기술경영학 석사 학위 프로젝트 보고서

동남권 중소기업 정보보안 수준 분석을 통한 개선방안 연구

2019년 2월

부경대학교 기술경영전문대학원

기술경영학과

김 건 오

기술경영학 석사 학위 프로젝트 보고서

동남권 중소기업 정보보안 수준 분석을 통한 개선방안 연구

지 도 교 수 옥 영 석

석사학위 논문에 준하는 보고서로 제출함.

2019년 2월

부경대학교 기술경영전문대학원

기술경영학과

김 건 오

김건오의 기술경영학 석사학위 프로젝트보고서를 인준함.

2019년 2월 23일

위 원 장 공학박사 천 동 필 (인)

위 원 공학박사 안 용 호 (인)

위 원 공학박사 옥 영 석 (인)

목 차

표 목 차

그 림 목 차

동남권 중소기업 정보보안 수준 분석을 통한 개선방안 연구

Gun Oh Kim

Graduate School of Management of Technology
Pukyong National University

Abstract

The threats to information security of enterprises are increasing day by day, but SMEs with poor financial environment are not able to implement budget easily for information security.

We will analyze the strengths and weaknesses of the information security related support projects implemented by the government for small and medium enterprises, and provide the results that SMEs can select the business suited to their environment.

And the evaluation of the level of information security of small and medium-sized enterprises in the Southeast, and how to support information security support policies for domestic enterprises.

Ⅰ. 서 론

1. 연구의 배경과 목적

다종, 대량의 데이터가 빅데이터로 지칭되고 도래하는 4차 산업혁명의 원유라 불릴 정도로 정보의 중요성이 증가함과 동시에 다양한 목적으로 데이터를 위협하는 요소들도 함께 증가하고 있다. 이러한 사이버범죄는 <그림 1-1>에서 제시된 바와 같이 2018년 3분기까지 총 108,825건이 발생하였으며, 2017년 같은 기간(101,653건)에 비교해 발생 건수가 약 7.1% 증가하였다.[1)]

<그림1-1> 2018년 3분기까지 국내 사이버 범죄 발생 건 수

이에 대비하여 대기업은 정보보안을 위한 지속적인 투자를 시행하고 있으며 국가는 관련 법을 제정하고 법령에 따라 매년 진단을 시행하는 등 지속적인 노력을 기울이고 있다. 반면, 예산과 인력이 부족한 국내 중소기업의 경우 심각할 정도로 방치되어 있다.

최근 3년간 중소기업이 기술유출만으로 입은 피해가 1,022억원이라는 조사가 있으며 피해 내용을 해킹, 암호화 공격 등으로 늘리면 그 규모는 더욱 늘어날 것이다. 또한 피해사실을 공개하지 않은 것을 포함한다면 중소

1) 2018년 3분기 사이버위협 분석 보고서(경찰청, 2018)

기업이 지불하고 있는 정보보안 피해 비용은 더욱 커질 수 밖에 없다.[2)]

본 고에서는 국내에서 이루어지고 있는 중소기업을 대상으로 하는 정보보호 지원사업을 개괄하고 동남권 중소기업을 대상으로 정보보안 수준 진단을 시행하고 분석하여 향후 지원사업의 방향에 대해 의견을 제시하고자 한다.

2. 선행 연구에 대한 검토

정보보안에 관한 연구들은 기술적 보안영역에 활발하게 진행되고 있으나, 이를 기업이나 기관에 적용하고 그 결과를 통해 더욱 효과적이고 효율적인 정보보안 지원과 활동에 대해서는 상대적으로 활발하지 않은 것으로 보인다.

서승우(2008)는 “보안 경제학 CEO를 위한 정보보안 투자 가이드”에서 보안에 대한 투자는 일회성이 아니라 위험 분석을 통한 반복적이고 순환적인 업무 프로세서로 정착되어야 진정한 효과를 거둘 수 있다고 주장하고 있다.[3)] 전 세계적인 경기 불황과 국내 경기 침체 등의 여건을 고려하더라도 우리 사회가 중소기업에 지속적인 보안 활동을 할 수 있는 과학적 근거와 분위기를 조정하지 못한 것은 양적으로 부족한 연구를 통해 가름할 수 있다.

배영식(2012)은 정보보호 관리체계 인증이 조직성과에 미치는 영향에 관한 연구를 통해 정보보호 인증이 경제성 확보에 기인한다는 결과를 제시하였다. 하지만, 한국인터넷진흥원의 홈페이지에 따르면 현재까지 발급된 인증서는 총 843건이며, 유지되고 있는 인증서는 591건으로[4)] 전체 산업의

---

2) 2017 중소기업 기술보호 수준 실태조사(대·중소기업·농어업 협력재단, 2018)
3) 보안 경제학 CEO를 위한 정보보안 투자 가이드(서울대학교출판부, 2008)
4) https://isms.kisa.or.kr/main/isms/issue/ (한국인터넷진흥원, 2018년 11월 5일)

사업체 수 3,950,192개의 0.014%에 불과한 수준이다. 인증서를 유지하는 곳도 대부분 법에 따라 의무적으로 수행을 하여 과태료를 면하는 것에 목적으로 두고 있다. 국내 대학들의 경우 3000만 원의 과태료를 내고 2억 원가량의 비용을 아끼자는 방향으로 의견이 모였다는 것이 언론에 소개가 되기도 했다.[5] 강력한 법적 장치나 힘의 논리로 대학들이 정보보호 관리체계를 수립하도록 강제하는 것 이상으로 중요한 것은 각 대학의 담당자들이 정보보호 체계를 기반으로 지속해서 정보보안 활동을 수행하는 것이 얼마나 중요한 것인지에 대한 충분한 설명과 현실 위험에 대한 인식을 심어주는 것이다. 과태료를 피하기 위한 기계적인 정보보안 체계 수립은 도입 비용만을 소모하고 실제로는 수립 이전보다 못한 불안전한 보안환경을 구축할 수 있기 때문이다.

ISMS(Information Security Management System) 인증을 통해 경제적인 효과를 기대할 수 있다는 이상의 연구들에도 불구하고 국내 중소기업은 언제 발생할지 모르는 보안 사고에 대비해 조직 전체를 관통하는 업무 프로세스의 변화 및 다양하고 수고스러운 심지어 비용까지 들어가는 인증에 매력을 느끼지 못한다. <표1-1>은 한국인터넷진흥원이 홈페이지를 통해 제공하는 ISMS 인증 취득 시 제공하는 혜택으로 중소기업이 흥미를 느낄만한 부문이 없다. [6]

---

5) http://www.ddaily.co.kr/news/article.html?no=155259 (디지털데일리, 2017년 4월 23일)

6) https://isms.kisa.or.kr/main/isms/intro/ (한국인터넷진흥원, 2018년 11월 5일)

<표1-1> ISMS인증 취득 시 혜택

구분	시행기관	혜택
평가항목	과학기술 정보통신부	SW 개발사업자 선정 특정평가항목 5점 부여
		보안관제 전문업체 지정 시 5점 부여
		정보보호 전문서비스 기업 지정 시 5점 부여
	KISA	정보보호 대상 평가 시 가점 부여
	한국기업 지배구조원	상장기업대상 ESG 평가 일부 항목 대체
요금할인	보험사	정보보호 관련 보험 가입 시 할인
권고	국토교통부	유비쿼터스 도시 기반 시설 인증 취득 권고
	교육부	사이버 대학 인증 취득 권고
ISMS 인증 수수료 할인	KISA	중소기업 할인(매출액 100억 미만, 30%)

최근 국내외 불경기 속에서 당장 효과나 혜택을 기대할 수 없는 ISMS 인증에 중소기업이 투자할 것이라고 기대할 수 없다. ISMS 및 ISO27001 인증을 기업에 적용해 나가는 것과는 별개로 상대적으로 자본력이 약한 중소기업이 당장 갖추어야 할 중요한 최소한의 정보보호 체계를 수립할 방법에 대해 많은 노력이 필요하다.

3. 연구의 내용과 구성

중소기업을 대상으로 시행되는 국내 정보보안 진단사업을 분석하여 기업의 입장에서 가장 자신에게 맞는 사업을 선택할 수 있는 기준을 제시하고 사업을 집행하는 기관에는 더 나은 정보보안 진단사업을 만들 수 있는 근거를 제공하고자 한다.

본 고는 전체 4장으로 구성되어 있고 각 장의 구성 내용을 다음과 같이 정리하였다. 제1장 서론 부문은 연구에 대한 배경과 목적 그리고 연구의 내용과 구성을 소개하였다. 제2장 정보보호 지원사업 국내현황에서는 대·중·소기업농어업협력재단에서 주관하는 기술보호 현장클리닉과 한국인터넷진흥원에서 주관하는 중소기업 정보보호 컨설팅 지원의 진단내용에 비교·분석한다. 그리고 제3장 중소기업들을 대상으로 진행된 정보보호 컨설팅 결과를 취합하여 관리, 물리, 기술적 분야로 나누어 분석한 결과를 제시한다. 제4장 결론에는 이상의 연구를 종합하여 시사하는 바를 설명하고 국내 중소기업에 대한 정보보안 연구가 지속해서 이루어져야 하는 당위성을 제시한다.

