보안시스템으로 인해 추가되는 예산 외 비용의 요인에 관한 연구

종신회원 전 정 훈*

A Study on the Costs Factors of an being additional Budget by the Security System

Jeong-hoon Jeon* *Lifelong Member*

요 약

최근 공격기술은 네트워크의 진화와 함께 다양한 형태로 나타나고 있으며, 대부분의 네트워크에서는 다양한 보안장치들을 통해 대응하고 있다. 또한 외부 공격으로부터 내부 네트워크의 정보자산을 보호하기 위해 기존 네트워크에 필요한 보안시스템들을 추가 배치하고 있다. 그러나 이와 같은 보안시스템의 사용은 내부 네트워크의 성능과 보안에 큰 영향을 미칠 뿐만 아니라 이로 인해 경제적인 추가비용을 발생시킨다. 따라서 본 논문은 내부 네트워크의 보안으로 인한 추가 비용의 요인들에 대해 예상하기 어려운 가변적 상황과 정보보호 인식수준, 보안시스템, 정보자산 평가유무 등을 관련 연구자료 및 실험결과를 분석함으로써, 향후 관련 정책수립과 내부 네트워크의 구축 및 설계에 따른 비용절감의 기초자료로 활용될 것으로 기대한다.

Key Words : Security System, Information Asset, Asset Assessment, Costs Factor, Additional Budget

ABSTRACT

Recently, Hacking Attacks are appearing as a various Attack techniques with evolution of the Network. and most of the network through a Various Security Systems are responding to an attack. In addition, it should be placed adding the Security Systems to protect the Internal Network's Information assets from External attacks. But, The use of Security Systems inside the network makes a significant impact on Security and Performance, as well as a result causes Economic Additional Costs. Therefore, In this paper, it will be to analyze by associated a case study and experimental results about the Additional Costs Factors(Variable situations difficult to predict and Information Security Recognition levels, Security Systems, Information Asset Assessment). This is expected to serve as a valuable Information for the Reduction of an Costs in a Network deployment and Design in a future.

Ⅰ. 서 론

최근 네트워크는 다양한 기술의 등장으로 빠른 성장을 보이고 있으며, 이에 따른 정보자산(information asset)의 가치도 함께 증가하고 있다. 그러나 이러한 변화와는 달리, 정보자산을 위협하는 공격기술 또한 상호 보완적 관계를 유지하며, 함께 진화하고 있어, 정보보호의 필요성이 더욱 요구되고 있다. 이와 같은 상황에서 대부분의 사업장들은 정보자산의 보호를 위해, 가장 보편적인 대응방안으로 보안시스템을 사용하고 있다. 보안시스템은 최근 이슈가 되고 있는 무선 인터넷이나 클라우드 컴퓨팅(cloud computing), 스마

* 동덕여자대학교 정보학부 (nerdrandy@dongduk.ac.kr)
논문번호 : KICS2011-07-277, 접수일자 : 2011년 7월 11일, 최종논문접수일자 : 2011년 11월 28일

트 그리드 컴퓨팅(smart grid computing) 등의 기술 분야에서도 취약부분을 보완할 중요한 시스템으로 선호되고 있다. 또한 보안시스템의 기능으로는 인가되지 않은 접속과 시도에 대해, 차단 및 탐지기능 뿐만 아니라, 역추적 자료를 제공하며, 추후 재공격에 대응할 수 있는 다양한 기능의 제품들도 출시되고 있다. 그러나 보안시스템은 많은 비용을 필요로 할 뿐만 아니라, 성능과 반비례하는 특성을 지니고 있기 때문에 사업장들은 도입 및 운용 관리에 추가적인 비용부담과 재구축 및 배치에도 많은 시간과 인력이 요구되고 있어, 경제성과 실용성 측면에 적지 않은 선택적 부담과 정보보호에 대한 인식저하의 요인이 되고 있다[1]. 또한 이와 같은 사업장들의 낮은 보안의식 수준은 사회적으로 전문 인력의 부족과 정보자산에 대한 위협 및 추가 비용의 요인이 되고 있으며[2], 최악의 경우, 사업장들이 보유한 정보자산 보다도 더 큰 손실을 가져다주는 악순환이 지속되고 있다.

따라서 본 논문은 보안시스템의 운용 및 관리로 인한 문제들과 이에 따른 정보보호 관련 예산 이외에 추가 비용의 요인들을 분석함으로써, 향후 보안시스템의 효율적인 보안 운영 및 내부 네트워크의 성능향상과 경제적 비용의 절감을 위한 자료로 활용될 것으로 기대한다. 연구내용에 대한 논리적 근거를 위해 논문의 2장은 가변 상황에 따른 추가 비용의 요인에 대해 기술하고, 3장은 정보보호의 인식에 따른 요인을 알아본다. 그리고 4장은 보안시스템에 따른 요인과 5장의 정보자산 평가의 유무에 따른 요인을 알아보며, 6장의 결론 부분으로 이글을 마치도록 한다.

