermire, S. Quinn, H. Booth, K. Scarfone, and D. Prisaca, “The Technical Specification for the Security Content Automation Protocol(SCAP): SCAP Version 1.3,” NIST Special Publication 800-126. Revision 3, National Institute of Standards and Technology, 2018.