인트라넷 취약점 분석·평가 방법론 연구

서정택° 정윤정 임을규 김인중 이철원
국가보안기술연구소
{seojt°, yjjung, imeg, cipher, cheolee}@etri.re.krr

A Vulnerability Analysis and Evaluation Method for Intranet

Jung-Taek Seo°, Youn-Jung Jung, Eul Gyu Im, In-Jung Kim, Cheol-Won Lee
NSRI(National Security Research Institute)

요 약

최근 인터넷을 이용한 침해사고가 급격하게 증가하고 있으며, 그 피해의 파급효과가 매우 커지고 있다. 침해사고로부터 네트워크와 시스템 등의 자산을 보호하는 것이 더욱 중요해지는 실정이다. 크래커들은 대상 네트워크와 시스템에 존재하는 취약점을 찾아내고, 그 취약점을 이용하여 대상 네트워크 및 시스템에 침투하여 악의적인 행동을 하게 된다. 인트라넷에 대한 취약점 분석 평가는 네트워크 및 시스템에 존재하는 취약점을 분석하고, 각각의 취약점을 이용한 침투의 가능여부와 피해 파급효과에 대한 평가를 수행한다. 취약점 분석 평가를 수행함으로써 대상 기관에 적합한 보호대책을 수립하여 침해사고를 사전에 예방하고, 사고 발생시 적절히 대응할 수 있도록 한다. 본 논문에서는 인트라넷 취약점 분석 평가 방법론을 제시하고자 한다.

1. 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 정보보안정책을 악용하는 방식을 사용하고 있다. 인트라넷 취약점 분석·평가는 네트워크나 시스템에 존재하는 취약점을 찾아내고, 모의해킹을 통하여 현재의 보안상태를 점검하며, 발견된 취약점이 어느 정도 위협이 되는지를 평가하게 된다. 또한, 발견된 취약점들에 대한 조치방안과 단기적, 중장기적 보호대책을 수립하여 적용함으로써 대상 기관 정보통신망의 보안성을 높이게 된다. 취약점 분석·평가는 물리적, 관리적, 기술적 부분으로 수행된다.

본 논문에서는 취약점 분석·평가의 수행경험을 토대로 하여 체계적인 취약점 분석·평가 방법론을 제시한다.

2. 정보통신망 취약점 분석·평가 방법론

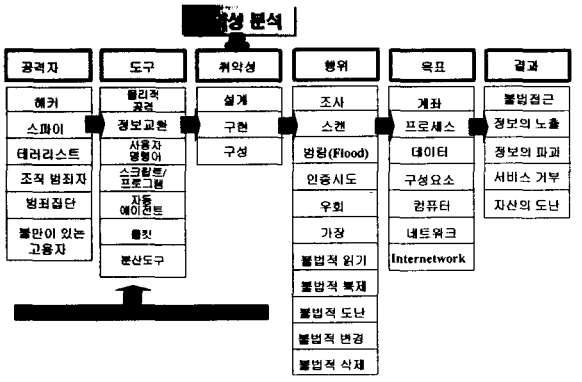
2.1 취약점 분석·평가 개념

취약점 분석·평가의 목적은 해당기관의 정보통신망 및 기존 보호대책에 대한 분석을 수행하고, 분석결과를 바탕으로 물리적, 관리적, 기술적 대응방안을 제시하여 정보통신시스템에 보안체계를 구축하는 것이다.

취약점 분석은 해당기관의 정보통신망에서 소유 및 운영하고 있는 정보시스템을 대상으로 하므로 네트워크, 시스템, 데이터, 소프트웨어 등이 포함된다. 보안시스템인 침입차단시스템 및 침입탐지시스템도 주요 분석 대상에 포함된다. 이러한 정보시스템을 대상으로 취약점 분석도구를 이용하여 진단하며, 침입차단시스템의 경우에는 시스템 자체에 대한 취약점 뿐만아니라 보안정책설정을 집중적으로 점검하게 된다.

