情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

기업의 침해사고 예방을 위한 관리 모델

강 신 범,† 이 상 진,‡ 임 종 인
고려대학교 정보보호대학원

A Study on the Effective Countermeasures for Preventing Computer Security Incidents

Shin-Beom Kang,† Sang-Jin Lee,‡ Jongin Lim
Korea University

요 약

우리나라의 정보화 수준과 비교하여 정보보호 수준은 상대적으로 낮다. 정보보호 예산 수준 역시 전체 정보화 예산 대비 5%대로 미미하며 기업들의 사후대응 중심의 정보보호 조치는 반복적인 피해비용을 야기한다. 정보보호 침해사고에 대한 대응은 사후대응 체계에서 예방과 사전탐지 중심으로 바뀌어야한다. 정보사회에서의 침해사고 대응은 개인의 책임보다는 국가와 기업이 공동으로 대처해야할 영역이라는 인식 전환이 필요하다. 2004년 정보보호조치 및 안전진단 관련 지침이 고시되면서 우리나라도 침해사고 예방을 위한 제도적 기반을 마련하였다. 하지만 제도적으로 시행되고 있는 관리적, 기술적, 물리적 보호조치가 실제 침해사고 대응에 완벽한 예방책이 되지는 못한다. 본 연구에서는 현행 제도적 보호조치의 예방 효과에 대해 살펴보고 제도적 한계와 개선점을 도출하여 기업들이 실질적인 목표 보안 수준을 유지하기 위해 필요한 효과적인 침해 예방 대응책으로써의 선행위협 관리 모델을 제안한다.

ABSTRACT

The level of information protection is relatively low, in comparison with the informatisation in this country. The budget for information protection is also quite marginal at 5% of the entire information-related policy budget. The passive information protection practices by companies, which focus more on the aftermaths, lead to repeated expenses for risk management. The responses to the violation of information protection should be changed from the current aftermaths-oriented focus to prevention and early detection of possible violations. We should also realize that the response to a violation of protected information is not a responsibility of an individual but a joint responsibility of the nation and the industry. South Korea has been working towards to building a systematic foundation since 2004 when guidelines were announced regarding the information protection policy and the safety diagnosis. The current level of safety policies cannot provide a perfect protection against actual violation cases in administrative, technological and physical ways. This research evaluates the level of prevention that the current systematic protection policy offers, and discusses its limitation and possible ways for improvement. It also recommends a list effective measures for protection against information violation that companies can employ to maintain the actual target safety level.

Keywords: Cyber Criminal Threat, Computer Security Incident, Security Policy

접수일(2011년 4월 1일), 게재확정일(2011년 10월 10일)

† 주저자, shinbeom@korea.ac.kr
‡ 교신저자, sjlee@korea.ac.kr

I. 서 론

2010년 ITU 보고서에 의하면 우리나라의 정보통신발전지수 순위는 세계 3위로 전세계 IT 산업의 83%를 차지하는 G20 국가 중에서도 상위권에 해당한다. 하지만 2011년 우리나라의 행정안전부 정보화 사업 예산 대비 정보보호 예산 비율은 5.9%, 국가 전체 정보화예산 대비 정보보호 예산의 비율도 6.2%에 머물고 있다. 미국의 경우 2005년 정보보호예산이 34억 달러에서 2006년 55억 달러로 크게 증가한 이후 지속적으로 관리되어 2009년 68억 달러의 예산 규모를 보여 전체 예산대비 10%대를 유지하며 우리나라와 상반된 정책을 보이고 있다.[1]

기업들의 침해사고에 대한 인식 역시 이러한 예산 편성과 무관치 않은데 2009년 방통위의 정보보호실태 조사 대상 63.6%가 정보보호 지출이 아예 없는 것으로 나타났고 정보보호 관련 예산이 없는 이유로는 응답자 중 65.1%가 "정보보안 사고로 인한 피해가 거의 없어 필요성을 느끼지 못한다"라고 응답했다. 하지만 인터넷침해대응센터의 자료에 의하면 2010년 악성코드 유포지/경우지 사이트 피해기관(도메인) 중 기업이 차지하는 비율은 63%로 전체 6,674건 중 4,212건에 이른다.[2]

이와 같은 제한된 예산과 잘못된 정보보호 인식은 기업들의 정보보호 정책을 사후대응 위주로 수립하게 만든다. 하지만 정보보호에 있어 사후대응 위주로 일관하는 대응체계 보다 예방 위주의 대응체계 운영이 효용성과 비용면에서 더 우수하다.[3][4] 정보보호 정책은 제도적 예방조치 수행과 기업 내부적으로 수립된 침해 예방 대응체계의 이행을 통한 방식으로 전환되어야 한다. 본 연구를 통해 침해사고 예방을 위한 보호조치의 중요성을 평가하고 기업들의 적극적인 침해 사고 예방을 위한 효과적인 침해위협 관리 모델을 제시한다.

