정보보호시스템도입에 따른 보안위협요소 대응방안수립에 관한 연구

경지훈* · 정성재** · 배유미*** · 성경****

*(주)시큐브, **(주)스컴씨엔에스, ***한남대학교 컴퓨터공학과, ****목원대학교 컴퓨터교육과

A Study on establishing countermeasures to security threats due to the introduction of information protection system.

ji-hun Kyung* · Sung-Jae Jung** · Yu-Mi Bae*** · Kyung Sung*****

*Secuve, Inc., **Sky Computing C&S, Inc., ***Hannam University, ******Mokwon University

E-mail : sia2001@secuve.com, posein@naver.com, yumidw@hanmail.net,

, skyys04@mokwon.ac.kr

요 약

정보보호시스템(Information protection system)기반의 IT 환경 구축이 보편화되면서 공공기관 및 기업체에서는 정보시스템 자원의 활용과 통합을 위한 하나의 필수적인 환경으로 인식하기 시작하였고, 클라우드 시스템(Cloud System), 클라우드 보안(Cloud Security), 빅데이터(Big Data), 빅데이터 보안(Big Data Security), 산업보안(Industry Security)등이 이슈화 되고 있다. 이러한 영향으로 인해 정보보호시스템(Information protection system) 구축에 따른 내외부적인 보안 위협요소 분석과 대응방안 수립하고자 한다.

본 논문에서는 정보보호시스템(Information protection system) 도입에 따른 여러 가지 보안 위협요소를 알아보고 특히 산업보안적인 측면과 내외부 보안위협요소에 관한 측면을 조명하여 대응방안 수립에 관한 기반 지식을 제공하고자 한다.

ABSTRACT

Information protection system (Information protection system)-based IT environment built popularity in public agencies and businesses take advantage of the resources for the integration of the information system one essential environment began to recognize, cloud systems (Cloud System), cloud security (Cloud Security), big data (Big Data), big data security (Big Data Security), industrial security (Security Industry), as well as the issue. Due to the influence of these information protection system (Information protection system) in response to my external security threats based on the analysis plan.

In this paper, data protection systems (Information protection system), resulting in the introduction, there are a number of security threats and particularly industrial security aspects and internal and external security threats in response by lighting about aspects of the plan is based on knowledge.

키워드

정보보호(Information protection), ,산업보안(Industry Security),
데이터보안(Data Security), 정보보안(Information security)

Ⅰ. 서 론

정보보호시스템(Information protection system) 기반의 IT 환경 구축이 보편화되면서 공공기관 및 기업체에서는 정보시스템 자원의 활용과 통합을 위한 하나의 필수적인 환경으로 인식하기 시작하였고, 클라우드 시스템(Cloud System), 클라우드 보안(Cloud Security), 빅데이터(Big Data), 빅데이터 보안(Big Data Security), 산업보안(Industry Security)등이 이슈화 되고 있다. 이러한 영향으로 인해 정보보호시스템(Information protection system) 구축에 따른 내외부적인 보안위협요소 분석과 대응방안을 수립 하고자 한다.

본 논문에서는 정보보호시스템(Information protection system) 도입에 따른 여러 가지 보안위협요소를 알아보고 특히 산업보안적인 측면과 내외부 보안위협요소에 관한 측면을 조명하여 대응방안 수립에 관한 기반 지식을 제공하고자 한다.

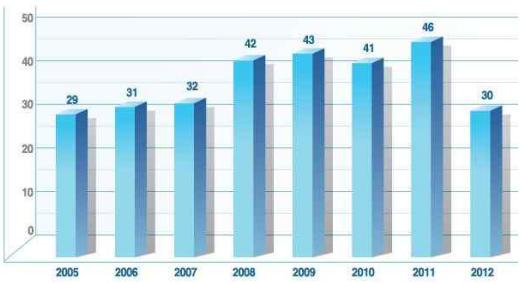
본 논문의 구성은 다음과 같다. 2장에서는 내부보안위협요소인 기술유출유형에 대해 기술하고 3장에서는 산업보안 관련법과 내부자에 의한 기술유출 사례에 대해 설명하고 마지막으로 4장에서는 내부보안 위협에 대한 대응방안을 제시하고 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 기술 유출 유형

