위험분석 성능의 향상을 위한 취약점 분석에 관한 연구

엄정호*, 정태명

*성균관대학교, 컴퓨터공학과

A Study on Vulnerability Anlysis for Improvement of Risk Anlysis's Performance

Jung-ho Eom*, Tae-myoung Chung

*Department of Computer Engineering Sungkyunkwan Univ.

요 약

본 논문에서는 현재 대두되고 있는 IT 보안정책중 위험관리의 한 분야인 위험분석 과정을 살펴보았다. 그 중에서도 위험분석의 핵심 역할을 수행하는 취약점 분석 과정에 대해서 연구하였다. 먼저 보안관리와 위험관리의 일반적인 개념을 설명하였고, 다음은 취약점 분석의 중요성을 설명하면서 효율적인 취약점 분석을 위해 단계별 분석과정을 도식화하였다. 그리고 각 분석 단계마다 간략한 모듈을 만들어 단순하면서도 체계적인 분석 방법을 제시하였다.

I. 서론

네트워크 기술의 발달로 컴퓨터 전산망과 정보기술이 급격히 발전하는 가운데, 정보화 사회로의 발전이 빠르게 진행되고 있다. 이에 따라 각 조직 및 기관에서의 정보시스템이 중요 자산으로 여겨지면서, 그에 대한 의존도도 크게 증가하게 되었다. 그러나, 최근에 발생빈도가 증가되고 있는 일련의 보안사고는 전산망과 정보기술의 급격한 발전에 따른 역기능으로 개인, 조직 및 기관의 정보시스템에 막대한 피해를 주고 있다. 이와 같은 보안사고에 각 기관이 체계적으로 대응하기 위해서는 다양한 정보시스템 환경에 적합한 보안정책 및 보안지침 수립의 중요성이 부각되고 있다.

이에 따라 보안관리의 핵심인 위험관리 및 분석에 대한 연구가 활발히 진행되어 왔으며, 최적의 정보시스템 보안을 구축하기 위해서는 조직의 정보시스템 운영환경을 분석하고, 취약점 요소와 위험요소를 파악하여 효율적인 대응책을 제시해주는 위험분석 과정이 반드시 필요하다. 특히, 위험분석 중 취약점 분석은 정보시스템이나 조직 목표에 손해를 끼치는 원인 될 수 있는 요소를 확인하고 분류하여 위협을 감소시키는 것으로 위험분석의 핵심 단계로 여겨지고 있다.

본 논문에서는 위험분석 단계중 취약점 분석의 성능을 향상시킬 수 있는 효율적인 취약점 분석의 모듈을 제시할 것이다. 2장 본문에는 보안관리 및 위험분석의 개념을 간략히 설명하고, 취약점 분석과 각 단계별 분석 모듈을 제시한다. 마지막 3장에서는 결론과 향후 연구방안에 대해서 제시할 것이다.

II. 본문

1. 보안관리의 개념

보안관리를 수행하는데는 그림 1과 같이 크게 4단계로 나누어지는데, 조직의 환경과 업무성격에 맞는 효과적인 정보기술 보안 지침과 규약을 수립하는 보안정책단계, 시스템의 위험을 평가하고 그 결과에 따라 비용 효과적인 대응책을 제시하여 시스템 보안정책과 보안대응책 구현 계획을 수립하는 위험관리단계, 위험관리 과정을 수행한 뒤 보안대응책 수행계획에 의한 대응책 구현단계, 보안관리 주기에서 가장 중요한 단계로 보안정책 수립에서 위험관리에 이르기까지 수행된 보안관리 단계가 조직의 보안성 향상 기여도를 점검하고 관리하는 사후관리단계가 있다[1].

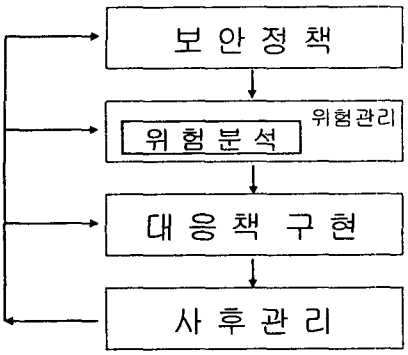

그림 1: 보안관리 흐름

2. 위험분석

가. 위험분석의 개념

위험관리 활동 중 안전한 정보시스템을 구현하고 정보자원에 대한 위험요소를 식별하고 평가하여 그러한 위험요소를 적절하게 통제할 수 있는 수단을 합리적, 체계적으로 구현하고 운영하는 전반적인 행위 및 절차로서 자산, 위협, 취약성, 영향을 고려하여 위험을 측정하고, 이 측정된 위험이 허용 가능한 수준인지 아닌지 판단할 수 있는 근거를 제공하는 것으로 절차는 그림 2와 같다[2].