II. 기업의 침해사고 예방을 위한 제도

2.1 정보보호 안전진단

정보보호 안전진단 제도의 목적은 주요정보통신서비스제공자, 집적정보통신시설사업자, 쇼핑몰 등의 정보통신서비스제공자의 정보통신망에 대한 침해사고 예방을 위함이다. 이 제도를 통해 기업은 관리적, 기술적, 물리적 보호조치 영역에서 48가지의 세부조치 사항에 대한 점검 및 정책을 수립할 수 있다.[5]

2003년 1.25인터넷침해사고로 인해 ISP, 쇼핑몰 등의 낮은 보안수준이 사회적 문제로 지적되며 정보보호조치 강화에 대한 필요성이 제기되었다. 이에 정보통신서비스의 정보보호 수준을 강화하여 안전한 이용기반을 조성하고자 관련법규들의 개정과 정보보호안전진단 제도를 도입하였다. 이로써 정보통신서비스 매출이 100억원 이상이거나 3개월간의 일일평균이용자가 100만명 이상인 사업자은 매년 정보보호 안전진단을 받아야 한다.

2.2 정보보호관리체계(ISMS)

정보보호 안전진단이 정보통신망의 안전성 확보를 위해 주요 정보통신서비스제공자를 대상으로 관리적, 기술적, 물리적 보호조치 항목에 대한 이행 여부를 점검하는 내부위험관리제도라면 ISMS는 조직에 적합한 수준의 정보보호를 제공하기 위해 정책 및 조직을 수립하고 위험관리, 대책 구현, 사후 관리 등의 정보보호 관리과정을 유기적으로 통합 운영하는 체계이다.

ISMS 인증제도는 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립・문서화 하고 지속적으로 관리・운영하는 시스템 즉, 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 체계에 대하여 제3자의 인증기관(한국인터넷진흥원)이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도로 관리체계가 없는 부분적 보안, 일회성 관리, 산발적 대응 방식을 균형적 보안, 지속적 관리, 체계적 대응 방식으로 개선시켜 준다. 이 제도 역시 기업의 주요 정보자산 유출 및 피해를 사전에 예방하고 대처할 수 있도록 하는데 목적이 있다.[6]

2.3 ISO 27001

ISO 27001이란 정보보호관리체계 요구사항(Information Security Management System Requirements)으로 정보보호관리체계에 대해 국제 인증시 요구사항을 정의하고 있다. ISO 27001 인증제도는 표준화기구에서 제정한 보안정책, 자산분류, 위험관리 등 11개 도메인, 133개 통제항목에 대한 심사를 진행하며 이미 검증된 국제적인 표준으로써 전 세계 선진

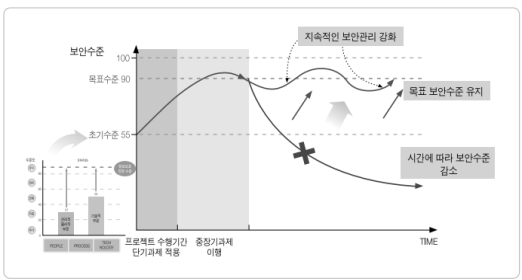
기업이 합의한 Best Practice를 활용해 자사에 적용할 수 있는 장점이 있다.

우리나라의 ISMS는 방송통신위원회 고시, TTA 표준에 근거한 인증 제도라는 차이가 있으며, 특히 KISA ISMS는 ISO/IEC27001 국제표준을 모두 포함하고 있으며 국내 상황에 맞게 침해사고 예방, 암호화, 전자거래 등의 보안요건을 강화하였다.

2.4 침해사고 예방을 위한 제도적 한계

기업의 침해 사고를 효과적으로 예방하기 위해서는 내부원들의 보안 의식(Awareness)이 매우 중요하다. 침해사고 예방을 위한 가장 효과적인 대응체계는 자신의 기업에 적합한 위험관리(Risk Management) 전략수립을 통해 시작된다. 기업마다 다른 환경의 정보통신망과 자산을 운영하기 때문에 침해 위협으로부터 자산을 보호하거나 피해가 발생할 경우 피해를 최소화 시키려면 반드시 해당 기업에 특화된 대응체계 수립이 필요하다. ISO 27001과 같은 표준도 검증된 선진기업들의 유형분석이 반영되어 있지만 이러한 제도적 보완책이 시행되는 동안 피검자인 기업들은 수동적으로 대응하는 경우가 많아 효과가 반감된다. 이러한 현상은 인증제도가 가지는 시행특성으로 피검자의 목표가 인증제도의 취지에 맞는 목표설정 후 달성 과정에 있지 않고 인증 과정 통과에 목적을 두는 경우가 많기 때문에 발생한다.

