간편 ISMS 인증을 위한 핵심 보안 통제 및 축약 보안 통제 진단 가이드 툴 개발

장채연, 이동준, 염흥열

순천향대학교

Development Security Controls And Abbreviated Security Control Diagnostic Guide Tools For Simplified ISMS

Chae-Yeon Jang, Dong-Jun Lee, Heung Youl Youm

Soon Chun Hyang University

요 약

4차 산업혁명과 그에 따른 정보보안 위협 이슈로 부터 많은 기업, 기관, 상급학교 및 병원들은 정보보호 관리체계(ISMS) 인증 제도를 준비하고, 이를 위한 많은 시간과 비용을 투자한다. 그러나 많은 중소기업 및 소규모 개인 정보통신서비스 제공자들은 ISMS 인증제도를 받기 위해서 상대적으로 더 큰 시간, 금전적 위험을 감수해야 한다. 이러한 문제점을 해결하기 위해서 본 논문에서는 105가지의 ISMS통제 항목과 영국의 Cyber Essentials(CES)을 참고하여 7가지 통제 항목으로 새로 축약하였다. 또한 축약한 간편 ISMS 인증을 원활하게 받기 위한 방안으로, 일부 통제 항목을 점검하기 위해 배치파일 및 스크립트, 자가진단 체크리스트를 이용하여 취약한 항목을 자동으로 진단하도록 구현했다. 이 진단 도구는 향후 간편 ISMS 인증을 위한 핵심 보안 통제 항목 및 진단 가이드 툴 혹은 프로그램을 만드는데 활용될 수 있을 것이다.

I. 서론

현재 우리나라에 존재하는 정보보호 관리체계 이하 ISMS는 중견규모 이상의 기업 및 기관에 적합한 정보보호 수준으로 설계 되었으며, 인증 취득 및 유지를 위해서 소요 되는 평균 비용과 기간은 각각 2180만원, 5.5 개월 이다.[1] 이에 따라 ISMS 점검 항목을 중소기업에게 보다 적합한 형태로 선별했으며, 위 축약 ISMS를 토대로 취약점 진단 가이드 툴을 제시한다. 취약점 진단 가이드 툴은 윈도우 시스템, 윈도우 서버, DBMS, 자가진단 이하 4부분의 점검 항목으로 구성되며 중소기업이 위 툴로 간단하며 효과적인 보안 점검이 가능하도록 제작했다.

본 논문에서는 Ⅱ장에서는 정보보호 관리체계에 대해서 설명하고, Ⅲ장에서는 ISMS 축약 참고 가이드인 essential 점검 항목과 취약점진단 가이드를 선별 기준과 함께 설명하며 Ⅳ장에서 취약점 진단 가이드 툴의 개발 환경에 대해서 다루고, 이어서 Ⅴ장에서는 취약점 진단 가이드 툴의 진단 항목과 취약점 진단 방식 등을 설명한다. 그리고 Ⅵ장에서는 결론을 맺는다.

II. 정보보호 관리체계(ISMS)

ISMS (Information Security Management System)는 KISA에서 ISO의 표준을 참고하여 개발한 국내 정보보호 관리체계이다.[2] 정보보호 관리체계는 기업/기관이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립/관리/운영하는 종합적인 체계를 말한다.

현재 ISMS는 관리과정과 정보보호 대책으로 구분되고, 각 5단계와 13개 분야로 구성되어 있다. 먼저 관리과정은 '정보보호정책 구축 및 범위설정', '경영진 책임 및 조직구성', '위험 관리', '정보보호대책 구현', '사후관리' 이하 5단계와 관리과정 12개의 상세 내용으로 구분된다. 정보보호 대책은 '정보보호 정책', '정보보호 조직', '외부자 보안', '정보자산 분류', '정보보호 교육', '인적 보안', '물리적 보안', '시스템개발 보안',

‘암호 통제’, ‘접근통제’, ‘운영보안’, ‘침해사고 관리’, ‘IT 재해 복구’ 이하 13가지 통제 목적과 92가지의 통제 항목으로 구성된다.

