제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

네트워크 보안수준 평가를 위한 위험 분석 방법에 관한 연구

박원주*, 서동일*, 김대영**

* 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀

** 충남대학교 정보통신공학과

요 약

기업 네트워크 환경 및 인터넷 상에서 발생할 수 있는 보안상의 취약점들은 악의를 가진 내외부의 공격자들에게 악용될 가능성이 있다. 이러한 상황은 기업으로 하여금 정보 자산의 유출 및 파괴 등의 물리적인 피해와 더불어 복구를 위한 인력 및 시간의 소요 등 금전적인 손해를 야기시킨다. 이에 정확한 네트워크 보안 위험을 분석하여 이러한 피해의 가능성을 사전에 파악하고, 예방할 수 있는 방안을 마련하여 최대한의 보안성을 확보하여야 한다. 본 고는 이를 해결하기 위한 네트워크의 보안 수준을 측정하고 분석할 수 있는 방법론을 살펴보고, 적절한 평가 절차 및 평가 수행 방법, 점검 항목을 해외이 대표사례와 국내 업체의 위험 분석 방법론 관하여 살펴본다.

1. 서 론

기업 네트워크 환경 및 인터넷 상에서 발생할 수 있는 보안상의 취약점들은 악의를 가진 내외부의 공격자들에게 악용될 가능성이 있다. 이러한 상황은 기업으로 하여금 정보 자산의 유출 및 파괴 등의 물리적인 피해와 더불어 복구를 위한 인력 및 시간의 소요 등 금전적인 손해를 야기시킨다. 이에 정확한 네트워크 보안 위험을 분석하여 이러한 피해의 가능성을 사전에 파악하고, 예방할 수 있는 방안을 마련하여 최대한의 보안성을 확보하여야 한다. 그러나 현재 실제 업무 환경에서는 보안조치(safeguard)를 적용할 때 네트워크의 보안 수준이 어느 정도 되며 (AS-IS), 또 어느 정도로 보안조치(safeguard)를 적용하여 보안 수준을 향상시켜야 할지 (TO-BE) 에 대한 정확한 판단 기준이 없는 실태이다. 이를 해결하기 위하여 현재 네트워크의 보안 수준이 어느 정도 되는가에 대한 분석 평가를 할 수 있는 방법론을 구축하고 적절한 평가절차 및 평가수행방법, 점검 항목이 필요한 실정이다. 이에 본 고는 위험을 분석하는 방법론 관하여 2절에서 해외 방법론 및 사례를 조사하고, 3절에서 현재 국내의 위험 분석 방법론을 살펴본다. 4절에서 국내의 취약성 점검 방법론을 검토한 후 네트워크 보안 수준을 측정하는 방법에 대하여 서술한 후, 5절에서 결론을 맺는다.

2. 해외에서의 위험분석 방법론

전세계적으로 많은 위험분석 방법론이 있으며 적용분야 및 분석 대상 정보시스템 환경에 따라 위험분석 방법론들이 차이점을 보이고 있다. 각 위험분석 모델은 사용자의 특정 환경이나 목적과 관련없이 일반적인 위험분석을 위하여 구성되어 있기도 하고 위험분석을 하고자 하는 사용자의 특성에 맞게 구성되어 있기도 하다.

해외 방법론 조사는 선진 위험분석 모델에 관한 평가기준을 토대로 이들 모델의 특징과 장단점을 수렴하여 국내 환경에 적합한 접근방법을 제시하기 위함이다.

2.1 영국(BSI)의 RA 방법론

RA는 BS7799의 Part 2에 따라 ISMS (Information Security Management System) 구축 지원을 포함하여 회사의 정보보호 경영을 향

상시키기 위하여 BS7799 Parts1과 2를 적용하도록 도와주는 완전히 BS7799에 특화된 위험분석 모델이다. 따라서 RA의 위험분석 수행결과는 인증 심사 시 BS7799 심사원에게 BS7799 part 2 규격서의 모든 과정을 수행하였음을 증거로 제시할 수 있는 장점이 있다. RA는 다음과 같은 5단계로 실시된다.

- 자산 중요성 평가 및 자산 그룹핑
  - 정보자산에 대한 보안 요구정도를 기밀성, 무결성, 가용성에 따라 평가
  - 해당 위험의 발생 빈도나 가능성을 기준으로 High, Mid, Low로 평가
  - 자산평가 결과를 바탕으로 비슷한 평가와 속성을 가진 자산들을 그룹핑
- 잠재 위험 파악
  - 파악된 취약점들을 기반으로 발생 가능한 위험을 파악
- 현 통제 파악
  - 자산관리자와의 인터뷰를 통해 파악된 잠재 위험에 대한 통제(safeguard)의 존재 유무와 실효성을 평가
- 위험 평가
  - (자산중요성평가값+위협, 취약점 평가 X 2)
  - 변형 가능
- 통제적용 및 관리
  - DOA(degree Of Assurance)에 따라서 자산별 개별 위험에 대한 통제를 적용.

