데이터 자산의 위험분석 방법론 설계

정윤정, 김인중, 이철원

국가보안기술연구소

The Design for Risk Analysis Method of Data Asset

Yoon-jung Jung*, Injung Kim, Cheolwon Lee

National Security Evaluation Institute

요 약

현대는 정보의 홍수라고 할 만큼 많은 정보들이 존재하는 정보화 사회로서 정보 경쟁력이 중요시되는 시대이다. 이에 발맞춰 이러한 정보를 운영하는 정보시스템의 안전성이 많은 조직에서 이슈가 되고, 자신의 조직의 정보 자산을 보호하기 위한 방법을 모색한다. 이러한 방법 중 가장 광범위하게 적용되는 방법이 조직의 자산에 대한 위험분석이다. 위험 분석은 조직에 내재되어 있는 위협, 취약성을 식별하고, 식별된 위협 및 취약성에 대하여 보호대책을 강구함으로써 안전한 정보시스템 운영을 가능케 한다. 그러나 아직까지 외국의 위험분석 방법론에도 데이터 자산의 위험분석 방법을 구체적으로 기술이 되어 있지 않기 때문에, 실제로 데이터 자산의 위험 분석은 굉장히 힘들다.

그러므로 본 논문은 업무 중심의 위험분석 방법론과 이 방법론의 프로세스를 따라 데이터 자산의 위험분석 수행방법을 제안한다.

I. 서론

위험분석은 대상 조직의 정보시스템 관련 자산의 식별 및 평가, 위협 및 취약성 평가, 기존 정보보호 대응책의 효과성 평가 등의 과정을 통해 위험을 상세하게 측정, 분석하는 것을 의미한다. 국내는 '01년 7월 정보통신기반보호법의 시행으로 인해 많은 조직에서 위험분석에 대한 필요성을 인식하고, 자신의 조직에서도 위험분석을 수행할 계획을 세우고 있다. 이렇게 위험분석에 대한 관심이 고조되면서 학문적 또는 실용적인 위험분석 방법론이나 위험분석 도구 개발이 활기를 띄고 있다. 위험분석의 구성은 기본적으로 자산 식별, 위협 분석, 취약점 분석, 보호대책 수립 등의 여러 프로세스로 이루어진다. 현재까지 국·내외 방법론은 각 프로세스에 대한 "what"은 정의가 되어 있으나, "how"에 대한 내용이 상세히 기술이 되어 있지 않다. 그래서 실제로 위험분석을 수행하기 위해서 자신의 조직에 기존 위험분석 방법론을 적용시키는 것은 매우 어려운 작업이다. 그 중에서 특히 어려운 작업은 데이터 자산과 애플리케이션 자산에 대한 식별 및 위협, 취약성 분석 및 보호대책 수립 프로세스를 일관되게 적용하는 것이다. 아직까지 데이터 자산에 대하여 전체 위험분석 절차가 정의된 문서가 없는 실정이다.

본 논문은 데이터 자산의 위험분석 방법에 대하여 프로세스별로 설명한다. 본 논문의 구성은 2장에서 전체 위험분석 방법론을 제시하고, 3장은 데이터 자산에 대한 자산 식별 단계, 위협 분석 프로세스를 설명한다. 그리고 4장은 데이터 자산과 데이터를 저장하는 서버에 대한 취약성 분석에 관한 프로세스를 설명하고, 마지막으로 5장은 결론 및 향후 진행 과제를 기술한다.

II. 제시하는 위험분석 방법론

본 장에서는 업무 중심의 위험분석 방법론을 제안하고, 데이터 자산을 대상으로 프로세스별 수행내용을 자세히 설명한다.

그림 1은 전체 위험분석 과정을 나타낸다.