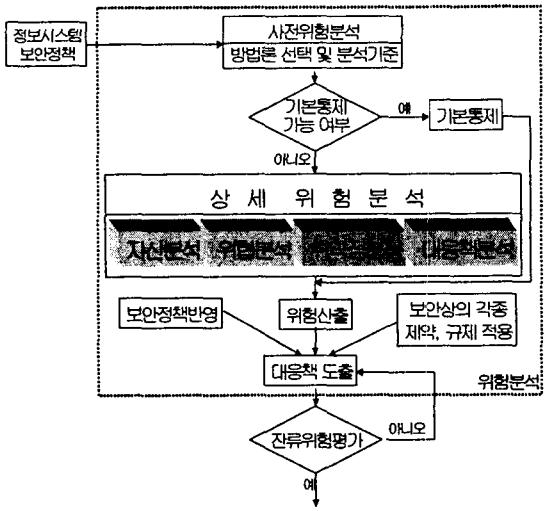

그림 2: 위험분석 절차

나. 위험분석의 분류

위험분석에는 시스템 환경에 맞는 위험분석 수준을 선택하는 사전 위험분석, 정보시스템에 대한 최소의 보안대책을 수립하는 것으로써 적은 비용으로 전 조직의 기본적인 보안수준을 수립하는 기본통제 방식, 정보시스템이 조직의 업무상 중요도가 높거나 자산 가치가 클 경우 적용되는 것으로써 자산분석, 위협분석, 취약성분석, 대응책분석, 위험산출의 일련의 과정을 거치는 상세 위험분석이 있다[2].

다. 상세 위험분석 요소 및 방법

1) 상세 위험분석 요소

상세 위험분석 요소에는 자산, 위협, 취약점, 대응책이 있다.

● 자산 : 조직의 환경에 따라 그 가치와 중요도가 높을 수도 있고 낮을 수 있는 요소로, 물리적 자산 , 소프트웨어, 정보/데이터 등이 있다.

● 위협 : 자산이 가진 고유의 취약성을 이용하여 자산에 직접적인 피해를 줄 수 있는 요소로, 인위적 위협과 자연적 위협이 있다. 인위적 위협에는 도청, 정보변조 등의 고의적 위협, 자료입력 실수, 전원 변동 등의 우발적 위협과 지진, 벼락 등 자연적 위협이 있다.

● 취약점 : 자산이 고유하게 가지고 있는 약점으로 존재 자체만으로는 자산에 어떠한 영향이나 피해를 주지 못하나, 위협에 의해서 이용될 수 있는 요소로, 관리적 취약점, 기술적 취약점, 물리적 취약점이 있다. 관리적 취약점에는 보안 관리, 전산요원 및 이용자 관리, 사고대책 관리가 있으며, 기술적 취약점에는 하드웨어, 운영체제, 네트워크 등이 있으며, 물리적 취약점에는 출입통제, 환경관리 등이 있다.

● 대응책 : 자산의 취약성이 위협에 노출되어 있음으로 인하여 자산이 피해를 볼수 있는 것을 막아주는 요소로, 각종 절차, 방법 등이 있다.

위의 위험분석요소들은 각각 분리되어 개별적이고 독립적인 위험분석 도구가 아니라 상호 연관되어 있어 총체적인 위험분석 도구의 하나의 요소로써 사용된다. 이 위험분석 요소들의 상호관계는 그림 3과 같다[1][3].

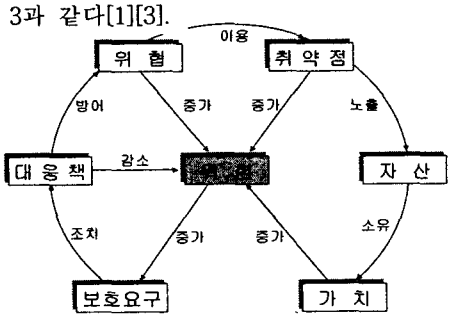

그림 3: 위험분석 요소들간 상관관계

2) 상세 위험분석 방법

상세 위험분석의 방법에는 위험요소로 분석하는 자산분석, 위협분석, 취약점분석, 대응책분석이 있다.

● 자산분석 : 위험분석 대상 정보시스템과 관련 있는 모든 자산을 조사하고 이들 자산들의 가치를 산정하는 과정이다.