RA의 방법론은 위험분석의 기본적 개념을 충실히 수용하고 있는 방법으로 위험분석을 처음 적용하는 조직이나 소규모의 조직에는 적용의 용이성 등의 이유로 적합하다고 할 수 있다. 하지만 수많은 정보시스템, 네트워크 자산을 가진 조직에서 효과적인 위험관리시스템으로 사용하기에는 기능이나 효과성 면에서 미흡하나 RA의 기본적 개념을 적용하여 조직 상황에 맞추어 변형하여 사용한다면 유용한 방법론 중의 하나가 될 수 있을 것이다[1]

2.2 영국(CCTA)의 CRAMM 방법론

CRAMM (CCTA Risk Analysis and Management Method)은 영국의CCTA(Central Computer and Telecommunications Agency)에서 영국 정부기관들의 정보시스템 위험분석을 위하여 개발되었다. 그러나 CRAMM이 자동화도구로 개발되어 민간 조직으로도 사용이 확대되었다. 자동화 도구는 1988년 이래 여러 번의 재검토와 수정이 더해져 현재에 이르고 있으며 기존 방법론의 장점에 더하여 분석과정 및 검증과정을 자동화하고 위험관리기능도 추가함으로써 사용이 확산되고 있다.

- 물리적인 자산, 소프트웨어 및 데이터 자산의 파악및 평가
  - 시스템 자산에 관한 파악과 가치 산정
  - 대상 조직의 보안요구사항을 결정
- 위협분석, 취약성 분석, 위험평가
  - 자산 그룹에 대한 취약성과 위협의 수준을 측정, 평가
  - 보안이 필요한 부문을 파악, 시스템과 관련한 모든 위험에 대한 분석 수행
- 현 시스템에 대한 대응책 파악 및 필요 대응책 선택
  - 위험분석의 효과를 극대화하기 위하여 위험관리 포함
  - 위험을 감소시키기 위하여 필요 대응책과 개선안 마련

각 단계에서 또한 거쳐야 할 것은 단계 동의(Stage Agreement) 부문으로, 각 단계에서 산출된 발견 사항 및 결과들의 정확성을 관리층에게 검증토록 하고 알림으로써 분석의 정확도를 높이고 시스템 관리자, 보안관리자, 관리층 모두가 위험분석에 참여하도록 하고 있다. 뿐만 아니라 자동화 도구로 구현된 CRAMM의 장점은 보안 시스템을 설계할 때에 위험분석을 적용할 수 있도록 하는데 있다. 물론 많은 자동화 도구가 이러한 기능을 가지고 있지만 CRAMM은 특히 이러한 기능이 강하다. 위험분석의 효과를 극대화

하기 위하여서는 시스템 설계 단계에서부터 위험분석을 적용하여 보안 위험을 최소화 시키는 것이 좋다. 그러나 보안 대응책을 검토하는 과정(Stage 1, 2)에서 잘못 설치/수행된 보안 대응책을 가려내는 작업이 어려운 점이 있는 단점도 있다. [2]

2.3 미국의 NIST 방법론

NIST(National Institute of Science and Technology)는 1979년 "FIPS PUB 65 자동화 데이터 처리에 관한 위험분석 지침서"를 발표하여 정량분석의 기초를 마련하였다. "FIPS PUB 191 LAN 보안을 위한 위험분석 지침서" 및 "Special PUB 500-174 자동화 위험분석 도구 선택을 위한지침서" 등은 위험분석에 관한 모델 및 흐름을 제시하고 있다. NIST 위험분석 모델의 특징은 전반적인 흐름을 제시하고 사용자에게 위험분석 기법의 선택을 자유롭게 함으로서 다양한 환경에서의 적용을 가능하게 하였다. NIST에서 제시한 위험분석 흐름은 (그림 1)과 같이 크게 7단계로 구분할 수 있다.