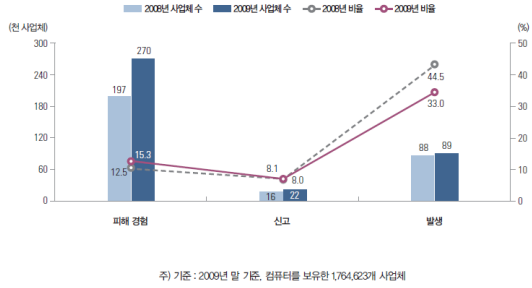
Ⅱ. 가변 상황에 따른 추가 비용의 요인

정보보호는 개인 및 기업, 기관들의 정보자산을 보호하기위해, 다양한 보안시스템과 전문 인력 그리고 많은 관련 예산들이 요구되며, 시간이 지남에 따라 초기 예산 이외의 추가 비용이 점차 증가하는 특징이 있다. 이와 같은 원인에는 보안시스템과 관련해 복구비용, 시스템의 구입 및 교체, 업그레이드, 내부공격, 성능저하, 전문 인력의 확보, 정보자산평가 등 여러 가변 상황(variable conditions)들로 인해 비용이 추가되기 때문이다. 이러한 가변 상황들은 최악의 경우, 사업장들이 보유한 정보자산보다도 더 큰 비용을 필요로 하며, 경제적 부담의 가중과 함께 보안시스템의 배치 목적 및 정보자산의 가치를 불분명하게 한다. 따라서 이와 같은 가변 상황들로 인해 발생하는 추가비용의 요인들을 다음에서 알아본다.

2.1 공격유형의 변화

네트워크 보안기술은 공격기술과 상호 보완적 관계를 유지하며 함께 진화하고 있다. 사업장들의 대표적인 대응기술로는 보안시스템이 있으며, 이러한 보안시스템은 새로운 공격유형의 출현으로 개발 및 업그레이드의 주기가 점차 짧아지고, 종류와 기능도 다양해지고 있다[3]. 그러나 보안시스템은 새로운 공격유형을 예측하여 개발 및 업그레이드되는 것이 아니라, 침해 후, 업그레이드되기 때문에 대부분의 사업장들은 정보보호 관련 예산산정에 있어, 공격유형의 변화에 따른 추가 비용의 부담을 고려하지 않게 된다. 이에 대해 국내 사업장들의 침해사고 현황과 보안시스템의 사용률에 관한 통계자료를 통해, 공격유형의 변화에 따른 보안시스템과의 관계를 알아본다.

그림 1은 국내 웜·바이러스에 대한 피해현황을 조사한 것으로 2009년의 피해가 2008년에 비해 약 2.8% 증가하였다[4]. 그리고 그림 2의 2010년 침해사고 통계 자료에서도 침해사고 건수가 2009년보다 2010년에 58.3%가 증가하여, 해마다 증가 추세에 있음을 알 수 있다[5]. 이러한 결과는 컴퓨터 바이러스로 인한 공격이 다른 공격유형에 비해 상대적으로 급증



주) 기준 : 2009년 말 기준, 컴퓨터를 보유한 1,764,623개 사업체

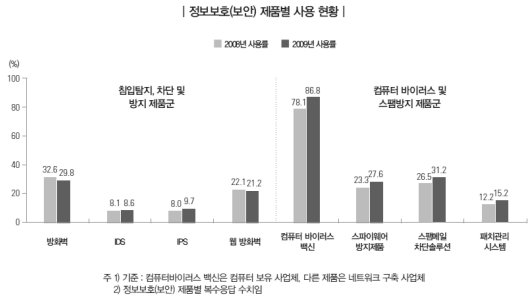
출처 : 한국정보화 진흥원 2010 [4]

그림 1. 국내 2010정보화 통계집

구 분	2009년 총계	2010년												2010년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
웜·바이러스	10,395	932	1,302	1,085	1,315	1,751	1,674	1,609	1,405	1,507	1,621	1,742	1,987	17,930
해킹신고처리	21,230	898	1,076	1,053	1,468	1,062	1,160	1,300	1,644	2,183	1,732	1,412	1,307	16,295
·스팸릴레이	10,148	154	317	222	431	285	169	556	666	889	594	549	384	5,216
·피싱경유지	988	78	106	116	102	95	77	66	50	56	54	58	33	891
·단순침입시도	2,743	232	230	345	396	404	411	404	423	310	265	326	360	4,126
·기타해킹	3,031	223	233	267	227	132	136	155	323	424	381	253	265	3,019
·홈페이지 변조	4,320	211	190	103	312	146	367	119	182	504	438	226	245	3,043
악성 봇(Bot)	1.0%	0.6%	0.6%	0.7%	0.9%	0.8%	0.6%	0.5%	0.4%	0.4%	0.4%	0.4%	0.5%	0.6%

출처: 인터넷침해대응센터 2010년12월 월보 [3]

그림 2. 침해사고 통계



출처 : 한국정보화 진흥원 2010 [5]

그림 3. 국내 2010정보화 통계집

하고 있음을 반증해 준다. 다음은 공격유형에 따른 보안시스템의 사용변화를 비교해 보기 위해, 최근 사업장들이 사용하고 있는 정보보호 제품들의 사용률 변화를 알아본다.