Ⅱ. 정보보호 지원사업 국내현황

본 장에서는 국내에서 진행되고 있는 국내 정보보호 지원사업 중 중소기업을 대상으로 진행되는 것에 한정하여 설명한다. 국가안전보장 등의 업무와 관련된 시스템의 경우 “정보통신기반 보호법”에 따라 매년 1회 이상의 취약점 진단을 강제하고 있으나 중소기업의 정보보안을 강제하는 법이나 기타 규제는 없는 상태이고 정부 지원사업의 경우 행정 예산에 따라 실시되고 있다.

1. 중소기업 기술보호

가. 개요

“중소기업 기술보호”는 기술보호 예방 진단, 상담자문을 통한 중소기업의 애로 해결을 목적으로 하는 사업이다. 지원대상은 중소기업기본법 제2조 제1항의 중소기업 및 중견기업법 시행령 제9조의 3에 따른 중견기업으로 하고 있다.

중소·중견기업을 대상으로 기술보호 무료진단 및 실태 점검을 통해 대책 제시 및 기술임치제도 이행 연계 지원을 목적으로 대·중소기업 농어업 협력재단이 주관하고 있다.

수행인력은 전문가로 지정된 전문위원 1명이 진행하고 현장 실사, 인터뷰 등을 통해 관리적 물리적 보안에 대해서 현장 클리닉이 진행된다. 심화단계를 통해 3일을 더 진단 및 지원을 받을 수 있다. 하지만, 지원 영역이 관리, 물리 영역으로 한정된다는 한계를 가지고 있으므로 기술적인 부문에

대한 지원은 불가하여 전반적인 정보보안 수준 향상에도 역시 한계를 가진다. 중소기업 기술보호 사업의 지원 내용을 정리하면 <표2-1>과 같다.

<표2-1> 중소기업 기술보호 개요

지원사업명	중소기업 기술보호
주관기관	대·중·소기업농어업협력재단
비용	무료
1개 기업당 투입인력	1명
주요진단영역	관리, 물리 부문
진행 기간	1일 진행 후 중소기업 희망 시 3일

나. 진단항목

<표2-2>에 제시된 “기술보호 현장클리닉”의 진단항목은 “중소·중견기업 보안역량 진단표”로 정리되어 있어 현장 클리닉을 수행하는 전문위원이 쉽게 접근할 수 있게 되어있다.

<표2-2> 중소기업 기술보호 진단항목

구분	항목 수	배점
Ⅰ. 기업의 보안정책	9	15
Ⅱ. 기업의 자산관리	7	13
Ⅲ. 기업의 인적자원관리	10	20
Ⅳ. 기업의 시설관리	7	12
Ⅴ. 기업의 IT 보안관리	14	30
Ⅵ. 기업의 유출 사고 대응 관련	3	10
계	**50**	**100**

<표 2-3>에는 15점이 배점되어 있는 “Ⅰ. 기업의 보안정책”영역은 보안 관련 업무절차가 수립되어 수립된 절차에 따라 준거성 있게 실시되고 있는지를 진단하는 항목으로 구성이 되어있다.

<표2-3> 기업의 보안정책 통제항목

구분	진단내용
1.1	보안규정을 보유하고 있는가? ① 보유하고 있다 (2점) ② 보유하고 있지 않다 (0점)
1.2	회사의 보안정책, 지침, 절차 등의 내용에 대해 임직원들에게 공지하고 있는가? ① 공지하고 있다 (1점) ② 공지하고 있지 않다 (0점)
1.3	보안전담조직이 존재하는가? ① 보안전담조직과 보안담당자가 존재한다 (2점) ② 보안담당자만 존재한다 (1점) ③ 보안전담조직과 담당자 모두 존재하지 않는다 (0점)
1.4	회사의 주요 정보(기술, 영업 등)는 어떻게 공유되는가? ① 업무담당자, 관계자 등 소수만이 볼 수 있다 (2점) ② 핵심정보를 제외하고는 직원들이 볼 수 있다 (1점) ③ 대부분 정보에 대해서 직원들이 볼 수 있다 (0점)
1.5	임직원의 업무에 기밀 사항의 보호 등 보안 관련 내용이 포함되어 있는가? ① 포함되어 있다 (1점) ② 포함되어 있지 않다 (0점)
1.6	회사 내 보안업무 수행을 위해 팀(혹은 그룹)간 업무 공조체계가 구성되어 있는가? ① 구성되어 있다 (1점) ② 구성되어 있지 않다 (0점)
1.7	정기적으로 보안감사를 실시하고 있는가? ① 정기적으로 실시하고 있다 (2점) ② 필요할 때 수시로 실시하고 있다 (1점) ③ 실시하지 않고 있다 (0점)

구분	진단내용
1.8	회사가 보유한 주요 정보 및 자산을 보호하기 위해 투자하는 비용 수준은 어떠한가? ① 기술적, 물리적, 관리적 보안을 위해 매년 일정 비용 이상을 꾸준히 투자하고 있다 (3점) ② 특정 보안분야에 대해 필요 시 비용투자가 이루어지고 있다 (1.5점) ③ 보안분야에 대한 투자가 이루어지고 있지 않다 (0점)
1.9	보안업무 추진을 위해 외부 전담기관의 도움을 받고 있습니까? ① 도움을 받고 있다 (1점) ② 도움을 받고 있지 않다 (0점)

<표 2-4>에는 총 13점이 배점된 <표 2-4>는 “Ⅱ. 기업의 자산관리”는 정보자산의 가치를 주기적으로 측정하고 기밀에 해당하는 정보와 특허에 대한 정보자산의 통제 하에서 관리되고 있는지를 측정한다.

<표2-4> 기업의 자산관리 통제항목

구분	진단내용
2.1	회사가 보유한 정보자산에 대해 목록 관리 등을 통한 관리기준을 수립하여 가지고 있는가? ① 그렇다 (2점) ② 그렇지 않다 (0점)
2.2	회사의 정보자산을 그 중요성에 따라 ‘극비’, ‘대외비’, ‘일반’ 등으로 등급을 구분하여 관리하고 있는가? ① 구분하여 관리하고 있다 (2점) ② 구분하지 않는다 (0점)
2.3	회사의 정보자산에 대해 관리책임자를 지정하여 관리하고 있는가? ① 그렇다 (2점) ② 그렇지 않다 (0점)

구분	진단내용
2.4	회사의 정보자산 분류는 정기적으로 이루어지는가? ① 정기적으로 이루어진다 (2점) ② 필요 시 이루어진다 (1점) ③ 이루어지지 않고 있다 (0점)
2.5	주요 기밀문서의 경우 어떻게 관리하고 있는가? ① 사용자별 권한 설정이 되어있다 (2점) ② 사용자별 일부 권한 설정이 되어있다 (1점) ③ 사용자별 권한 설정이 되어있지 않는다 (0점)
2.6	특허, 실용신안, 디자인 등 지적 재산권에 대한 관리방안이 마련되어 있는가? ① 권리출원 및 대응전략이 모두 마련되어 있다 (2점) ② 권리출원과 대응전략 중 하나만 마련되어 있다 (1점) ③ 마련되어 있지 않다 (0점)
2.7	장비, 정보 또는 소프트웨어 등의 회사 자산의 반출은 어떤 식으로 이루어지는가? ① 사전 인가가 있어야만 반출이 가능하다 (1점) ② 사전 인가 없이도 반출이 가능하다 (0점)

<표 2-5>에는 “Ⅲ. 기업의 인적자원관리”에는 총 20점이 배점되어 있으며 10개 문항으로 구성되어 있다. 인력에 대한 보안교육 시행 여부 및 보안서약서 징구 등 인력 통제 전반에 대해 확인현황을 검토하도록 하고 있다.