대부분 제도적 보완작업을 수행하는 기업들은 〔그림 1〕과 같이 침해사고 대응을 위한 프로젝트 수행기간 최고조의 보안수준을 유지하다가 인증 과정이 종료되고 정작 기업의 서비스가 제공되는 과제 이행기에는 지속적인 보안관리 부족으로 목표 보안수준보다 낮은 보안수준을 유지하게 되고 이는 시간에 따라 점감되는 형태를 보인다. 제도적 인증 후 보안조치 시행을 통해 수립된 정책의 실행과정을 점검할 수 있으나 〔그림 2〕



〔그림 1〕 기간별 보안수준

Top 10	2009년 ISMS 인증 기업 보안관리 결함(50개 기업)	결함건수	발생비율
1	관리자 계정 등 주요 패스워드 관리 미흡	14건	28%
2	개인정보보호법 등 법적 요구사항 준수 미흡	13건	26%
3	내부 보안감사 지적사항 조치 미흡	12건	24%
4	정보보호 직무에 대한 책임과 역할 불명확	11건	22%
5	사용자 접근권한에 대한 정기적인 점검 미 이행	11건	22%
6	주요시스템 보호를 위한 네트워크 대책 미흡	11건	22%
7	주요 정보자산의 변경관리 절차 미흡	10건	20%
8	백업관련 지침(계획) 부재 및 미 준수	10건	20%
9	정보보호시스템 접근통제 정책(Rule Set) 검토 미흡	10건	20%
10	보안사고 정의, 대응 복구 절차 등 보안관리 미흡	10건	20%

〔그림 2〕 ISMS 인증기업 보안관리 결함 통계

와 같이 정보보호관리 체계 수립 이후 기업들의 보안관리 결함 발생률은 매우 높다.〔7〕〔8〕 실질적으로 현재의 제도 기반의 점검과 정책 수립만으로는 실제 기업들의 침해사고 예방을 위한 해결책이 될 수 없다.

III. 기업의 침해사고 위협 현황 - 사례 연구

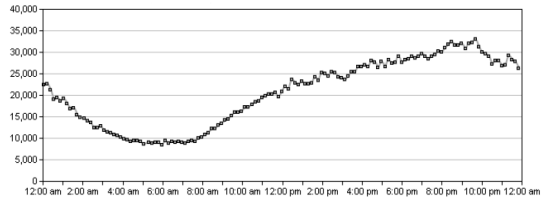
보다 효과적인 기업의 침해사고 예방 대응책에 대한 연구를 위해 현행 제도적 예방 조치를 충실히 수행중인 기업의 실제 침해사고 위협 현황을 살펴볼 필요가 있다. 정보보호 안전진단을 통해 수립된 보호조치가 적용된 시스템으로부터 관리적 정보보호지침에 따라 서비스 시스템 로그를 수집하고 이를 분석해 2010년 1월부터 12월까지의 침해 위협 상황을 분석해 보았다.

3.1 침해위협 정보 수집

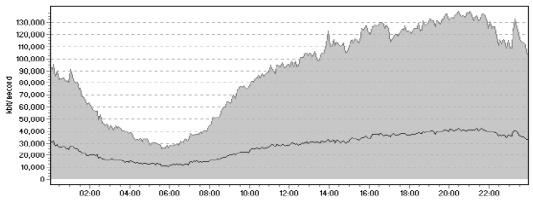
사례 연구를 위한 대상 기업은 안전진단대상자 범위 내의 사업자로 매년 제도적 예방 조치를 수행하고 있다. 침해 위협 유형을 수집한 서버 영역은 로그 분석의 효율성을 위해 하루 최대 동시 세션을 35,000 세션으로 설정하여 구성하였으며 수집기간인 2010년 1월부터 12월 동안 특별히 유입되는 세션 수를 늘리거나 줄이지 않았다. 〔그림 3〕과 〔그림 4〕는 수집 기간 중에 하루 시간대별 동시 세션 수 및 네트워크 대역폭 모니터링 자료이다.