그림 3은 2009년 기관 및 기업들의 정보보호 제품별 사용현황으로 침입탐지 및 차단, 방지 제품군 중, 방화벽의 사용률이 29.8%로 가장 높았으며, 2008년보다 2009년에는 2.8%가 감소하였다. 그리고 컴퓨터 바이러스 및 스팸방지 제품군에서는 백신의 사용률이 86.8%로 가장 높았으며, 2008년보다 2009년에는 8.7%가 증가하였다. 이와 같은 자료를 종합해 볼 때, 공격 유형의 변화에 따라 보안시스템의 사용률이 함께 변화하고 있어, 공격유형과 보안시스템의 상호 보완적 관계를 알 수 있다. 또한 이러한 공격유형의 변화는 예산 산정 시, 예측하기 어려운 가변 상황으로써 예산 외의 추가적인 비용요인이 되고 있다.

2.2 내부 사용자 공격

내부 공격은 트러스티드(Trusted) 네트워크 내의 공격을 의미하며, 최근 내부 취약점과 위협에 따른 공격이 급증함으로써, 공격의 비중이 점차 커지고 있다. 특히, 내부 사용자에 의한 공격은 내부 공격의 유형 중, 매우 큰 비중을 차지하고 있으며, 다른 공격유형들과는 달리, 공격의도가 내부 사용자의 의지에 기인하고 있어, 내부 보안의식 강화가 필요하다. 이에 대해 주요 사고유형별 자료를 통해 내부 공격의 현황을 알아본다.

그림 4는 주요 사고 유형을 나타낸 것으로 내부 사용자에 의한 사고가 전체 내부 공격 중, 44%로 매우 높다. 이러한 원인에 대해 [6]은 트러스티드 네트워크의 보안정책에 있어, 내부 사용자를 허가된 사용자로 전제함에 따른, 여러 취약점들이 발생하기 때문인 것으로 기술하고 있다. 이는 내부 사용자에 의한 공격이 사업장들에게 추가적인 보안시스템 및 소프트웨어의

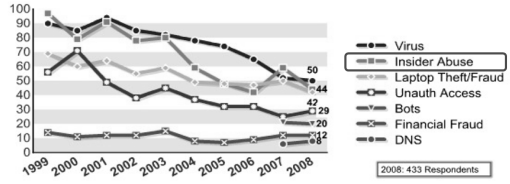
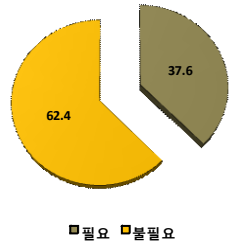


그림 4. 주요 사고유형별 현황 [6]

도입이나 정보자산의 손실 및 유출에 따른 비용추가가 불가피하다. 따라서 사업장들은 이러한 내부 공격의 가변 상황들을 배제시키기 위해, 보다 강화된 사내 보안교육 및 통제와 정보보호에 대한 인식의 고취가 필요하다. 이와 같은 국내 사업장들의 정보보호 인식 수준에 대해서는 다음 3절에서 알아본다.

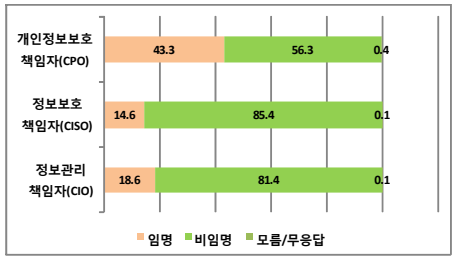
Ⅲ. 정보보호의 인식에 따른 요인

사업장들은 사이버 공격으로 인한 침해사고가 급증하고 있음에도 불구하고, 정보보호에 대한 예산을 계속해서 감축하고 있다. 이러한 원인으로는 언제, 어디서, 어떻게 발생할지 모르는 공격을 대비하기 위해, 많은 비용을 투자해야하는 경제적 부담과 정보보호에 대한 인식이 미흡하기 때문이다. 이에 대해 사업장들의 정보보호 교육의 필요성에 대한 인식 조사자료와 국내 정보보호 관련 책임자의 임명현황을 통해, 정보보호의 인식 수준이 추가 비용의 요인으로 작용하는지를 알아본다. 그림 5는 사업장들의 정보보호 교육의 필요성에 대한 조사결과로 62.4%의 '불필요 하다'라는 응답을 나타냈으며, 이를 통해 국내 사업장들의 정보보호의 낮은 인식 수준과 보안에 매우 취약한 상태임을 알 수 있다. 이에 대해 [4]는 보안 사고의 증가원인으로 사업장들의 정보보호에 대한 인식부족과 전문인력의 부족을 지적하고 있다. 다음 그림 6의 국내 사업장들의 정보보호 관련 책임자의 임명 현황을 통해,



