한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

Windows PC 보안 설정 가이드라인 적용 방안 연구

박성호[O], 이수연[*], 원유재[*]
[O*]충남대학교 컴퓨터공학과
e-mail: shpark5280@cnu.ac.kr[O] djm02309@cnu.ac.kr[*] yjwon@cnu.ac.kr[*]

A Study on Applying Windows PC Security Guidelines

Seong-Ho Park[O], Soo-Yeon Lee[*], Yoo-Jae Won[*]
[O*]Dept. of Computer Engineering, Chungnam National University

● 요 약 ●

본 논문에서는 Windows PC에 대해 보안을 설정하는 가이드라인을 적용하는 프로그램을 제안한다. 이 프로그램은 Windows PC의 보안 정책들을 USGCB를 기반으로 사용자 PC의 로컬그룹 정책을 점검하고, 자동으로 USGCB에 적합하게 설정을 바꿔 준다. 이 프로그램을 통해 체계적인 보안 점검 환경을 구축하여 보안성을 최적화할 기반을 마련하고 자동화된 관리를 통해 운영과 관리에 소요되는 비용을 절감하며, 보안 설정을 편리하게 관리할 수 있게 한다. 또한 PC보안 설정을 규격화함으로써 PC의 보안성을 일정하게 유지시키고 IT비용과 조달 기간을 단축한다. 본 논문에서는 PC보안 설정의 필요성과 국내외 현황, 프로그램에 사용한 보안 가이드라인(USGCB)에 대한 소개와 이 밖에 프로그램에 대한 자세한 내용을 기술한다

키워드: PC 보안(PC security), USGCB, 보안 설정(Security Settings), 자동화(Automation)

I. Introduction

기관의 시스템에는 각종 기밀문서 등 많은 중요정보가 저장되어 있어 보안 관리의 중요성이 높아지고 있다. 이에 따라 기관에서 운영하는 PC에 대한 체계적인 보안 기준이 필요하다. 하지만 현재 공공기관에서 PC를 구매하는 절차에 제품명이나 제품에 대한 규격에 대한 제한은 있지만 운영체제에 대한 요구사항은 기술되어 있지 않다. 또한 PC의 보안을 담당하는 인력이 부재하여 이를 해당 PC를 사용하는 사용자에게 위임하고 있다. 그리고 PC 사용 환경을 표준화하는 절차가 없으며, PC 보안을 규정하는 정책이 없다. 이러한 정책상의 문제점들로 인해 관계자의 PC가 보안상의 취약점을 보유하고 있어 악성코드에 감염될 위험이 생긴다. 이러한 예로는 2014년, 2016년에 카드사, 인터파크 등에서 관리자의 PC가 악성코드에 감염되어 발생한 고객정보 유출사고 등이 있다.

이와 같은 사고의 대책으로 비전문가들도 간단하게 체계적으로 보안 취약점을 점검할 수 있고 일정기준의 보안성을 유지할 수 있도록 하는 방안을 연구한다.

II. Related works

1. 국내 동향

현재 공공기관과 학교 등에서 주로 사용하는 솔루션으로 '내PC지키미'가 있다. 이는 PC의 보안 상태를 점검하고 조치하여 전반적인 보안 수준을 개선하는 취약점 점검 솔루션이다. 하지만 특정 기업에서 생성한 기준을 이용해 PC의 보안 상태를 점검하기 때문에 체계적이고 규격화 된 관리가 어렵다는 단점이 있다.

이 외에 주요 통신 기반 시설 담당자들을 대상으로 제공되는 취약점 점검 기준과 가이드가 있지만 주로 서버와 네트워크 장비 등을 위한 내용으로 구성되어 있어 PC의 경우 그 내용이 부족하고 기본적인 내용만을 담고 있어 수준 높은 보안성을 제공하지 못하고 있다.

2. 해외 동향

해외에서의 Windows PC 보안 설정에 대한 방안으로는 SCAP, FDCC, USGCB 등이 있다.

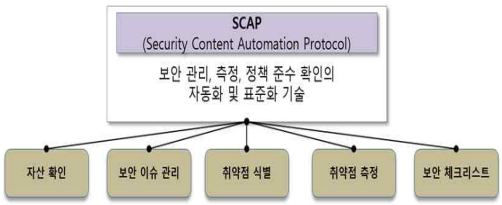

fig 1. SCAP Key Features

SCAP은 보안 결점과 보안 설정 정보를 보안 S/W 간에 공유하기 위해 형식과 명칭을 표준화한 규격으로 자동화된 취약성 검사, 보안 평가 등을 지원하는 등의 목적을 가진 프로토콜이다[1,2]. fig 1.은 SCAP의 주요 특징들을 나타낸다. CVE, CCE, CPE, CWE 등이 있으며 가장 대표적인 것으로 CVE가 있다. CVE는 보안 관련 취약점과 위험 노출에 대한 데이터를 표준화한 규격으로 취약점이나 결점에 대한 유일한 이름을 지정하여 기관들 간에 데이터 공유와 서비스 및 관련 도구 간에 정확하고 빠른 연계를 가능하게 한다.

FDCC는 2007년에 미국 NIST에서 제안된 연방기관 내 업무용 PC와 노트북의 보안강화를 위한 체크리스트이다[3]. 연방기관에서 사용하는 모든 PC와 노트북에 동일한 수준의 보안 설정을 강제화하여 기준을 만족하지 못할 경우 연방정부에 납품을 제한한다. 이를 통해 각 PC의 동일한 보안 수준의 유지를 기대할 수 있다. Windows

XP, Vista, Internet Explorer 7.0 등에 적용되며 SCAP을 통해 FDCC의 설정을 검증한다. 이후 FDCC는 다양한 통제 항목과 가이드가 개선된 USGCB로 통합되었다.