3.2 수집된 침해위협 분석

수집된 침해 위협 정보에 대해 각 위협들이 발생할 수 있는 조건과 결과의 특성을 기준으로 5가지 유형으로 분류하였다. 〔표 1〕은 나눠진 유형별로 실제 기록된 침해 시도 횟수와 비율을 나타낸다.



〔그림 3〕 서비스 장비 동시 세션수 모니터링



〔그림 4〕 서비스 장비 네트워크 대역폭 모니터링

대부분 의도된 침해 위협의 경우 Reconnaissance 작업이 선행되기 때문에 무작위적인 Traffic 위협과 Reconnaissance 유형을 제외한 나머지 경우를 대상으로 보면 〔표 2〕와 같이 Network Equipment 위협이 전체의 58.61%를 차지하게 된다. 하지만 Network Equipment 공격의 대부분은 장비 자체에 대한 침해 행위 보다는 장비의 취약점을 이용한 Spoofing을 통해 Vulnerability나 Security Policy 유형의 의도된 침해 행위를 위한 선행 작업으로 해석된다.

결국 악의적 침해 위협 유형은 〔표 3〕과 같이 Vulnerability 유형이 6.20%이고 Security Policy 유형이 93.80%로 나타나 잘못된 보안정책 운영이 실제 기업의 서비스나 자산에 얼마나 큰 위협이 되는지 알 수 있다.

〔표 4〕와 〔표 5〕는 Security Policy 유형과 Vulnerability 유형의 세부적인 침해 위협 이벤트에 대한 통계 자료이다. 세부적인 침해 위협 이벤트들의

〔표 2〕 침해 위협 유형별 통계치

Network Equipment	Security Policy	Vulnera-bility	계
10,962	7,261	480	18,703
58.61%	38.82%	2.57%	100%

〔표 3〕 악의적 침해 위협 유형별 통계치

Security Policy	Vulnerability	계
7,261	480	7,741
93.80%	6.20%	100%

Trace 정보를 통해 알 수 있듯이 이들 침해 유형은 시도 자체가 시스템의 위협이 되고 사고에 대한 예방이나 관리의 기회가 주어지지 않고 즉시 사후 대응 단계로 진행되기 때문에 매우 심각한 위협이 된다.

3.3 보호조치 평가 및 개선점

제도적 예방 조치는 기업의 침해사고 예방을 위해 반드시 필요하다. 실제 수집된 로그를 분석한 결과 기업의 침해 위협 중 예방을 위한 보호 조치가 수행되어 있지 않은 경우 즉시 침해사고로 인한 피해가 예상되는 침해 위협은 전체 위협 중 4.73%(표〔1〕의 총위협에서 표〔3〕의 총악의적침해위협 비율)에 이른다.

정보보호관리체계를 통한 정보보호 조치가 이행되고 있는 상황에서도 안심할 수 없는 부분은 Vulnerability 유형의 침해 위협이다. 기업의 영속적 영업 행위는 끊임없이 자사의 정보자산이나 서비스 시스템에 새로운 취약점을 야기할 수 있다. 부서원의 이동과 같은 물리적 변화부터 새로운 서비스 모듈의 업데이트를 통한 소프트웨어적인 변화까지 새로운 취약점이 생성될 수 있는 곳은 다양하다. 결국 정보보호조치가 시행되고 있는 매순간 새로운 침해 위협의 발생에 대비

〔표 1〕 침해 위협 부류별 통계치

유형	Traffic	Reconnaissance	Network Equipment	Security Policy	Vulnerability	계
발생조건	DDoS 및 패킷오류	사전조사 및 보안정책 조회	기능부족 및 취약점	잘못된 설정 및 보안정책	보안 취약점	
예상결과	시스템 부하	시스템 부하 및 추후 공격	시스템 부하 및 추후 공격	시스템 오류 및 악의적 해킹	시스템 오류 및 악의적 해킹	
기록건수	98,393	46,280	10,962	7,261	480	163,376
비율	60.22%	28.33%	6.71%	4.44%	0.29%	100%

〔표 4〕 Security Policy 부류 세부 위협

Code	Layer	Trace	Frequency
S-1	HTTP	SQL Server Error Response Gathering	91
S-2	SSH	Invalid SSH Login Attempt	18
S-3~4	SQL	Invalid SA Login Attempt	5,426
S-5~12	HTTP	SQL Injection using Invalid Identity	638
S-13~15	HTTP	Cross Site Scripting (Form-Data)	73
S-16	HTTP	Paros Proxy HTTP Request	1,015

해야 하며 가장 효과적인 침해사고 예방 조치는 위협에 대한 사전 탐지이다. 사전 탐지를 위해서는 보호조치 시행은 물론 기업의 특성에 맞는 침해 위협의 분류와 지속적인 모니터링을 통한 통계 처리와 위협들의 선후 관계 분석이 필요하다.

