인터넷 사이트 보안 정책

박 진 섭*

요 약

본 고에서는 인터넷 공동체 안에서 보안문제를 어떻게 해결할 것인가에 대하여 시스템과 네트워크 관리자가 구축해야 할 인터넷 보안정책에 관한 보안정책의 개념, 보안목표의 설정, 보안정책의 구축단계 등을 다룬다. 특히 인터넷 사이트 보안정책에서 다루어야 할 영역과 방화벽 보안정책을 중심으로 서술한다.

1. 서 론

많은 기관은 자신의 LAN을 인터넷에 연결하고 그 사용자들은 인터넷 서비스를 편리하게 접근할 수 있기를 원한다. 전체적으로 인터넷을 신뢰하지 않기 때문에 자신의 사설 시스템은 외부공격과 오용에 취약할 수 있다. 방화벽은 안전장치로 신뢰하는 네트워크와 신뢰하지 않는 네트워크 사이에 접근제어를 하는 것이다. 방화벽은 단일 요소가 아니며 조직의 인터넷을 보호하기 위한 전략이다. 방화벽은 비신뢰 네트워크와 좀 더 신뢰하는 내부 네트워크 사이에 출입문 역할을 한다. 방화벽의 주 기능은 접근제어를 집중화하는 것이다. 외부 혹은 원격사용자가 방화벽을 통과하지 않고 내부네트워크를 접근할 수 있다면 그 효용성은 희석된다. 예를 들면 여행중인 관리자가 자신의 사무실 PC에 연결된 모뎀을 가지고 있다면 여행중에 다이얼 할 수 있고, 그 PC가 또한 보호된 내부 네트워크상에 있다면 그 PC에 다이얼 할 수 있는 공격자가 방화벽을 속일 수 있다.

사용자가 상업적 인터넷 서비스 사업자(ISP)로 다이얼-업 인터넷 계정을 가지고 있고 가끔 모뎀을 통하여 자신의 사무실 PC로부터 인터넷에 연결한다면 그는 방화벽을 속인 인터넷에 비보안연결을 하게 된다. 방화벽은 조직의 인트라넷 세그먼트를 보호하기 위해 사용될 수 있으며, 다양한 형태의 보호를 제공한다.

- 방화벽은 원하지 않는 트래픽을 막을 수 있다.
- 방화벽은 좀 더 신뢰하는 내부 시스템에 입력되는 트래픽을 안내한다.
- 방화벽은 인터넷으로부터 쉽게 보호될 수 없는 취약한 시스템을 숨긴다.
- 방화벽은 자신의 네트워크를 통과하는 트래픽을 로그할 수 있다.
- 방화벽은 시스템 이름, 네트워크 토폴로지, 네트워크 장비형태, 인터넷으로부터 내부사용자 ID를 감출 수 있다.
- 방화벽은 응용시스템에 보다 공고한 인증을 제공할 수 있다.

방화벽이 다양한 형태의 정보보호를 제공할 수 있는 기능을 가지고 있다고 할지라도 그 보안정책이 잘 수립되어 있지 못하면 소기의 목적을 달

*대전대학교 컴퓨터공학과 교수

성할 수 없다. 따라서 우선 보안정책의 개념과 목적, 수립 단계를 살펴보고자 한다.

2. 보안 정책

보안 정책은 어떤 조직의 기술과 정보자산 유지를 위해 접근할 수 있는 사람이 따라야하는 규칙의 형식적인 서술이며, 보안 정책의 주된 목적은 사용자와 직원, 관리자들에게 보호 기술과 정보자산의 필수적인 요구조건을 알리는 것이다. 정책은 이러한 요구조건을 충족시킬 수 있는 메커니즘을 명시해야 한다. 그리고 또 다른 목적은 정책을 따르는 컴퓨터 시스템과 네트워크를 획득, 형성, 감사로부터 베이스라인을 제공하는 것이다. 그러므로 어떤 암시된 보안정책이 없는 상태에서 보안 툴을 사용하려는 의도는 무의미하다.

