情 報 保 護 學 會 誌
第 13 券 第 5 號, 2003. 10

정보통신망 취약점 분석 · 평가 방법론

서 정 택*, 임 을 규*, 이 철 원*

요 약

최근 정보통신망을 이용한 해킹사고가 급격하게 증가하고 있으며, 그 피해의 파급효과가 매우 커지고 있다. 따라서, 해킹사고로부터 네트워크와 시스템 등의 자산을 보호하는 것이 더욱 중요해지고 있다. 크래커들은 네트워크와 시스템에 존재하는 취약점을 찾아내고, 그 취약점을 이용하여 네트워크 및 시스템에 침투하여 악의적인 행동을 한다. 정보통신망에 대한 취약점 분석 · 평가에서는 네트워크 및 시스템에 존재하는 기술적, 관리적, 물리적 취약점을 분석하고, 각각의 취약점을 이용한 침투의 가능여부와 피해 파급효과에 대한 위험도 평가를 수행한다. 취약점 분석 · 평가를 수행함으로써 대상 기관에 적합한 보안대책을 수립 및 적용하여 해킹사고를 사전에 예방하고, 사고 발생시 적절히 대응할 수 있도록 한다. 본 논문에서는 정보통신망 취약점 분석 · 평가 방법론을 제시하고자 한다.

Ⅰ. 서 론

정보통신망은 정보화 사회 진전에 따라 인류생활과 떨어질 수 없는 핵심시설로 자리잡고 있다. 그 중에서도 행정, 금융, 교통 등의 영역에 구축된 정보통신망은 국민생활, 사회경제생활의 안전과 직결된 시스템으로서 국가가 특별히 보호해야할 시설이며 이에 대한 각종 침해는 국가적·사회적 혼란을 야기할 수도 있음이 여러 가지 사례에서 입증되고 있다. 최근 침해사고가 급증하고 있으며, 그 피해의 파급효과가 더욱 확대되고 있다. 실제 침해사고의 대부분이 네트워크나 시스템 상에 존재하는 취약점이나 잘못된 보안정책 설정을 악용하는 방식을 사용하고 있다[6,7]. 따라서, 정보통신망에 대한 취약점 분석 · 평가가 필요하다. 정보통신망 취약점 분석 · 평가는 네트워크나 시스템에 존재하는 취약점을 찾아내고, 모의침투시험을 통하여 현재의 보안상태를 점검하며, 발견된 취약점이 어느 정도 위협이 되는지를 평가하게 된다. 또한, 발견된 취약점들에 대한 즉시조치방안과 단기적, 중장기적 보안대책을 수립하여 적용함으로써 대상 기관 정보통신망의 보안성을 높일 수 있다. 취약점 분석 · 평가는 물리적, 관리적, 기술적 부분으로 수행된다[3,4].

본 논문에서는 취약점 분석 · 평가의 수행경험을 토대로 하여 체계적인 취약점 분석 · 평가 방법론을 제시한다. 먼저, 취약점 분석 · 평가의 개념과 중요성을 설명하고, 취약점 분석 · 평가의 수준 및 범위 결정에 대하여 설명하며, 취약점 분석 · 평가의 수행절차로 준비단계, 사전단계, 실시단계, 사후단계, 추후 보안관리단계에 대하여 각 단계에서 수행하는 업무내용에 대하여 제시한다[1,2].

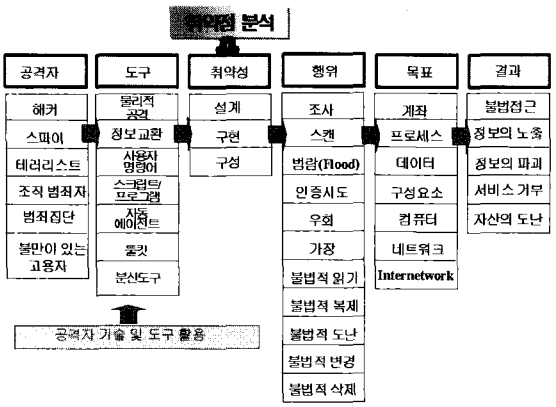
Ⅱ. 정보통신망 취약점 분석 · 평가 방법론

2.1 취약점 분석 · 평가의 개념

취약점 분석 · 평가의 목적은 해당기관의 정보통신망 및 기존 보안대책에 대한 분석 및 평가를 수행하고, 그 결과를 바탕으로 물리적, 관리적, 기술적 대응방안을 제시하여 정보통신시스템에 보안체계를 구축하는 것이다.