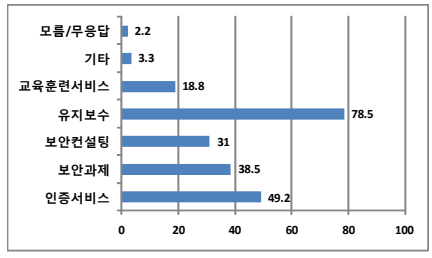
출처: 인터넷진흥원 2009년 정보보호 실태조사-기업편[7]

그림 5. 정보보호교육의 필요성 인식



출처 : 인터넷진흥원 2009년 정보보호 실태조사-기업편

그림 6. IT관련 책임자의 명시적 임명 현황 [1]



출처 : 인터넷진흥원 2009년 정보보호 실태조사-기업편

그림 7. 이용 중인 정보보호 서비스 [1]

전문 인력과 정보보호 인식수준에 대해 알아본다.

그림 6은 국내 사업장들의 'IT관련 책임자의 명시적 임명현황'자료로 책임자 임명 비율이 개인정보보호 책임자에 43%, 정보보호 책임자에 14.6%, 정보관리책임자에 18.6%만을 임명하고 있다[1]. 이러한 결과는 국내 사업장들의 정보보호에 대한 인식이 매우 미흡함을 확인할 수 있으며, 새롭게 진화하고 있는 공격기법들을 고려해 볼 때, 향후 사업장들의 피해와 이에 따른 예산 외에 발생하는 추가 비용의 증가를 예시해 주고 있다. 이와 관련해 3.1과 2절에서는 정보보호 인식을 기반으로 한, 위탁관리와 전문 인력의 확보 여부가 사업장들의 정보보호 예산에 어떠한 영향을 미치는지를 알아본다.

3.1 사업장들의 위탁관리

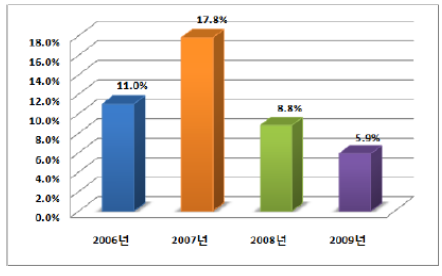
대부분의 사업장들은 정보자산의 보호를 보안 전문업체에 위탁하고 있다. 이러한 사업장들의 위탁관리는 일시적인 비용절감과 편의성을 제공해 줄 수는 있지만, 위탁관리에 따른 가변 상황들로 인해, 추가적인 경제적 손실비용을 감안해야 한다. 이에 대해 국내 사업장들이 이용하고 있는 '정보보호 서비스의 실태조사' 자료를 통해, 위탁 관리의 현황을 알아본다.

그림 7은 사업장들이 이용하고 있는 정보보호 서비스에 대한 조사 자료로 '유지보수'가 78.5%로 가장 높았으며, 인증 및 보안관제, 컨설팅 순서로 나타났다. 여기서 유지보수가 가장 높은 이용률을 나타내는 점은 사업장의 전문 인력확보율과 자체 대응능력이 미비하다는 것을 반증해주며, 긴급 상황 시, 신속한 대응과 유지보수 및 복구에 따른 추가 비용의 발생이 불가피함을 시사하고 있다[2]. 또한 이외에도 위탁관리로 인한 내부 정보자산의 높은 유출 가능성과 정보자산의 통제력 약화가 예상된다. 이와 같이 사업장의 위탁관리는 정보자산을 위협하는 근본적인 원인을 제공함으로써, 추가 비용의 요인이 되고 있다.

3.2 사업장들의 전문 인력

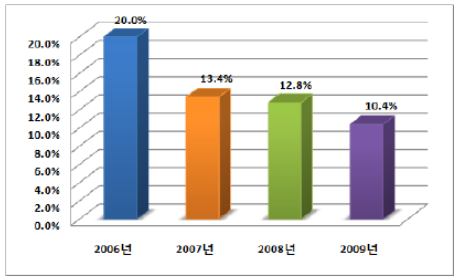
보안 전문 인력은 보안관련 분야의 학위 또는 자격증 소지자나 실무경험을 갖춘 경력자들이라 할 수 있다. 이러한 전문 인력들은 정보보호와 관련한 네트워크 운영 및 관리 등의 업무를 수행함으로써 신속한 대응을 가능케 한다. 그러나 현실적인 상황들을 고려해 볼 때, 대부분의 사업장들은 정보보호 인식 부족과 전문 인력의 감소로 인해, 위탁관리에 의존하고 있는 실정이다. 이에 대해 국내 학위와 자격증 소지여부에 대한 자료를 통해, 국내 전문 인력의 현황과 사회적 영향에 대해 알아본다.