III. The Proposed Scheme

USGCB는 미국 연방기관에서 사용하는 PC에 일정수준 이상의 보안을 유지하기 위한 목적으로 2010년에 발표된 보안 가이드이다. PC 공급 벤더보다 엄격한 수준의 설정을 통해 보안문제에 대한 위험을 감소시킨다. 이를 모든 PC에 동일하게 적용함으로써 효율적인 관리가 가능하고 문제 발생 시에도 빠르게 대처할 수 있다는 장점이 있다. 또한 전반적인 보안수준이 높아지기 때문에 기관 내의 정보에 대해 기밀성과 무결성이 보장된다 [4, 5].

이를 PC 보안 솔루션에 접목하여 표준화 된 기준으로 취약점 조치 자동화 프로그램을 개발한다.

본 논문에서 제안하는 USGCB를 적용한 보안프로그램(이하 보안 프로그램)의 목적은 체계적인 보안 점검 환경을 구축하여 보안성을 최적화할 기반을 마련하고 자동화된 관리를 통해 운영과 관리에 소요되는 비용을 절감하며 편리하게 보안 설정을 관리하는 것이다. 또한 PC보안 설정을 규격화함으로써 PC의 보안성을 일정하게 유지시키고 IT비용과 조달 기간을 단축한다.

보안 프로그램을 이용한 PC 보안 설정을 통해 보안 기본 지침을 제공하고 보다 엄격한 수준의 설정항목을 표준으로 사용하여 위협과 취약점으로 인한 위험을 감소시키며, 보안 비전문가도 PC보안성 관리와 시스템자원의 사용을 효율적으로 할 수 있다.

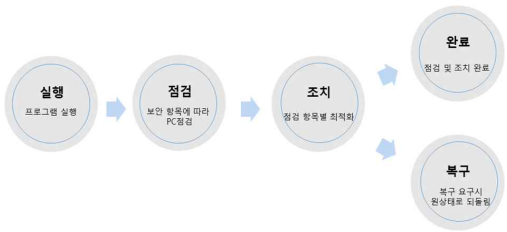

fig 2. Program Execution Process

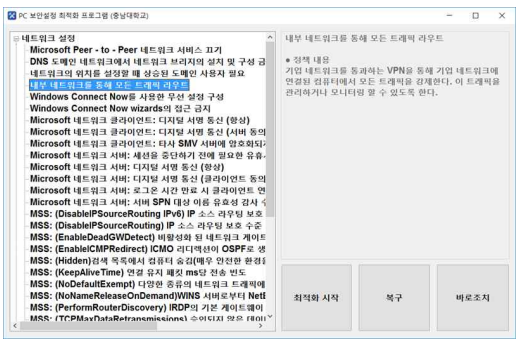

fig 3. Program Execution Screen

fig 2.와 fig 3.은 각각 기능의 동작 과정과 보안 프로그램의 실행 화면이다. 프로그램을 실행하면 전체 가이드 항목들을 점검하고 각각의 항목을 개별적으로 기준에 맞게 설정값을 변경하거나 기준에 적합하지 않는 모든 설정을 일괄적으로 변경하여 보안성을 유지하도록 한다. 설정에 문제가 있다면 복구를 통해 기존 설정으로 되돌릴 수 있다.

프로그램의 왼쪽에는 가이드라인들의 리스트가 나오고 오른쪽 상단에는 선택한 항목에 대한 설명이 출력된다. 오른쪽 하단에 있는 버튼들은 주요 기능을 동작한다. '최적화 시작' 버튼은 전체 가이드라인 항목들에 대한 기준에 맞는 설정 값으로 일괄적으로 변경해주고 '바로 조치' 버튼은 왼쪽에서 선택한 항목에 대해서만 해당 설정 값으로 변경해주는 기능을 한다. '복구' 버튼은 변경한 설정에 문제가 있다면 기존에 설정되어 있던 값으로 복구해주는 기능을 한다.

fig 4. Program Execution Result

fig 4.는 프로그램을 실행한 결과를 보여준다. Windows의 설정들은 레지스트리로 관리되고 변경된 설정에 해당되는 레지스트리의 값도 변경된 것을 확인할 수 있다.

IV. Conclusions

본 논문에서 국내 및 해외의 보안 설정 가이드라인 제도를 조사 및 분석하였다. 이를 통해 제안하는 USGCB를 접목한 보안 프로그램은 표준화 된 PC보안 통제 정책으로 조직의 보안 체계 관리 효율성을 강화할 수 있으며, 전체 정보시스템의 보안정책 및 PC 보안성 강화와 함께 자동화 도구를 이용한 시간과 비용 절감 효과를 기대할 수 있다.

또한 국내에서도 국내 기관들의 실정에 맞춘 보안 설정 가이드라인을 표준화하여 체계적으로 관리해야 한다.

Acknowledgment

This research was supported by the MISP(Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW)(R7115-16-1007) supervised by the IITP(Institute for Information & communications Technology Promotion)

References

[1] NIST SCAP, https://scap.nist.gov/
[2] SCAP wikipedia, https://en.wikipedia.org/wiki/Security_Content_Automation_Protocol
[3] FDCC wikipedia, https://en.wikipedia.org/wiki/Federal_Desktop_Core_Configuration
[4] NIST USGCB, https://usgcb.nist.gov/index.html
[5] Kab-Seung Kou, Gil-Jong Mun, Nam-il Lee, Dong-Soo Jeong, Dong-Ju Ryu, "Analysis of USGCB (The United States Government Configuration Baseline) in USA for Sustainable U-City Service"