韓國컴퓨터情報學會 論文誌
第14卷 第7號, 2009. 7.

2009-14-7-4-3

중소기업 정보시스템의 안정적 운영 전략

여 상 수*, 황 수 철**

A Safe Operating Strategy for Information System of Small and Medium Enterprises

Sangsoo Yeo*, Suchul Hwang**

요 약

중소기업은 대기업에 비해서, 정보기술에 대한 의존도가 높지만, 재정적인 어려움과 한정된 자원 및 노하우의 부족 등의 이유로 인해서 정보기술 및 정보 보안에 투자하는 비용은 크지 않다. 이로 인해서 정보 보안에 취약점이 많으며, 그로 인한 침해 사고도 많아지게 된다. 중소기업의 정보 보안 실무자들은 바이러스 방역 솔루션을 업데이트하고, 방화벽을 운영하며, 정기적인 시스템 패치를 적용하는 것이 정보 보안의 전부라고 생각한다. 하지만 보안 사고를 줄이기 위해서는 보안 정책, 정보 유출 방지, 사업 연속성, 접근 제어 및 기타 많은 정보 보안 이슈들이 고려되어야지만 한다. 본 논문에서는 이러한 관점에서 대기업 위주의 보안 대책과 전략들을 중소기업 정보시스템의 안정적 운영에 적합하도록 새롭게 정리하여, 4가지의 관점에서 정보 보안 고려 사항들을 도출하고, 정보 보안 전략을 제안한다.

Abstract

Small and medium enterprises have more dependency on their information technology than large enterprises have, but they can't pay much for information technology and information security due to financial restrictions, limited resources, and lack of know-how. So there are many vulnerabilities in small and medium enterprises and these would make many security incidents. Security managers of small and medium enterprises think that information security in their company is simply equivalent to updating the antivirus solutions, managing firewall, and patching systems regularly. However, security policies, prevention of information theft, business continuity, access controls, and many other information security issues should be considered for mitigating security incidents. In this context, we redefined security countermeasures and strategies which are only appropriate to large enterprises, for making them appropriate on a secure operating for information system of small and medium enterprises, and we investigate information security issues in the four views of information system and company, and finally we present information security strategies for each view, in this paper.

• 제1저자 : 여상수 교신저자 : 황수철
• 투고일 : 2009. 05. 18, 심사일 : 2009. 06. 08, 게재확정일 : 2009. 07. 02.
* 목원대학교 컴퓨터공학부 전임강사 ** 인하공업전문대학 컴퓨터시스템과 교수

▸ Keyword : 정보시스템(Information system)), 정보기술(information technology), 보안(security)

Ⅰ. 서 론

대부분의 국가에서 중소기업의 중요성은 높이 평가되지 않고 있지만, 실제로는 대기업 보다 훨씬 많은 수의 고용을 하고 있으며, 경제적으로도 중요한 역할들을 하고 있다. 또한 중소기업도 대기업과 마찬가지로 그 사업의 많은 부분을 정보 통신 기술에 의존하는 정도가 계속해서 높아지고 있다. 이것은 정보 통신 기술과 전자 상거래 기술들이 중소기업들에게 큰 발전의 기회를 제공한다는 것을 입증해주는 것이다. 하지만 이러한 장점과 더불어서 정보 통신 기술에 관련된 새로운 양상의 위험들 또한 함께 고려되어야만, 장점을 잘 살릴 수 있다는 것이 간과되어서는 안 된다.

한국인터넷침해사고대응지원센터(KrCERT)에 신고 되는 침해 사고 변화 추이를 볼 때[1], 2006년을 기점으로 전체적인 신고 건수는 많이 감소하였다[표 1]. 이는 대기업 및 규모가 큰 공공 기관들이 자체적으로 침해사고대응지원센터(CERT)를 운영하기 때문으로 해석될 수 있다. 이는 자체적인 침해대응센터를 운영할 수 없는 중소기업들은 여전히 침해사고에 취약할 수밖에 없는 것으로 볼 수 있다. 이는 앞서 말한 바와 같이 대기업과 마찬가지로 정보 통신 기술에 의존도는 높지만, 정보 보안에 대한 투자와 관심이 적은 중소기업의 상황을 파악할 수 있는 면이라고 할 수 있다.