취약점 분석은 출입통제 및 백업시설 등의 물리적 부분과, 보안조직, 보안정책 및 지침, 보안교육, 사고대응 등의 관리적 부분과, 해당기관의 정보통신망에서 소유 및 운영하고 있는 정보시스템을 대상으로 네트워크, 시스템, 데이터, 소프트웨어 등에 대한 기술적 부분으로 수행된다. 보안시스템인 침입차단시스템 및 침

* ETRI 부설 국가보안기술연구소({seojt, imeg, cheolee}@etri.re.kr)



〔그림 1〕 취약점 분석

입탐지시스템도 주요 분석 대상에 포함된다. 이러한 정보시스템을 대상으로 취약점 분석도구를 이용하여 진단하며, 침입차단시스템과 라우터의 경우에는 시스템 자체에 대한 취약점 뿐만 아니라 보안정책설정 룰을 집중적으로 점검하게 된다.

취약점 평가는 취약점 분석을 통해 발견된 취약점들이 실제 침입이 가능한지 또한 침입에 성공했을 때 그 피해파급효과가 어느 정도 영향을 미치는지 등을 모의침투시험을 통해 시험하고, 이 결과를 이용하여 발견된 취약점들을 우선순위화 한다.

보안대책제시에서는 발견된 취약점들에 대한 즉시 조치사항과 단기적, 중장기적 보안대책을 수립한다.

2.1.1 취약점 분석·평가의 중요성

1990년대 이전에는 국가안보 및 비밀성 측면에서 보안이 중요시되었으나, 2000년대에는 보안이 국가 주요정보 기반구조 보호와 직결되고 있는 상황이며, 공격을 당한 후에 보안대책을 세우고 적용해도 이미 주요 정보가 유출 및 파괴되거나, 시스템이 망가진 상태이므로 거의 의미가 없어진다. 따라서, 취약점 분석·평가를 수행하여 존재하는 취약점을 식별하고, 발견된 취약점에 대하여 적절한 보안대책을 수립 및 적용하는 것이 중요하다.

2.1.2 취약점 분석·평가 수준 결정

취약점 분석·평가를 수행하기 전에 대상기관에 대한 취약점 분석·평가의 수준을 결정해야 한다. 대상기관의 정보통신망의 형태가 개방망, 폐쇄망, 제어망의 보유 여부와 해당기관의 서버 및 호스트의 개수, 해당기관의 시스템 및 네트워크에 보안사고 발생시 그 파급효과가 국가안보, 국가경제, 사회질서 유지, 국민생명 등에 어떠한 영향을 미칠 수 있는지를 고려하여 취약점 분석·평가 수행의 수준을 결정한다.[4]

2.1.3 취약점 분석·평가의 내용

취약점 분석·평가는 물리적, 관리적, 기술적 부분으로 구분되어 실시한다.

〔표 1〕 취약점분석·평가 내용

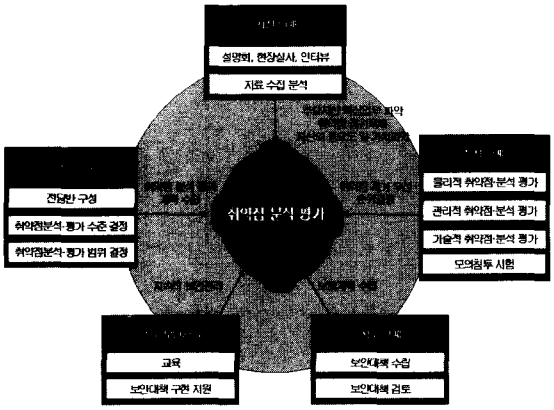
분야	내용	세부내용
물리적	출입통제	- 건물 및 전산실에 대한 물리적 접근 통제 - 보안요원 및 CCTV
	재난방지 시설	- 소방설비 및 재난대비시설 - 전기설비(UPS 등)
	백업시설	- 백업장비(시스템 및 매체) - 백업 실시 주기, 이중보관
관리적	보안조직	- 효율적인 보안조직의 구성 및 운영 - 보안조직의 업무 효율성 분석 - 보안조직의 구성원 업무 능력 - 제3자 및 아웃소싱에 대한 보안관리
	보안정책 및 지침	- 보안정책 및 지침의 적절성 - 보안정책 및 지침의 이행여부
	보안교육	- 보안교육 및 훈련의 실시 현황 - 보안교육 내용 및 효과
	사고대응	- 보안사고 발생시 보고 - 보안 취약점에 대한 보고 - 징계 절차 및 내용
	보안관리 활동	- 보안관리 - 직원들의 보안의식 수준 - 직원들의 보안활동
기술적	전체 네트워크 구성	- 내부망과 외부 인터넷 망의 독립성 - 외부로부터 내부 주요 시스템에 대한 침입 가능성
	웹서버	- 웹서버 시스템 취약점 점검 - 웹프로그램 개발상의 취약점 점검
	주전산기	- 시스템 취약점 점검
	보안 시스템	- 보안시스템 자체에 대한 시스템 취약점 점검 - 침입차단시스템 보안정책설정 점검 - 침입탐지시스템 탐지능력 및 탐지룰 Update 현황 - 라우터 패스워드 관리 및 Access List 점검
	개인 PC	- 악성코드 및 바이러스 감염여부 - 백신 프로그램의 사용현황 - CMOS 암호 및 패스워드 관리 - 공유 폴더 사용 현황 - 패치 프로그램 설치 현황