<표2-5> 기업의 인적자원관리 통제항목

구분	진단내용
3.1	신규 입사자에 대해 보안교육을 실시하고 있는가? ① 실시하고 있다 (1점) ② 실시하고 있지 않다 (0점)

구분	진단내용
3.2	기존 임직원을 대상으로 보안교육을 실시하고 있는가? ① 정기적으로 실시하고 있다 (2점) ② 필요 시 실시하고 있다 (1점) ③ 실시하고 있지 않다 (0점)
3.3	임직원 보안의식을 제고하기 위해 퇴근 시 혹은 자리 이탈 시에 다음과 같은 활동을 수행하고 있는가? ① PC 전원 Off 여부 확인 ② 장시간 자리 이탈 시 화면보호기 설정 여부 확인 ③ 노트북 방치 여부 확인 ④ 출입문, 캐비넷, 개인서랍 시건 여부 확인 ⑤ 문서 및 도면 방치 여부 확인 ※ 4개 이상 - 3점, 2~3개 - 2점, 1개 - 1점
3.4	신규 입사자에 대해 보안서약서를 징구하고 있는가? ① 보안서약서를 근로계약서와 별도로 징구하고 있다 (2점) ② 별도로 보안서약서를 징구하고 있지는 않지만, 고용계약서에 보안책임을 명시하고 있다 (1점) ③ 징구하고 있지 않다 (0점)
3.5	주요 R&D 프로젝트 참가자에 대해 보안서약서를 징구하고 있는가? ① 징구하고 있다 (2점) ② 징구하고 있지 않다 (0점)
3.6	종업원이 보안정책, 지침, 절차 등을 위반하는 경우 직원에 대한 공식적인 징계 절차가 마련되어 있는가? ① 징계절차가 마련되어 있으며, 필요 시 징계조치가 이루어진다 (2점) ② 징계절차는 마련되어 있으나, 징계조치는 거의 이루어지지 않는다 (1점) ③ 징계절차가 마련되어 있지 않다 (0점)
3.7	퇴직자에 대해 회사 정보자산의 유출방지를 위한 보안서약서를 징구하고 있는가? ① 징구하고 있다 (2점) ② 징구하고 있지 않다 (0점)
3.8	퇴직자의 향후 진로 및 동향을 파악하고 있는가 ? ① 모든 퇴직자의 동향을 파악하고 있다 (2점) ② 주요 임직원에 한하여 파악하고 있다 (1점) ③ 전혀 파악하고 있지 않다 (0점)

구분	진단내용
3.9	제3자(협력업체, 외국인 등)에 대한 관리를 하고 있는가? ① 별도의 관리방안이 마련되어 있으며, 대상자에 대한 보안서약을 하고 있다 (2점) ② 별도의 관리방안은 마련되어 있지 않으나, 대상자에 대한 보안서약은 하고 있다 (1점) ③ 별도의 관리방안이 마련되어 있지 않으며, 대상자에 대한 보안서약도 하고 있지 않다 (0점)
3.10	회사의 정보자산에 대한 사용자(임직원, 계약자, 제3의 사용자 등)들의 접근 권한은 퇴사, 계약종료, 역할 조정 등의 사유발생시 조정되어지고 있는가? ① 사유발생 즉시 조정되어진다 (2점) ② 사유발생 1주일 이내에 조정되어진다 (1점) ③ 조정이 지연되거나 이루어지지 않는다 (0점)

12점이 배점되어 있는 “Ⅳ. 기업의 시설관리”부문은 물리적 보안현황을 점검하는 항목으로 <표2-6>과 같이 구성되어 있다.

<표2-6> 기업의 시설관리 통제항목

구분	진단내용
4.1	회사 내 중요시설에 대한 관리기준이 있는가? ① 관리기준이 존재한다 (2점) ② 관리기준이 존재하지 않는다 (0점)
4.2	협력업체, 방문객 등 외부인의 회사 내 출입절차가 존재하는가? ① 출입절차가 존재하며, 출입관리대장을 기재한다 (2점) ② 출입절차가 존재하지만, 출입관리대장은 기재하지 않는다 (1점) ③ 별도의 출입절차가 존재하지 않는다 (0점)

구분	진단내용
4.3	회사 내 중요시설에 대해 출입통제시스템을 설치하여 운영하고 있는가? ① 출입통제시스템을 운영하고 있으며, 내부의 한정된 인원만 출입이 가능하다 (2점) ② 출입통제시스템을 운영하고 있으며, 내부 인원은 자유로이 출입이 가능하다 (1점) ③ 출입통제시스템을 운영하고 있지 않으며, 내외부 인원의 자유로운 출입이 가능하다 (0점)
4.4	외부인 식별을 위하여 임직원의 사원증 패용을 의무화하고 있는가? ① 의무화 하고 있다 (1점) ② 의무화 하고 있지 않다 (0점)
4.5	건물 출입구나 중요시설에 대해 CCTV 등의 감시 장치가 설치되어 있는가? ① 설치되어 있다 (2점) ② 설치되어 있지 않다 (0점)
4.6	중요시설 및 통제구역에 대해 화재, 전원, 수해 등으로부터의 보호방안이 강구되어 있는가? ① 보호방안이 강구되어 있다 (2점) ② 보호방안이 강구되어 있지 않다 (0점)
4.7	회사 내 중요시설에 카메라, 비디오 카메라 등의 장비반입이 규정에 의해 통제되고 있는가? ① 규정에 의해 통제되고 있다 (1점) ② 규정에 의해 통제되고 있지 않다 (0점)

30점이 배점된 “Ⅴ. 기업의 IT보안관리“는 중소기업의 IT관련 보안을 측정하는 것으로 기술적 보안 수준을 측정하는 것으로 <표2-7>과 같이 구성되어 있다.

<표2-7> 기업의 IT보안관리 통제항목

구분	진단내용
5.1	다음과 같은 정보처리 설비의 운영절차가 문서화되어 규정되어 있는가? ① 컴퓨터의 가동과 종료절차

구분	진단내용
	② 백업절차 ③ 유지 보수절차 ④ 예상치 못한 운영상 또는 기술적인 어려움 발생시 지원연락처 ⑤ 비밀정보를 포함한 출력물의 관리 및 폐기절차 준수 ⑥ 시스템 오작동시 시스템의 재시작 및 복구절차 준수 ※ 해당되는 문항마다 0.5점
5.2	통신망에 대한 보안점검을 실시하고 있는가? ① 보안상태에 대해 주기적으로 점검하고 있다 (2점) ② 필요가 있을 때만 실시하고 있다 (1점) ③ 보안점검을 실시하고 있지 않다 (0점)
5.3	서버 및 DB 현황에 대한 보안점검을 실시하고 있는가? ① 보안상태에 대해 주기적으로 점검하고 있다 (2점) ② 필요가 있을 때만 실시하고 있다 (1점) ③ 보안점검을 실시하고 있지 않다 (0점)
5.4	바이러스 침입, 해킹, 내부로부터의 정보유출을 방지하기 위한 대책을 강구하고 있는가? ① 각종 보안솔루션을 도입하여 사용하고 있다 (3점) ② 일부 보안솔루션을 도입하여 사용하고 있다 (1.5점) ③ 보안솔루션 도입은 아직 이루어지고 있지 않다 (0점)
5.5	내부에서 생성된 주요 정보 및 소프트웨어는 백업되어 관리되고 있는가? ① 정기적으로 백업하여 관리하고 있다 (2점) ② 필요시 백업하여 관리하고 있다 (1점) ③ 백업하여 관리하고 있지 않다 (0점)
5.6	지식관리시스템(KMS), 전자결재시스템 등 회사 내 주요 정보에 대한 관리시스템이 존재하는가? ① 관리시스템이 존재하며, 권한에 따라 정보의 공유가 이루어진다 (2점) ② 관리시스템이 존재하며, 모든 임직원들에게 정보의 공유가 이루어진다 (1점) ③ 관리시스템이 존재하지 않는다 (0점)
5.7	FD, CD, USB 등 정보의 저장이 가능한 매체에 대한 관리절차가 마련되어 있는가? ① 관리절차가 마련되어 있다 (2점) ② 관리절차가 마련되어 있지 않다 (0점)

구분	진단내용
5.8	외부로의 전자문서 발송에 대한 통제시스템이 마련되어 있는가? ① DRM, DMS 등 문서관리시스템이 마련되어 있다 (2점) ② 문서관리시스템은 마련되어 있지 않으나, 중요 문서에 한해 사전승인을 필요로 한다 (1점) ③ 전자문서 발송에 대한 통제가 존재하지 않는다 (0점)
5.9	PC 및 주요 시스템 사용자에 대한 패스워드 관리를 하고 있는가? ① 정례적으로 패스워드를 변경하고 있으며, 이를 수시로 점검한다 (2점) ② 정례적으로 패스워드를 변경할 것을 권장하고 있으나, 이행여부를 점검하지는 않는다 (1.5점) ③ 각 시스템에 패스워드를 사용한다 (1점) ④ 각 시스템에 대한 패스워드 사용을 강제하지 않는다 (0점)

10점이 배점된 “Ⅵ. 기업의 유출사고 대응”의 경우 중대재해가 발생했을 때 중소기업이 업무연속성을 가지고 진행될 수 있는 체계를 갖추고 있는지를 측정하기 위한 항목으로 <표2-8>과 같이 구성되어 있다.

<표2-8> 기업의 유출사고 대응 통제항목

구분	진단내용
6.1	정보시스템에 대한 재해발생시 다음과 같은 대응절차가 수립되어 있는가? ① 비상시 따라야 할 절차와 관련자의 책임규정 ② 유관기관과의 연락체계 구성여부 ③ 제한된 시간 내에 필수 업무 및 지원서비스를 대체장소로 이전하여 운영하기 위한 절차 ④ 정상적인 사업 활동으로 복귀하기 위한 원상복귀 절차 ⑤ 위기관리를 포함한 비상절차 및 프로세스에 대한 임직원 교육 ※ 해당되는 문항마다 1점

구분	진단내용
6.2	기술유출 및 침해사고 발생시 회사 차원의 대응방안이 마련되어 있는가? ① 구체적으로 마련되어 있다 (3점) ② 일부분이 마련되어 있다 (1점) ③ 마련되어 있지 않다 (0점)
6.3	부정경쟁방지 및 영업비밀 보호에 관한 법률, 산업기술의 유출방지 및 보호에 관한 법률, 국가연구개발사업 공통보안지침 등 기술유출 방지와 관련된 주요 법규에 대해 인지하고 있는가? ① 법규의 내용 대부분에 대해 알고 있다 (2점) ② 법규의 내용 일부분에 대해 알고 있다 (1점) ③ 법규의 내용에 대해 거의 알지 못한다 (0점)

이와는 별도로 중소기업 기술보호 10대 핵심수칙을 수립하여 중요사항을 점검하고 있는데 <표2-9>와 같이 구성되어 있다.