국가정보원 산업기밀보호센터에서 발표한 자료에 따르면 2005년부터 2012년까지 발생한 첨단 산업기술의 해외 유출 사건은 총 294건에 이르고 있으며 연도별로 2005년 29건, 2006년 31건, 2007년 32건, 2008년 42건, 2009년 43건, 2010년 41건, 2011년 41건, 2012년 30건으로 매년 꾸준히 증가하고 있는 추세이다. 연도별 기술유출 현황은 그림 1 과 같다[1].

구분	계	2005년	2006년	2007년	2008년	2009년	2010년	2011년	2012년
건수	294건	29건	31건	32건	42건	43건	41건	46건	30건



※최근 5년간 유형별 분석(2008년~2012년)

출처: 국가정보원 산업기밀보호센터 기술유출 통계

그림 1. 연도별 기술유출 현황

2.2 기술 유출 주체

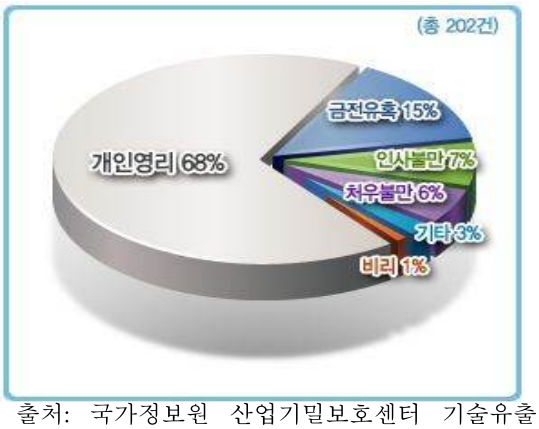
기술 유출 주체는 그림2에서와 같이 전직직원이 60%로 가장 많고, 현직직원 20%, 협력업체 12%, 기타 6%, 유치과학자 1%, 투자업체 1% 순으로 나타났다. 이와같이 내부데이터 및 산업기술 유출은 기업및 공공기관 내부에서 일어나는 경우가 대부분임을 알 수 있다.

출처: 국가정보원 산업기밀보호센터 기술유출 통계

그림2. 기술 유출 주체

2.3 기술 유출 동기

기술 유출 동기는 그림3과 같이 개인영리 68%, 금전유혹 15%, 인사불만 7%, 처우불만 6%, 기타 3%, 비리 1% 순으로 나타났다.



출처: 국가정보원 산업기밀보호센터 기술유출 통계

그림3. 기술 유출 동기

Ⅲ. 산업보안 관련법과 기술유출 사례

3.1 산업보안 관련법

· 정보통신망 이용촉진 및 정보보호에 관한 법률 (법 제22조 및 제28조)

해킹을 통한 산업기술 형태의 영업비밀 유출행위는 형법상 비밀침해죄에 우선하여 이 법을 적용할 수 있는데, 누구든지 정보통신망에 의하여

처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 되며, 이에 위반한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다[2].

· 통신비밀보호법 (법 제3조 및 제16조)

통신의 내용을 도청하는 행위 등으로 산업기술을 알아내는 행위를 통신비밀보호법 위반으로 처벌 할 수 있다. 즉 전기통신·우편·대화· 등을 통하여 송·수신되는 영업비밀을 감청·녹음하거나 또는 그 취득한 내용을 공개·누설하는 경우 10년 이하의 징역과 5년 이하의 자격정지에 처한다[2].

· 개인정보보호법

당사자의 동의 없는 개인정보 수집 및 활용하거나 제3자에게 제공하는 것을 금지하는 등 개인정보보호를 강화한 내용을 담아 제정한 법률이다. 이 법은 각종 컴퓨터 범죄와 개인의 사생활 침해 등 정보화 사회의 역기능을 방지하기 위해 1995년 1월 8일부터 시행됐던 법률인 '공공기관의 개인정보보호에 관한 법'을 폐지하고 새로 제정한 법률이다. 2011년 3월 29일 제정되어 같은 해 9월 30일부터 시행되었다.