IV. 침해위협 예방을 위한 효과적인 관리 모델

기업의 침해사고 예방을 위한 제도적 보완장치가 모든 기업들의 정보보호 이슈를 제거하지는 못한다. 대부분의 제도적 보완장치는 수행기관과 대상자간의 점검 및 목표 설정, 모델 적용이 한계이고 실제 상황에서는 진단대상자 내부의 실행조치가 더욱 중요하다.

4.1 선행 위협 관리 모델

앞서 연구 자료를 통해 실제 보호조치가 수행되고 있는 실제 기업의 위협 상황을 살펴보았다. 효과적인 기업의 침해사고 예방을 위해서는 해당 기업의 내부원들이 자사가 보유한 자원과 자사가 제공하는 서비스, 회원, 외부 환경 등의 요소들에 대한 깊이 있는 이해가 반드시 필요하다. 이와 같이 보호되어야할 자원과 환경에 대한 이해로부터 침해 예방 모델은 수립되어야 하며 포괄적, 표준에 의한 모델이 구체화되고 개별화된 모델을 우선할 수 없을 것이다.

본 연구를 통해 수집된 위협의 5가지 부류들은 각기 위협의 대상과 목적이 상이하지만 모든 위협이 현실화 되었을 경우 최종적인 목적은 공격자의 의도한 바와 같게 된다. 이러한 특성은 범죄 성공을 위한 과

〔표 5〕 Vulnerability 유형에 대한 세부 위협

Code	Layer	Trace	Frequency
V-1~3	HTTP	Cross Site Scription Attack (POST, GET, Header)	177
V-4	HTTP	SQL Injection using CMDShell	27
V-5	RTSP	Negative POST Content-Length using Buffer Overflow	2
V-6	HTTP	Login Bypass using Telnetd Vulnerability	179
V-7	HTTP	Microsoft Jet Database Engine Buffer Overflow	2
V-8	WINS	Name Validation Vulnerability	93

정상의 특징이 부분적으로나마 그대로 사이버범죄로 이어져 나타나기 때문이다. 즉, 모든 범죄는 준비, 계획, 이행의 단계를 필요로 하고〔9〕 이러한 특성에 따라 침해 위협 역시 관리되어질 수 있을 것이다.

결국 지금까지의 제도적 침해 대응체계의 한계는 각 기업에 특화되고 개별화된 위험관리 사이클을 통해 예방→탐지/분석→대응→복구 일련의 과정을 반복하면서 평가되고 목표한 수준의 보안수준을 설정하고 이를 유지하기 위한 모델로 변화되어야 할 것이다.즉, 앞서 살펴본 제도적 예방책은 반드시 기업의 침해 현황과 맞물려 기업의 내부시스템으로 이식되어야만 설정된 보안수준을 유지할 수 있다. 수립된 정보보호 관리체계 하에 운영되는 기업의 실제 위협 현황을 일정기간 수집하고 분석하여 해당 기업에 특화된 침해 예방 및 대응 체계의 도출 과정이 인증 과정 이후에도 반복 시행되어야 한다.

선행 위협 관리 모델은 이러한 현행 제도적 대응체계에서의 부족한 점을 보강해 줄 수 있다. 침해 위협 관리에 범죄 성공의 과정상의 특징을 접목시켜 각 위협들을 그룹화 하고 해당 위협이 준비 단계의 위협인지 계획 단계의 위협인지 이행 단계의 위협인지를 관리하도록 한다. 이를 통해 각 단계별 위협 요소들이 관리되고 선후관계의 위협들이 관리될 수 있어 보다 실질적인 운영상의 위협 관리 모델이 될 수 있다. 또한, 단계별 목표 수준을 수립할 수 있으며 목표 지향적인 관리 업무가 가능해져 담당부서나 자원에 대한 성과측정 과정에도 기여할 수 있게 된다.