<표2-9> 중소기업 기술보호 10대 핵심수칙

항목
① 기술보호 관리 규정 보유 및 실시 여부
② 보안관리 전담인력 지정 여부(담당자지정 및 보안감사 실시 등)
③ 정기적인 기술보호 교육 실시 여부(전직원 대상)
④ 전직원 비밀유지서약 및 핵심직원 전직금지서약 체결 여부
⑤ 핵심기술 인력 퇴직후 사후관리(영업비밀 인수인계, 준수의무 등)
⑥ 중요 기술 영업비밀 분류 및 관리 여부(자산중 영업비밀 등급부여)
⑦ 중요 서류 별도 관리 여부(중요문서 관리번호 부여 등)
⑧ 중요 설비 및 장치에 대한 통제구역 설정 및 관리 여부
⑨ 중요 기술 특허 및 임치 여부
⑩ 정보시스템 보안 관리 여부(데이터 암호화, 허가 USB활용 등)

2. 중소기업 정보보호 컨설팅 지원

가. 개요

올해 처음 진행하는 사업으로 한국인터넷진흥원에서 발주하고 민간 컨설팅 업체가 수주하여 진행되었다. 정보보안 수준을 파악하기 위한 관리, 물리에 대한 수준 진단을 실시하고 정보시스템과 응용의 취약점 진단은 원격 및 방문으로 나누어 진행된다. 특히, 개인정보 취급현황에 대한 추가 진단도 함께 시행되었다. 구체적인 구성 내용은 <표2-10>과 같이 구성되어 있다.

<표2-10> 중소기업 정보보호 컨설팅 지원 개요

지원사업명	중소기업 정보보호 컨설팅 지원
주관기관	한국인터넷진흥원
비용	컨설팅은 무상, 보안제품 구매 바우처 사용 전제
1개 기업당 투입인력	원격 2명 내외, 방문 2명 내외
주요진단영역	관리, 물리, 기술, 개인정보, 응용
진행 기간	유동적

나. 진단항목

중소기업 정보보호 컨설팅 지원사업은 일반적으로 컨설팅이 가져야 하는 조건을 가장 근접한 구성을 하고 있다. 우선 관리적 진단의 진단항목은 <표 2-11>에서 나열된 바와 같이 총 65개 항목으로 구성되어 있는데, 주요정보통신기반시설의 관리진단항목 114개에 비해 적은 숫자이지만, 앞서 다른 기

관의 중소기업 정보보안 진단에 비해 많은 통제항목을 제공하고 있다.

<표2-11> 중소기업 정보보호 컨설팅 사업의 관리체계 점검항목

대분류	중분류	항목 수
정보보호 정책 및 조직	정책지침 수립·운영	4
	전담조직/인력 운영	2
	취약점 진단/보안감사	2
	정보보호 대책 수립·예산투자	1
인원 보안 및 자산관리	직무분리 및 비밀유지서약서	3
	인사 상벌규정, 퇴직자 보안관리	2
	외부자 보안관리(계약 등)	2
	정보보호인식교육/보안담당자 전문교육	2
	정보자산 식별 및 분류/보안등급 운영관리	2
시설보안	보호구역지정	1
	출입통제/외부인 출입절차	1
	출입통제장치/CCTV모니터링	1
	사무실/전산실 보안관리	4
IT보안관리	임직원 인증, 서비스 이용자 인증, 관리자 인증 절차	2
	접근권한관리 및 접근통제, 비밀번호관리	3
	통신 암호화/저장 암호화	2
	보안로그 저장/검토	1
	운영/개발시스템 분리 및 보안관리	2
	네트워크 접근통제/망분리	1
	서버 접근통제	1
	응용프로그램 접근통제	1
	데이터베이스 접근통제/암호화	1
	PC/노트북 보안관리	1
	모바일기기 보안관리	1
	인터넷 접속통제	1
	보안시스템 운영	1
	원격 운영관리/통제	1
	무선네트워크보안	1
	웹서버/홈페이지보안	1
	USB/CD 등 저장매체통제	1
	악성코드 통제(PC/이메일/유해사이트/웹)	2
	보안패치적용	1
보안사고관리	침해사고 대응절차/비상연락망	1
	장애/재난관리/백업	2
개인정보관리	개인정보책임자지정/조직	2
	개인정보관리지침/정책	1

대분류	중분류	항목 수
	개인정보의 기술적 보호조치	3
	개인정보 수집 고지 및 동의획득	1
	이용자 권리 보호	1
	개인정보 파기	1
	개인정보처리방침 운영	1
계		65

기술진단의 경우 Windows Server, UNIX, 네트워크, 정보보호 시스템, 그리고 PC로 나누어지며, 각 항목은 중요도에 따라 점수가 달리 책정되어 있다.

Windows Server는 41개 항목을 점검하도록 진단항목이 구성되어 있으며 항목별로 중요도를 달리하고 세부적인 진단 내용은 <표2-12>와 같이 구성되어 있다.

<표2-12> 중소기업 정보보호 컨설팅 사업의 Windows 점검항목

영역	점검항목	중요도
계정관리	Administrator 계정 이름 바꾸기	상
	Guest 계정 상태	상
	불필요한 계정 제거	상
	계정 잠금 임계값 설정	상
	해독 가능한 암호화를 사용하여 암호 저장	상
	관리자 그룹에 최소한의 사용자 포함	상
	Everyone 사용 권한을 익명 사용자에게 적용	중
	계정 잠금 기간 설정	중
	패스워드 복잡성 설정	중
	패스워드 최소 암호 길이	중
	패스워드 최대 사용 기간	중
	패스워드 최소 사용 기간	중
	마지막 사용자 이름 표시 안함	중
	로컬 로그온 허용	중
	최근 암호 기억	중
서비스	공유 권한 및 사용자 그룹 설정	상
	하드디스크 기본 공유 제거	상

영역	점검항목	중요도
관리	불필요한 서비스 제거	상
	NetBIOS 바인딩 서비스 구동 점검	상
	FTP 서비스 구동 점검	상
	FTP 디렉토리 접근권한 설정	상
	최신 서비스팩 적용	상
	터미널 서비스 암호화 수준 설정	중
	SNMP 서비스 구동 점검	중
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중
	Telnet 보안 설정	중
	원격터미널 접속 타임아웃 설정	중
패치관리	최신 HOT FIX 적용	상
	백신 프로그램 업데이트	상
로그관리	정책에 따른 시스템 로깅 설정	상
	원격으로 액세스할 수 있는 레지스트리 경로	상
	이벤트 로그 관리 설정	하
보안관리	백신 프로그램 설치	상
	화면보호기 설정	상
	로그온하지 않고 시스템 종료 허용	상
	원격 시스템에서 강제로 시스템 종료	상
	Autologon 기능 제어	상
	이동식 미디어 포맷 및 꺼내기 허용	상
	디스크볼륨 암호화 설정	상
	사용자가 프린터 드라이버를 설치할 수 없게 함	중
	경고 메시지 설정	하

UNIX도 35개 점검항목을 가지고 있으며, 항목별로 중요도를 달리하고 있다. 각 점검항목과 중요도는 <표2-13>과 같다.

<표2-13> 중소기업 정보보호 컨설팅 사업의 UNIX 점검항목

영역	점검항목	중요도
계정관리	root 계정 원격 접속 제한	상
	패스워드 복잡성 설정	상
	계정 잠금 임계값 설정	상
	패스워드 파일 보호	상
	root 이외의 UID가 '0' 금지	중
	root 계정 su 제한	하
	패스워드 최소 길이 설정	중

영역	점검항목	중요도
	패스워드 최대 사용 기간 설정	중
	패스워드 최소 사용기간 설정	중
	불필요한 계정 제거	하
	관리자 그룹에 최소한의 계정 포함	하
	Session Timeout 설정	하
파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상
	파일 및 디렉터리 소유자 설정	상
	/etc/passwd 파일 소유자 및 권한 설정	상
	/etc/shadow 파일 소유자 및 권한 설정	상
	/etc/syslog.conf 파일 소유자 및 권한 설정	상
	/etc/services 파일 소유자 및 권한 설정	상
	UMASK 설정 관리	중
서비스 관리	접속 IP 및 포트 제한	상
	Anonymous FTP 비활성화	상
	r 계열 서비스 비활성화	상
	cron 파일 소유자 및 권한 설정	상
	automountd 제거	상
	RPC 서비스 확인	상
	tftp, talk 서비스 비활성화	상
	ssh 원격접속 허용	중
	ftp 서비스 확인	하
	Ftpusers 파일 소유자 및 권한 설정	하
	Ftpusers 파일 설정	중
	SNMP 서비스 구동 점검	중
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중
	로그온 시 경고 메시지 제공	하
패치관리	최신 보안패치 및 밴더 권고사항 적용	상
로그관리	정책에 따른 시스템 로깅 설정	하

네트워크 장비를 진단해야 하는 항목은 37개로 구성되어 있으며 각 항목별로 중요도가 달리 책정되어 있으며 항목과 중요도는 <표2-14>와 같다

네트워크 장비 진단은 네트워크 장비의 설정값(Network-configuration) 파일을 받아서 분석하는 작업이므로 설정값을 도출할 수 없는 장비의 경우 진단이 불가능하다.