대기업과 비교했을 때, 중소기업들은 일반적으로 정보 보안 정책 및 운영 업무에 더 적은 자원과 인력을 가지고 있으며, 특히 보안 담당 실무자들 또한 보안 전공자 또는 전문가가 아닌 경우가 많다. 보안 담당 부서가 없이 한두 명의 실무자가 보안 정책 및 운영 업무를 담당하거나, 담당 부서가 있다고 하더라도 소수의 인원이 상주하는 형태로 운영이 된다. 이러한 상황에서 전문가 또는 노하우가 쌓인 실무자들의 존재는 찾아보기 힘들다고 할 수 있다. 대부분의 경우 전산 담당자가 자기가 할 수 있는 수준에서 보안 정책을 운영하고 있으며, 보안 관련 서적이나 1-2회 정도의 외부 보안 관련 세미나 참석을 통한 학습이, 그들이 받은 보안 관련 교육의 전부인 경우도 많다. 또한 외부 IT 서비스 업체를 통해 IT 관련 서비스를 제공받는 중소기업의 경우에도 전문 IT 서비스를 이용하기에는 비용 문제 등의 이유로 인해, 보안 관련 개념이가 기준이 미흡한 영세 IT 서비스 업체를 이용하는 경우가 많다.

표 1. 보안 침해 사고 신고 추이[1]
Table 1. Trend of Security Incidents Reports[1]

구분	2002	2003	2004	2005	2006	2007	2008	2009
스팸릴레이	5,537	8,276	3,297	6,334	14,055	11,668	6,490	6,844
피싱경유지	0	0	220	1,087	1,266	1,095	1,163	892
단순침입시도	0	0	0	0	3,711	4,316	3,175	2,572
기타해킹	6,684	13,179	16,027	9,520	4,570	2,360	2,908	3,172
홈페이지변조	5	5	4,812	16,692	3,206	2,293	2,204	2,452

본 논문에서는 대기업이 아닌 중소기업에 대해 논점을 맞추고, 중소기업에서 어떻게 하면 안정적으로 정보시스템을 운영할 수 있는지에 대한 전략에 대해서 논하고자 한다. 중소기업에서 적절한 정보 시스템 운영 전략 및 정보보안 전략 수립을 위한 방향을 제시하고자 한다. 먼저 중소기업을 위한 정보보안 고려 사항에 대한 국내외 기존 연구들을 분석하고, 국내 실정에 맞고 현실에 맞는 보안 전략을 제안하고자 한다. 연구를 위해서 본 논문에서는 중소기업이란 400명 미만의 고용자를 가지는 기업으로 한정하도록 한다.

Ⅱ. 관련 연구

경쟁의 수준이 높아진 글로벌 시장에서는 고객에게 높은 수준으로 커스터마이징된 솔루션을 공급해야지만 중소기업이 성공할 수 있다는 것이 일반적인 견해이다[2]. 고객의 지식과 경험까지도 흡수하여 솔루션에 활용할 수 있어야지만 경쟁력 있는 중소기업으로 발전할 수 있다.

대기업과 중소기업의 정보 보안에 대한 인식의 차이는 매우 크다고 할 수 있으며, 이 차이는 경영층의 참여와 지원의 수준 차이로 해석될 수 있다[3]. 효과적인 보안 정책은 대기업뿐만 아니라 중소기업에 있어서도 주요한 성공요인이지만, 경영층의 참여와 인식이 부족한 국내 중소기업의 현실은 효과적인 보안 정책의 실현을 어렵게 하고 있는 것이 사실이다.

국내의 중소기업은 혈연관계에 의존해서 운영되는 경우의 비중이 높은 편이다. 이로 인해서, 중소기업이 고객의 필요와 기업의 핵심 업무에 대한 파악의 수준이 높다할지라도, 경영의 측면에서는 시스템화 된 비즈니스 프로세스의 구축이 부족할 수 있다는 문제가 여전히 존재하고, 일반적으로 고려되어야 하는 경영의 요소들이 다각적으로 고려되지 않고 구성원들

간의 암묵적인 신뢰와 인정으로 일관하는 경우가 많다고 할 수 있다.

친인척 관계에 근거한 경영진이든, 그렇지 않은 경우이든 간에, 많은 경우에서 중소기업의 경영에 있어서, 자신의 기업들이 해커의 공격이나 침입의 대상이 될 것으로는 고려하지 않는다. 이로 인해서 정보통신 보안은 기업 경영에서 매우 낮은 우선순위를 가지거나 기업 경영의 고려 사항에 두지 않는 양상을 만들어낸다. 이러한 상황은 정보통신을 기반으로 하는 중소기업에게 있어서는 매우 위험한 잘못된 인식이라고 할 수 있다.

또 다른 측면으로서 산업 스파이에 대한 다소 낮은 인식이 중소기업의 경영에 있어서 위험한 요소가 될 수 있다. 기업 기술 및 경영의 노하우는 중소기업의 가장 중요한 자산 중의 하나이다. 국내의 중소기업은 대기업 못지않은 정보통신 기반 시설을 사용하고 있으며, 회사 내에서의 인터넷 사용이 일반적이며, 이와 더불어 이메일 전송 및 인스턴트 메신저 등의 응용 프로그램의 사용도 일반화되고 있다. 또한 외근 중이거나 출장 중인 직원들이 회사 네트워크 또는 회사 내의 PC에 접근해서 업무 처리하는 것들도 가능하도록 하는 것이 국내의 현실이다. 결국은 국내의 중소기업은 불법적인 침입자뿐만 아니라 불순한 의도를 가진 임직원 및 이전 임직원으로부터 기업 자산을 보호하기 위한 적절한 경비 및 정책을 운영하는 것이 매우 중요하다. 그러나 국내의 현실은 이러한 영역에 대한 이해 및 고려가 부족하며, 투자로의 연결은 매우 미흡하다고 할 수 있다.