취약점 평가는 취약점 분석을 통해 발견된 취약점들이 실제 침입이 가능한지 또한 침입에 성공했을 때 그 피해 파급효과가 어느 정도인지 등을 모의해킹을 통해 시험하고, 이를 이용하여 발견된 취약점들을 우선순위화 한다.

보호대책제시에서는 발견된 취약점들에 대한 즉시조치 사항과 단기적, 중장기적 보호대책을 수립한다.



[그림 1] 취약점 분석

2.1.1 취약점 분석·평가의 중요성

1990년대 이전에는 국가안보 및 비밀성 측면의 보안이 중요시되었으나, 2000년대에는 보안이 국가 주요정보기반구조 보호와 직결되고 있는 상황이며, 공격을 당한 후에 보호대책을 세워도 이미 주요 정보가 유출 파괴되거나, 시스템이 망가진 상태이므로 거의 의미가 없어진

다. 따라서, 취약점 분석·평가를 수행하여 보호대책을 수립하고 적용하는 것이 중요하다.

2.1.2 취약점 분석·평가 수준 결정

취약점 분석·평가를 수행함에 있어 해당기관의 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.

2.1.3 취약점 분석·평가의 범위

취약점 분석·평가는 물리적, 관리적, 기술적으로 구분되어 실시한다.

<표 1> 취약점분석·평가 내용

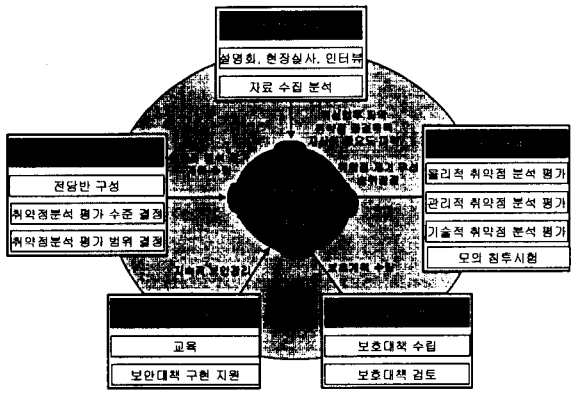
분야	내용	세부내용
물리적	출입통제	- 건물 및 전산실 물리적 접근통제 - 보안요원 및 CCTV
	재난방지 시설	- 소방설비 및 재난대비시설 - 전기설비(UPS 등)
	백업시설	- 백업장비(시스템 및 매체) - 백업 실시 현황(주기, 장소)
관리적	보안조직	- 별도의 보안조직의 구성여부 - 보안조직 업무 효율성 분석 - 보안조직 구성원 업무 능력
	정책 및 지침	- 정책 및 지침의 적절성 - 정책 및 지침의 이행여부
	보안교육	- 보안교육의 실시 현황 - 보안교육 내용
	인터뷰 및 설문	- 보안의식 - 직원들의 보안활동 파악
기술적	전체네트워크 구성	- 외부로부터의 침입 가능성 점검 - 인터넷망과 내부망의 독립성 - 주요 시스템으로의 접근 가능도
	웹서버	- 웹서버 시스템 취약점 점검 - 웹프로그램의 취약점 점검
	주전산기	- 시스템 취약점 점검
	보안시스템	- 침입차단시스템 정책설정 점검 - 침입탐지시스템 탐지능력 및 탐지룰 Update 현황 - 라우터 Configuration

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·평가 범위를 결정한다. 기술적 측면의 범위 결정을 위해서는 해당기관의 주요 자산에 대한 식별하고, 중요도를 점검하여 범위를 결정한다. 또한, 취약점 분석·평가를 효율적으로 수행하기 위하여 전담반을 구성한다. 전담반 구성에는 해당 기관의 네트워크 및 시스템 담당자들이 포함된다.