2.2 취약점 분석·평가 수행 절차

취약점 분석·평가는 준비단계, 사전단계, 실시단계, 사후단계, 추후보안관리의 5단계로 수행된다.

2.2.1 준비단계

준비단계에서는 취약점 분석·평가의 수준을 결정하고, 물리적, 관리적, 기술적 측면에서의 취약점 분석·평가의 범위를 결정한다. 기술적 측면의 범위 결정을 위해서는 해당기관의 주요 자산을 식별하고, 중요도를 점검하여 범위를 결정한다. 또한, 취약점 분석·평가를 효율적으로 수행하기 위하여 전담반을 구성한다. 전담반 구성에서는 효율적인 분석을 위하여 대상기관의 네트워크 및 시스템 담당자들을 포함시킨다.



〔그림 2〕 취약점 분석·평가 수행절차

2.2.2 사전단계

사전단계에서는 대상기관의 임원 및 각부서의 네트워크 및 시스템 담당자들을 대상으로 하여 취약점 분석·평가 수행에 대한 설명회를 개최하고, 대상기관의 시스템 개발문서, IP 현황 및 네트워크 구성도, 정보보안지침서 및 주요 시스템 관리대장과 같은 현황자료들을 이용하여 물리적, 관리적, 기술적 현황분석을 수행하고, 네트워크 및 시스템 담당자와 부서장들을 대상으로 인터뷰를 실시하여 각 시스템들에 대한 운영현황 및 중요도와 조직 전반적인 보안관리 현황 등을 파악하며, 전체 직원을 대상으로 설문조사를 실시하여 직원들의 보안의식 및 보안관리 현황을 파악한다.

• 물리적 현황분석

물리적 현황분석에서는 출입통제, 재난 방지 시설, 백업 대책 등에 대한 현황분석을 실시한다. 건물 및 전산실에 대한 출입통제 현황을 확인하고, 제한구역 및 통제구역에 대한 출입관리현황을 분석한다. 주요 시스템 및 데이터에 대한 백업 실시 여부와 사용하는 백업 실시 현황을 분석하고, 백업실시 주기 및 이중보관 실시 등에 대한 현황도 분석한다. 또한, 전기시설의 안정성 분석으로 UPS 등의 전기시설 사용 현황을 분석한다. 또한, 지진, 홍수, 화재 등의 자연재해로부터의 재난대비시설을 점검한다.

각종 사고 발생에 대하여 마련되어 있는 재난관리 대책의 내용을 확인하여 재난 발생시에 적절히 대응할 수 있는 준비가 되어 있는지를 확인하고, 이전의 사고 발생 사례 등에 대한 분석을 실시한다.

• 관리적 현황분석

관리적 현황분석에서는 보안조직, 보안정책 및 지침, 보안교육, 사고대응에 대한 현황분석을 실시하며, 그 방법의 하나로 인터뷰 및 설문도 실시한다. 대상기관이 별도의 보안조직을 구성하여 효율적인 보안관리 업무를 수행하고 있는지 분석하고, 그 인원구성과 업무내용의 적절성도 함께 분석한다. 또한, 대상기관에 정보통신보안지침이 마련되어 있는지 확인하고, 마련되어 있으면 해당 정보통신보안지침 내용의 적절성을 분석한다. 또한, 보안관리자가 보안관리를 수행하는데 필요한 기술을 얻을 수 있는 교육 참여 현황을 분석하고, 전 직원을 대상으로 실시하고 있는 보안교육 및 훈련에 대한 현황을 분석한다. 이때, 보안교육 실시 횟수와 교육내용의 적절성도 점검한다. 또한, 사고대응에 대한 분석을 위하여 보안사고 발생 시에 대한 보고절차 및 시행 내용을 분석한다.[5]