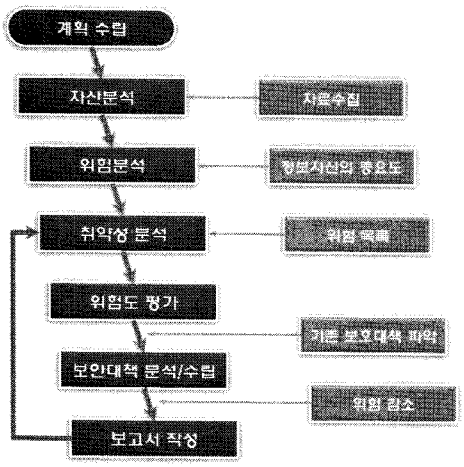

그림 1. 일반적인 정보 보안 정책 적용 절차
Fig. 1. General Information Security Policy Adoption Steps

중소기업의 정보 보안 교육 훈련의 수준도 미비하며, 중소기업의 관점에서의 특성에 맞게 차별화된 교육 훈련 모델 또한 존재하지 않는다[4]. 정보 보안 환경의 동적인 특성상 지속적인 보안 경보 및 대응 기술에 대한 정보가 신속히 전달되고 조치되어야함에도 불구하고 이들의 보안 역량 강화와 경보 및 대응 체계에 대한 교육 및 연구는 많이 부족하다고 할 수 있다.

결국은 국내 중소기업의 현실은 정보통신 경영 및 보안에 있어서 매우 열악한 환경에 처해 있으며, 외부 및 내부의 잠재적인 공격에 대한 대비가 매우 부족하다.

본 논문은, 기존에 사용되고 있는 정보시스템 운영 전략들이 대부분 인적, 물적, 시간적 자원의 여유가 있는 대기업에 적합한 것이며, 중소기업에 적합한 정보시스템의 안정적인 운영을 위한 기존의 연구가 거의 없다는 사실을 배경으로 시작한, 정책 관련 논문이다. 본 논문의 구성은 다음과 같다. III장에서는 중소기업 정보시스템의 안정적인 운영을 위한 전략을 4가지의 관점에서 살펴보기 위해서 이에 대한 소개를 한다. IV장~VII장에서는 구분된 4가지 관점에서의 보안 관련 이슈들을 각각 소개하고 이에 대한 중소기업의 전략 방향을 제시한다. VIII장에서는 결론을 낸다.

III. 중소기업 정보시스템의 안정적인 운영을 위한 전략의 4가지 관점

Common Criteria, COBIT, ISO/IEC 17799:20004, British Standard (BS) 77995 , and Code of Practice (CoP), ISO/IEC 13335 등과 같은 많은 정보 보안 프레임워크들이 이미 계발되어서 활용되고 있다. 이러한 보안 프레임워크에서는 일반적으로 다음과 같은 정보 보안 정책 수립의 절차를 제시한다[5]. (1) 계획 수립, (2) 자산 분석, (3) 위험 분석, (4) 취약성 분석, (5) 위험도 평가, (6) 보안대책 분석 및 수립, (7) 보고서 작성[그림 1]. 그러나 이러한 프레임워크들은 대부분 대기업이나 공공 기관의 서비스 품질 보증 및 보안을 위해서 만들어진 것들로서 중소기업의 예산 및 인력으로서는 적용이 어려운 수준의 것들이다. 따라서 중소기업의 현실을 고려한 저예산의 적절한 수준의 정보 보안 프레임워크가 필요하다. 이와 관련해서, Donald Pipkin은 소규모 기업에 적합하도록 기존의 정보 보안 프레임워크를 변형하여 소개하였지만[6], 좀 더 다각적이고 현실적인 측면에서 중소기업의 정보 보안 고려 사항들을 정리하고 보안 전략을 제시하고자 하는 것이 본 논문의 목적이다.

본 논문에서는 대기업과는 다른 정보시스템 운영 방식과

환경이 다른 중소기업의 현실을 반영하기 위해서, 아래와 같은 4가지 관점에서의 중소기업의 보안 관련 이슈들을 정리하고, 각 관점별로 필요한 중소기업에 적합한 전략을 제시한다.