적절한 보안정책의 사용은(AUP:Appropriate Use Policy) 보안정책의 한 부분이다. 사용자들은 시스템의 다양한 구성요소들 위에서 무엇을 할지 여부를 명확히 설명해야 하고, 네트워크 상에서 허락된 트래픽의 형태를 포함해야 한다. AUP는 애매함과 오해를 피하기 위해 가능한 한 명확하게 해야 한다. 예를 들면, AUP는 어떤 금지된 USENET의 뉴스그룹들을 목록화해야 한다

컴퓨터 보안 정책을 만드는 가장 중요한 이유 중의 하나는 비용/효과적인 면에서 이익을 확실하게 하는 것이다.

2.1 보안 목표의 결정

보안과 관련된 결정은 대부분 관리자가 네트워크의 안전여부, 제공기능, 사용하기 쉬운 방법에 대해 결정했을 때에 만들어진다. 그러나, 보안의 목표를 결정하지 않고서는 보안에 관하여 적절한 결정을 할 수 없다. 보안의 목표를 결정할 때까지 무엇을 체크하고 무엇을 제한할 것인지를 전혀 알지 못하기 때문에 어떤 보안도구도 효과적으로 사용할 수 없다.

보안의 목표는 대개 다음과 같은 기준으로 결정된다.

(1) 제공된 서비스 대 준비된 보안

각 서비스는 서비스 자체의 보안 위험을 사용자에게 전하는 것을 제공한다. 왜냐하면 몇몇 서비스에서, 위험의 비중이 서비스의 장점보다 더 크고, 관리자는 이를 안전하게 하려고 하기보다는 서비스를 제거하는 것을 선택할 것이다..

(2) 용이성 대 보안

가장 사용하기 쉬운 시스템은 어떤 사용자든지 접근이 가능하고, 패스워드 없이 획득이 가능한 것이다. 즉 보안책이 없다. 패스워드를 요구하는 것은 시스템 사용이 힘들지만 안전을 보장한다. 1 회용 패스워드 장치 생성을 요구하는 것은 시스템 사용을 더욱 어렵게 하지만 더욱 안전하게 한다.

(3) 보안비용 대 손실위험

· 보안에 대한 많은 다른 비용이 있다.

즉, 재정상(다시 말하면, 하드웨어 보안 장치의 비용, 방화벽이나 패스워드 생성기같은 소프트웨어), 실행상(즉, 암·복호화 시간), 그리고 용이성에 대한 비용이 있다.

· 많은 위험의 레벨들이 있다.

사생활에 대한 손실(즉, 권한이 없는 사용자가 정보를 읽는 것), 정보의 손실(즉, 정보의 변조 또는 삭제), 그리고 서비스에 대한 손실(즉, 데이터의 저장 장소가 가득 찼거나 컴퓨터 사용자원 감소, 그리고 네트워크 접근의 부인)등과 같은 손실 등이 있다.

각 비용의 형태는 각 손실의 형태에 따라 심사 숙고해야만 한다.

보안의 목표는 "보안 정책"이라고 하는 보안 규칙을 통해 모든 사용자와 운영자, 관리자들간에 정보를 전달하는 것이다. 보안 정책의 영역이 정보 기술, 저장된 정보, 기술에 의해 조작되는 정보의 모든 형태를 포함하기 때문에 협의의 "컴퓨터 보안 정책"이란 단어보다 여기에서는 "보안 정책"이란 단어를 사용할 것이다.

2.2 보안정책 구축단계

사이트의 보안정책을 구축하기 위해서는 일반적으로 다음과 같은 단계를 수용한다[Fites].

(1) 보호대상을 명시하기.

(2) 무엇으로부터 보호할 것인지를 결정.

(3) 있음직한 위협을 결정.

(4) 경제적인 요소를 고려하여 자산을 보호할 수 있는 방법을 구현.

(5) 지속적인 검토를 통하여 취약점을 발견시 수준을 향상.