- 인터뷰 : 보안관리자, 점검 대상이 되는 네트워크 및 시스템의 담당자, 부서장을 대상으로 인터뷰를 실시하여 보안관리 현황을 분석한다. 이때, 현재 운영되고 있는 보안관리의 적절성 여부에 대한 인터뷰 대상자의 의견을 듣고, 대상자의 보안의식 수준 및 보안관리업무 현황을 분석한다.
- 설문조사 : 전체직원을 대상으로 설문조사를 실시하여 보안정책, 보안조직구성, 직무보안, 사용자 보안교육 정도, 보안사고 대응체계, 보호지역에 대한 관리, 보안의식, 개인 PC 보안관리 등에 대한 현황을 분석한다. 설문조사 응답 결과에 대한 체계적인 통계 및 분석을 실시하여 현황분석 자료로 활용한다.

• 기술적 현황분석

기술적 현황분석에서는 전체네트워크 구성, 웹서버, 주전산기, 보안시스템, 네트워크 장비 등에 대한 현황분석을 실시한다. 대상기관의 전체네트워크 구성을 통하여 내부망과 외부인터넷망의 독립적 운영여부를 확인하고, 외부인터넷으로부터 내부 주요시스템에 대한 접근 가능성을 확인한다. 또한, 내부 시스템간에도 불필요한 접속을 허용하고 있는 부분은 없는지 분석한다. 침입차단시스템의 보안정책 설정 내용을 점검하고, 운영관리 현황을 분석한다. 침입탐지시스템은 공격에 대한 탐지 기능을 확인하고, 탐지 룰의 update 주기 및 실시여부 등을 확인한다. 웹서버는 보안운영 현황으로 내부 DB서버와의 데이터 흐름도 및 게시판의 운영현황 등을 분석한다. 내부 주전산기 시스템들에 대해서는 시스템 기능, 하드웨어 사양, 운영체제 정보, 사용 응용프로그램 등의 정보를 분석하며, 각 시스템들 간의 데이터흐름을 분석한다.

2.2.3 실시단계

실시단계는 취약점 분석·평가를 실질적으로 수행하는 단계이다. 물리적, 관리적, 기술적 측면의 취약점을 찾아내고, 발견된 취약점에 대하여 모의침투시험을 실시하여 발견된 취약점이 실제로 침입이 가능한지 테스트하고, 침입 가능시에 어느 정도 악영향을 미칠 수 있는지 등의 위험도를 산정한다. 점검 결과를 토대로 하여 발견된 취약점들에 대하여 우선순위화를 실시한다. 또한, 발견된 취약점들 중 즉시조치가 필요한 취약점들에 대해서는 점검요원과 시스템 담당자가 협조하여 즉시조치를 실시한다.

• 물리적 취약점 분석·평가

건물 및 전산실에 대한 출입통제 운영의 적절성과 실시현황을 점검하고, 우회경로의 존재여부를 확인하고, 통제를 받지 않고 접근 시에 발생할 수 있는 문제점을 파악한다. 주요 시스템 및 데이터에 대한 백업 실시 여부와 사용하는 백업장비의 안정성을 점검하며, 백업실시 주기가 적절한지, 백업 데이터가 지진이나 홍수 등의 재난에 대비하여 어느 정도 거리를 두고 이중보관 되는지에 대하여 점검한다.

전기시설의 안정성 분석으로 UPS 등의 전기시설 설치여부와 주요 시설에 대한 이중화 여부를 점검한다. 또한, 지진, 홍수, 화재 등의 재난에 대하여 대비하기 위해 설치된 재난 대비 시설의 동작여부를 점검한다.

이와 같은 각종 사고 발생에 대한 재난관리 대책 마련 내용을 확인하여 재난 발생시에 적절히 대응할 수 있는 절차가 마련되어 있는지 점검하고, 재난발생에 대한 모의시험을 실시하여 직원들의 적절한 행동여부를 확인한다.