<표2-14> 중소기업 정보보호 컨설팅 사업의 네트워크 점검항목

영역	점검항목	중요도
계정관리	패스워드 설정	상
	패스워드 복잡성 설정	상
	암호화된 패스워드 사용	상
	사용자 명령어별 권한 수준 설정	중
접근관리	VTY 접근 (ACL) 설정	상
	Session Timeout 설정	상
	VTY 접속 시 안전한 프로토콜 사용	중
	불필요한 보조 입출력 포트 사용 금지	중
	로그온 시 경고 메시지 설정	중
패치관리	최신 보안 패치 및 밴더 권고사항 적용	상
기능관리	SNMP 서비스 확인	상
	SNMP community string 복잡성 설정	상
	SNMP ACL 설정	상
	SNMP 커뮤니티 권한 설정	상
	TFTP 서비스 차단	상
	Spoofing 방지 필터링 적용	상
	DDoS 공격 방어 설정	상
	사용하지 않는 인터페이스의 shudown 설정	상
	TCP keepalive 서비스 설정	중
	Finger 서비스 차단	중
	웹 서비스 차단	중
	TCP/UDP small 서비스 차단	중
	Bootp 서비스 차단	중
	CDP 서비스 차단	중
	Directed-broadcast 차단	중
	Source 라우팅 차단	중
	Proxy ARP 차단	중
	ICMP unreachable, Redirect 차단	중
	identd 서비스 차단	중
	Domain lookup 차단	중
	pad 차단	중
	mask-rely 차단	중
로그관리	원격 로그서버 사용	하
	로깅 버퍼 크기 설정	중
	정책에 따른 로깅 설정	중
	NTP 서버 연동	중
	timestamp 로그 설정	하

정보보호 시스템의 경우 26개 항목으로 구성이 되어 있고 각 항목과 중요도는 <표2-15>와 같이 구성되어 있다. 정보보호 시스템 진단은 시스템 운영자와 장비 콘솔을 통해 확인하는 방식으로 진행되며 가장 수작업에 가깝고 담당자의 도움이 필요한 진단이다.

<표2-15> 중소기업 정보보호 컨설팅 사업의 정보보호 시스템 점검항목

영역	점검항목	중요도
계정관리	보안장비 Default 계정 변경	상
	보안장비 Default 패스워드 변경	상
	보안장비 계정별 권한 설정	상
	보안장비 계정 관리	상
	로그인 실패횟수 제한	중
접근관리	보안장비 원격 관리 접근 통제	상
	보안장비 보안 접속	상
	Session timeout 설정	상
패치관리	벤더에서 제공하는 최신 업데이트 적용	상
로그관리	보안장비 로그 설정	중
	보안장비 로그 정기적 검토	중
	보안장비 로그 보관	중
	보안장비 정책 백업 설정	중
	원격 로그 서버 사용	중
	로그 서버 설정 관리	하
	NTP 서버 연동	중
기능관리	정책 관리	상
	NAT 설정	상
	DMZ 설정	상
	최소한의 서비스만 제공	상
	이상징후 탐지 경고 기능 설정	상
	장비 사용량 검토	상
	SNMP 서비스 확인	상
	SNMP community string 복잡성 설정	상
	부가 기능 설정	중
	유해 트래픽 차단 정책 설정	중

PC는 24개 진단항목으로 구성이 되어 있다. “개인정보 관리” 영역을 통해 개별 PC의 개인정보 취급 수준에 대해 진단하고 있다. 구체적인 항목과 중요도는 <표2-16>과 같다.

<표2-16> 중소기업 정보보호 컨설팅 사업의 PC 점검항목

영역	점검항목	중요도
사용자 계정 점검관리	Guest 계정 비활성화	상
	SAM 파일 접근통제	상
	패스워드 최소길이	중
	패스워드 최대 사용기간 설정	상
	최근 패스워드 기억	상
	패스워드 사용기간 제한	상
	패스워드 복잡성 설정	상
공유폴더관리	공유폴더 제거	중
서비스 및 방화벽관리	불필요한 서비스 제거	상
	방화벽 서비스 동작	상
화면보호기관리	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상
백신 및 업데이트	백신 설치 및 실시간 탐지 최신 보안패치	중
	운영체제 HOT FIX 설치 및 자동 업데이트	중
개인정보관리	주민등록번호: 항목이 하나라도 검색시 감점	상
	전화번호: 항목이 100개 초과 검색시 감점	상
	신용카드번호: 항목이 100개 초과 검색시 감점	상
	이메일주소: 항목이 초과 검색시 감점	상
	사업자등록번호: 항목이 1만개 초과 검색시 감점	상
	계좌번호: 항목이 100개 초과 검색시 감점	상
	여권번호: 항목이 100개 초과 검색시 감점	상
	주소: 항목이 1만개 초과 검색시 감점	상
	새주소: 항목이 1만개 초과 검색시 감점	상
	외국인등록번호: 항목이 100개 초과 검색시 감점	상
	운전면허번호: 항목이 100개 초과 검색시 감점	상

3. 동남권 중소기업 정보보호 서비스 및 컨설팅

가. 개요

부산정보산업진흥원에서 매년 진행하는 지원사업으로 부산에 거점을 두고 있는 약 180개 기업에 기술적 진단, 모의해킹 등을 제공하여 지역의 정보보안 수준 향상에 이바지하는 바가 적지 않다. 해당 사업의 구성은 <표3-1>과 같이 정리 할 수 있다.

<표3-1> 동남권 중소기업 정보보호 서비스 및 컨설팅 개요

지원사업명	동남권 중소기업 정보보호 서비스 및 컨설팅
주관기관	부산정보산업진흥원
비용	무상
1개 기업당 투입인력	유동적
주요진단영역	현장 컨설팅, 웹, 민감정보 진단
진행 기간	유동적

나. 진단항목

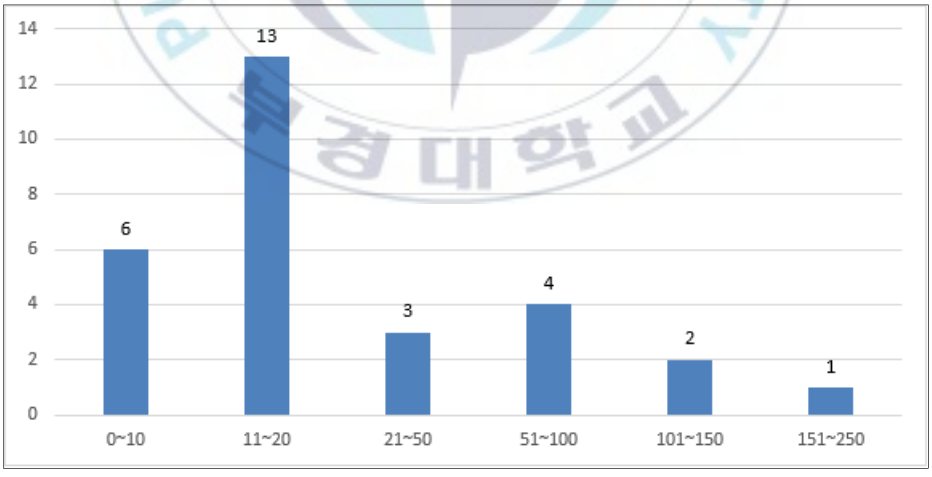
별도의 진단항목이 지정되어 있지 않으며, 수행하는 업체가 수립하여 진행하고 있다.

