온라인 위험 가능성 평가를 통한 지속적인 보안관리 체계[5)]

주성진*, 김종**

*포항공과대학교, 정보통신학과
**포항공과대학교, 컴퓨터공학과

A Framework for Continuous Security Management through Online Risk Likelihood Assessment

Sung-jin Ju*, Jong Kim**

*Graduate School of Information Technology, Pohang Univ. of Science and Technology
**Dept. of Computer Science & Engineering, Pohang Univ. of Science and Technology

요 약

최근 들어 인적 보안위험과 같이 단기간에 변화가 심한 위험이 증가하고 있어 이에 대한 관리가 요구되고 있다. 그러나, 기존 위험평가만으로는 이러한 보안위험에 대한 적절한 평가 및 관리가 어려우므로 이에 대한 보완이 필요하다. 이에 기존에 적용된 보안관리 도구에 의해 생성되는 온라인 데이터를 이용하여, 이러한 위험에 대한 평가를 지속적으로 실시할 수 있는 보안관리 체계를 제안한다. 이를 통해 조직내 보안위험 수준을 감내할 수 있는 수준으로 유지할 수 있도록 한다.

I. 서론

컴퓨터를 이용한 업무처리가 급속히 확장됨에 따라 사이버 범죄가 빠르게 증가하고 있으며, 많은 사회적, 경제적 손실이 발생되고 있다. 2002년 CSI/FBI Computer crime and Security survey에 따르면, 응답자의 90%가 지난 1년 내에 컴퓨터 보안 위협을 탐지하였으며, 이러한 위협으로 인해 80%가 재정적인 손실을 본 것으로 파악되었다 [1]. 이러한 이유로 보안의 중요성은 더욱 강조되고 있으며, 대부분의 기업체 또는 관공서에서는 보안사고 예방 및 보안사고 발생시 피해를 최소화하기 위한 보안대책을 적용하고, 지속적인 점검과 Feed-back 체계를 유지하고 있다. 적절한 보안체계 수립을 위해서는 보호가 필요한 대상을 파악하고, 관리가 필요한 위험이 무엇인지를 파악하여 이에 대한 적절한 보안대책을 수립하는 위험평가가 수행되어야 한다. 이러한 위험평가는 중장기적인 보안관리 체계 수립을 위해 일반적으로 매우 복잡한 절차를 거치고, 많은 자원 - 시간, 인력 등 - 을 필요로 하기 때문에 대개 2~3년의 기간을 두고 실시된다. 또한, 위험평가를 통해 설계, 구축된 보안관리 체계는 보안관리 생명주기에 따라 지속적으로 평가, 설계, 구축, 운영된다[2]. 그러나, 현재와 같이 IT 환경이 급속하게 변화하고, 새로운 보안 위협이 수시로 보고되는 등 조직내 위험 상황이 빠르게 변화하는 환경에서는 신속한 평가와 대응이 필요하므로 기존 위험평가만으로는 적절한 대응이 어렵다. 따라서, 단기간에 빠르게 변화하는 인적 보안위험 등에 대한 지속적인 평가 체계의 마련이 필요하며, 이를 통해 보안위험에 대한 지속적인 관리가 필요하다. 이에 본 논문에서는 인적 보안위험과 같이 급격하게 변화되는 위험에 대한 지속적인 관리 체계를 제안하고자 한다. 이 체계는 기존에 적용되어 있는 보안관리 도구를 이용해 위험평가에 필요한 데이터를 수집하고 이를 통해 각 자산 및 조직의 위험을 평가하게 된다. 이러한 평가를 통해 조직 내에서 설정한 위험수준에 도달 하게 되면, 모니터링을 강화하거나 보안통제를 강화하는 등의 보안활동을 강화함으로써 위험발생을 억제하고, 조직내 위험에 대한 지속적인 관리가 가능하다.