(1) 조직 체계의 관점: 기업의 전체 조직의 관점에서 필요한 보안 이슈들이 포함 된다. 경영진, IT 및 보안 관리자, 일반 직원 및 외부 컨설턴트 등의 책임과 업무의 연관성이 중요한 이슈가 된다.
(2) 업무 프로세스의 관점: 기존 비즈니스 프로세스에 대한 보안 적용과 관련된 이슈들이 포함 된다.
(3) 정보 자산 단위의 관점: 중소기업의 정보 자산에 대한 접근 제어 및 사용자별 접근 권한의 관리 등이 주요 이슈로 포함 된다.
(4) 기술적인 관점: 일반적으로 많이 다루어져 왔던 기술적인 측면의 보안 이슈들이 여기에 포함 된다.

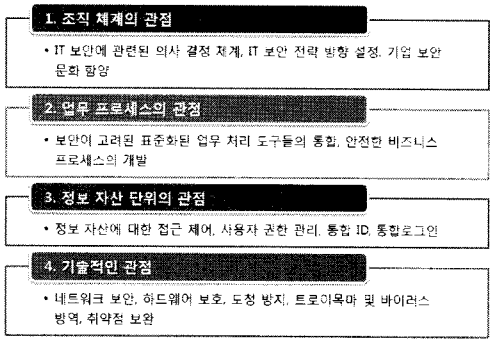

그림 2. 일반적인 정보 보안 정책 적용 절차
Fig. 2. General Information Security Policy Adoption Steps

IV. 조직 체계의 관점

1. 정보 보안 관점에서의 조직 구성원 및 체계

중소기업의 정보 보안 정책 IT은 기술적인 관점에서 뿐만 아니라 심리학적, 사회적, 조직적 관점에서도 다루어져야만 하며, 이것은 회사의 정보 보안 정책에 많은 영향을 주는 것으로 보고되었다[7]. 여기서는 이러한 사항들을 고려해서 중소기업에 적합한, 정보 보안 관점의 조직 체계와 그 구성원에 대해서 다룬다. 중소기업에서의 가장 일반적인 조직의 형태는 의사 결정을 하는 경영진, IT (또는 보안) 관리자, 일반 직원, 그리고 외부 전문가(컨설턴트) 등으로 구성된다[8-12]. 이들 구성원은 정보 보안 업무에 대해서 그림 3에서 보는 바와 같이 서로 간의 업무 흐름을 가지고 움직여야 한다. 다음 절에서부터는 이들 구성원 각각을 살펴보도록 한다.

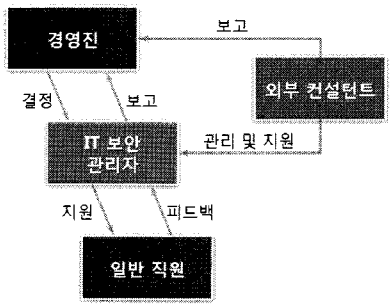

그림 3. IT 보안 관련 조직 체계
Fig. 3. Organization of regarding IT Security

2. 경영진

이러한 조직 체계의 가장 중요한 구성원은 경영진이며, 경영진의 정보 보안에 대한 이해와 투자, 그리고 적극적인 후원이 뒷받침 되지 않으면 효과적인 정보 보안 체계를 운영하기가 어렵다고 할 수 있다.

중소기업의 경영진은 정보 보안을 위해서 다음과 같은 업무를 수행해야 한다[2].

(1) IT 및 보안 관리자를 공식적으로 선임하고 적절한 권한을 부여하여야 한다.
(2) 기업 전체의 보안 정책을 설계하거나, 이에 대한 제안서를 평가하는 데에 직접적인 참여를 해야 한다.
(3) 수립된 보안 정책에 대한 책임을 져야 한다.
(4) 외부 컨설턴트와 IT(보안) 관리자, 그리고 일반 직원들 사이의 권한 사용에 대한 적절한 균형을 잡아주어야 한다.
(5) 자신이 신뢰할 수 있는 기준과 원리를 설정하고, 이를 공정하게 적용 유지하는 데에 지속적인 노력을 기울여야 한다.

결국, 경영진은 이러한 업무를 수행하기 위한 개인적인 전략을 계발해야할 필요가 있다. 여기서부터 중소기업의 보안 정책은 시작된다고 볼 수 있다. 경영진이 구성원들 간의 권한 사용에 대한 균형을 잡기 위한 올바른 방향을 찾기 위해서, 한 명의 직원이나 하나의 IT 서비스 기업에 너무 의존해서는 안 되며, 자기가 신뢰할 수 있는 기준과 원리를 설정하는 것이 필요하다.

3. IT 및 보안 관리자

일반적으로 중소기업에서의 IT 관리자는 거의 모든 기술적인 이슈들을 책임져야만 하는 입장인 경우가 대부분이다. 이러한 책임 사항들에는 레이저 프린터의 토너를 교체하는 것에서 비롯해서, 운영체제의 사용자를 추가하거나 권한을 조정하는 것, 인터넷 연결 상태를 점검하는 것, 기업 웹사이트의 웹페이지를 관리하는 것, 게시판에 올라온 글에 답변을 다는 일까지 포함되기도 한다.