Ⅲ. 정보보호 컨설팅 결과 분석

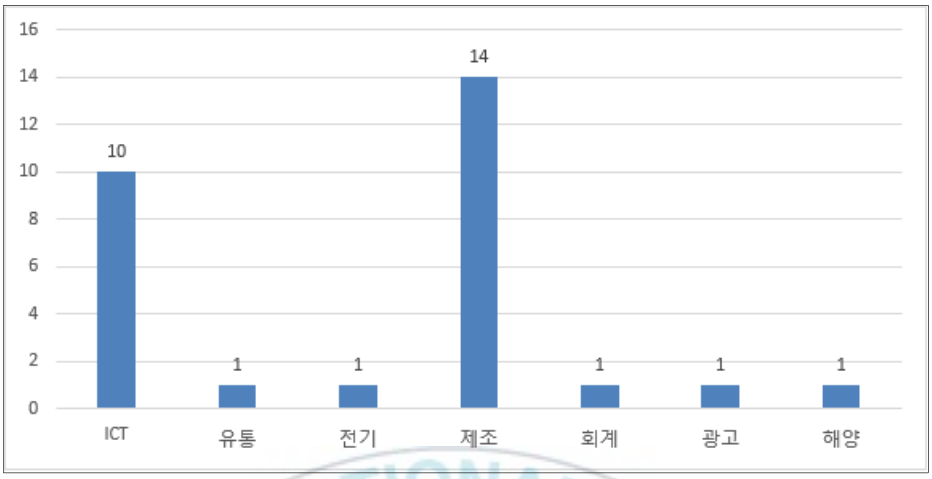
1. 컨설팅 대상 중소기업 개요

가. 동남권 거점 기업을 대상으로 정보보호 컨설팅 진행 수행

정보보안 수준 진단을 희망하는 중소기업을 대상으로 지원사업과 동일한 기준으로 컨설팅을 진행하였으며, <그림 3-1>은 대상 중소기업의 고용 현황을 집계하고 도식화한 것으로 11명 이상 20명 이하로 고용하고 있는 중소기업이 가장 많은 것으로 나타났으며 <그림 3-2>에 나타난 바와 같이 ICT와 제조에 가장 많이 분포되어 있었다.



<그림3-1> 중소기업 진단 대상 기업의 직원현황



<그림3-2> 중소기업 진단 대상 기업의 업종

연구 방향을 설정함에 있어 업종별로 고르게 대상을 선정하여야 하지만 대부분의 중소기업들이 정보보안에 대해서는 적대적이고 비협조적이기 때문에 선정에 많은 어려움이 있었다. 이러한 반응의 배경은 자사의 정보가 유출되는 것에 대한 막연한 불안감에서 오는 보수적 반응이기도 하지만 정보보안에 대한 투자가 없었던 만큼 비용 발생으로 연결될 가능성이 높은 것에 대한 불안으로 해석할 수 있다.

2. 보안 수준 분석

가. 모의해킹 결과 분석

대상 기업 중 웹사이트를 운영하는 경우에 한하여 모의해킹을 실시하였는데, 대부분의 경우 기초적인 취약점이 확인되었다. <그림3-3>는 대상 기업 중에서 웹사이트를 운영하고 있는 13개 회사의 모의해킹을 결과를 도표

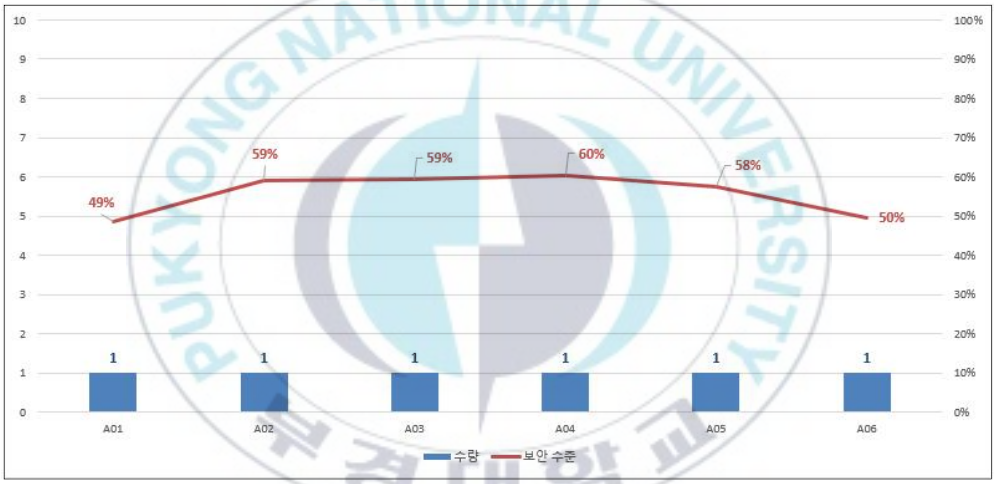
로 나타낸 것이다. Y축은 발견된 취약점 개수를 나타내고 있으며 X축은 회사별로 A01에서 A13까지 명칭을 대신해 나타내었다. 이하 모든 그림에서 나타나는 회사의 순서는 각각 다르게 표시되어 있어 동일한 순서를 가진다고 동일한 기업은 아니다

<그림3-3> 모의해킹으로 발견된 대상기업 웹페이지 취약점 수

다행스럽게도 개인정보를 수집하거나 회사의 기밀과 연동하여 운영되는 곳이 없으며, 크래킹이 발생하여도 금전적 혹은 기업평판에 직접 영향을 주는 상황은 발생하지 않는 상태로 확인되었다. 또한, 모의해킹을 통해 확인된 취약점의 경우 위험한 정도가 취약점의 개수에 종속되지 않는다. 즉, 많은 취약점이 더 많은 위험을 나타내지 않는다. 따라서 모의해킹 결과에 따른 위험도 측정은 보다 많은 연구가 필요하다.

나. UNIX 기술적 보안수준

대상 기업 중에 UNIX 시스템을 가지고 있는 곳은 6개 기업이었으며, 각 기업이 1개의 UNIX 시스템을 가지고 있었다. <그림3-4>는 UNIX 취약점 진단 결과를 나타낸 것으로 Y축의 좌측의 경우 각 기업이 보유하고 있는 UNIX 시스템의 수량을 나타내며 Y축의 우측의 경우 위험도를 나타내고 있다. 그리고 X축은 기업명칭 대신하여 나타내었다.

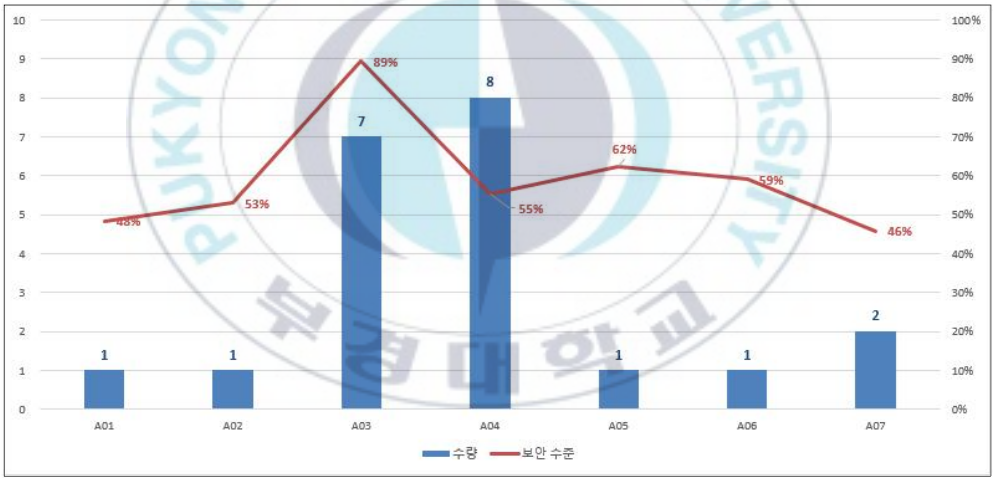


<그림3-4> 대상 기업의 UNIX 보유수량 및 안전지수

가장 안전한 것으로 평가된 시스템조차 60%를 넘지 못했는데 기술적으로 모두 취약하다고 해석할 수 있다. 기술적 취약점은 시스템 엔지니어가 단기간에 개선할 수 있는 항목들인데 전반적으로 안전지수가 낮게 측정되어 시스템에 대한 이해 혹은 보안적인 시스템 구성에 대한 이해 없이 설치 운영되는 것으로 평가할 수 있다.

다. Windows Server 기술적 보안수준

Windows Server는 7개 기업이 총 21대를 설치·운영하는 것으로 확인되었는데, 그중 7, 8대를 운영하는 기업도 있었다. <그림3-5>의 경우 기업별 Windows Server 운영현황을 나타낸 것으로 Y축의 좌측은 보유하고 있는 서버의 수량이며 Y축의 우측은 안전지수를 나타내고 있다. 그리고 X축은 기업의 실제 명칭 대신에 나타내었다. UNIX와는 달리 여러 대의 서버를 운영하는 경우가 있어 중소기업들이 상대적으로는 많은 수량을 도입하고 있은 것으로 해석할 수 있다.