• 관리적 취약점 분석·평가

조직내의 보안조직의 존재여부와 인원 구성의 적절성, 보안업무의 효율성 및 적절성, 각 부서간의 업무 협조도 등을 분석하며, 정보통신보안지침의 세부항목들에 대한 적절성 검사와 지침에 따른 이행여부를 분석한다. 또한, 사고대응 능력으로 보안사고 발생시의 보고절차 및 실시 내용, 보안 취약점 발생 시의 보고절차 및 실시 내용 등을 확인하고, 보안사고 발생시에 담당자에 대한 징계의 절차 및 내용 등을 확인한다. 또한, 가상 모의 침투 시험 시 관련 직원들의 대응능력 등도 점검한다. 인터뷰 및 설문조사 결과의 분석을 통하여 직원들에 대한 보안교육 내용 및 회수의 적절성을 분석하며, 직원들의 보안의식 및 보안관리 능력의 수준들을 분석 및 평가한다.

• 기술적 취약점 분석·평가

전체 네트워크 구성, 웹서버, 주전산기, 침입차단시스템, 침입탐지시스템, 개인 PC 등에 대하여 취약점 점검도구를 이용하여 취약점을 식별하고, 발견된 취약점들에 대한 모의침투 시험을 통하여 침입 가능여부와 침입 가능시의 파급효과 등에 대한 분석·평가를 실시한다. 또한, 즉시 조치가 필요한 취약점을 식별하여 점검요원과 시스템 담당자가 협조하여 즉시 조치를 실시한다.

- 전체네트워크 구성 취약점 분석·평가

대상기관의 전체네트워크 구성에 대한 취약점 점검으로 내부망과 외부인터넷망이 독립적으로 운영되고 있는지, 내부 주요 시스템에 대하여 외부인터넷망으로부터의 접속가능 여부를 점검한다. 또한, 내부망 내에서 각 부서간, 시스템간에 불필요한 접속을 허용하고 있는 부분은 없는지를 분석·평가한다.

- 침입차단시스템 취약점 분석·평가

취약점 점검도구를 이용하여 침입차단시스템 자체에 대한 시스템 차원의 취약점을 분석한다. 대부분의 침입차단시스템은 별도의 open 포트를 사용하지 않으므로 불필요하게 열려있는 포트가 있는지 점검하고,

운영체제 및 서비스 상에 존재하는 취약점을 식별한다. 모의침투시험을 통하여 식별된 취약점을 이용한 exploit을 실시하여 침투가 가능한지를 점검하고, 침투 이후에 실행 가능한 명령어의 범위 등을 확인하여 대상 취약점의 위험도를 산정한다.

또한, 침입차단시스템의 보안정책 설정에 대한 적절성 점검으로 보안정책 설정 룰 하나하나에 대하여 허용하는 source 및 destination 네트워크 그룹에 불필요한 IP가 포함되어 있지는 않은지, 사용하는 서비스 외에 불필요한 서비스 포트를 허용하고 있지는 않은지, 현재 사용되지 않는 보안정책 설정이 남아 있지 않은지 등을 점검한다.

- 침입탐지시스템 취약점 분석·평가

취약점 점검도구를 이용하여 침입탐지시스템 자체에 대한 시스템 차원의 취약점을 분석한다. 불필요하게 open되어 있는 포트는 없는지, 서비스에 대한 패치가 설치되어 있지 않아 취약한 부분은 없는지를 점검하고, 운영체제 및 서비스 상에 존재하는 취약점을 식별한다. 식별된 취약점에 대한 모의침투시험을 통하여 exploit을 실시하여 실제로 침투가 가능한지를 점검하고, 침투 이후에 실행 가능한 명령어의 범위 등을 확인하여 대상 취약점의 위험도를 산정한다.

또한, 취약점 점검도구를 이용하여 점검 시나, 다양한 모의침투시험에 대하여 침입탐지시스템이 공격으로 정상적인 탐지를 수행하고 있는지를 점검하고, 침입탐지시스템의 기능상 가장 중요한 탐지룰에 대한 업데이트가 실시간으로 적절하게 이루어지고 있는지를 분석·평가한다.

- 웹서버 취약점 분석·평가

취약점 점검도구를 이용하여 시스템 자체에 대한 취약점을 분석하고, 웹서버 점검도구를 이용하여 웹프로그램 개발 상에 존재하는 취약점을 분석한다. 웹서버는 외부로부터의 http 접속에 대해서는 모두 허용하는 시스템으로 해킹에 대하여 노출되어있는 시스템이다. 운영체제 및 서비스에 대한 취약점 점검뿐만 아니라 게시판 및 인증관련 부분에 대해서는 소스코드 분석을 통한 취약점 분석을 실시하여 웹프로그램 개발상의 오류로 인하여 존재할 수 있는 취약점에 대해서도 식별한다. 식별된 취약점들에 대하여 모의침투시험을 실시하여 시스템에 대한 침입 가능 여부를 확인하고, 웹서버 침입 가능 시에는 웹서버로부터 내부 시스템으로의 침투 가능성을 점검한다. 내부망의 DB서버와 연동하여 운영되는 웹서버의 경우 내부망의 DB서버로의 자료 업데이트 기능을 이용한 악성코드의 실행 여부 등을 분석·평가한다.