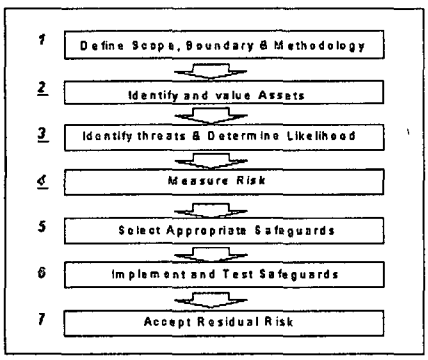

그림 1. NIST의 위험분석 모델

NIST에서 제안한 위험 분석 공식은

Risk = Likelihood of threat occurring X Loss measured

이다. 위 공식은 이미 많은 위험분석 기법이 채택하고 있는 기본 공식이며 발생가능성이 높지만 손실이 낮은 경우와 발생가능성은 낮지만 손실이 높은 모든 경우에 한해서도 비교적 합리적인 결과를 산출해 준다.

2.4 미국의 OCTAVE 방법론

OCTAVE는 Carnegie Mellon University의 SEI에서 1999년에 개발한 위험분석 방법론이다. 정보자산 중심의 위험요소 분석에 중점을 두고 있으며 기존에 연구된 보안 취약점 극복요소를 통한 실용적 위험요소 완화 방안에 초점을 맞추고 있다. OCTAVE 접근방법은 (그림 2)와 같이 3단계와 8가지 절차로 구성되어 있다.

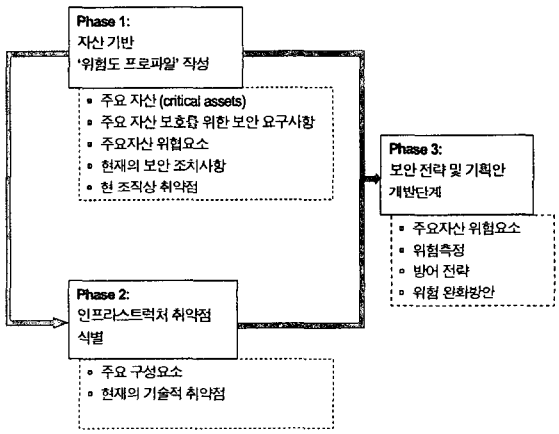

그림 2. OCTAVE 위험분석 3단계

OCTAVE의 위험분석은 IT 부서 및 비즈니스 부서 등 전반적 조직을 대상으로 하고 있으며 관련 부서 및 조직 전 인원에 대한 다각적인 평가를 수행할 수 있는 장점이 있다.[3]

2.5 Cisco의 SAFE 모델

SAFE는 Cisco사에서 제안하는 네트워크보안을 위한 청사진이다. Cisco AVVID(Architecture for Voice, Video, and Integrated Data)를 기반으로 하는 SAFE는 네트워크 설계, 실전 배치(rollout), 관리를 단순화시켜 주는 모듈을 통해 어떤 보안 솔루션을 전체 네트워크에 배치해야

하는지를 명시해 준다. 각 모듈에는 각 네트워크 영역에서 파악된 특정 위협을 줄일 수 있는 보안 및 VPN 요소들이 포함되어 있다

SAFE는 네트워크 아키텍처를 보호하기 위한 가이드의 역할을 하는 것으로, 대규모 캠퍼스 네트워크, 전자상거래나 익스트라넷을 포함하는 엔터프라이즈 네트워크, 중소 규모 네트워크 그리고 원격 사용자 네트워크 별로 크게 구분하여 각각 세부 모듈을 정의함으로써 각 유형별 위협과 이를 완화하는 대책을 제시하고 있다

3. 국내의 위험 분석 방법

현재 국내에서 정보시스템 위험 분석은 조직 자체에서 내부의 역량으로 수행되는 경우는 거의 없으며 다만 간단한 체크리스트나 취약점 분석솔루션을 이용한 내부 시스템 점검이 대부분이다. 국내에서 시행되는 정보시스템 위험분석업무는 크게 정보보호컨설팅과 정보보호관리체계의 인증 도중에 병행하여 이루어진다.

국내에서의 위험분석 방법론은 보안관리를 수행함에 있어 IT자산, 위협, 취약성, 대응책을 중심으로 대상IT조직 환경의 위험을 세부적으로 측정하는 절차와 기술을 말한다. 앞장에서 살펴보았던 것처럼 전세계적으로 수 많은 위험분석

표 1. 국내위험분석 방법론

구분	내용
분석 수준	- 본적 접근 방법 (Baseline Approach) - 상세접근 방법 (Detailed Approach)
측정 방법	- 정량적 방법 (Quantitative Approach) - 정성적 방법 (Qualitative Approach)
분석 도구	- Manual Approach - Tool Based Approach

방법론이 존재하며 국내 보안컨설팅 업계에서도 각자의 방법론을 개발하여 업무에 적용하고 있다. 위험분석 방법론의 선택의 문제는 적용하고자 하는 조직의 정보시스템 환경과 조직특성, 속해진 산업 군에 따라 다양한 방법론을 검토해 볼 수 있으며 적정한 방법론의 선택이 중요하다.