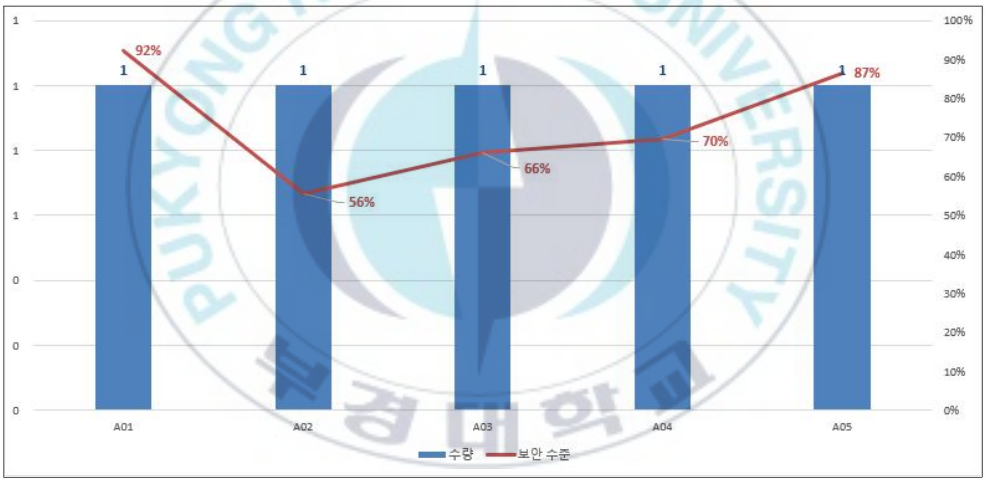


<그림3-5> 대상 기업의 Windows Server 보유수량 및 안전지수

A03 기업의 경우 7대의 서버를 운영하여도 높은 수준으로 운영되고 있고 A04의 경우 가장 많은 서버를 운영하고 있어도 안전하게 운영되고 있지는 않은 것으로 확인되었다. 대부분의 경우 기술적 공격에 취약한 문제를 안고 운영되는 것으로 확인되었다.

라. 정보보호 시스템 기술적 보안수준

정보보호 시스템의 경우 대상 기업 중 5곳만이 도입하고 있었으며 1개 기업을 제외하고는 보통이상 수준으로 운영되고 있는 것으로 측정되었다. 정보보호 시스템의 안전지수보다 중소기업의 도입 현황에 좀 더 집중할 필요가 있다. 29개 기업 중 단 5개 기업만이 정보보호 시스템을 그나마 도입하고 있다는 것은 나머지 24개 기업의 경우 외부 침입에 대한 최소한의 기술적 대안도 없는 상황으로 해석할 수 있다.

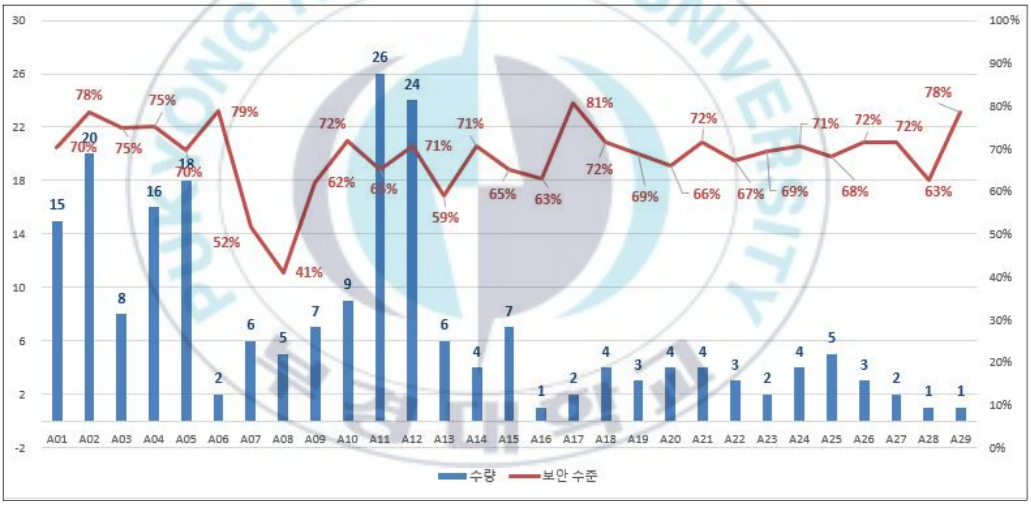


<그림3-6> 대상 기업의 정보보호 시스템 보유수량 및 안전지수

<그림3-6> 좌측 Y축은 정보보호 시스템의 수량이며 우측 Y축은 측정된 정보보호 시스템의 안전지수를 나타내고 있다.

마. PC 기술적 보안수준

대상 중소기업에서 사용하는 모든 PC를 대상으로 진행되지 않고 한정된 범위로 진행하였으며 기업별 대상 PC의 수량은 <그림3-7>와 같이 집계하였다. 좌측 Y축은 보유하고 있는 PC의 수량이며 우측 Y축은 각 기업의 PC 안전지수를 나타내고 있다. 그리고 X축은 기업의 실제 이름 대신에 나타내었다. PC의 안전지수가 다른 정보시스템에 비해 상대적으로 높은 안전지수를 나타내고 있는 것을 확인할 수 있다.



<그림3-7> 대상 기업의 PC 보유수량 및 안전지수

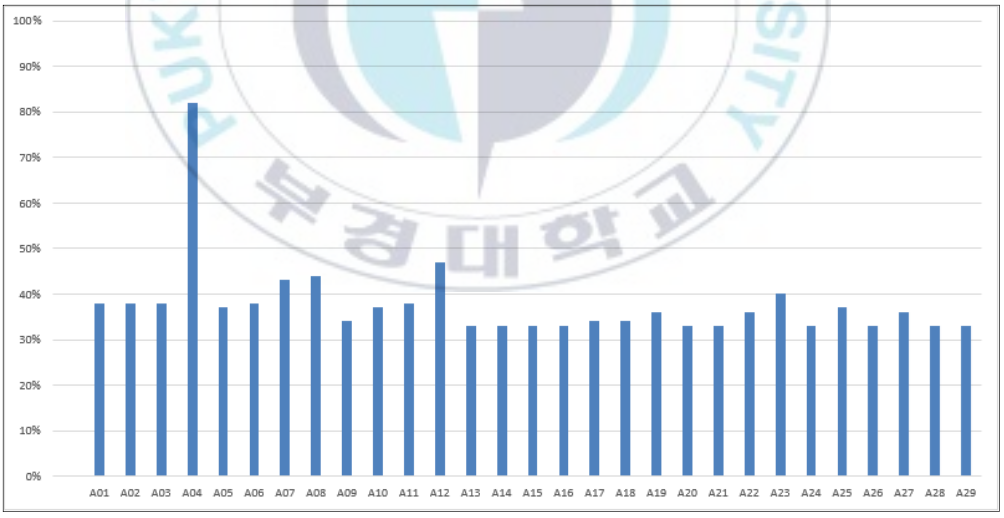
관리적 진단에서 기업이 개인들에게 정보보안을 강제하는 지침이나 규정이 존재하지 않기 때문에 PC의 안전지수가 상향 평준화되어 있다는 것은 기업이 아닌 사원들이 각자 관리를 잘하고 있는 것으로 해석할 수 있다. 그러나 이런 현황 해석이 긍정적이지 못한 것은 각 개인이 PC를 알아서 관리하고 있다는 것은 기업이 정보자산에 대한 통제가 이루어지지 않아 정

보유출 등과 같은 보안사고 발생을 방치하고 감지할 수 없는 상태에 있다는 것을 의미함으로 부정적인 면도 존재한다.

바. 관리적 보안수준

대상 중소기업들의 관리적 보안은 아래 같이 측정되었고 평균 37.8%로 나타났다. 기업의 보안을 위해 이름을 공개하지 않고 기호화하여 나타내었다. 측정 결과 1개 기업을 제외하고는 관리적 보안수준이 불량인 것으로 나타났다. 즉 정보보안 업무에 대한 절차가 없거나 미흡하고 할 수 있으며 절차에 따른 보안활동이 이루어지지 않는다는 것이다.

악의적 목적으로 직원의 업무 배임이 발생할 경우 이를 발견할 수도 없으며, 이를 기소할 수 있는 최소한의 근거도 없는 상태라는 것이다.