● 위협분석 : 조직내에서 발생했거나 앞으로 발생할 가능성이 있는 위협을 조사하고 이들 위협이 자산에 미칠 영향을 분석하는 과정이다.

● 취약점분석 : 자산분석을 통하여 도출된 자산의 속성과 중요도를 바탕으로 자산이 근본적으로 가지고 있는 약점인 취약성을 발굴하고 취약점이 전체적인 위험에 미칠 수 있는 영향을 분석하는 과정이다.

● 대응책분석 : 정보시스템을 새로 구축하는 경우에는 필요한 대응책을 조사하는 과정이고, 운영중인 정보시스템인 경우는 운영중인 대응책들을 파악하는 과정으로 이들 대응책들이 위험을 감소시키기 위한 보안조치로 적절히 수행하고 있는지를 파악하는 단계이다[1].

3. 취약점 분석

취약점은 자산의 약점으로 자체로는 큰 위험은 되지 않으나, 위협요소들에게 침입을 할 수 있는 근거를 제공하며, 하나의 취약점은 하나이상의 영향을 자산에 입힐 수 있다. 그래서 그 어느 위험요소보다도 위험분석에 중요한 요소가 되며, 취약점분석은 충분한 자산분석을 통한 면밀성, 정확성, 완전성을 가져야 한다. 이러한 취약점은 일반적으로 다음과 같은 특성을 지니고 있다[4].

● 취약점은 정보자산의 환경적 특성이다.

● 복잡한 정보자산은 단순한 정보자산보다 더 많은 취약점을 가지고 있다.

● 위협이 정보자산의 취약점을 파고들어 조직의 손실을 가져온다.

● 정보자산의 취약 정도는 현재 보안 상태에 영향을 받는다.

● 모든 정보자산은 취약점을 보유하고 있다.

시스템 취약점분석에는 보안의 각 분야 항목을 포함시켜 세부항목으로 도출하는 취약점 파악단계, 취약점과 자산, 위협, 대응책의 관계를 파악하여 취약점의 속성을 특정짓는 취약점 속성 파악단계, 자산이 잠재적으로 지닌 취약점의 수준을 파악하여 대응책 수립시 우선순위를 고려할 수 있는 취약점 위험수준 산출단계가 있으며, 취약점 분석 흐름은 그림 4와 같다.

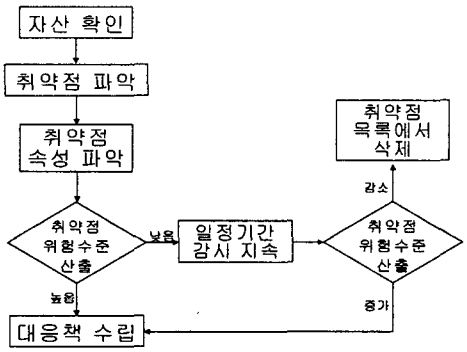

그림 4: 취약성 분석 흐름도

취약점 분석 과정중 위험수준 산출은 보통 5단계(매우높음, 높음, 보통, 낮음, 거의없음)로 나타낼 수 있는데 '낮음'단계로 판정되었을 때는 일정기간동안 감시를 하고 있다가 다시 위험수준을 실시해서 위험수준이 증가했을 때는 대응책을 수립하고 거의없음'단계까지 감소하면 취약점 목록에서 삭제하여 불필요한 보안정책을 수립하지 않도록 한다. 다음은 각 단계별 취약성 분석을 세부적으로 살펴보겠다.

1) 취약점 파악 단계

우선 조직이 보유하고 있는 정보자산을 파악하고 조사를 실시한다. 조사방법에는 관련인원들을 대상으로 한 설문조사, 정보자산이 위치한 장소에 대한 환경조사, 시스템에 대한 기술적 조사 등이 있다. 그리고 조사한 자료를 수집하여 위험정도를 측정한 후, 마지막으로 그 조직의 정보 자산가치에 맞게 위험순위를 결정한다.

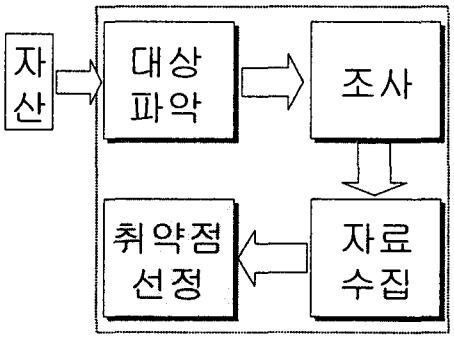

그림 5: 취약성 파악 모듈

2) 취약점 속성 파악 단계

취약점 속성 파악 단계에서는 각 취약점과 위험

요소간의 상관관계를 살피고, 그에 따라 자산의 중요 취약점을 확인하고, 위협요소의 주 침입경로를 판단하고, 정확한 대응책 수립의 자료를 제공한다.