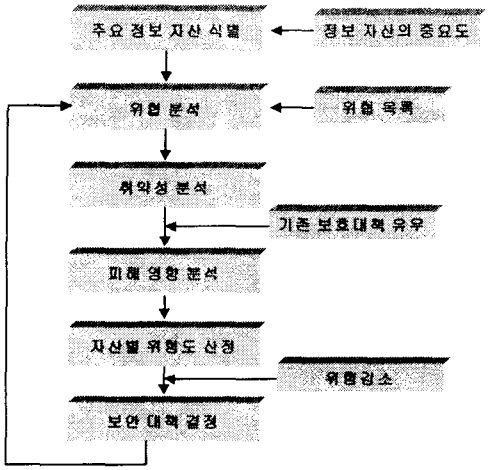

그림 1. 위험분석 프로세스

1) 주요 정보 자산식별

주요 자산을 식별하기 위하여 우선 해당 조직의 핵심업무를 파악한다. 그리고 파악된 핵심 업무를 지원하기 위한 정보 시스템을 분석하고, 그 시스템을 업무 프로세스별에 따른 접근 경로를 파악함으로써 핵심 인프라를 추출 가능하다. 이 인프라의 컴포넌트가 위험분석을 수행하는 조직의 주요 자산으로 정의된다. 이 방법은 미국의 카네기멜론 대학의 소프트웨어 공학 연구실에서 개발 중인 위험분석 방법론이 OCTAVE의 일부분을 적용하였다.[1]

2) 위협 분석

자산 식별 프로세스를 통하여 선정된 주요 자산별로 어떤 위협이 있는지 위협 목록을 통하여 파악한다. 데이터 자산에 대한 위협은 데이터에 국한된 것이 아니고, 그 데이터를 저장하고 있는 서버에 의존성을 가지고 있다. 그러므로 서버에 대한 위협 분석도 동시에 이루어져야 한다.

3) 취약성 분석

취약성 분석을 수행하기 위해서 우선 네트워크 및 호스트 취약성 진단도구를 이용한다. 취약성 분석은 데이터 자산에 대해서 수행되는 것이 아니라, 데이터를 저장하고 활용하기 위한 서버 및 DB 프로그램에 대하여 수행한다. 또한 DB 프로그램 이외에도 서버에서 사용하는 애플리케이션에 대하여 취약성을 분석한다. 이것 또한 위협 분석에서 기술한 바와 같이 데이터와 데이터를 저장하는 서버, 운영하기 위한 DB 프로그램의 의존성으로 인하여 발생한다.

4) 피해 영향 분석

위협 및 취약성 분석을 통하여 발견된 위협요소와 취약성 요소로 인하여 발생할 수 있는 피해를 분석한다. 이 프로세스에서 기존에 적용되어 있는 보호대책 유무 및 적절성을 분석한다. 또한 향후 적용할 보호대책 계획이 있으면 마찬가지로 유효성에 대하여 상세히 파악한다.

5) 자산별 위험도 산정

상기의 프로세스를 통하여 자산별로 위험을 계산하고, 위험도 순서대로 자산을 우선순위화 시킨다.

6) 보안대책 결정

위협 분석, 취약성 분석을 통하여 식별된 위험에 관하여 보안대책을 수립한다. 그리고 해당 조직에서 허용하는 위험을 수준을 결정을 한 후 적용할 보안대책을 결정한다.

이렇게 전체 위험분석 방법론을 실명하고, 데이터 자산에 대해서 일관되게 이 방법론에 대입하여 기술하였다.

III. 자산평가 및 위협분석

본 장은 조직의 핵심 업무를 지원하는 시스템 중 데이터 자산에 대한 평가와 어떠한 위협이 있는지를 분석하는 프로세스를 제시한다. 우선 자산평가 과정에서 국제 표준 ISO 17799로 발전한 BS7799의 자산 분류 방법을 설명하고, 특히 정보자산 중 데이터 자산의 자산 평가와 위협분석 방법을 실명한다.