III. 간편 ISMS

3.1 Cyber Essentials[3]

Cyber Essentials 이란 영국의 정부통신본부(GCHQ)에 의해서 설립된 해킹 방어 센터인 국립사이버안보센터(NCSC)에서 운영하는 사이버 보안 인증제도이다. CES는 Cyber Essentials와 Cyber Essentials Plus로 구성 되며 Plus는 기술 감사가 추가로 이루어진다.[4] 타 보안제도와는 달리 사이버 공격의 규모에 덜 의존적이며 일반적이고, 만연한 사이버 공격을 다룬다. 중소기업을 대상으로 설계된 제도이며 복잡하지 않지만 조직에 실질적인 도움이 되고, 효과적인 정부 지원 제도라는 점이 장점이다. CES는 12개월의 만료 날짜가 존재하고, 인증을 받기 위해서 300유로(약 41만원) 정도의 비용이 발생한다. 보안 통제(control)에는 조직, 보험, 보안 사업 운영, 접근 제어, 멀웨어 및 기술 침입 이하 5개의 항목과 8개의 하위 카테고리가 존재한다.[5] 우리나라의 정보보호체계인 ISMS와는 간략한 항목, 간단한 심사 과정, 비교적 저렴한 취득 가격(ISMS는 약 2000만원) 과 같은 부분이 다르며 규모가 큰 기업에 적합한 ISMS와는 달리 CES는 비교적 작은 규모 기업에 적합하다.

3.2 취약점 진단 가이드[6]

국내 보안가이드라인에 따라 항목별 점검 방법의 이해를 돕기 위해 과학기술정보통신부와 KISA가 발간한 가이드로, 일반적으로 통용되는 권고사항과 함께 양호 혹은 취약을 가르는 실제 판단 기준은 각 주요정보통신기반시설 현업에 적용되고 있는 다양한 정책 및 운용 상황을 고려하여 취약점 분석·평가 수행자가 최종적으로 결정하게 도와주는 역할을 한다.

3.3 간편 ISMS 인증 기준 제시 근거

점검 항목 선별은 우리나라의 정보보호체계를 중심으로 하되 선별 기준점을 CES에 맞춰서 진행했다. 앞서 설명 했던 바와 같이 우리나라의 정보보호체계는 규모가 큰 기업에 적합한 반면에 CES는 중소기업들을 대상으로 설계된 제도이므로 점검 항목 면에서 보다 더 적합하다고 판단했다. 간편 ISMS의 큰 항목들은 CES의 카테고리들을 참고했으며 서브 카테고리와 그에 따른 세부 설명들을 참고하여 ISMS의 점검 항목들 중 적합한 항목들을 선별해서 제안했다.

[표 1] 간편 ISMS 핵심 통제 항목

통제 항목	통제 분야	세부 통제 항목
사무실 방화벽 및 인터넷 게이트웨이	접근통제 영역	서버 접근
		인터넷 접속
보안 구성	암호 정책	암호 정책 수립
유저 계정	접근권한 관리	사용자 등록 및 권한부여
	사용자 인증 및 식별	사용자 패스워드 관리
관리자 계정	접근권한 관리	관리자 및 특수 권한 관리
	접근통제 영역	인터넷 접속 제한
악성 프로그램 보호	악성코드 관리	악성코드 통제
패치와 업데이트	접근통제 영역	네트워크 접근
		데이터 베이스 접근
	시스템 및 비스 운영 보안	공개서버 보안
		취약점 점검
	악성코드 관리	패치 관리
정보보호교육	교육 프로그램 수립	교육 계획
		교육 내용 및 방법
	교육 시행 및 평가	교육 시행 및 평가

3.4 간편 ISMS 핵심 통제[7]

간편 ISMS는 7개의 통제 항목과 16개의 세

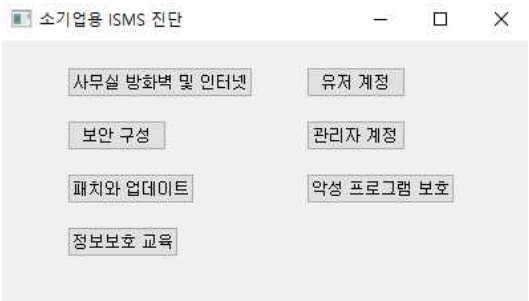
부 통제 항목으로 구성 되어 있다. 세부적인 통제 항목 내용은 다음과 같다.