- 주전산기 취약점 분석·평가

취약점 점검도구를 이용하여 시스템에 대한 취약점을 분석한다. 사전단계에서 주전산기 시스템에 대한 기능 및 응용프로그램에 대한 분석을 수행하였으므로 대상시스템에서 운영되는 서비스 및 기능을 파악하고 있다. 이를 이용하여 대상 시스템에서 불필요하게 운영되고 있는 서비스는 없는지 확인하고, 주요 시스템들간에도 불필요하게 접근을 허용하고 있는 부분은 없는지 확인한다.

운영체제 및 서비스 상에서 식별된 취약점들에 대하여 모의침투시험을 실시하여 시스템에 대한 침입 가능성을 확인하고, 침입 이후에 실행 가능한 명령어의 범위를 확인하여 대상 취약점에 대한 위험도를 산정한다. 또한, 이 시스템에 대하여 침입 성공 시 동일 네트워크 상에 존재하는 다른 시스템들에 대한 침입 가능성을 다양한 모의침투시험을 통하여 분석·평가한다.

- 개인 PC 취약점 분석·평가

개인 PC에 대한 취약점 분석은 백신프로그램을 이용하여 대상 개인 PC에 악성코드 및 바이러스의 감염 및 설치 여부를 점검한다. 또한, PC에 백신 프로그램이 설치되어 있는지를 확인하고, 백신프로그램에 대한 탐지룰 업데이트를 주기적으로 수행되고 있는지 확인한다.

CMOS 암호의 사용여부 및 로그인 시 암호를 사용한 인증과정을 수행하는지 점검하고, PC 상에 공유폴더에 대한 암호 사용여부와 read/write 권한의 적절한 사용 여부를 점검한다.

또한, PC에 대한 운영체제 및 서비스에 대한 패치 프로그램의 설치 여부를 점검한다.

- 라우터 및 스위치 취약점 분석·평가

네트워크간의 접점에 위치하는 라우터의 access list를 점검하여 각 네트워크간에 접속이 필요한 IP 대역에 대해서만 접속을 허용하고 있는지를 확인하고, 사용하는 포트에 대해서만 허용하는 정책으로 운영되고 있는지 점검한다.

또한, 라우터 및 스위치에 관리자 패스워드 관리가 안전하게 이용되고 있는지 점검도구를 이용하여 점검하고, 패스워드 크랙 프로그램을 이용하여 사용하는 암호의 안정성을 점검한다.

• 취약점 우선순위화

취약점 분석·평가를 수행한 각 시스템들을 대상으로 식별된 취약점들에 대하여 모의침투시험을 실시하여 각각의 취약점을 이용한 침입의 가능성 및 침입 가능시의 파급효과 등을 분석·평가하였다. 산정된 위험도를 이용하여 각 시스템별로 식별된 취약점들에 대한 위험도에 따라 High, Medium, Low의 형태로 분류하고, 우선적으로 조치되어야 하는 것부터 순위화 한다. 대상기관에서는 순위화 된 데이터를 확인하여 우선적으로 조치 가능한 부분에 대하여 조치를 실시하는데 이용한다.

2.2.4 사후단계

사후단계는 보안대책 수립단계로써 현황분석 및 취약점 분석·평가 단계에서 분석·평가된 내용을 기반으로 대상기관의 특성 및 현실에 적합한 보안대책을 제시하는 단계이다. 물리적, 관리적, 기술적 부분에 대한 보안대책을 제시하며, 중요시스템이거나 위험도가 높게 판정된 시스템에 대해서는 즉시조치사항으로 제시하며, 전체적인 내용으로 중/장기적 보안대책을 제시한다. 또한, 실시단계에서 즉각적인 조치가 필요한 부분에 대해서 조치를 실시하였으므로 조치 여부를 확인한다. 이때, 대상기관의 네트워크 환경과 향후의 정보통신시스템운영계획과 적합하도록 보안대책을 제시하는 것이 중요하다.

• 물리적 보안대책

물리적 측면에서 대상기관의 보안성을 향상시키기 위해 추가적으로 필요한 출입통제 방안 및 추가시설을 제시한다. 중요 시스템들이 설치되어있는 전산실에 대해서도 추가적으로 필요한 출입통제 방안 및 추가시설을 제시한다. 또한, 지진, 홍수 및 화재 등의 재난에 적절하게 대응하기 위한 소화시설 및 재난대비 시설에 대한 추가적인 설치 설비나 운영방안을 제시한다.