<그림3-8> 대상 기업의 관리적 보안수준

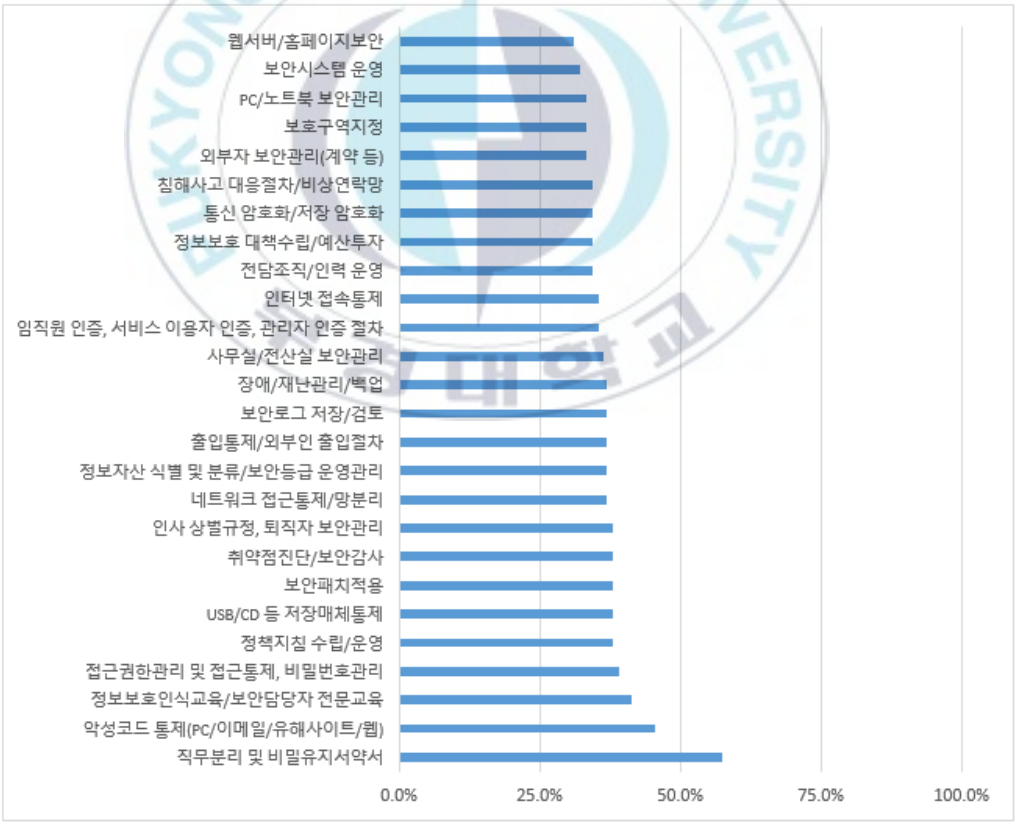
<그림3-8>은 대상 기업의 관리적 보안수준을 나타낸다. Y축은 안전지수를 나타내며 X축은 기업을 나타내는데 기업의 이름이 공개되는 것이 보안

적으로 적합하지 않아 A01부터 A29까지로 치환하여 나타내었다.

관리적 안전지수는 보안수준을 수치로만 나타내는 기능도 있지만, 기업의 정보보안에 대한 의지를 나타내는 가장 기본적인 지표이다. 1개 기업을 제외하고 정보보안에 대한 인식 자체가 없는 수준으로 해석할 수 있다.

기술적 보안 취약점을 조치는 권고되는 설정과 구성 기준에 맞추는 것으로 제거가 가능하지만, 관리적 보안의 경우 해당 기관의 성격에 맞게 업무를 수립해야 하는 차이와 특징을 가진다.

본 연구를 통해 확인된 관리적 보안의 취약점을 집계하면 <그림 3-9>와 같이 나타낼 수 있다.



<그림3-9> 관리적 진단 통제항목별 안전지수 집계

<그림 3-9>에서 Y축은 관리적 보안 진단항목을 부분별로 나누고 대상 중소기업들의 각 부분 안전지수를 집계한 것을 X축으로 나타낸 것으로 취약 분포를 확인할 목적으로 생성하였다. 중소기업들의 관리적 보안수준이 우열을 가늠할 수 없을 정도로 하향평준화 되어있으나 중소기업이 정보보안 관련 투자 등의 계획을 수립할 때 우선순위에 참고 할 수 있다.

Ⅳ. 결론

1. 연구 결과의 요약

대상 중소기업들은 관리적 보안이 취약하여 영업비밀 등 주요 정보가 유출되었을 경우 법적인 대응을 하거나 보호받는 것이 불가능한 상태이며, 기술적으로는 내부 정보를 보호하기 위한 네트워크 통제가 없으며, 전자정보의 무결성을 위협하는 크래킹 공격에 그대로 노출이 되어있는 것을 정량적으로 확인하였다.

정보보호 장비 도입 등 기술적인 방법으로 전체적인 정보보안 수준을 높일 수도 있지만, 정보보안 규정과 지침 등을 업무절차에 적용하여 적은 비용으로 효과가 큰 부분부터 진행하는 것이 바람직하다. 이 과정에서 정부의 관련 기관이 정보보안 분야의 지식과 경험이 상대적으로 부족한 일반 중소기업에서도 쉽게 적용할 수 있는 규정 등을 제공하는 것도 좋은 방법이 될 수 있다.

중소기업 정보보안에 대한 정부 지원사업이 서로 다른 영역에서 각개로 전개되어 동반 상승효과를 기대할 수 없다.

2. 연구의 시사점

국내 중소기업들의 정보보안 수준이 미흡한 것을 정량적으로 재확인하고 지금처럼 방치해서는 안 된다는 것을 재확인하였다.

대・중・소기업 농업협력재단에서 진행하고 있는 중소기업 기술보호의 경우 2014년에는 중소기업기술정보진흥원에서 지원사업을 주관했으며, 그 이전에는 똑같은 사업을 다른 기관에서 진행했었다. 중소기업 정보보안을

위해 가장 오래전부터 존재해온 지원사업이지만, 축적된 경험을 바탕으로 국내 중소기업에 맞는 통제항목을 제시하지 못했으며, 예산 등의 여건에 따라 주관기관, 담당자들이 계속 변경이 되어 왔다. 중소기업의 정보보호에 대한 지원이 지속력을 가지고 연속성 있게 진행되어오지 않았다는 것을 알 수 있다.

3. 연구의 한계점과 향후 연구의 방향

중소기업 정보보안 현황에 대한 연구는 매년 진행되고 있다.[7] 하지만, 대상 기업의 생애주기를 따라 정보보안 수준 향상 여부를 지속적으로 분석하는 연구는 이루어질 필요가 있다. 기업의 정보보안 활동은 단발성 업무가 아니라 준거성을 가지고 반복적으로 이루어져야 하는 업무절차가 되어야 한다. 본 연구와 같이 단발성 연구는 현황이나 상황을 측정하고 분석하는 수준을 벗어날 수 없다.

모의해킹 부문에 있어 취약점의 개수와 위험도가 비례하지 않는다. 따라서 이를 정량화하여 비교할 수 있는 기법 개발이 필요하다. 물론 이러한 기법이 여러 개의 기업을 대상으로 집계하는 곳에 사용하는 것으로 그 사용처가 한정되어 있지만, 정부 부처별로 진행되는 주요정보통신기반시설 등과 같이 확실한 수요처가 있으므로 연구 당위성은 충분하다.

중소기업의 경영활동을 위축시키지 않는 범위 내에서 공공기관과 같이 일정한 통제와 지원이 필요하다. 이를 어떻게 현실적으로 이루어갈지에 대한 연구도 필요하다.

정보보안 투자를 통해 매출 증가를 기대할 수 없고 정보보안 이전에 안전한 IT 인프라 구축에 대한 기본적인 인식과 지식이 없는 상황에서 지속

7) 중소기업기술정보진흥원(2018), “2017 중소기업 정보화수준조사”, 중소기업청

적인 연구까지 기대한다는 것은 비현실적인 학문적 이상일 수 있다. 그러나, 주요정보통신기반시설이 매년 취약점 진단을 통해서 개선되는 것을 볼 때 우리의 중소기업이 정보보안 수준 향상 및 응용을 위한 개선대책 도출을 위해 지속적인 정보보안 수준 측정 및 연구는 계속되어야 하고 본 고에서는 그 필요성을 다시 확인하였다.

참고 문헌

1. 국내 문헌

서승우(2008), “보안 경제학 CEO를 위한 정보보안 투자가이드”, 서울대학교 출판부

경찰청 사이버안전국(2018), “2018년 3분기 사이버위협 분석 보고서”, 경찰청

중소기업기술정보진흥원(2013), “2013 중소기업 기술보호 역량 및 수준조사”, 중소기업청

중소기업기술정보진흥원(2017), “2016 중소기업 정보화수준조사”, 중소기업청

중소벤처기업부(2018), “2017 중소기업 기술보호 수준 실태조사”, 대·중소기업·농어업 협력재단

배영식(2012), "정보보호관리체계[ISMS] 인증이 조직성과에 미치는 영향에 관한 연구“, 한국산학기술학회논문지, 13(9), 4224-4233

감사의 글

이 석사 학위 논문을 작성하는데 주변의 많은 지원과 독려와 가르침이 있었습니다. 바쁘신 가운데에도 항상 배려와 격려로 지도하여 주신 옥영석 지도교수님께 먼저 진심으로 감사를 드립니다.

한없이 배우고 싶은 욕망의 발로가 마주한 MOT 과정은 지적 갈증을 달래기에 충분한 역할을 해주었습니다. 교수님들과 원우님들의 열정과 성실함을 통해 배운 것은 지식이 아니라 겸손이었고 배움 자체가 아니라 배움에 대한 방향성과 열정이었습니다. 모든 분의 존재 자체만으로 배우고 느낀 것에 경중이 없었기에 그 모든 분에게 경중 없이 감사한 마음을 전하고 싶습니다.

주말의 등교를 묵묵히 응원해준 아내에게 또한 감사하며, 나이든 아빠의 주말 등교와 밤을 잊은 공부가 두 딸에게는 공부하라는 백 마디 말보다 명확하게 교훈이 되었을 것으로 생각하면서도 미안하고 이해하고 참고 기다려준 것에 대해 고마운 마음을 전합니다.