[그림 2] 취약점 분석·평가 수행절차

2.2.2 사전단계

사전단계에서는 해당기관을 대상으로 하여 취약점 분석·평가 수행에 대한 설명회를 개최하고, 현황분석단계로 물리적, 관리적, 기술적 현황분석을 수행하고, 네트워크 및 시스템 담당자와 부서장들을 대상으로 인터뷰를 실시하며, 전체 직원을 대상으로 설문조사를 실시한다.

o 물리적 현황분석

건물 및 전산실에 대한 출입통제 현황, 제한구역 및 통제구역에 대한 관리현황, 백업장비의 현황 및 백업실시 현황, UPS 등의 전기시설 현황, 소방시설을 포함한 재난대비 시설현황을 분석한다.

o 관리적 현황분석

효과적인 보안업무를 수행을 위한 보안조직의 현황, 보안정책 및 지침의 적절성, 보안교육의 실시 및 교육내용 현황 등을 자료와 인터뷰 및 설문을 통하여 분석한다.

- 인터뷰 : 네트워크 및 시스템 담당자, 정보통신업무 부서 담당자 및 임원진을 대상으로 인터뷰를 통하여관리적 보안현황을 분석한다.

- 설문조사 : 전체직원을 대상으로 설문조사를 실시하여 보안정책, 보안조직구성, 개인 PC 보안관리, 직무보안, 사용자 교육도, 보안사고 대응체계, 보호지역에 대한 관리, 보안의식 등에 대한 현황을 분석한다.

o 기술적 현황분석

해당기관의 전체네트워크 구성도를 통하여 내부망과 외부망의 독립운영현황 및 주요시스템에 대한 접근경로 등을 파악하며, 침입차단시스템 및 침입탐지시스템 등의 보안시스템의 운영현황을 분석하며, 웹서버는 DB서버와의 데이터 흐름도 및 게시판 운용현황 등을 분석하며, 주요 시스템들에 대하여 하드웨어 사양, 운영체제 정보, 응용프로그램 등의 정보를 분석하며, 각 시스템간의 데이터 흐름도를 분석한다.

2.2.3 실시단계

실시단계에서는 취약점 분석·평가를 실질적으로 수행하는 단계이다. 물리적, 관리적, 기술적 취약점을 찾아내고, 발견된 취약점에 대하여 침투시험을 통하여 실제로 침입이 가능한지 테스트하고, 발견된 취약점들에 대한 평가를 통하여 우선순위화 한다.

o 물리적 취약점 분석·평가

건물과 전산실에 대한 출입통제 시설을 점검하고, 건물 내 CCTV 운영현황, 소방설비 설치 현황, UPS 등의 전기설비의 안정성 및 이중화 여부, 자료에 대한 백업 실시 현황과 백업데이터의 이중화 보관 등에 대한 물리적 관점의 취약점을 분석·평가한다.

o 관리적 취약점 분석·평가

조직내의 보안조직의 존재여부와 보안업무의 효율성 및 적절성을 분석하며, 정보통신보안지침의 내용과 지침에 따른 이행여부를 분석한다. 또한, 인터뷰 및 설문조사 결과를 분석하여 보안교육 현황 및 직원들의 보안의식 수준 등을 분석하고, 보안담당자들의 관리 수준 등을 분석·평가한다.

o 기술적 취약점 분석·평가

네트워크 및 시스템에 대한 세부적인 취약점 분석·평가를 수행한다.

- 전체네트워크 구성 취약점 분석·평가 : 전체네트워크 구성에 대한 점검으로 내부망과 외부망의 독립운영여부, 내부 주요서버에 대한 외부로부터의 접속가능 여부와 내부망에서도 필요하지 않은 시스템으로부터의 접근 가능 여부 등을 분석한다.

- 침입차단시스템 취약점 분석·평가 : 진단도구를 이용하여 침입차단시스템 자체에 대한 시스템 취약점을 분석하고, 각각의 보안정책에 대한 적절성을 점검한다. 이때, 불필요한 IP들에 대하여 허용하고 있는지, 불필요한 서비스들에 대하여 허용하고 있는지 각각의 보안정책을 세밀히 분석한다.

- 침입탐지시스템 취약점 분석·평가 : 진단도구를 이용하여 침입탐지시스템 자체에 대한 시스템 취약점을 분석하고, 침입탐지시스템의 탐지 능력, 탐지룰에 대한 Update 현황 등을 분석한다.