그림 8은 2010년 국회입법조사처의 정보보호 관련 학위소지 비율을 나타낸 것으로 전문 인력에 대한 학위 소지비율이 2007년을 기점으로 계속 감소하고 있으며, 2009년에는 2007년에 비해 약 11.9%가 감소하였다[2]. 또한 그림 9의 관련 자격증 소지비율에 대한 통계자료에 따르면, 2009년에는 2006년에 비해 약 9.6%가 감소하였으며, 2006년을 기점으로 해마다 자격증 소지비율이 감소하고 있다. 이와 같은 자격증 소지비율의 감소는 정보보호에 대한 사업장들의 인식부재를 근본적인 원인으로 꼽을 수 있으며[2], 사업장들의 전문성 저하와 사회적으로 정보보호 관련 종사자들에 대한 처우가 매우 미흡함을 간접적으로 시사해



출처: 국회입법조사처 2010.10.20

그림 8. 학위소지자 비율



출처: 국회입법조사처 2010.10.20

그림 9. 정보보호관련 자격증 소지비율

준다. 또한 사업장들의 전문 인력 부재는 신속한 대응 및 복구를 어렵게 하고, 복구비용의 추가가 불가피하다. 다음의 수식 1을 통해, 전문 인력의 부재에 따른 복구비용과의 연관성을 알아본다.

* 피해복구 비용 산출 식 (수식 1)

$$\text{자산복구총비용} = \frac{\text{시스템 관리자 또는 복구인력수당}}{hr} \times \text{복구시간}(hr)$$

수식 1[9]-[11]은 사업장들이 손실된 정보자산을 복구하는데 필요한 총비용의 계산식으로 국내 표준을 따르고 있으며, 자산 복구 총비용은 복구시간과 복구인력에 대한 인건비로 구성하고 있다. 여기서 전문 인력의 부족은 인력수당과 복구 시간을 상대적으로 증가시킴으로써, 전체 자산 복구에 필요한 총비용을 함께 증가시킨다. 따라서 사업장들의 전문 인력 확보와 사업장들의 정보보호에 대한 인식이 복구비용에 영향을 미치고 있음을 알 수 있다.

Ⅳ. 보안시스템에 따른 요인

4.1 보안시스템의 성능저하

보안시스템은 가장 일반적인 대응방법으로 네트워크와 기타 정보자산을 보호하는 역할을 수행한다. 그러나 보안시스템은 배치위치와 정책 및 연결 수 등에 따라, 내부 네트워크의 성능을 저하시키고 있어, 전체 네트워크의 효율성 저하와 경제적인 손실을 야기 시킨다. 이에 대해, 보안시스템으로 인한 네트워크의 성능저하가 예산 이외 추가 비용에 어떠한 영향을 미치는지에 대해 실험결과를 통해 알아본다. [7]의 실험에서는 내부 네트워크의 성능저하요인을 알아보기 위해, 보안시스템의 사용유무와 정책 수, 연결 수에 따라 성

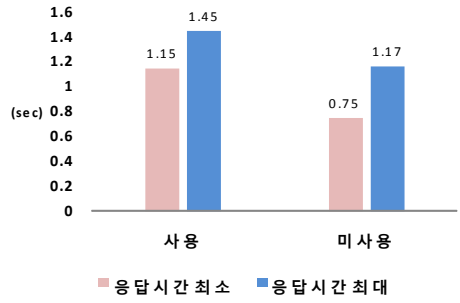


그림 10. 방화벽의 사용유무에 따른 응답시간 비교

능을 비교하고 있다.

그림 10은 방화벽의 사용유무에 따른, 응답시간을 측정한 것으로 방화벽을 사용하지 않을 때보다 약 1.35배의 응답지연을 나타냈으며, VPN의 사용유무에 따른 응답속도를 측정한 그림 11에서는 VPN을 사용하지 않을 때보다 약 3.6배의 응답지연을 나타냈다.

그리고 그림 12는 방화벽의 보안레벨(가장 낮은 레벨인 1과 가장 높은 레벨인 7)과 연결 수(3에서 300)가 증가할수록 최대 509.66배정도의 전송지연을 보였으며, 그림 13에서는 VPN의 연결된 네트워크(최소 3