4.2 선행위협 관리 모델 예상 효과

제도적 보완장치가 주는 사전 점검 및 관리체계구축의 효과와 기업의 침해사고 현황에 맞는 개별적 대응체계가 유기적으로 연동될 필요가 있다. 제도적 침해예방을 통한 대응체계를 구축함으로써 침해사고 분석과 신속한 경보가 가능해지고, 정보수집 및 새로운 기술의 적용, 자원의 관리적 운영 등 모든 보안요소들에 대한 준비작업에 효율성은 재고되지만 기업의 특성을 파악하고 기업 환경에 맞는 보안 대책과 침해 유형 분석을 통한 대응체계를 수립하지 못하면 효과적인 사전 탐지의 실패와 실제 침해사고 발생 상황에서 최선의 조치를 취할 수 없다.

앞 장에서 살펴본 침해 위협 분석과 같은 과정을 통해 해당 기업이 평상시 겪고 있을 침해 상황을 모델링해 볼 수 있다. 이러한 통계 자료는 서비스 시스템에 대한 침해 위협에 효과적으로 대응하기 위한 관리 모델을 설계하는데 도움이 된다. 운영 자원의 유한성을 고려했을 때 가장 최적화된 관리 모델은 모니터링 및 예방 작업의 효율성을 극대화 시켜준다.

4.2.1 침해 상황 모델링 - 위협현황 분석 및 관리 목표 설정 효과

본 연구를 위한 침해 유형 수집기간 동안 수집된 총 위협 시도수가 163,376회라면 정상 서비스 중인 기업의 네트워크 트래픽 중에 하루 평균 447회 이상의 비정상적인 트래픽이 존재하고 이중 19.7회는 자사 시스템의 보안 정책이 완벽하지 않을 경우 서비스 오류 및 침해사고 발생이 가능한 위협 시도로 해석된다.

X=163,376 (12개월간 기록된 총 위협 시도횟수), Y=447 (일 평균 공격횟수, 365일 무정지 서비스 가정)

a=4.44% ([표 1]의 Security Policy 유형 비율), b=0.29% ([표 1]의 Vulnerability 유형 비율)

연구 모델에서의 하루 평균 침해사고 위협 건수 : aY=19.7 회, bY=1.3 회

위 결과가 보여주는 의미는 매우 심각하다. 대상 기업과 유사한 조건의 기업이 [그림 3]과 [그림 4]가 보여주는 수치와 비슷한 네트워크 상황으로 운영되고 있는 서비스 시스템이 있다면 해당 시스템의 경우 하루 평균 1.3회 이상의 취약점 공격에 노출되어 있다고 볼 수 있다. 즉, 단 하루라도 보안 취약점 패치가 늦어진다면 이미 해당 시스템이 운영 중인 서비스의 오류나 침해 사고가 발생했다고 볼 수 있는 근거가 된다.

정의 1. 순간위협율: 시스템이 처리하고 있는 동시 세션 중에 위협이 되는 세션이 갖는 비율

네트워크 서비스 시스템의 순간 위협율을 동시 처리 가능한 정상 세션 대비 비정상 세션의 비율로 정의한다면, [그림 3]을 기준으로 평균 서비스 상태에서의 세션 수를 20,000으로 설정하고 하루평균 447회 발생할 비정상적인 트래픽이 순간에 몰릴 경우 전체 서비스 세션 중 2.2% 가량의 세션은 언제든 순간 위협이 될 수 있다.

정의 2. 선행위협: 특정 위협이 발생하기 위해 일반적으로 요구되는 사전 작업 또는 위협 시도

정의 3. 순차위협율: 선행위협이 발생된 이후 특정 위협이 연속하여 발생될 가능성

어떠한 위협이 발생되기 전에 순차적으로 발생되는 위협 중 먼저 발생한 위협을 선행위협이라고 하면 Reconnaissance 유형의 위협은 대부분 이후 위협을 위한 선행위협으로 분석되기 때문에 실제 위협관리의 대상으로 보기 보다는 선행위협으로의 관리가 필요할 것이다. 즉, Reconnaissance 〉 Network Equipment 〉 Security Policy or Vulnerability 이라는 순차적 위협 발생 상황을 가정하면 선행위협의 발생비율을 1이라고 보고 향후 순차적 위협 발생율을 상대적으로 나열하면 Network Equipment 유형은 0.24가 되고 다시 Network Equipment 유형이 Security Policy 유형과 Vulnerability 유형의 선행위협이라고 보면 Security Policy 유형은 0.66, Vulnerability 유형은 0.04의 순차위협 관계도를 갖게 된다.

정리된 [표 6]의 내용을 해석해 보면 해당 기업의 서비스 시스템에 대한 취약점을 스캔하는 위협이 발생한 후에 실제 의도적 공격을 위한 순차위협이 발생할 확률이 24%에 이르며, 이후 적극적인 공격시도로 Security Policy 유형의 위협이 발생할 확률은 66%, Vulnerability 유형의 위협이 발생할 확률은 4%가 된다.