국내의 위험분석 방법론은 크게 (표 1)과 같이 분류 할 수 있다.[4]

4. 국내 취약성 점검 방법론

국내 정보보호전문업체의 정보보호컨설팅 수행방법론을 살펴보면 국외의BS7799, ISO17799, ISO13335, GMITS, OCTAVE와 국내의 정보보호관리체계인증방법론(ISMS, 한국정보보호진흥원) 등을 참고하여 자체 환경에 맞게 수정하여 개발한 것으로서, 환경/현황분석에서부터 자산분석, 위협/취약성분석, 위험분석/평가, 보호대책수립/정보보호모델링, 정보보호정책/지침 등 체계 구현 및 사후 관리의 모듈로 구성되어 있다.

위험분석에 대한 정보보호컨설팅업체들의 일반적인 접근방법은 크게 다른바 없으나 개별 모듈에 대한 분석 기법에는 다소 차이가 있다. (표 2)는 국내의 대표적인 정보보안 컨설팅 업체들의 방법론에 대한 단계별 진행흐름을 요약 비교한 것이다.

5. 결 론

최근까지 정보시스템 보안 관리의 주요 활동으로 개별 정보시스템에 대한 취약점 분석 및 대책 수립이 주를 이루었으나 앞으로는 개별 취약점 분석활동을 통합한 위험분석 및 관리가 필수적인 보안관리 활동이 될 것이다. 또한 자동화된 위험 분석 도구를 개발하여 Tool-Base화된 방법이 주를 이루게 될 것이다. 추가적으로 앞서 언급한 해외 방법론의 장점과 국내 환경에 적합

하게 개발된 위험분석 방법론의 핵심 활동들을 이험 분석 도구에 적절하게 구현하는 것이 중요할 것이다.

표 2. 국내 정보보안컨설팅 방법론 비교

A사	B사	C사
● **현황분석**	● **환경분석**	● **현황파악**
-요구사항분석	-업무현황분석	-업무현황파악
-보안현황분석	-자산파악	-GAP분석
-범위선정	-진단 및 평가	-요구사항분석
● **위험관리**	기준 보완	● **위험평가**
-자산분석	● **정보보안관**	-자산분석
-위협분석	**리체계수립**	-위협분석
-취약성분석	-관리체계진단	-취약성점검
-위험평가	계획수립	-모의해킹
-관리대상위험	-관리체계진단	-취약점분석
선정	-관리체계분석/	-기존보호대책분
● **정보보호**	평가	석
모델링	● **기술적 취약**	-위험평가
-보안조직	**점진단 및 평**	● **체계설계**
-보안지침/절	**가**	-단기대책적용
차	-기술적 취약점	-정보보호체계수
-정보보호체계	진단계획수립	립
수립	-기술적취약점	-솔루션설계구현
-마스터플랜수	진단	-정보보호 정책/지
립	-기술적취약점	침 수립
● **보안관리**	진단/평가	-마스터플랜수립
-보안교육	● **마스터플랜**	● **이행지원**
-기술이전	**수립**	-이행지원 및 모
-사후관리	-이행과제도출	니터링
-유지보수	-우선순위결정	-모의감사
	-Roadmap설정	

참고문헌

[1] British Standards Institution (BSI), "BS-7799," 1999

[2] CCTA, "CCTA Risk Analysis and Management Methodology (CRAMM)," Datapro Reports On Information Security, 1992

[3] OCTAVE, "OCTAVE Criteria, Version 2.0" Carnegie Mellon Software Engineering Institute, 2001

[4] 한국정보보호 진흥원 "위험분석 도구 선정지침", 2002

박원주

1998년 충남대학교 정보통신공학과(공학사)

2000년 충남대학교 정보통신공학과(공학석사)

2000.2 ~ 현재 한국전자통신연구원 정보보호연구단 재직

서동일

1989년 경북대학교 전자공학과(공학사)

1994년 포항공과대학교 정보통신공학과(공학석사)

2002년 충북대학교 전자계산학과 박사과정 수료

1989. 1.~1992. 2. : 삼성전자종합연구소

1994. 3.~현재 한국전자통신연구원 네트워크보안구조연구팀장

김대영

1975년 서울대학교 전자공학과(공학사)

1977년 KAIST 전기 및 전자공학과 (공학석사)

1983년 KAIST 전기 및 전자공학과 (공학박사)

1983.5 ~ 현재 충남대학교 정보통신공학과 교수