주요 시스템 및 데이터에 대한 백업운영대책으로 백업대상 시스템 및 데이터를 정의하고, 적절한 백업 실시 주기를 제시하며, 백업된 데이터에 대한 이중보관 대책을 제시한다.

• 관리적 보안대책

효율적인 보안관리를 위한 보안조직의 구성방안을 제시하며, 보안조직에서 수행해야 하는 보안업무에 대하여 정의하고, 해당업무가 효율적으로 수행되기 위한 방안을 제시한다.

별도의 정보통신보안지침이 마련되어있지 않은 대상기관에게는 대상기관의 정보통신시스템의 운영현황과 주요업무에 적합한 정보통신보안지침(안)을 제시하며, 정보통신보안지침이 마련되어 있는 기관에 대해서는 그 내용상에 추가 및 삭제되거나 수정되어야 하는 내용을 제시한다.

또한, 네트워크 및 시스템 담당자, 보안관리자, 일반사용자 등으로 대상을 구분하여 적절하고 효과적인 보안교육 계획을 수립 및 제시한다. 각 대상별로 적절한 보안교육 내용과 횟수를 제안한다. 보안교육 내용은 대상자의 업무에 실질적으로 적용 가능한 내용을 위주로 한다.

그리고, 대상기관에 적합한 보안사고대응 절차 및 방안을 제시하여 보안사고 발생 시에 적절한 대응이 가능하도록 한다.

• 기술적 보안대책

- 전체네트워크 구성 취약점 분석·평가

대상기관의 업무 및 현재의 네트워크 구성 상황을 기본으로 하여 효과적이고, 안전한 네트워크 구성방안을 제시한다. 이때, 추가적으로 필요한 비용 및 향후 대상기관의 정보통신시스템운영계획을 참조하여 적절한 방안을 제시한다. 또한, 주요 시스템간에 불필요하게 접속을 허용하는 부분에 대해서는 각 시스템의 기능 및 데이터흐름을 이용하여 접속 허용방안을 제시한다. 또한, 부득이하게 외부 DMZ 구간의 시스템으로부터 내부망으로의 접속이 필요하게 되면 보안상 안전하게 운영될 수 있는 방안을 제시한다.

- 침입차단시스템 취약점 분석·평가

침입차단시스템의 보안정책 설정에 불필요한 서비스 및 open 포트에 대한 삭제방안을 제시한다. 또한, 대상기관의 보안정책 운영에 적합하도록 침입차단시스템의 보안정책 설정 룰의 삽입, 삭제 및 수정안을 제시한다.

- 침입탐지시스템 취약점 분석·평가

침입탐지시스템에 불필요한 서비스 및 open 포트에 대한 삭제방안을 제시한다. 또한, 침입차단시스템의 적절한 운영을 위한 운영방안을 제시한다.

- 웹서버 취약점 분석·평가

웹서버에 불필요한 서비스 및 open 포트에 대한 삭제방안을 제시한다. 또한, 웹서버의 안전한 운영을

위하여 운영체제 및 IIS, Apache 등의 패치 설치 방안을 제시한다. 그리고, 웹프로그램 개발상의 버그로 판별된 취약점들에 대해서는 프로그램 소스의 변경 방안을 제시하고, 향후 웹 프로그램 개발시 유의사항을 정리 및 제시한다.

- 주전산기 취약점 분석·평가

주전산기의 운영체제 및 서비스에 대한 패치 설치 방안과 불필요한 서비스 및 open 포트에 대한 삭제방안을 제시한다. 또한, 주요 시스템간에 불필요하게 접속을 허용하는 부분에 대해서는 꼭 접속이 필요한 시스템간의 연결을 정의한다.

- 개인 PC 취약점 분석·평가

개인 PC에 대한 백신프로그램 운영방안, CMOS 암호 및 로그인 암호관리 방안, 공유폴더 암호 및 read/write 권한 관리에 대한 방안을 제시하며, 주기적인 운영체제 및 서비스에 대한 패치 프로그램 설치 방안을 제시한다.

- 라우터 및 스위치 취약점 분석·평가

각각의 라우터에 적합한 access list 구성방안을 제시하여 네트워크간의 접속 상에서 불필요한 접속을 차단하도록 한다. 또한, 라우터 및 스위치에서 발견된 취약점들에 대한 대응방안을 제시한다.