〔표 6〕 침해 위협 부류별 순차 위협 관계

위협 관리모델 요소	순차위협율
Reconnaissance	1
Reconnaissance → Network Equipment	0.24
Network Equipment → Security Policy	0.66
Network Equipment → Vulnerability	0.04

4.2.2 관리모델 및 관리지표 설정 - 개별화된 대응체계 수립 효과

보호조치가 시행 중인 기업의 침해사고 대응 모델의 효율을 극대화시키기 위해서는 앞서 살펴본 순차적 위협 발생 상황에 대한 초기 대응이 중요하다. 또한, 공격 유형의 특성별 관리 단위를 설정하여 선행공격이 발생한 이후 대응 시스템이 즉시 기동될 수 있도록 대비해야 한다. 공격 시도가 기록된 IP 들의 경우 대부분 시간차를 두고 같은 서브넷의 다른 IP들도 비슷한 시도가 기록되며 특히 PC방의 경우 지속적인 서브넷 감염이 진행되고 있는 것으로 의심된다.

〔표 7〕의 내용은 사례 연구의 결과로 작성된 해당 기업에 최적화된 침해 위협에 따른 관리 모델이다. 기업이 관리해야할 침해 위협을 그룹화 하였고 해당 그룹들이 갖는 특성을 의미있는 시간 동안의 로그분석을 통해 정립할 수 있었다. 각 그룹에 소속된 침해 위협이 다른 침해 위협과의 선후 관계에서 어떻게 관리되어야할 것인지가 정의되어 있고 각 그룹들의 관리 영역과 처리 기준은 세부지침을 통해 완성할 수 있다.

살펴본 바와 같이 실제 기업 내부의 위협상황은 각기 다를 수 있다. 가장 효과적인 관리 모델을 수립하기 위해서는 자체적인 위협에 대한 분석과 감사가 필수적이다. 본 연구의 사례분석을 위해 수집된 위협 현황을 통해 제시된 관리 모델은 다른 기업들의 대응 모델 수립에 참고가 될 수 있다.

4.2.3 결과 고찰

모든 선행 위협이 내부 관리를 통해 제어될 수는 없다. 선행 위협의 절대적 수치 관리는 ISP 또는 국가 수준에서 이뤄지는 정책에 의존할 수밖에 없다. 하지만 기업의 효과적인 침해 위협 예방을 위해서는 외부로 규정된 위협들에 대해서는 대외협업을 통한 세부수칙을 수립하고 내부로 규정된 후행 위협과 적극 대응형 위협에 대해서는 운영 중인 서비스에 특화된 세부수칙을 수립할 필요가 있다. 대부분의 기업들이 보호조치 장비나 관제 서비스를 통해 보고된 침해 위협 리포트에 의존하여 수동적이고 사후 대응으로 일관하는 정보보호조치 이행 상황에서는 적극적인 침해사고 예방 효과를 기대할 수 없다.

기업 내부 상황에 맞는 침해 위협 관리 모델 수립을 통해 관리지표를 설정하고 해당 지표관리를 중심으로 위험관리 사이클을 수행하는 경우 보호조치 시행 과정상의 결함 발생률을 낮추고 제도적 보호조치의 운영평가를 위한 이행확인이나 개선권고시에 매우 중요한 요소로 활용될 수 있다.

기업의 이러한 노력도 매우 중요하지만 국가적인 침해사고 위협관리 체계에 의한 선행형 위협 관리 지표 설정과 이를 낮추기 위한 노력이 반드시 필요하다. 선행형 위협의 경우 일반적인 기업 시스템에서는 원천적인 관리가 불가능한 외부 위협으로 국가적인 위협 비용으로 관리되어야 할 것들도 있기 때문이다. 기업들의 이러한 대응 모델 수립과 관리 지표 운영은 예산의 활용 평가 기준이 될 수 있고 또한, 기업들의 선행형 위협을 관리지표로 활용한다면 국가 사이버 보안 시스템의 효율성을 검토할 수 있는 중요한 자료가 될 수도 있다.