본 논문은 이후 다음과 같이 구성된다. 본문의 1장에서는 기존 위험평가 방법 및 문제점에 대해서 분석하며, 다음 2장에서 제안하는 온라인 위험가능성 평가체계의 요구사항 및 기본 특징 등 기본적인 개념에 대하여 살펴보고, 3장에서는 구체적인 평가 절차 및 방법에 대하여 기술한다. 마지막으로 본 논문의 결론을 맺고자 한다.

1) 이 논문은 정보통신부 대학정보통신 연구센터 지원사업의 지원 및 한국소프트웨어진흥원의 관리로 수행되었음

II. 본문

1. 위험 평가

1) 기존 위험평가 절차

적절한 보안관리 체계를 마련하기 위해 위험평가가 필요하지만, 사고발생 빈도 및 손상정도에 대한 데이터가 제한되기 때문에 정확한 위험 평가가 어려운 상황이며[3], 이러한 제한으로 인해 위험평가 자체에 대한 불필요성이 제기되기도 한다. 이러한 한계를 극복하기 위하여 다양한 위험평가 방법 및 기법 - 인터뷰, 설문지, 체크리스트, 문서검토, 자동화된 점검도구, 침투시험, 위험 시나리오 기법, 위험수준 매트릭스 등 - 들이 사용되고 있으며[4], 일반적으로 위험평가 절차는 다음 그림 1과 같이 7단계의 절차로 구성된다.

2) 문제점

근래에 들어 인적 위협에 의한 사이버 범죄가 증가하고 있고, 이로 인해 조직의 보안위험 상황이 빠르게 변화하는 양상을 보이고 있다. 특히, 고의적인 위협으로 인한 사고발생의 경우, 가우스 확률분포 보다는 계단식 함수(step function)를 따르는 경향을 보인다[5]. 따라서, 이러한 위험에 대해서는 지속적인 평가를 통해 관리할 수 있는 체

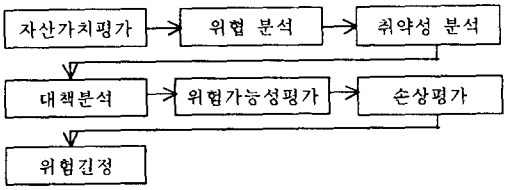

그림 1 : 기존 위험평가 절차

계가 요구된다. 그러나, 기존 위험평가는 중장기 보안체계 설계를 목적으로 하기 때문에 단기간에 빠른 변화를 보이는 위험에 대해서는 적용이 어렵다. 이를 보완하기 위해서는 기존 위험평가를 마친 이후, 다음 위험평가까지의 기간동안 발생되는 위험에 대하여 평가할 수 있는 체계 마련이 필요하다.

2. 온라인 위험가능성 평가 기본개념

1) 요구사항

지속적인 위험평가를 위해서는 다음의 2가지 요소가 필요하다. 첫째는 절차의 간결성이다. 즉, 단기간에 빠르게 변화하는 위험에 대한 평가는 짧은 시간 내에 이루어져야 한다. 이러한 간결성은 기존 위험평가 절차 중 불필요한 부분을 생략하는 방법에 의해 진행될 수 있다. 지속적인 위험평가 체계는 기존 위험평가 수행을 전제로 진행되기 때문에 기존 절차 중에 변화가 없거나, 미미한 부분에 대해서는 생략이 가능하다. 이러한 부분으로는 자산평가, 대책분석, 손상평가가 해당된다. 다음 요소는 데이터 수집의 용이성이다. 지속적인 평가를 통한 신속한 대책 적용이 필요하므로 시간과 자원이 많이 필요로 되는 기법 - 인터뷰, 질문지, 체크리스트 등 - 을 사용하기에는 부적절하다. 이러한 요구조건은 기존 보안 도구 - 방화벽, 취약점 점검도구, IDS 등 - 를 이용한 온라인 데이터 수집을 통해 가능하다.