본 서술의 대부분은 항목 4에 초점이 맞춰져 있다. 그러나 효율적인 계획을 세우기 위해 다른 단계를 간과해서는 안된다. 진부할 수 있지만 보안시, 예방비용이 회복비용보다 덜 투자된다는 것을 염두해 두어야 한다. 이에 관련해서 비용은 실제 통화, 평판, 신용, 그 밖에 측정도구 등에 의해 나타나는 손실을 포함하게 된다. 보호대상과 가능한 위협에 대한 지식이 없이 이런 규칙을 적용해서는 안된다.

2.2.1 보호 대상의 식별

위험 분석은 보호를 위해 필요한 것이 무엇인가, 무엇으로부터 보호해야 할 지, 그리고 어떻게 그것을 보호할 것인가를 결정하는 과정을 포함한다. 이 분석은 모든 위험을 시험하고 보안 단계에 의해 위험들의 순위를 매기는 과정이다. 그리고 보호 대상에 대한 경제적인 요인을 고려하여 결정을 하는 것을 포함한다.

위험 분석에 대한 완전한 처리는 여기에서는 영역 밖의 것이다. 그러나 여기에서 간단히 살펴보고자 한다.

- 자산 식별하기
- 위협 식별하기

보안의 기본 목표는 가용성, 기밀성, 무결성이다. 각 위협은 어떻게 이들의 영역에 영향을 미치는가를 눈으로 시험할 수 있다.

(1) 자산 식별

위험 분석의 첫 번째 단계는 보호되어야 할 모든 대상들을 식별하는 것이다. 그들 대상은 가치있는 특허 정보, 지적 자산 그리고 하드웨어의 다양한 부분들과 같이 다양하다. 그러나 시스템을 실제로 사용하는 사람의 경우를 감시해야 한다. 기본적인 요지는 보안 문제에 영향을 주는 모든 일들을 목록화하는 것이다.

일반적으로 자산의 식별 항목은 다음과 같이 분류한다 [Pfleeger 1989].

(ㄱ) 하드웨어 : CPUs, 보드, 키보드, 터미널, 워크스테이션, PC, 프린터, 디스크 드라이브, 통신라인, 터미널 서버, 라우터

(ㄴ) 소프트웨어 : 소스프로그램, 목적프로그램, 유틸리티, 진단프로그램, 운영 체제, 통신 프로그램 등등

(ㄷ) 데이터 : 실행하는 동안 통신 매체를 통과한 저장된 온-라인, 수행된 오프-라인, 백업, 감시기록, 데이터베이스 통신매체의

위에 전송

(ㄹ) 인적자원 : 사용자, 관리자, 하드웨어 유지 보수자 등등

(ㅁ) 문서화 : 프로그램과 하드웨어 시스템, 부분적인 관리 절차 등에 대한 것

(ㅂ) 공급자 : 종이, 형식, 리본, 자기 매체 등등

(2) 위협 식별

보호를 요구한 자산들이 식별될 때, 그 자산에 대한 위협을 식별해야할 필요가 있다. 그런 후에 위협은 잠재적인 손실을 갖고 있는지를 시험하게 된다. 그 결과는 자산을 보호하기 위해 어떤 위협이 있는지를 알 수 있게 한다. 사이트마다 특정의 위협이 있으나 일반적으로 다음과 같은 위협을 고려 할 수 있다.

(ㄱ) 권한 없는 자원과 혹은 정보에 대한 불법 접근

(ㄴ) 부주의 혹은 불법 정보 누설

(ㄷ) 서비스의 거부

2.2.2 보안정책 구축

적절하고 효과적인 보안 정책의 구축을 위해, 조직내 구성원 모든 계층의 수락과 지지를 갖는 것이 필요하다. 특히 공동 관리에 있어서 구성원들 모두에게 영향을 줄 수 있는 보안 정책은 구축 과정에서 완전히 지지가 특히 중요하다. 다음은 보안정책 구축과 관련하여 참여해야 될 구성원 대표를 나타낸 것이다.