그렇기 때문에 IT 관리자에게 보안 업무를 추가로 맡기는 경우에는, 다른 책임 업무들보다 보안 업무를 소홀히 하게 되는 상황이 발생하기 쉽다. 보안 관련 업무는 업무의 특성상 밖으로 잘 드러나지 않기 때문에 관리를 잘한 것에 대해서 증명을 하기도 어렵고, 그로 인해 보상 받기도 쉽지 않기 때문이다. 결국은 이와 같은 이유로 인해서, 보안 관련 업무는 가볍게 처리되거나 오히려 다른 업무들에 밀려버리는 상황이 발생할 수밖에 없다. 결국 심각한 보안 관련 사건이 발생한 직후에만 관심을 받게 되고 높은 우선순위에서 처리되게 되는 것이 바로 중소기업에서의 보안 업무의 특징이다. IT 관리자가 없는 경우에는 이러한 양상은 더욱 빈번하게 발생하게 된다.

결국 중소기업의 IT 전담 인력의 수에 따라서, 보안 업무에 대한 다음과 같은 3가지의 시나리오가 나올 수 있다.

(1) 전담 관리자가 없는 경우: 일반 직원 1명이 자신의 일반 업무 이외에 추가로 IT 네트워크를 관리하게 되는 경우가 될 것이다. 이 경우에는 책임의 영역이 불분명하게 되고, 정책 적용의 혼동이 발생할 수 있으며, 비 전문성으로 인해 최소한의 보안 솔루션 운영 등이 기업의 정보 보안 관련 업무의 전부가 될 수 있다. 앞서 말한 바와 같이, 해킹 또는 백업 전략 부재로 인해 심각한 피해를 받은 직후에나 정보 보안에 대한 재정적인 투자와 인력 투입이 시작될 수 있다. 중소기업에서는 이와 같은 상황을 미연에 방지하기 위해서, 적어도 1명 이상의 IT 및 보안 관리자를 두는 것이 필요하다.

(2) 1명의 전담 관리자가 있는 경우: 이 경우는 (1)의 경우보다는 낫지만, 여전히 문제가 있는 경우이다. 모든 관리 업무가 한 사람의 전담 관리자에게 집중되기 때문에, 관리자에 대한 업무 의존도가 높아지게 되고, 결국 정보 보안 관리가 효과적으로 이루어질 수는 없게 된다. 이러한 경우에는 추가적인 전담 관리자를 두거나 외부 전문가를 이용하는 것을 고려해야만 한다.

(3) 1명 이상의 전담 관리자가 있는 경우: 한 사람에게 업무가 집중되는 형태를 감소시키고, 여러 명의 관리자가 상호 업무를 운영, 관리, 책임질 수 있는 상황이기 때문에 효율적인 관리 업무를 기대할 수 있다. 이때에는 IT 전담 관리자와 보안 전담 관리자를 따로 두고, 이들이 서로 발전적인 방향으로 협의하면서, 기업 전체의 정보 및 정보 보안 업무를 처리하도록 하는 것도 좋은 방향이라고 할 수 있다.

4. 일반 직원

기존 연구들에 의하면, 기업의 정보 유출 사고의 70% 이상은 내부 직원에 의해서 일어나고 있다고 보고되고 있다[2,8-10]. 특히, 중소기업에서는 접근 제어와 접근 기록 관리 방법이 보다 덜 엄격하고, 내부자에 의한 정보 유출의 위협에 대한 고려가 더 부족하다고 할 수 있다. 이를 위해서는 일반 직원들에 대한 교육 및 정책 적용이 필요하다.

그러나 웹서핑, 개인적인 이메일 이용, 개인 PC 데스크톱 환경 설정 등과 같은 개인 권리에 대한 제약 사항을 두는 것은 현명하지 못한 결정이 될 수 있기 때문에 유의해야 한다. 이러한 부수적인 제약들은 기업 정보 보안의 수준을 향상시키는 것과는 연관이 없으며, 오히려 정보 보안 정책 및 기술 등에 대한 직원들의 반발 의식을 일으킬 수 있으며, 전체적인 보안 수준을 낮추게 되는 결과를 불러일으킬 수도 있다.

심각한 보안 사고가 난 이후라 할지라도, 직원의 일반적인 권리에 대한 제약을 가하는 정책을 도입하는 데에는 많은 주의가 필요하다. 먼저 제약 사항 도입 사유를 직원들과 충분히 공유하는 것이 필요하며, 새로운 제약 사항에 의해서 극복되는 위협 요소들을 실제적으로 알려주는 것이 직원들의 원만한 이해와 지지를 얻어내는 데에 도움이 된다.