‘사무실 방화벽 및 인터넷 게이트 웨이’ 통제 항목의 세부적인 통제 내용은 다음과 같다. 기업의 주요한 서비스를 제공하는 서버는 독립적으로 운영되고, 외부 서비스와 개인정보를 제공하는 웹 또는 DB와 응용프로그램 등은 독립적인 서버를 활용해야 한다. 또한 내부 직원의 PC의 외부 악성코드 유입을 사전 차단하기 위해 유해 사이트에 대한 차단 조치를 수행해야 한다. ‘사무실 보안 통제’ 통제 항목의 세부적인 통제 내용은 다음과 같다. 개인 PC업무 환경에서의 정보보호에 대한 정책을 수립, 이행하고, 이동식 저장매체 이용 주의와 중요문서 파기대책을 마련 한다. 민감한 정보를 다루는 PC의 경우 내부 저장장치 보안에 유의하며 암호화 정책을 수립, 이행해야 한다. ‘패치와 업데이트 통제’ 통제 항목의 세부적인 통제 내용은 다음과 같다. 사내 네트워크를 구성하는 점검 항목들을 최신으로 유지하고, 안전하게 관리해야 하며 중요 정보를 저장하는 DB의 경우 접속내역과 접근 목적을 항시 검토해야 한다. ‘사용자 계정 설정 통제’ 통제 항목의 세부적인 통제 내용은 다음과 같다. 조직 내부 모든 시스템에 보안 가이드에 맞는 패스워드를 사용하며 안전하게 관리되어야 한다. ‘관리자 계정 통제’ 통제 항목의 세부적인 통제 내용은 다음과 같다. 관리자, 특수권한 할당은 책임자의 승인과 올바른 절차를 거쳐야하며 최소한으로 제한하고, 별도의 목록으로 통제 및 관리해야 한다. ‘악성프로그램 보호 통제’ 통제 항목의 세부적인 통제 내용은 다음과 같다. 외부 악성코드로부터 보호를 위해 올바른 절차 및 지침을 수립하고, 백신 프로그램의 실시간 탐지 및 최신 소프트웨어 유지가 필요하다. ‘정보보호 교육’ 통제 항목의 세부적인 통제 내용은 다음과 같다. 사내 직원의 정보보호 교육 계획을 수립, 시행해야 한다. 정보보호 교육에는 기본적인 정보보호의 개념, 정보보호 관리체계 구축과 정보보호 관련 법률, 최신 침해 사례 등을 포함하여야 한다.

IV. 간편 인증을 위한 보안 통제 진단 툴 구현 결과

4.1 개발환경

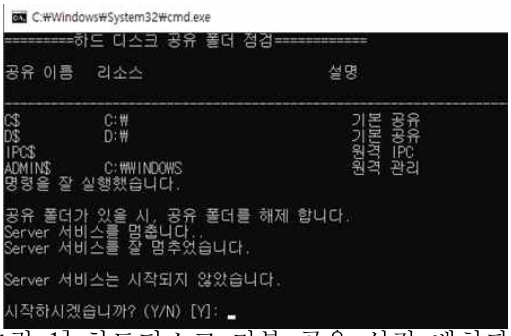
보안 통제 진단 가이드 툴을 만들기 위한 개발 환경이다. 먼저 파이썬(python) 편집기는 PyCharm, 파이썬 패키지는 Anaconda3을 사용했다. 또한 DBMS 진단 부분에서의 DB 보안 통제 진단을 위해 오라클 DB를 사용했다.



[그림 1] 보안 통제 진단 툴 구현 메인 화면

4.2 윈도우 시스템 진단[8]

윈도우 시스템 진단 부분은 축약 ISMS의 ‘유저 계정’, ‘관리자 계정’, ‘악성 프로그램 보호’ 통제 항목과 취약점진단가이드의 W-01 항목의 윈도우 최상위 관리자 계정 명 변경 여부, W-02 항목의 guest 계정 상태, W-05 항목의 해독 가능한 암호화 사용 여부, W-06 항목의 관리자 그룹 최소한 사용자 설정, W-08 항목의 하드디스크 기본 공유 제거, W-32 항목의 HOT FIX 적용 여부 총 6가지 가이드를 활용했다. 현재 6개 항목 전부 개발이 완료 되어 있으며 추후 개선사항 또한 계속 수정해 나갈 예정이다. 6가지 진단 항목들은 전부 취약함 판단 기준을 사용자에게 설명하고, 윈도우 스크립트를 활용해서 현재 진행 사항과 함께 조치 방법 또한 표시하며 위 가이드는 배치파일을 이용하여 사용자에게 안내된다.