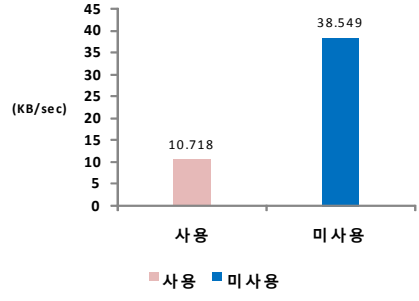


그림 11. VPN의 사용유무에 따른 응답속도 비교

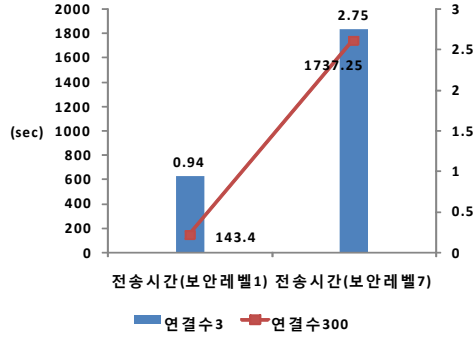


그림 12. 방화벽의 연결 수에 따른 전송시간비교

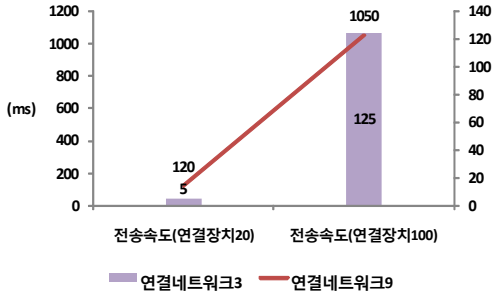


그림 13. VPN의 연결 수에 따른 전송속도 비교

에서 9까지)와 연결 장치(20에서 100개의 장치)의 수가 증가할수록 최대 9배 정도의 속도 저하를 나타냈다. 이러한 실험결과를 통해, 방화벽과 VPN은 연결수와 보안레벨, 연결 네트워크 및 장치가 높거나 증가할수록 내부 네트워크의 성능이 저하되고 있음을 알 수 있다.

또한 방화벽과 VPN의 정책 수 변화에 따른 전송속도 및 응답시간의 비교에서 방화벽은 그림 14와 같이 정책(최소 10과 최대 30개)과 방화벽의 수(2대에서 5대)에 대해 최대 4배정도의 속도 지연을 나타냈으며,

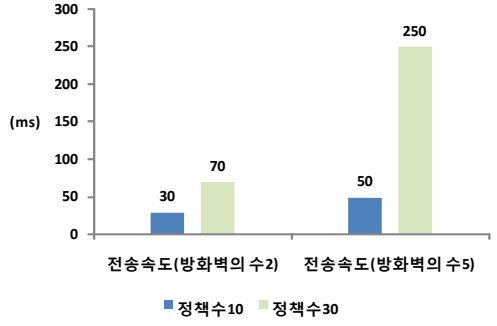


그림 14. 방화벽의 정책 수에 따른 전송속도비교

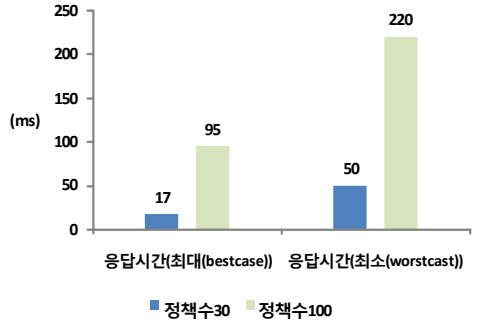


그림 15. VPN의 정책 수에 따른 응답시간 비교

VPN은 그림 15와 같이 정책 수(최소 30개와 최대 100개)의 Worst Case와 Best Case에 대한 응답시간이 약 4.7배의 차이를 보였다. 이와 같은 결과를 통해, 방화벽과 VPN은 보안시스템의 수와 정책의 수가 증가할수록, 내부 네트워크의 성능이 저하됨으로써, 네트워크의 확장과 공격유형의 변화가 가변 상황으로 작용하고 있음을 알 수 있다.

그러나 이와 같이 네트워크의 성능저하가 지속될 경우, 경제적 손실이 가중되고, 보안시스템의 운영 및 정책, 배치 등의 구조적 개선과 이에 따른 비용의 추가가 불가피하다. 따라서 내부 네트워크의 보안 설계 시, 보안시스템은 성능과 기능을 고려해, 향후 공격에 탄력적 대응을 위한 배치가 필요하다.