중소기업에서는 이제까지 직원들의 이해에 대한 측면을 고려하는 경우가 많지 않은 것으로 파악된다[2,4]. 그러나 예를 들어 직원들의 컴퓨터 사용과 인터넷 사용이 어떻게 정보 유출 및 의도하지 않은 해킹의 시발점을 제공하게 되는지를 알려준다면, 직원들은 이에 대해서 충분히 공감하고 이해할 수 있게 되고 이를 방지하기 위한 정책에 손을 들어 줄 것이다[4]. 결국 직원들의 이해와 지지를 얻어 내는 것이 IT 보안 수준을 향상시키기 위한 각종 보안 정책을 적용하는데 거쳐야 할 하나의 중요 과정이라고 판단된다.

5. 외부 컨설턴트

극소수의 IT 관리 인력이 있는 기업이나 외부 IT 서비스 업체를 이용하는 기업에 있어서, 정보 보안 관리를 위한 외부 컨설턴트나 외부 감사를 활용하는 것은 효과적인 방법이 될 수 있다. 그러나 외부 전문가를 활용하는 것은 내부 직원을 불신하기 때문이라는 인상을 심어줄 수도 있기 때문에, 관리자들이 좋은 의도를 가지고 있다는 것을 내부 직원들에게 인

식시켜주는 것이 필요하다.

외부 전문가 제도 도입과 더불어 직원들에 대한 교육 프로그램을 활용하는 것도 외부 감사 프로그램에 대한 내부 반발을 감소시킬 수 있는 방법이 될 수 있다. 직원들에 대한 외부 전문가 또는 외부 강사의 교육은, 외부 감사/컨설팅의 객관성과 필요성을 직원들에게 인식시켜주는 데 기여할 수 있기 때문이다. 또한 외부 감사의 결과들은 항상 "향상을 위한 제안"이 되어야 하며, 특정 그룹이나 개인에 대한 "비판"이 되어서는 안 된다. 예를 들어 1년에 한 번씩 정기적으로 외부 감사를 받는 것은 IT 관리자들에 대한 의존하는 정도를 매우 효과적으로 감소시킬 수 있다.

이러한 외부 컨설턴트를 활용한 감사 제도는 중요 위치의 직원의 갑작스런 사고, 입원, 퇴직 등에 대한 기업의 효과적인 대처 방법이 될 수 있다. 이런 경우를 그냥 방치할 경우에는 기업의 IT 상황을 곤란하거나 취약한 상태로 만들 수 있기 때문이다.

IT 관리자를 변경하는 것이 기업의 정보 보안 정책에 새로운 외부 신뢰 기관을 도입할 수 있는 좋은 기회가 될 수도 있다. 새로운 직원은 아직 회사의 분위기에 익숙해져 있지 않기 때문에 오히려 관리 및 상담을 더 쉽게 받아들일 수 있다.

V. 업무 프로세스의 관점

대기업은 일반적으로 핵심 업무를 더욱 최적화하기 위해서 업무 처리와 관련된 도구들을 더욱 많이 사용하고 있다. 요즘은 중소기업에서도 업무 프로세스를 중요하게 생각하고 이에 대한 관리에 관심을 기울이고 있다. 기업의 문제들을 다루는 방법을 어떤 것을 사용하던지 간에, 가장 핵심적인 업무 프로세스들은 정의하게 된다.

보안의 관점에서 업무 프로세스를 관리하기 위해서, 다음의 두 가지 영역으로 나누어서 다룰 수 있다.

(1) 기존 업무 프로세스에 대한 보안

(2) 보안에 관련된 업무 프로세스

기존의 업무 프로세스에 고려되어야 할 보안성을 파악할 필요가 있으며, 또한 보안에 관련된 업무 프로세스를 운영할 필요가 있다.

1. 기존 업무 프로세스에 대한 보안 적용

업무 프로세스를 구현 및 관리하는 정보 시스템들은 변경을 거듭하는 시스템이다. 이러한 시스템을 분석하고 보안 사항을 적용하기 위해서는, 정보 시스템의 개발 기간 및 사용 기간이라는 두 가지 생명주기를 독립적으로 점검하는 것이 필요하다.

개발 기간 동안에 필요한 보안 관련 사항 및 신뢰성 측면을 분석하기 위해서는 개발 인력, 개발 도구 및 테스트 환경 등이 분석의 대상으로 포함되어야 한다.

사용 기간 동안에 필요한 보안 관련 사항 및 신뢰성 측면을 분석하기 위해서는 관리자, 사용자, 서비스 제공업체, 기반 시스템, 및 인가되지 않은 외부 사용자 등이 분석의 대상으로 고려되어야 한다.