- 웹서버 취약점 분석·평가 : 진단도구를 이용하여 시스템 자체에 대한 시스템 취약점을 분석하고, 웹 진단도구를 이용하여 웹프로그램에 대한 취약점을 분석한다. 웹서버는 외부 해커로부터 많은 위협을 직접적으로 받는 시스템이므로 웹프로그램의 소스레벨까지 점검하여 프로그램 개발과정에서 발생된 취약점에 대하여도 세밀히 분석한다.

- 주전산기 취약점 분석·평가 : 주요 시스템에 대하여 운영체제 및 응용프로그램 패치 여부, 불필요한 서비스의 사용여부 등과 시스템에 존재하는 취약점을 진단도구를 이용하여 찾아내고, 발견된 취약점들에 대해서는 침투시험을 통하여 침투 가능여부를 점검한다. 이때, 웹상에 존재하는 각종 exploit code와 도구들을 사용하게 된다.

- 개인 PC 취약점 분석·평가 : 개인 PC들에 대하여 바이러스 감염여부 및 백신프로그램 운영 현황, 공유폴더 패스워드 관리 현황, 각종 패치 설치여부 등을 점검하고, 공유폴더의 경우 크랙도구를 이용하여 패스워드의 크랙을 시도한다.

- 라우터 및 스위치 취약점 분석·평가 : 라우터의 access list를 점검하여 필터링의 실시 내용을 점검하고, 라우터 및 스위치의 관리자 패스워드 사용여부와 패스워드에 대한 크랙 여부 등을 점검한다.

o 취약점 운선순위화

발견된 취약점들을 위험도에 따라 High, Medium, Low의 형태로 분류하고, 우선적으로 조치되어야 하는 것부터 순위화한다.

2.2.4 사후단계

사후단계는 보호대책 수립단계로써 현황분석 및 취약점 분석·평가 단계에서 분석·평가된 내용을 기반으로 대상기관의 특성 및 현실에 적합한 보호대책을 제시하는 단계이다.

o 물리적 보호대책

추가적으로 필요한 출입통제 방안 및 추가시설, 전산실에 대한 출입통제 방안 및 추가시설, 소화시설 및 백업대책에 대한 단기적, 중장기적 보호대책을 수립한다.

o 관리적 보호대책

보안조직의 구성방안, 정보통신보안지침에 추가되어야 하는 내용, 보안교육의 계획 및 교육 내용 등에 대한 단기적, 중장기적 보호대책을 수립한다.

o 기술적 보호대책

네트워크 구성의 변경, 보안장비 및 보안프로그램의 설치, 침입차단시스템의 보안정책설정 변경, 시스템 운영체제 및 응용프로그램 Upgrade, 패치 설치, 불필요한 서비스에 대한 제거 등의 보호대책을 즉시조치 사항과, 중장기적 보호대책으로 구분하여 수립한다. 이때, 침입차단시스템의 보안정책과 같이 즉시조치가 필요한 부분에 대해서는 취약점 분석·평가 단계에서 즉시 조치할 필요가 있다.

2.2.5 추후보안관리

사후단계에서 제안한 보호대책이 적절히 적용되고 있는지에 대한 검토와 보안관리자, 시스템 및 네트워크 관리자, 일반사용자에 대하여 체계적인 보안교육을 실시한다.

3. 결론

본 논문에서 제안하는 체계적인 취약점 분석·평가 방법론을 통하여 대상기관에 존재하는 보안 취약점을 찾아내고, 이에 대한 적절한 보호대책을 수립 및 적용할 수 있다. 계속해서 새로운 취약점이 발견되어 해커들이 이를 이용함으로, 취약점 분석·평가를 수행하였다 하여 모든 취약점이 제거되었다고 단정지을 수는 없지만, 주기적인 취약점 분석·평가의 수행을 통하여 취약점을 최소화해나가는 것이 중요하다.

[참고문헌]

[1] 이형옥, "초고속국가망의 제도적·관리적 보안대책 방안", 정보보호학회학회지, 제 11권, 제 1호