1) 자산평가

영국 BSI에서 제시한 BS7799에서 제시하는 자산의 분류는 다음과 같다.[2]

- 정보 자산 : DB, 데이터 파일, 시스템 문서, 사용자 지침서, 연수자료, 운영적 또는 보조 절차, 연속 계획, 대체 시스템 준비
- 문서 자료 : 계약서, 지침서, 회사 문서, 중요한 비즈니스 결과를 포함하는 문서
- 소프트웨어 자산 : 응용 소프트웨어, 시스템 소프트웨어, 개발도구와 유틸리티
- 물리적 자산 : 컴퓨터와 통신장비, 자기 테이프, 자기 디스크, 전원 공급, 공기 조절 장치, 가구, 주거시설
- 인적 자산 : 개인, 고객, 가입자
- 회사 이미지와 명성
- 서비스 : 컴퓨터와 통신 서비스, 열, 빛, 세기, 공기 조절

식별된 데이터 자산이 기밀성, 무결성, 가용성 중 어떤 정보보호 요구사항을 더 중요시하는 지를 분석한다. 중요도의 등급은 R(ed), Y(ellow), G(reen)로 3단계로 구분을 한다.

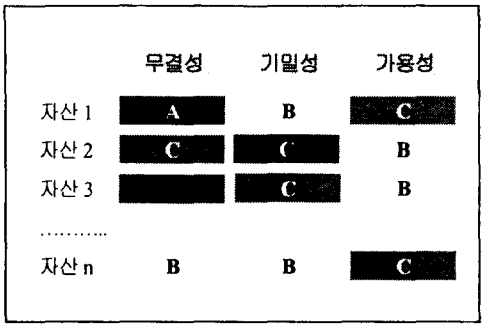

그림 2. 자산의 중요도

그림 2를 통해 자산 1은 무결성을 가장 중요시하고, 자산 2는 기밀성을 요구하는 자료임을 알 수가 있다. 또한 데이터의 민감도(Sensitivity)를 분석하고, 표 1과 같이 등급을 결정한다.

표 1. 데이터 민감도

등급	공공기관	민간기관
R	비밀자료 (Classified)	대외비 (Classifed)
Y	민감한 자료 (Sensitive Unclassifed)	· 개인 신상정보 · 조직의 능동적인 목표에 필요한 정보
G	공개 자료 (Unclassified)	공개 자료

2) 위협분석

위협분석은 인터뷰나 설문을 통하여 이루어지고, 대상은 해당 조직의 경영 또는 사업 부서의 고급관리자, IT 관련 부서 고급관리자, 중급관리자 및 실무자이다. 위협분석 목록의 예시[표 2, 3, 4]는 다음 표들과 같고, 위협 평가는 R(ed), Y(ellow), G(reen)로 등급화를 한다.

- R(ed) : 위협이 크다.
- Y(ellow) : 위협이 어느 정도 있다.
- G(reen) : 위협이 거의 없다.

표 2. 데이터의 저장, 파괴

내용	평가등급	보호대책
시스템 관리자용 매뉴얼에 시스템 또는 네트워크에 대하여 적절하게 설명되어 있다	R Y G	
사용자의 매뉴얼에 시스템이나 네트워크에 대하여 적절하게 설명되어 있다	R Y G	
시스템의 백업은 정책적으로 정의가 되어 있다	R Y G	
데이터 파괴에 대한 정책이 정의되어 있는가	R Y G	
백업 미디어는 연속적 계획에 의한 복사본을 Off-Site에 저장이 되어 있다	R Y G	

표 3. 접근제어

내용	평가등급	보호대책
접근권한이 명백히 정의되어 있다	R Y G	
Default 접근은 허용하지 않는다	R Y G	
데이터를 이용한 사람을 제어·추적 가능한 accountability(책임추적성)가 있다	R Y G	

표 4. 데이터 전송

내용	평가등급	보호대책
Off-line으로 데이터를 전송한다	R Y G	
전송 통로는 암호화되어 있다	R Y G	

IV. 취약성 분석 및 보호대책 결정

1) 취약성 분석

취약성 분석 프로세스는 2장에서 설명하였듯이, 데이터를 저장하는 서버와 서버에 제공하는 서비스, 애플리케이션에 대하여 1차적으로 취약성 진단도구를 통하여 취약성 분석을 수행한다. 2차적으로 취약성 진단도구에서 발견하지 못한 취약성에 대하여 수작업을 통하여 분석한다.