4.2 보안시스템의 교체 및 업그레이드

보안시스템은 네트워킹 기술과 공격기술이 함께 진화하면서, 업그레이드 주기가 점차 짧아지고 있다[4]. 이러한 업그레이드에는 하드웨어와 소프트웨어가 있으며, 유형에 따라 비용과 주기에 차이를 갖는다. '하드웨어 형' 업그레이드는 비교적 많은 비용이 요구되며, 신속한 업그레이드가 어려운 반면, 업그레이드 주기가 매우 길어 추가 비용이 거의 발생하지 않는다. 그리고 '소프트웨어 형' 업그레이드는 '패턴 형[1]'과 '정책 형[2]'으로 나누어 볼 수 있으며, '패턴 형'은 기존의 보안기능 모듈의 업그레이드 및 교체가 용이하고, 신속한 대응이 가능하다[4].('패턴 형'을 사용하는 보안시스템으로는 IDS와 IPS, PMS(Patch Management System), 백신 등이 있다.) 또한 '정책 형'은 신속한 업그레이드가 가능하지만, 관리자가 직접 입력한 정책과 혼재되어, 정책의 중복 및 삭제될 수 있으며, 이로 인해 내부 네트워크의 성능이 저하되는 단점이 있다. ('정책 형' 업그레이드를 적용하는 보안시스템으로는 방화벽(Firewall)과 VPN, IPS 등이 있다.) 이와 같은 보안시스템의 업그레이드는 시스템의 교체나 공격유형의 변화가 주된 요인이 되기 때문에 앞서 2.1절에서와 같이 공격유형에 따른 가변 상황들을 제공함으로써, 추가 비용의 요인이 되고 있으며, 업그레이드 유형에 따라 추가 비용에 차이를 갖게 된다. 따라서 업그레이드로 인한 추가 비용의 절감을 위해서는 보안시스템의 도입 시, 업그레이드 방식과 주기를 고려한 선택이 필요하다.

1) 웜, 바이러스와 같은 악성코드의 패턴
2) 접근통제 규칙(ACL)과 같은 보안정책

Ⅴ. 정보자산 평가의 유무에 따른 요인

정보자산의 평가(information asset assessment)는 데이터의 부가가치성을 자산의 의미로 재평가한 것으로, 주기적인 평가를 통해, 사업장들의 예산 산정 및 집행을 효율적으로 수행할 수 있게 하며, 보다 안정적인 보안시스템들의 배치 및 네트워크의 구축을 가능하게 한다. 그러나 사업장들은 정보자산의 평가에 따른 비용과 번거로움으로 대부분 주기적인 평가가 이뤄지지 않고 있으며, 국가 관련 기관 및 보안 전문 업체의 일관된 보안정책에 의해 위탁 관리됨으로써, 실질적인 정보보호 관련 예산의 효율적인 집행이 사실상 어려운 실정이다[8]. 이와 같이 정보자산의 평가가 이뤄지지 않을 경우, 사업장들은 보유한 정보자산의 가치보다도 더 많은 비용이 소요될 수 있으며, 불필요한 예산의 낭비를 초래하게 된다. 따라서 사업장들의 정보자산 관리의 미흡함으로 인해 발생할 수 있는 상황을 2가지로 가정해 보면 다음과 같다.

Case1(정보자산 < (정보보호 예산+예산 외 추가 비용))은 평가한 정보자산의 가치가 정보보호에 필요한 비용보다도 적은 경우이다. 이러한 경우는 보호해야할 보안 목적이 명확하게 정의되어 있지 않으며, 정보자산의 평가가 정기적으로 수행되지 않았다는 것을 의미한다. 그리고 전문 인력의 부족 또는 부재로 인해 신속한 대응과 복구가 어려워 추가 비용이 계속해서 증가하는 경우를 의미한다.

Case2(정보자산 > (정보보호 예산+예산 외 추가 비용))은 정보자산의 가치가 정보보호에 필요한 비용보다 클 경우로 이러한 관계가 지속적으로 유지되어야 한다.

대부분의 사업장들의 초기 예산상황은 Case2부터 시작하지만, 2절에서와 같이 다양한 가변 상황들로 인해 Case1의 경우에 가까워진다. 따라서 정보자산과 정보보호 예산의 관계가 지속적으로 유지될 수 있도록 정기적인 정보 자산의 평가를 통해, 정보자산의 보호 목적을 유지하고, 예산 외의 추가 비용을 절감이 요구된다. 결과적으로 사업장들은 정기적인 정보자산의 평가를 통해, 정보보호 관련 예산을 계획해야 하며, 예산외에 발생 가능한 가변 비용의 고려가 필요하다. 여기서 정보자산 평가는 사업장들의 정보보호 예산 산정의 기준 모델로써, 평가의 유무가 예산 외의 추가 비용을 발생시키는 요인이 되고 있음을 알 수 있다.

5.1 정보자산의 위험률

사업장들은 보안체계를 구축하기 위해서 정보자산의 평가와 함께 위험률(risk rate)에 대한 측정이 필요하다. 정보자산에 대한 위험률은 보안시스템의 배치 및 선정과 보안 설계에 매우 중요한 기초자료가 되기 때문에 사업장들은 주기적인 평가를 통해, 정보자산에 대한 취약점(vulnerability)과 위협(threat)을 분석하고, 이에 적합한 보안 체제를 구축해야 한다. 그러나 대부분의 사업장들은 자산 평가가 이뤄졌다 할지라도 자산에 대한 취약점과 위협들을 보안 설계 및 예산책정에 반영하기가 쉽지 않다. 이는 정보자산의 취약점과 위협에 따라 정보보호 관련 예산이 변동됨으로써 관련 예산 외의 추가비용을 증가시키게 된다. 따라서 정보자산의 위험률을 측정하여 취약점과 위협에 적합한 정책이 보완되어야 한다[9]. 이에 대해 수식2를 통해 정보자산에 따른 위험과 취약점 및 위협의 관계를 알아본다[11].