2) 기본 특징

온라인 위험 가능성 평가 체계는 기본적으로 대상 및 방법에 있어 다음과 같은 특징을 가진다. 첫째로 단기간에 빠르게 변화하는 위험을 대상으로 한다. 이러한 위험에는 기술적 방법에 의한 인적위험이 있으며, 특히 고의적인 공격으로 인한 위험이 해당된다. 두 번째로 방법에 있어서는 기존 위험평가에 의해 수립된 보안체계를 기반으로 수행되므로, 기존 위험평가 체계에 의한 결과물 - 중요 자산의 가치평가, 현재 적용된 보안대책 현황분석, 가능한 위험 시나리오, 각 네트워크 간의 신뢰관계 등 - 을 바탕으로 위험평가를 실시한다.

3) 위험 가능성 지수

위험 가능성 평가에서는 위험 가능성 지수를 사용하여 위험수준을 평가한다. 위험 가능성 지수는 특정 자산에 대한 사고 발생 확률로 정의되며, 0부터 1사이의 값으로 나타낸다. 위험 가능성 지수는 크게 4가지 - *단일, 자산, 잠재, 전체 위험 가능성 지수* - 에 의해 표현된다. 먼저, "*단일 위험 가능성 지수*"는 각 위협과 취약성의 조합으로 하나의 사고가 발생될 가능성을 말하며, 하나의 위험 시나리오가 발생될 가능성을 의미한다. 두 번째 "*자산 위험 가능성 지수*"는 하나의 사고에 의해 자산에 대한 손상이 발생될 가능성을 의미한다. 세 번째 "*잠재 위험 가능성 지수*"는 알려지지 않은 위협이 특정 취약성에 작용하여 사고가 발생될 가능성을 말하며, 자산의 잠재적인 위험 발생 가능성을 표현한다. 마지막으로 "*전체 위험 가능성 지수*"는 각 자산에 대한 위험 가능성 지수에 대한 평가를 바탕으로 조직 전체에서 사고가 발생되어 손상이 일어날 가능성이며, 조직 전체 위험수준을 나타낸다.

3. 온라인 위험 가능성 평가 절차

온라인 위험 가능성 평가 절차는 위험 시나리오 그래프 작성, 위협 및 취약성 분석, 단일/자산/잠재 위험 가능성 평가, 전체 위험 가능성 분석의 4가지 단계로 구성된다.

1) 위험 시나리오 그래프 작성

온라인 위험 가능성 평가를 위한 첫 번째 단계는 기존 위험평가에 의해 도출된 각 자산별 위험 시나리오를 이용해 위험 분류 체계에 따라 관련 위협과 취약성을 분석하여 아래 그림 2와 같은 위험 시나리오 그래프를 작성하는 것이다.

위험 시나리오 그래프는 위협과 취약성 분류에 따라 몇 개의 차원으로 구분된다. 위협은 크게 *원천(source), 방법(method), 결과(result)*의 3가지 범주에서 분류된다[6]. 먼저, "*원천*"은 인적 위협

과 기타 위협으로 세분될 수 있으나, 본 논문에서 인적인 위협만 고려하므로 첫 번째 vertex는 인적 위협이 된다. 인적 위협은 다시 동기, 태도, 숙련도, 책임성, 인증여부, 지역의 속성 등에 의해 구분된다.[6] 두 번째부터 네 번째까지의 vertex는 이러한 속성을 나타낸다. 즉, 두 번째 차원은 지역, 세 번째 차원은 인증여부, 네 번째 차원은 동기이다. 다음으로 "*방법*"은 기술적 방법과 기타 방법으로 세분될 수 있다. 이중 위험 상황에 빠른 변화를 가져올 수 있는 기술적 방법에 따라 위협을 구분하면, 직접적 방법과 간접적 방법으로 세분될 수 있다.[7]. 다섯 번째 차원은 이러한 공격 방법을 나타내는 vertex로 구성되며, 간접적 방법은 공격 방법의 유사성에 의해 직접, 탐색, 인증우회, 권한획득으로 묶을 수 있고, 각각은 유사 공격그룹으로 정의된다. 마지막 차원은 해당 공격