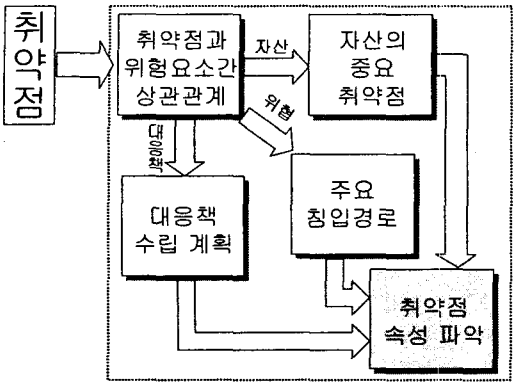

그림 6: 취약성 속성 파악 모듈

3) 위험수준 산출 단계

위험수준 산출 단계에서는 각 취약점을 두가지 방법(유형별, 자산별)으로 나누어 산출하여 각 방법에 맞게 우선순위를 선정한 후, 마지막에 통합하여 우선순위를 결정하므로써 취약성의 위험수준을 산출한다.

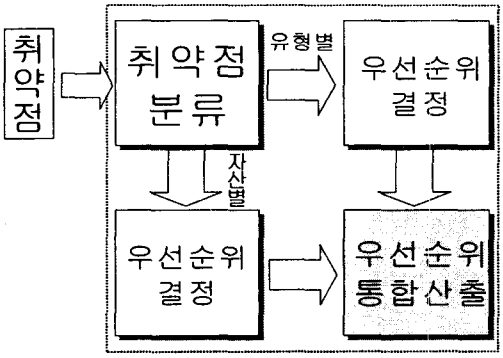

그림 7: 위험수준 산출 모듈

III 결론 및 향후 연구 방향

최적의 정보자산의 보안체계를 구축하기 위해서는 조직의 정보자산의 운영환경을 분석하고 취약점과 위험요소를 파악하여 그에 따른 적절하고 효율적인 위험관리가 요구된다. 위험관리 중에서도 효과적인 대응책을 제시해 줄 수 있는 위험분석이 반드시 필요한 과정이다.

위험분석은 정보자산의 위험을 평가하고 효과적인 대응책을 제시하여 보안대책 구현 계획을 수립할 수 있게 한다. 위험분석에는 자산분석, 취약점분석, 위협분석, 대응책분석으로 나눌 수 있는데 본 논문에서는 취약점분석에 대해서 집중적으로 연구하였다.

취약점분석은 정보자산이 보유하고 있는 약점을 파악하고 분석하여 취약점을 줄이므로써 위협요소가 침입할 수 있는 경로를 줄일 수 있게 한다. 하나의 취약점이 하나 이상의 위협이 될 수 있기 때문에 취약점 분석은 다른 어떤 분석보다도 중요하다. 면밀하고 완전한 분석만이 정확한 위험수준의 우선순위를 산출할 수 있으며 위협요소의 침입경로를 사전에 차단할 수 있다.

취약점분석 과정은 취약점 파악, 취약점 속성 파악, 위험수준 산출로 구성되어 있다. 본 논문에서는 취약점 분석의 정확도를 향상시키기 위해 각 분석 단계별 모듈을 형상화 시켰으며 모듈의 구성요소의 기능을 설명하였다. 각 모듈들은 복잡성을 배제한 가운데 순차적이고 단순한 흐름을 유지하면서 효율성을 증대시키려고 노력하였다.

그러나 아직까지 여러 조직들이 보유하고 있는 정보자산들의 중요도를 정확하게 파악하고 있지 못하고 있는 실정인 바, 설문조사 및 환경조사시 오류 데이터 생성이 많으며 각 조직마다 정보자산의 중요도가 상이하기 때문에 취약점 분석 결과도 판이하다. 그래서 조직이나 정보자산의 실태에 맞는 취약성 분석도구 개발이 요구된다.

참고문헌

[1] 한국정보통신기술협회, 공공정보시스템 보안을 위한 위험분석 표준-개념과 모델, Nov. 1998.

[2] 한국정보통신기술협회, 공공정보시스템 보안을 위한 위험분석 표준-위험분석 방법론 모델, Mar. 2000.

[3] 한국전산원, 정보시스템 보안을 위한 위험분석 소프트웨어(V.1.0) 개발 연구, Dec. 1996.

[4] 한국전산원, 국가기간 전산망 시스템의 안전관리체계에 관한 연구, Dec. 1991.