(1) 사이트 보안 관리자

(2) 정보기술 기술직원(예를 들면, 전산소의 직원)

(3) 조직 안의 거대한 사용자 그룹의 관리자 (예를 들면, 사업 분야, 대학의 전산학과 등등)

(4) 보안 사건 대응팀

(5) 보안 정책에 영향을 받는 사용자 그룹의 대표

(6) 책임있는 관리자

(7) 법적 자문역

위 목록은 많은 구성원들을 대표하지만, 그러나 반드시 포괄적인 것은 아니다. 아이디어는 운영비와 정책 권한을 가진 관리자, 지지할 대상을 아는 기술직원, 다양한 정책 선택의 법적 효과를 알고 있는 법적 자문역 등으로 제 3 자의 도움이 필요할 수 도 있다. 어떤 조직에서는 EDP 감사 직원을 포함하는 것이 적절할 것이다. 또한 최종 정책문이 가장 폭넓게 배포되어지는 기관을 포함해야 하며, 국가간에 법적 자문역이 변화를 줄 수도 있다.

좋은 보안 정책의 특징은 다음과 같다.

(1) 수용가능한 지침 또는 다른 적절한 방법을 세우고 시스템 관리절차를 통해 구현이 가능해야 한다.

(2) 적당한 곳에 보안도구가 실행되어야 하고, 보호책이 기술적으로 실행 불가능한 곳에서는 사용에 제약을 가해야 한다.

(3) 사용자, 관리자, 기술요원에 대한 책임 영역이 명확하게 정의되어야 한다.

3. 인터넷 사이트 보안정책

모든 인터넷 사이트는 포괄적인 보안 계획(정보 보호 강령)을 정의하고, 개별적인 정책들은 포괄적인 사이트 보안구조를 일관되게 하기위한 하부구조를 갖는것이 중요하다. 예를들어, 인터넷 접근에 대한 강력한 정책을 갖는것과 모뎀 사용에 대한 미약한 제한은 외부 접근에 대한 강력한 보안정책과 전반적인 원리에서 상반되어 소기의 목적을 달성할 수 없다.

인터넷 보안정책에는 일반적으로 다음 사항들을 정의해야 한다.

· 제공된 네트워크 서비스의 목록
· 조직이 서비스를 제공하는 영역
· 서비스에 접근할 수 있는 사람
· 접근방법
· 서비스의 관리자

보안정책에는 또한 보안사건을 어떻게 처리할 것인가를 포함하여야 한다.

인터넷에 연결한 사이트에서 인터넷에 관련된 보안 사건은 내부 보안문제보다 더 신중하고 중요하게 고려해야만 한다.

3.1 인터넷 서비스의 분리

외부 사용자에게 제공되는 사이트는 많은 서비스 종류가 있다. 전용 호스트 컴퓨터의 서비스를 격리시키기 위한 보안상의 이유는 다양하다.

대부분 사이트가 제공하는 서비스는 다른 단계의 접근 요구와 신뢰 모델을 가지고 있다. 사이트의 원만한 운영에 기초를 둔 서비스들은 불안전한 서비스를 제공하는 기계보다는 접근제한을 제공하는 전용기계에 배치하는 것이 더 낫다.

다른 신뢰모델 안에서 작동하는 호스트간의 구별도 또한 중요하다(예를 들면, 방화벽 안에 있는 모든 호스트들과 노출된 네트워크에 있는 호스트).

보안이 체인 안의 가장 약한 링크만큼 유지된다는 것을 기억하는 것은 중요하다. 최근 몇 년 동안 가장 공식화된 침해는 전자우편의 취약점을 이용한 것이다. 침입자는 전자우편을 훔치려고 시도하지는 않지만 다른 시스템에 대한 접근을 얻기 위해 서비스의 취약점을 이용한다.

가능한 한 각 서비스는 상이한 기계에서 특정 서비스를 제공하도록 할 필요가 있다. 이것은 침입자를 고립시키고 잠재된 피해를 제한하기 위함이다.

3.2 모두 부인/모두 허용

보안정책을 정의할 때 사용되는 두개의 정 반대적이고 근원적인 철학이 있다. 합법적인 모델은 두 가지를 모두 수용하는 것이며 한 가지를 선택하는 것은 사이트와 보안에 대한 요구에 의존한다.