(수식 2)

Total Risk

= Information asset × Vulnerability × Threat

- 전체위험(Total Risk) - 취약점(Vulnerability)
- 정보자산(Information asset) - 위협(Threat)

수식2[9]-[11]는 앞서 수식1과 같이 국내 사업장들이 정보자산에 대한 위험(risk)을 산출하는 식으로써, 정보자산(information asset)의 평가 이후 자산에 대한 취약점(vulnerability)과 위협(threat)을 통해 전체 위험률을 산정한다. 그리고 이렇게 산정된 위험(risk)은 보안체계의 구축과 보안시스템의 도입, 전문 인력 확보 등 구체적인 정보보호 예산 산정에 필요한 기초자료가 된다. 이로써, 정보보호 관련 예산의 효율적인 산정을 위해서는 정보자산과 위험도(risk rate)의 주기적인 평가가 필요하며, 이는 추후 정보보호 예산 외의 추가 비용을 절감시킬 요인으로 작용함을 알 수 있다.

Ⅵ. 결 론

최근 네트워크의 기술들이 새롭게 등장하면서, 이에 따르는 공격 대응에 필요한 보안시스템의 사용도 매우 보편화되었다. 그러나 보안시스템의 운용 및 관리에 있어, 사업장들의 정보보호에 대한 인식부족과 위탁관리, 전문 인력의 부족 등으로 신속한 대응 및 복구를 어렵게 하고, 여러 가변 상황들로 인해 추가 비용이 계속해서 발생되고 있다. 또한 정보자산 및 위험률의 평가를 통해, 효율적인 보안시스템의 선택 및

배치가 이뤄지지 않고 있어, 사업장들의 경제성 예측을 어렵게 하고 있다. 따라서 네트워크의 효율적인 정보자산 관리 및 유지를 위해서는 정보보호 예산 외에 추가되는 비용의 요인들을 분석하고, 정기적인 정보자산과 위험관리를 통해, 정보보호의 목표에 부합한 보안운영으로 경제적 비용의 절감과 성능향상이 필요하다. 또한 사업장들의 정보보호에 대한 인식의 재고와 이를 바탕으로 한 정보보호 전문 인력의 양성, 제도 및 정책, 홍보 등의 지속적인 개선이 필요함을 알 수 있었다.

본 논문은 보안시스템 관련 예산 외에 예측하기 어려운 추가 비용의 요인들을 분석함으로써, 보다 효율적인 예산 산정과 경제적 비용의 최소화를 통해, 향후 활성화될 클라우드 및 그리드 컴퓨팅의 환경구축에 성능향상 및 효율적인 관리를 위한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후 효율적인 보안시스템의 배치를 위해서는 정보보호에 대한 인식개선과 정보자산의 객관적인 가치평가를 위한 표준이 마련되어야 하며, 이에 따른 보안시스템의 효율적인 기능개선 및 유지비용 절감을 위한 추가적인 연구가 지속적으로 이뤄져야 할 것이다.

참 고 문 헌

〔1〕 한국인터넷진흥원 "2009 정보보호 실태조사(기업편)" p.40, 2009.

〔2〕 국가입법조사처 "국가 정보보호 정책현황과 개선방안" p.23, 2010.10.20.

〔3〕 한국인터넷침해대응센터 "2008년 인터넷 및 침해사고 동향 및 분석보고 월보(8월)", pp.11-21, 2010

〔4〕 한국정보화진흥원, "2010년 정보화통계집" p.8, 2010.

〔5〕 한국인터넷침해대응센터, "2010년 인터넷 및 침해사고 동향 및 분석보고 월보(12월)" p.3, 2010.

〔6〕 Robert Richardson, CSI Director "CSI &FBI CSI Computer Crime & Security Survey" p.15, 2008.

〔7〕 전정훈, "내부 네트워크의 성능저하요인에 관한 연구", 한국통신학회 Vol.36, No.1, pp.43-50, 2011.1.

〔8〕 Farhad Foroughi WCE "Information Asset Valuation Method for Information Technology Security Risk Assessment" July 2-4, London UK, 2008.

〔9〕 Steve Elky, SANS Institue "An Introduction to Information System Risk Management" May, 31, p.4, 2006.

〔10〕 ISO 27001/BS 7799 "Risk Assessment"

〔11〕 한국정보통신기술협회 TTA "IT 서비스 위험분석 방법 국내 표준" TTAK.KO-12.007, pp.16-32, 2000.3.28.

전 정 훈 (Jeong-hoon Jeon) 종신회원

2008년 숭실대학교 컴퓨터공학과 공학 박사

2005년~현재 동덕여자대학교 교수

<관심분야> 네트워크보안, 시스템보안, 무선보안, 암호, 컴퓨터 포렌식