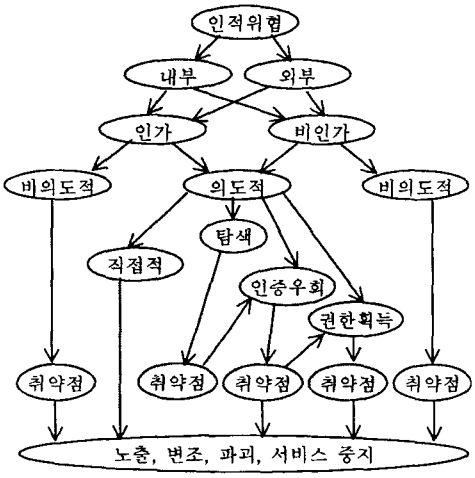

그림 2 : 위험 시나리오 그래프

방법에 대응되는 취약성 vertex로 구성된다. 이와 같이 인적 위협에서 시작하여 취약성 vertex까지의 경로를 이으면 하나의 위험 시나리오를 구성하게 된다. 마지막 범주인 "*결과*"는 사고발생 결과에 따른 분류이므로 위험자체의 발생 가능성에는 영향을 끼치지 않기 때문에 그래프에서 제외된다.

2) 위협 및 취약성 분석

두 번째 단계에서는 먼저, 적용된 보안도구 - 방화벽, 침입탐지 시스템, 취약점 점검 도구 등 - 를 통해 위협 및 취약성과 관련된 데이터 수집이 필요하다. 정확한 평가를 위해서는 보안도구를 통해 수집된 데이터의 정확성을 확보하는 방법이 중요하나, 본 논문에서는 여기에 대한 부분은 다루지 않기로 하며, 정확한 데이터가 수집된 것을 전제로 한다. 다음으로 수집된 데이터를 분석하여 위험 시나리오 그래프 상의 각 vertex에 대한 값을 아래 표 1의 방법으로 결정하게 된다.

Vertex			결정방법
비인가	지역	내부	□ 호스트 방화벽 로그, $V = \frac{A}{N}$
		외부	□ 네트워크 방화벽 로그, $V = \frac{A}{N}$
	공격 방법		□ IDS, 취약점 점검도구 기록 □ 양쪽에 다 존재하면 값은 1 □ 취약점 점검기록에 없거나, 취약점 점검기록에 있으면서 IDS기록에 유사 공격이 없으면 0 □ 취약점 점검로그에 있고, IDS기록에 유사 공격이 있으면 $V = \frac{A}{N}$

표 1 : Vertex 값 결정 (vertex 값 : V, 허용 패킷 수 : A, 총 패킷 수 : N)

위 표 1은 대부분의 조직에서 적용하고 있는 보안대책인 방화벽 및 침입탐지 시스템, 취약점 점검 도구를 기준으로 vertex의 값을 결정하는 방법을 나타내며, 다른 보안도구에 의해 수집된 데이터에 대해서도 적용이 가능하다. 각 vertex의 초기값은 모두 1로 부여되며, 수집된 데이터를 이용해 평가가 시작되면, 표 1의 방법에 따라 각 vertex의 값이 변경된다.

3) 단일/자산/잠재 위험 가능성 평가

두 번째 단계에서 결정된 각 vertex의 값을 이용해 단일/자산/잠재 위험 가능성 지수를 평가한다. 단일 위험 가능성 지수는 위험 시나리오 경로상의 각 vertex 값의 곱으로 표현된다. 따라서, 최종 취약성 vertex의 값은 위험 시나리오의 지수가 된다. 다음으로 자산 위험 가능성 지수는 위험 시나리오 그래프 상에서 각 단일 위험 가능성 지수 중 최대값으로 결정된다. 마지막으로 잠재 위험 가능성 지수는 단일 위험 가능성 지수를 이용해 예측할 수 있다. 실제 비인가자에 의한 공격 시도는 탐색, 인증우회, 권한획득 등 사전 과정을 거치게 되므로 알려지지 않은 인증우회 또는 권한획득 방법을 이용해 공격을 시도할 경우, 사전 단계의 공격시도가 많아지는 경향이 있다. 즉, 알려지지 않은 권한획득 공격을 수행하기 위해서는 사전 단계인 탐색 및 인증 우회의 과정을 거치게 되며, 이 과정에서 단일 위험 가능성 지수의 증가를 가져오게 된다. 따라서, 알려지지 않은 공격에 의한 잠재적인 위험 가능성은 단일 위험 가능성 지수의 평균 - 단일 위험 가능성 지수의 합 / 자산 내 위험 시나리오의 수 - 에 의해 결정된다.