〔표 7〕 침해 위협에 따른 관리 모델

위협 유형	선행형	후행형	적극대응형	자원관리형
위협 부류	Reconnaissance	Network Equipment	Security Policy Vulnerability	Traffic
관리 지표	후행형 전이 24% 미만 유지	적극대응형 전이 66% 미만 유지	각 케이스별 추적 및 감사 기록 의무	네트워크 자원 관리
관리 영역	외부	내부	내부	외부
처리 기준	ISP, 사이버수사대 협조	모니터링 강화 및 전이 추적	케이스별 인력 할당 및 수동 처리	ISP, 사이버수사대 협조

V. 결론

본 연구를 통해 기업이 침해사고 예방을 위해 취할 수 있는 효과적인 침해 위협 관리 모델을 살펴봤다. 연구 자료 분석을 통해 제도적 범위에서 취할 수 있는 사전 예방 작업으로써의 정보보호 안전진단이나 ISMS와 같은 관리체계의 기대 효과를 평가하였다. 제안된 관리 모델을 통해 기업의 위협 현황 분석은 물론 실질적인 침해 위협 관리 지표 수립과 목표 지향적인 대응이 가능함을 보였다.

본 논문에서 제시된 관리 모델은 실제 서비스를 제공하는 다른 기업들의 보안 정책 수립과 운영을 위한 견본이 될 수 있다. 국가적 사이버 테러 수준 관리를 위해서는 기업들의 체계화된 관리 모델 수립이 함께 이뤄져야 하며 이와 함께 기업 외부에서 관리되어야 할 위협들에 대한 국가적 관리 정책도 함께 협력되어야 함을 지적했다. 또한, 기업들간의 이질적인 내부 위협 상황과 원활한 상업적 서비스 운영을 위해서는 극단적 위협 관리를 할 수 없는 현실 또한 고려되어야 할 것이다. 이러한 이슈들은 향후 추가적인 연구를 통해 민간 수준에서의 기업 침해사고 예방을 위한 통합 위협관리센터의 수립과 이를 통한 효율적인 공조대응 모델의 연구 필요성을 보여준다.

참고문헌

〔1〕 ITU-D, Measuring the Information Society, 2010

〔2〕 한국인터넷진흥원, 인터넷 침해사고 동향 및 분석 월보, 2010년 12월

〔3〕 공희경, 기태성, 정보보호 투자효과에 대한 연구 동향, 정보보호학회지 제17권 제4호, pp. 26-33, 2007년 8월.

〔4〕 한국인터넷진흥원, 정보보호 사전점검 제도 활성화에 관한 연구, 2010년 7월

〔5〕 방송통신위원회, 한국인터넷진흥원, 정보보호 안전진단 해설서, 2010년 3월

〔6〕 한국인터넷진흥원, 정보보호관리체계(ISMS) 인증제도 소개, 2009년 2월

〔7〕 방송통신위원회, 한국인터넷진흥원, 정보보호관리체계(ISMS) 인증 모범사례, 2010년

〔8〕 장상수, 이호섭, 정보보호관리체계 인증심사 결함사항 분석에 관한 연구, 정보보호학회지 제20권 제1호, pp. 31-38, 2010년 2월.

〔9〕 Susan W. Brenner, “Cybercrime: re-thinking crime control strategies”, Crime Online, Willan Publishing, NCJ 218883, pp. 15, 2007.

〈著者紹介〉

강 신 범 (Shin-Beom Kang) 정회원
1997년 2월: 전북대학교 정보통신공학과 졸업
1999년 2월: 전북대학교 정보통신공학과 공학석사
2012년 2월: 고려대학교 정보보호대학원 공학박사
현재: (주)티앤에스 대표이사
소프트포럼 기술개발실장 / 전략기획본부장, 국정원 CA 보호프로파일 개발 연구위원, 국내 최초 인터넷뱅킹 시스템 개발 및 상용화, KTH 신사업전략팀장 / 금융사업TF장
〈관심분야〉 정보보호정책, 암호 프로토콜, 금융보안시스템, 통신공학 등

이 상 진 (Sang-Jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 졸업
1989년 2월: 고려대학교 수학과 이학석사
1994년 8월: 고려대학교 수학과 이학박사
1989년 10월 ~ 1999년 2월: ETRI 선임연구원
1999년 3월 ~ 2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월 ~ 현재: 고려대학교 정보보호대학원 정교수
고려대학교 디지털포렌식연구센터 센터장, 한국디지털포렌식학회 편집이사, 세계포렌식경진대회 2년 연속 세계1위, 경찰청 휴대폰증거분석협의체 자문위원 등
〈관심분야〉 대칭키 암호, 정보은닉, 디지털포렌식 등

임 종 인 (Jongin Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
1986년 3월 ~ 2001년 1월: 고려대학교 자연과학대학 정교수
2001년 2월 ~ 현재: 고려대학교 정보보호대학원 원장
대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 방송통신위원회 인터넷협의회 운영위원 등
〈관심분야〉 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등