[그림 1] 하드디스크 기본 공유 설정 배치파일

4.3 윈도우 서버 진단

윈도우 서버 진단 부분은 간편 ISMS의 '사무실 방화벽 및 인터넷 게이트 웨이' 통제 항목의 '서버 접근', '인터넷 접속' 세부 항목을 사용했다. 먼저 서버 접근 항목에서는 주요 서비스를 제공하는 서버는 독립된 서버로 운영하고 있는지를 점검 하고, 주요 서비스를 이용하는 PC는 독립된 사용을 위해 로컬 인터넷과 무선 인터넷 연결을 해제하는 배치파일을 만들었다. 또한 내부직원의 업무용 PC에서 유해 사이트 등의 접속을 차단하고 있는지 확인하고, 이에 대한 차단 조치를 위해 \etc\hosts 파일에 유해 사이트를 입력해서 해당 사이트에 접근할 수 없도록 했다.

4.4 DBMS 진단[9]

DBMS 취약점 진단 부분은 간편 ISMS의 '패치와 업데이트' 보안 통제 항목의 '데이터베이스 접근','패치관리','취약점 점검' 세부 통제 항목과 취약점진단가이드의 D-01 항목의 기본 계정의 패스워드 및 권한 변경, D-03 항목의 기관 정책에 따른 패스워드 설정, D-04 항목의 DB 관리자 권한 설정, D-05 항목의 원격 DB 서버의 접속 제한, D-10 항목의 DB의 최신 보안패치 총 5가지 가이드를 활용했다. 현재는 첫 번째 항목만 실질적으로 개발이 완료 되어 있고, 나머지 부분은 추후에 계속해서 개발해 나아갈 예정이다. 첫 번째 항목은 데이터베이스 계정의 기본으로 생성되는 디폴트 패스워드의 변경을 권고하는 항목이다. 개발 환경으로 사용한 oracle 데이터베이스를 기준으로 설치 시 생성되는 기본 디폴트 계정 정보를 안내하고, 현재 데이터베이스에 생성된 계정도 사용자에게 보여준 후 위와 같은 패스워드를 사용할 경우에는 패스워드 변경을 유도하는 방식이다.

4.5 보안 프로그램 수립 자가진단 체크리스트

자가진단 체크리스트는 간편 ISMS 통제 항목 중 '정보보호교육' 항목의 세부 통제 항목을 이용해서 개발 될 예정이며, 교육 시기, 교육 대상, 교육 내용 등 사내 직원들의 전반적인 보안 교육의 질 향상을 위한 것이다.

V. 결론

본 논문에서는 우리나라의 정보보호체계와 CES에 대한 이해를 돕고, 위를 바탕으로 작성한 간편 ISMS를 이용해서 중소기업에 적합한 보안 점검 항목을 제시한다. 간편 ISMS의 통제 항목 축약 기준과 정보보호 관리체계의 선별 항목을 설명하며, 보안 통제 진단 가이드 툴을 통해서 툴의 가이드 항목과 사용자에게 제공되는 방식, 개발 방법을 설명한다. 간편화된 ISMS 항목을 바탕으로 개발된 보안 통제 진단 가이드 툴은 영국 보안 제도인 CES 점검 항목을 참고하여 선별 되었으며, 정보보호 관리체계 취득 및 유지에 부담을 느끼는 중소기업 및 소기업들에게 도움이 될 것이다.

[참고문헌]

[1] 영세/중소기업을 위한 정보보호 관리체계 (ISMS) 간편 인증 신설(2021.1.11.) "https://blog.naver.com/softwidesec/222200522615"
[2]CyberEssentials(CES) 위키피디아 "https://ko.wikipedia.org/wiki"
[3] Cyber Essentials "https://iasme.co.uk/cyber-essentials/"
[4] Cyber Essentials "https://iasme.co.uk/cyber-essentials/"
[5] IASME(2021) "Cyber Essentials"
[6] KISA(2021.03) "주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드"
[7] KISA(2013.05.15) "ISMS 인증기준 세부점검항목"
[8] KISA(2021.03) "주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드"
[9] KISA(2021.03) "주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드"