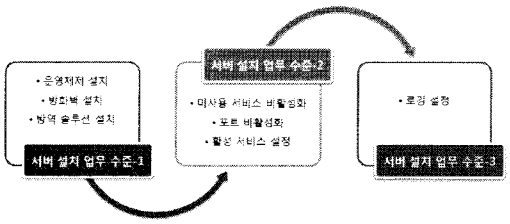

그림 4. 수준별 서버 설치 업무 프로세스 목록
Fig. 4. Server installation processes by Levels

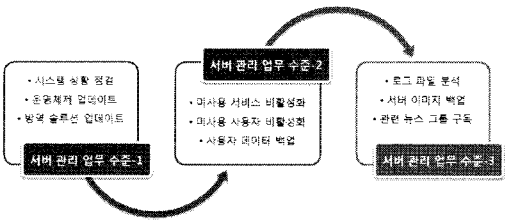

그림 5. 수준별 서버 관리 업무 프로세스 목록
Fig. 5. Server maintenance processes by Levels

2. 보안에 관련된 업무 프로세스 운영

중소기업에서도 보안에 관련된 업무 프로세스들이 정식으로 도입되어야만 한다. 관리자가 수행해야 하는 보안에 관련된 업무 프로세스들에 대한 기준은 다양하다. 대기업의 경우에는 기존의 기준들을 도입하여, 기업의 프로세스를 적절하게 운영할 만한 충분한 여력을 가지고 있다. 중소기업의 경우에도 기업의 핵심 업무를 제외한 부분의 보안 업무 프로세스들은 매우 유사한 부분이 많기 때문에 쉽게 보안 관련 업무 프로세스를 표준화할 수 있다.

보안 관련 업무 프로세스를 모델링하기 위해서, 기존의 프로세스 관리 도구들을 사용할 수 있다. 이를 통해서 예상 비용을 산출할 수도 있으며, 가장 비용-효율적인 업무 프로세스 집합을 결정할 수도 있다.

그림 4는 서버 설치 업무와 관련된 프로세스들을 수준별로 예를 들어 구분해 놓은 것이며, 그림 6은 서버 관리 업무에 관련된 프로세스들을 수준별로 예를 들어 구분해 놓은 것이

다. 각각에 있어서 수준-1은 가장 기본적인 업무들만을 그룹화해 놓은 것이다. 비용과 인력을 고려하여서 수준-2까지의 업무들을 추가할 수도 있다. 수준-3까지의 업무를 수행함으로써, 높은 수준의 보안성과 신뢰성을 확보할 수도 있다. 어느 수준의 업무까지 수행할 것인지는 기업의 업무 영향도 분석을 통해서 결정지을 수 있다[2]. 결국 정보 시스템이 기업의 생존과 얼마나 영향을 끼치는가가 결정에 있어서 중요한 요인이 된다.

VI. 정보 자산 단위의 관점

정보 시스템에 존재하는 정보를 하나하나의 단위로 구분하여, 정보 자산으로 정의하고, 이에 대한 접근 권한을 설정하는 것이 필요하다. 대기업에서처럼 세분화된 구분은 어려울지라도 적절한 수준의 정보 자산 단위 구분이 필요하며, 그 이후에 정보 자산 단위별 접근 제어에 대한 정책을 수립하고 적용하는 것이 필요하다.

기존의 접근 제어와 관련된 방법들보다 더욱 효율적인 접근 제어의 방법은 역할 기반 접근 제어(Role-based Access Control, RBAC)이다[10,11]. 역할 기반 접근 제어 방법에서는, 먼저 역할별로 접근할 수 있는 정보 자산을 구분해 놓고, 각 사용자가 어떤 역할을 담당하는지를 정한다. 이에 따라서, 사용자별로 접근 가능한 정보 자산이 구분이 되게 된다.

역할 기반 접근 제어의 기본적인 개념 중의 하나는 "업무의 구분"이다. 기존 접근 제어 방식들에 비해서, 역할 기반 접근 제어 방식은 업무의 구분을 통해서, 기업의 정책을 상세화하고 적용하는 데에 우수한 특징을 가지고 있다.

업무의 구분은 정적인 업무 구분(Static separation of duties, SSD)과 동적인 업무 구분(Dynamic separation of duties, DSD)으로 나누어질 수 있으며, 역할 기반 시스템에서 필요에 따라 적용되고 있다. 정적인 업무 구분에서는 한 사용자가 정해진 하나의 역할 그룹에만 속할 수 있으며, 동적인 업무 구분에서는 필요에 따라 사용자의 역할 그룹이 추가로 활성화 시킬 수 있도록 되어 있다.