산업기술과 관련하여 개인정보를 침해하는 경우가 발생하면 개인정보보호법의 적용을 받을 수 있다. 즉 거짓이나 그밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자는 3년 이하의 징역 또는 3천만 원 이하의 벌금에 처한다[2].

3.2 내부자에 의한 기술 및 개인정보 유출사례

내부자의 연도별 기술유출 사례는 그림4와 같다.

출처: 국가정보원 산업기밀보호센터 기술유출 사례

그림4. 연도별 기술유출 사례

그림4와 같이 매년 기업 및 공공기관에서 내부 중요자료 유출이 끈임없이 발생되고 있으며 증가하는 추세를 확인 할 수 있다.

또한 이렇게 유출된 정보들의 위협정도는 아래 그림 5와 같다[3].

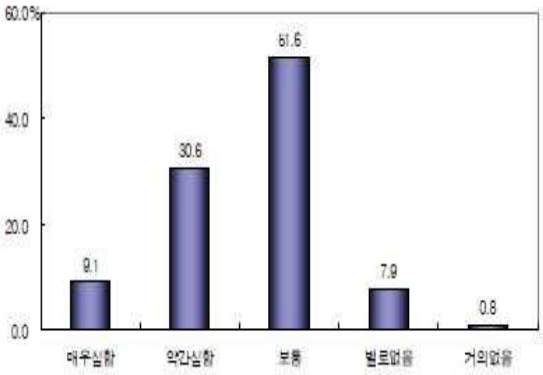


그림5. 산업기밀 유출에 대한 위협정도

Ⅳ. 내부 보안 위협에 대한 대응방안

4.1 보안정책

기업 및 공공기관의 비밀정보를 효과적으로 관리하고 보호하기위해서는 보안관리에 관한 명문화된 규정을 제정하여 시행하여야한다.

아울러 기관 및 기업의 인력규모에 상관없이 보안전담조직을 구성하거나 보안책임자를 임명하여 보안업무를 수행하도록 하고, 직원 개개인의 업무에 보안관련 내용을 포함시켜야 한다. 또한 정기적인 보안감사를 통하여 감독활동이 이루어져야 하며 감사내용은 아래와 같다.

· 대외비 정보 (문서 및 도면) 방치여부
· 개인서랍, 캐비넷, 출입문 시건여부
· 개인휴대용 정보저장매체 출입규정 준수여부
· PC 데이터 공유설정 여부
· 사내 사용허가 전산저장매체 관리현황

위와 같은 정기 및 수시 보안감사 결과에 따른 유공자 포상과 위반자 징계활동을 병행 하여야한다[3].

4.2 자산관리

사내 자산에 대하여 자산별 소유관계와 등급을 명확히 정의하여 이를 문서화 처리하고 각각의 중요도에 따라 접근 권한 및 자산의 반출입여부도한 보안성 검토를 통하여 기록 유지 보관 하여야 한다[3].

4.3 인적자원관리

신규채용자 및 재직자에 대해선 보안 서약서를 작성토록하여 재직 중에 지득한 회사의 기밀을 누설할 경우 손해배상은 물론 민·형사상 책임을 지겠다는 내용을 숙지 시켜줘야한다.

또한 주기적인 보안교육을 실시하여 보안에 대한 경각심을 제고하여야한다.

아울러 퇴직자에 대해선 정보반납 및 개인정보를 삭제하고 개인 PC 및 업무관련 자료를 퇴시사 반납토록 하여야하며 주요 반출물품에 대한 검색을 실시 하여야한다. 이와 더불어 개인PC와 회사 메일계정 및 ID와 패스워드 삭제또한 병행되어야 한다[3].

4.4 IT 보안관리

사내에서 업무용으로 사용된 개인PC에 대하여 ID및 패스워드를 설정하고 주기적으로 변경하도록 하되 쉽게 유추할 수 있는 패스워드 사용은 지양토록 해야한다.