2.2.5 추후보안관리

사후단계에서 제안한 보안대책이 적절히 적용되고 있는지에 대한 검토와 보안관리자, 시스템 및 네트워크 관리자, 일반사용자에 대하여 체계적이고 효과적인 보안교육을 실시한다.

Ⅲ. 결 론

내부 정보의 유출 및 주요시스템의 파괴 등 침해사고가 급증하고 있는 현재 상황을 고려해 볼 때 취약점을 식별하여 제거하는 것은 자사의 보안성을 높이는데 아주 효과적이며 필수적인 사항이다. 본 논문에서 체계적이고, 효과적인 취약점 분석·평가 방법론을 제시하였다. 제안하는 취약점 분석·평가 방법론을 이용하여 대상기관에 존재하는 보안 취약점을 식별하고, 해당 취약점의 위협 정도를 파악하며, 이에 대한 적절한 보안대책을 수립 및 적용할 수 있다.

하지만, 취약점 분석·평가를 수행하였다고 하여 대상기관의 취약점이 모두 제거되었다고는 볼 수 없다. 존재하는 모든 취약점을 식별해 내는 것도 불가능하며, 계속해서 새로운 취약점이 발견되고 공격자는 이러한 취약점을 이용하여 침입을 시도하기 때문이다. 따라서, 주기적으로 취약점 분석·평가를 실시하여 존재하는 취약점을 식별 및 제거하고, 대상기관에 적합한 보안대책을 수립 및 적용하는 것이 효과적이며, 중요하다.

참 고 문 헌

[1] 서정택, 정윤정, 임을규, 김인중, 이철원 "인트라넷 취약점 분석·평가 방법론 연구", *한국정보과학회 춘계학술대회논문집*(A), pp.296~298, 2003.

[2] 박현동, 정윤정, 이철원 "공공기관 취약성 분석·평가 체계", 국가보안기술연구소 기술문서, 2001.

[3] Alberts, Christopher J, Behrens, Sandra G, Pethia, Richard D, Wilson, William R, "Operationally Critical Threat, Asset, and Vulnerability Evaluation(OCTAVE) Framework, Version1.0", Carnegie Mellon University, June 1999.

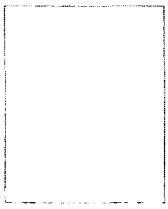
[4] Clifford May, "Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy", Computer Fraud & Security, May 2003.

[5] Hone, K., Eloff, J. H. P, "Information Security Policy-What Do International Information Security Standards Say?", Computers and Security, Oct 2002.

[6] Dhillon, G., Moores, S., "Computer Crimes : Theorizing about the Enemy within", Computers and Security, Dec 2001.

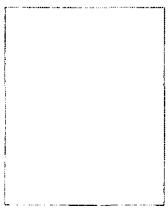
[7] Gerber, M., Von Solms, R., "From Risk Analysis to Security Requirements", Computers and Security, Oct 2001.

〈著 者 紹 介〉



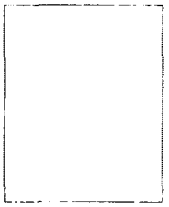
서 정 택 (Jung-Taek Seo)

1999년 2월 : 충주대학교 컴퓨터공학과 졸업(공학사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학석사)
2000년~현재 : ETRI 부설 국가보안기술연구소 연구원
〈관심분야〉 정보전, 시스템/네트워크 보안, 취약점 분석·평가



임 을 규 (Eul Gyu Im)

1992년 2월 : 서울대학교 컴퓨터공학과 졸업(공학사)
1994년 2월 : 서울대학교 대학원 컴퓨터공학과 졸업(공학석사)
2002년 2월 : Univ. of Southern California Computer Science Dept 박사 졸업
2000년~2002년 : WiseNut Inc
2002년~현재 : ETRI 부설 국가보안기술연구소 선임연구원
〈관심분야〉 시스템 및 네트워크 보안, 취약점 분석·평가



이 철 원 (Cheol-Won Lee)

1987년 2월 : 충남대학교 수학과 졸업(학사)
1989년 2월 : 중앙대학교 대학원 전자계산학과(석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 박사과정 수료
1989년~1996년 : 한국전자통신연구원 선임연구원
1996년~2000년 : 한국정보보호센터 선임연구원/통신모델링 과제책임자
2000년~현재 : ETRI 부설 국가보안기술연구소 팀장
〈관심분야〉 컴퓨터 및 네트워크 보안, 정보통신 기반보호, 정보보호시스템 평가기준