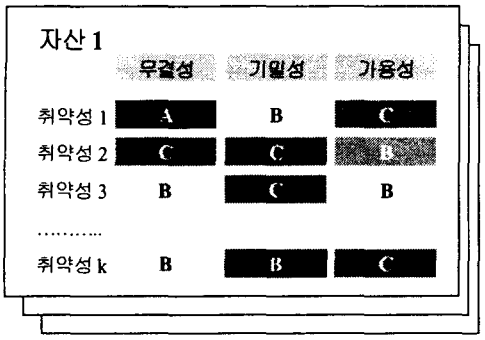

그림 3. 자산별 취약성 목록

그림 3은 자산별로 취약성이 어떤 정보보호 요구사항에 영향을 미치는 지를 분석한다. 위의 그림에서 자산 1의 경우, 3장에서 무결성이 가장 중요한 정보보호 요구사항이므로 취약성 1이 가장 크게 영향을 미치는 것을 알 수 있다. 이러한 방법으로 위험도가 큰 취약성을 파악한다.

2) 보호대책 결정

보호대책 결정 프로세스는 조직에서 허용 가능한 위험을 판단하는 위험 감소를 고려하여, 어느 수준까지 보호대책을 적용할 것인지를 결정하는 단계이다.

위협분석 과정에서 설문이나 인터뷰를 통하여 위협을 파악하고, 그를 해결하기 위한 보호대책을 결정을 하게 된다. 그리고 취약성 진단도구를 사용하여 발견된 취약성을 분석하고, 발견된 취약성에 대한 보호대책을 결정한다. 대부분 취약성 분석 프로세스에서 발견된 취약성들은 시스템 OS나 사용 포트, 지원하는 애플리케이션에 의존적이므로 소요예산 발생 없이 보호대책을 적용이 가능하다. 그러나 전문적인 지식을 가진 보안 담당자와 시간을 요구하는 보호대책이므로 적용하기 위해서 시간 분할을 잘 해야 한다.

V. 결론

기존의 위험분석 방법론인 캐나다의 CSE에서 발표한 위험분석 방법론[3], 미국의 GAO에서 발표한 정보보호관리지침[4], ISO/IEC의 GMITS[5, 6] 등에는 프로세스에 대한 설명이 되어 있으나, 분류된 자산별로 실제로 위험분석을 수행하기에는 많은 어려움이 있다. 특히 데이터 자산에 대하여 위협 및 취약성을 분석하고, 보호대책을 수립하기까지 모든 프로세스를 따라서 진행하기가 힘들다.

본 논문에서는 업무 중심의 위험분석 방법론을 제시하고, 이 위험분석 방법론의 프로세스를 따라서 데이터 자산에 대하여 실제로 적용하는 방법을 제시하였다. 위험분석을 수행하고자 하는 조직에서는 이 방법론을 따라서 자가진단(Self Direction)이 가능하리라 기대한다.

향후에는 실제 위험분석·평가 수행시, 데이터 자산의 위험분석만큼 어려움을 겪게 되는 조직에서 자체 개발·사용 중인 애플리케이션에 대한 위험분석을 어떻게 수행할 것인지에 대한 연구를 계속 할 예정이다.

참고문헌

[1] Carnegie Mellon Software Engineering Institute, *"OCATVE Criteria, Version 2.0*

[2] BSI, BS7799 - Code of Practice for Information Security Management, British Standards Institute, 1999.

[3] CSE, Threat and Risk Assessment Working Guide, Government of Canada, Communications Security Establishment, 1999.

[4] GAO, *Information Security Risk Assessment - Practices of Leading Organizations, Exposure Draft*, U.S. General Accounting Office, August 1999.

[5] ISO/IEC JTC 1/SC27, Information technology - Security technique - Guidelines for the management of IT security (GMITS) - Part 3: Techniques for the management of IT security, ISO/IEC JTC1/SC27 N1845, 1997. 12. 1.

[6] Solm, R., "Information Security Management (2): Guidelines to The Management of Information Technology Security (GMITS)", Information Management & Computer Security, Vol. 6, No. 5, 1998, pp.221-223.