또한 PC 보안용 소프트웨어를 설치하여 라이선스 없는 불법 소프트웨어 사용은 금지토록 하며 백신 프로그램을 이용한 정기검사 실시, 예약점검을 적극 활용토록 하여야한다.

아울러 중요문서는 평문 조회가 불가능하도록 암호화하여 저장하도록 권고하며 외부로 데이터 이메일 발송시 보안담당자의 승인을 얻도록 조치시켜고 CD 및 외부저장매체 또한 별도의 승인을 득한 후 사용하도록 조치하여야 한다[3].

4.5 기술적 산업보안기술 체계관리

Table 1. Industrial Security Framework

<table>
<tr><th colspan="2">보안 목적</th><th colspan="2">보안 기술</th></tr>
<tr><td rowspan="6">예방
(Protection)</td><td rowspan="2">유출 통제
(Responsible Use)</td><td colspan="2">메일 및 메신저 보안</td></tr>
<tr><td rowspan="2">기업
DRM</td><td>이동 저장장치 보안</td></tr>
<tr><td rowspan="4">접근 통제
(Secure Use)</td><td>문서 보안</td></tr>
<tr><td rowspan="2">DB
보안</td><td>DB 활동 모니터링 및 차단</td></tr>
<tr><td>DB 암호화</td></tr>
<tr><td colspan="2">네트워크 접근제어</td></tr>
<tr><td>모니터링
(AuditTrail)</td><td colspan="3">콘텐츠 모니터링 및 필터링</td></tr>
</table>

그림6. 기술적 산업보안기술 체계[4].

그림6 과 같이 산업기술에 대한 접근을 통제하는 목적은 데이터 보안을 목적으로 파일 암호화, 각종 권한관리, 인증관리가 첨부되어 인증되지 않은 사람은 데이터에 접근조차 불가능 하게 하여야 한다.

Ⅳ. 결 론

국내의 공공기관 및 기업들은 내부의 데이터 유출을 방지하고자 정보보호시스템을 도입하는 추세이다. 국내외 데이터 유출사고의 대부분은 내부자소행에 따른 유출사고가 대부분이 였으며 이들에 대한 효과적인 관리와 통제가 이루어지지않아 발생되었다.

아울러 내부 보안에 위협은 기술유출 유형에 대해 분석을 하고 이에 대한 내용을 분류하면 주로 산업스파이 행위, 핵심 연구·기술 인력의 영입, 기업 내부자의 매수, 해킹 및 스테가노그래피와 같은 전문적인 IT기술을 활용한 위협, 위장침투, 도·감청 등을 통한 정보 절취, 정보브로커 및 비윤리적 정보 수집행위, 제3자 매수, 무단침입 등으로 나타났다. 이러한 위협에 대한 보안 사고를 막기 위한 기본사항으로 인적 자원을 관리하는 것이 중요하다고 볼수 있으며 이러한 인적 자원의 의식과 행동을 통제할 수 있는 정책과 법률을 통하여 조직원 들의 보안의식을 제고 시켜야 한다[4].

본 논문에서는 정보보호시스템 도입과 운영함에 있어 산업보안측면중 하나인 내외부적인 보안위협요소를 알아보고 그에 따른 효과적인 대응방안을 마련하고자 하였다. 앞서 다루었던 보안위협요소들을 분석하여 정보보호시스템 도입 전 대응방안이 확실히 마련되어지고 조치 및 실행되어진다면 향후 데이터 유출사고에 대하여 미연에 방지할 수 있을것이며 본 논문의 내용 이외에도 다른요인에 대한 더욱 심도 있는 연구가 논의 될 필요가 있다.

참고문헌

[1] 국가정보원, 산업기밀보호센터, http://service4.nis.go.kr/page

[2] 류인선 “기업의 내부보안 위협에 대한 대응방안 수립”, 서울과학종합대학원대학교, pp. 30-31, 2013년 2월

[3] 중소기업청 “중소기업 기술유출 대응매뉴얼”, pp.40-158 2007년 12월

[4] 김경규, 최서윤, 허성혜 “산업기술 보호를 위한 기술적 보안의 탐색적 연구”, 한국항행학회 논문지 제13권 1호 pp.3-5, 2009년 2월