VII. 기술적인 관점

기술적인 관점에 대해서 자세하게 언급하는 것은 본 논문의 영역을 벗어나는 것이기 때문에 간략하게만 다룬다. 지금은 컴퓨터 바이러스, 웜, 트로이목마 프로그램, 스파이웨어, 그레이웨어 등의 악성 코드들이 어디에나 존재하고 있으며, 컴퓨터를 켜는 순간부터 끄는 순간까지 언제나 이러한 위협들로부터 안전할 수가 없다. 따라서 기업의 관리자들은 이에 대한 방어 대책을 마련하고, 바이러스 방역 솔루션, 방화벽, 침입차단 시스템, 침입탐지 시스템 등의 기술적 관점의 보안 솔루션 도입을 추진해야 한다. 기업에 IT 및 보안 서비스를 제공하는 서비스 업체의 경우에 있어서도 중소기업에 맞게 적절하게 구성된 기술적 솔루션과 서비스를 제공해야 한다. 여기에 대한 중소기업의 수요가 늘어날수록 이에 맞는 서비스가 제공될 것으로 예상된다.

VIII. 결론

현대의 중소기업은 대기업처럼 정보 통신 기반 시설 및 서비스를 비슷한 수준으로 사용하고 있지만, 여러 면에서 대기업과 다른 점이 존재하며, 이러한 다른 점들이 바로 중소기업에서 정보 보안이 잘 다루어지지 않는 이유가 된다. 본 논문에서는 중소기업 정보시스템에 적합한 정보 보안 적절한 전략을 제시하고자, 조직 체계의 관점, 업무 프로세스의 관점, 정보 자산 단위의 관점, 기술적인 관점 등의 4가지 관점에서 중소기업의 정보 보안 고려 사항들을 구분해서 살펴보았다. 본 논문에서는 다루어진 내용들은 중소기업이 자신의 회사에 적용 가능한 정보 보안 전략을 수립하고자 할 때 필요한 가이드라인으로 사용될 수 있을 것으로 기대한다. 앞으로는 대기업의 정보 시스템은 해킹하기가 점점 더 어려워질 것이기 때문에, 역량 있는 중소기업이 해커들의 공격 목표가 될 확률이 높아질 것이라고 판단된다. 이를 대비해서 중소기업의 경영진 및 IT 관리자들은 기업의 정보 보안에 대한 관심을 좀 더 가져야만 할 것이며, 본 논문은 이를 위한 기초 자료로 활용될 수 있을 것으로 예상된다.

참고문헌

[1] 인터넷침해사고대응지원센터(KrCERT), *"인터넷침해사고 동향 및 분석 월보"*, 2000년 1월판 - 2009년 3월판.

[2] E. Weippl, and M. Klemen, "Implementing IT Security for Small and Medium Enterprises," Information Security and Ethics, pp. 2970-2985, Information Science reference, New York, 2006.

[3] 김종기, 전진환, "대기업과 중소기업 간의 정보보안 요소에 대한 사용자의 인지 비교: 컴퓨터 바이러스를 중심으로," 정보보호학회논문지, 제16권, 제5호, 2006년 10월.

[4] 문현정, "우리나라 중소기업의 정보 보호 역량 강화를 위한 교육 훈련 현황과 문제점," 정보보호학회지, 제19권,

제1호, 2009년 2월.
[5] 김인중, "*정보통신 기반시설에 대한 위험 분석 및 피해 산정 연구*," 성균관대학교 대학원 박사학위논문, 2006년 2월.
[6] D. L. Pipkin, "Information Security: Protecting the Global Enterprise," Prentice Hall PTR , May 2000.
[7] R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Ed.," John Wiley & Sons, April 2008.
[8] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts And Taxonomy Of Dependable And Secure Computing," IEEE Transactions of Dependable and Secure Computing, Vol. 1, No. 1, pp. 11-33, January 2004.
[9] D. Bell, and L. LaPadula, "Secure computer system: Unified exposition and multics interpretation," ESD-TR-75-306, Technical Report MTR-2997, Mitre Corporation, 1975.
[10] D. Bell, and L. LaPadula, "Secure computer system," Mitre Technical Report 2547, Journal of Computer Security, Vol. 4, No. 2, pp. 239-263, 1996.
[11] K. J. Biba, "Integrity considerations for secure computer systems," Technical Report ESDTR-76-372, ESD,/AFSC, MTR 3153, Mitre Corporation, 1977.
[12] cy"D. Brewer, M. Nash, "The Chinese wall security policy," In Proceedings of IEEE Symposium on Security and Privacy, Oakland, May 1989.

저 자 소 개

여 상 수(Sangsoo Yeo)

1997.2 : 중앙대학교 컴퓨터공학과 학사
1999.2 : 중앙대학교 대학원 컴퓨터공학과 석사
2005.8 : 중앙대학교 대학원 컴퓨터공학과 박사
2009.현: 목원대학교 컴퓨터공학부 전임강사
관심분야: 정보보안, 정보시스템

황 수 철(Suchul Hwang)

1986.2 : 중앙대학교 전자계산학과 학사
1988.2 : 중앙대학교 대학원 전자계산학과 석사
1993.2 : 중앙대학교 대학원 전자계산학과 박사
2009.현: 인하공업전문대학 컴퓨터시스템과 교수
관심분야: 인공지능, 지능형시스템(보안)