4) 전체 위험 가능성 분석

전체 위험 가능성의 분석을 위해서는 기존 위험평가를 통해 각 자산 간의 네트워크 신뢰관계를 정의한 자산 연관 그래프의 작성이 선행되어야 한다. 그림 3은 자산 연관 그래프의 예이다.

그림에서와 같이 각 자산의 위험 가능성 지수는 화살표를 따라 지수가 높은 곳에서 낮은 곳으로 전이된다. 만약, A의 자산 위험가능성 지수가 전체 지수 중 가장 높다고 하면, A의 지수는 화살표를 따라 B와 E로 전이되고, 다시 B에서 D로, D에서 C로 전이되어 조직 전체의 위험 가능성 지수가 A에 의하여 결정됨을 알 수 있다. 따라서, 조직 전체의 위험 가능성 지수는 각 자산의 위험 가능성 지수 중 최대값으로 결정된다.

이러한 위험 가능성 지수를 통해 지속적인 보안관리를 수행할 수 있다. 기존 위험평가에 의해 조직 및 자산의 위험 감내 수준이 결정되면, 이를 초과하는 경우에 강화된 보안활동을 전개함으로써 지속적인 보안관리가 가능하다. 즉, 자산 및 조직의 위험 가능성 지수가 위험 감내 수준을 초과하게 되면, 모니터링의 강화, 방화벽 접근통제의 강화, 보안교육 실시 등 보안활동을 강화하여 이 지수를 이전의 수준으로 환원시킴으로써 위험 수준을 지속적으로 유지, 관리할 수 있다. 또한, 보안활동의 강화가 필요한 시기를 결정할 수 있으므로 보안활동의 효율을 극대화 할 수 있다.

III. 결론

기술적인 방법에 의한 인적 위협, 특히 고의적 위협으로 인한 위험 등은 단기간에 빠르게 변화하기 때문에 지속적인 관리가 필요하다. 본 논문에서 제안한 온라인 위험 가능성 평가를 통해 이러한 위험에 대한 지속적인 평가가 가능하며, 이를 통해 조직 내 보안위험 수준을 지속적으로 관리할 수 있으며, 알려지지 않은 공격에 의한 피해를 예방할 수 있다. 본 논문에서는 인적 위협 중 인가자에 의한 고의적 위협으로 발생되는 위험에 대해서는 고려되지 않았다. 그러나, 내부 인가자에 의한 보안사고는 사전에 탐지가 어렵고, 사고 발생시 많은 피해를 야기 시키므로 이에 대한 지속적인 관리 체계가 필요하다. 따라서, 이러한 부분에 대하여 제안된 체계의 보완이 필요하다.

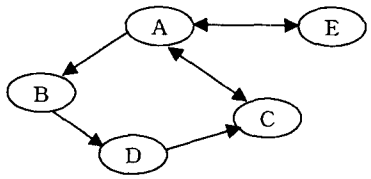

그림 3 : 자산 연관 그래프

참고문헌

[1] CSI, "Computer Crime and Security Survey," http://www.gocsi.com/press/20020407.html, 2002.

[2] Lee Wan Wai, "Security Life Cycle-1. DIY Assessment," SANS Information Security Reading Room, 2001.

[3] GAO, "Information Security Risk Assessment," GAO/AIMD-99-139, 1999.

[4] NIST, "Risk management Guide for Information Technology Systems 2001," NIST SP 800-30, 2001.

[5] F. Cohen, "Risk Management or Risk Analysis?," Network Security Magazine, 1998.

[6] NIAP, "CC Profiling Knowledge Base," http://niap..nist.gov/tools/cctool.html, 1999.

[7] MITRE, "NIMS Information Security Threat Methodology," Technical Report, 1998.