첫 번째 옵션은 모든 서비스를 제거하고 필요로 하는 서비스를 개개의 사례에 따라 사용 가능하게 하는 것이다. 이 방법은 호스트나 네트워크 단계에서 적절히 할 수 있다. "모두 부인"으로 간주되는 이 모델은 일반적으로 다른 모델보다 더 안전하다. 많은 작업에서 "모두 부인"상태를 구현한다. 알려진 서비스들을 수용하는 것이 특정 서비스와 프로토콜의 분석과 사이트의 보안 수준에 맞는 보안 메커니즘의 설계를 제공한다.

"모두 허용"이라고 불리는 다른 모델은 구현하기에는 무척 쉬우나 일반적으로 "모두 부인"모델보다 불안전하다. 호스트 단계에서 묵시적으로 모든 서비스를 설치한 뒤 모든 프로토콜이 라우터 단계에서 네트워크에 접근하는 것을 허용한다. 보안의 허점이 나타나면 그들은 호스트나 네트워크 단계에 제한을 가하거나 임시 교정을 하게 된다.

각 모델들은 기능상의 요구와 관리 통제, 사이트 정책 등에 의존한 사이트의 부분에 적용된다. 예를 들어, 정책이 워크스테이션에 수용될 때 "모두 허용"모델을 채택할 수 있다. 그러나 전자우편 허브와 같은 정보서버를 설치할 때 "모두 부인"모델을 사용할 수 있다. 그리고 "모두 허용"정책은 LAN의 내부와 사이트간에 트래픽을 위해 사용할 수 있고, "모두 부인"정책은 사이트와 인터넷 사이에서 채택될 수 있다.

위에서 설명한 두 가지 형태의 모델 철학을 혼합할 때 주의해야 한다. 많은 사이트들은 엄격하거나 유연한 보통의 이론을 채택한다. 이 사이트들은 그들의 외부 트래픽의 보안에 투자하고자 강한 보안도구를 요구한다.

3.3 필요한 서비스의 식별

일반적으로 인터넷에서 제공되는 매우 다양한 서비스들이 있다. 보안관리는 사이트의 내부서비스에 대한 접근관리, 어떻게 원거리 사이트에 있는 내부 사용자의 접근 정보를 관리하는가에 대한 많은 방법들이 있다.

서비스들은 인터넷을 통해 파도와 같이 쇄도하는 경향이 있다. 몇 년동안 꼭 필요한 것은 아니지만 많은 사이트들은 어노니모우스 FTP 서버, 고퍼 서버, whois 서버, WWW 서버 등을 발표했다. 그러나 모든 사이트에서 특히 필요한 것은 아니다. 회의적인 태도를 보이면서 발표된 모든 새로운 서비스들이 인터넷에 사실상 필요한지 아니면 일시적인 유행인지를 평가해야 한다.

보안의 복잡성에서 명심해야 하는 것은 제공된 서비스가 지수적으로 증가하고 있다는 것이다. 라우터에서 필터링하는 것은 새로운 프로토콜을 지지하기 위해 변경될 필요가 있다. 본질적으로 몇몇 프로토콜은 안전하게 통과되기가 힘들다(예를 들면, RPC와 UDP 서비스). 이와같은 경우에 내부 네트워크에만 개방을 제공해야 한다.

3.4 네트워크와 서비스의 구성

3.4.1 하부구조 보호

많은 네트워크 관리자들은 그들의 네트워크 호스트들을 철저히 보호한다. 물론 극히 소수의 관리자들은 네트워크를 보호하기 위한 노력을 하지 않기도 한다. 이것에 대해 몇몇 이론적 근거가 있다. 예를 들어, 네트워크보다 호스트를 보호하는 것이 더욱 쉽다. 또한 네트워크에 손상을 입히는 것이 목적이 아니므로 침입자들은 호스트상의 데이터에 잠복하기를 좋아한다. 그러나 침입자는 데이터를 시험하기 위해 외부의 호스트를 통해 네트워크의 트래픽을 유용한다. 하부구조에는 네트워크와 그들을 상호 연결하는 라우터를 포함한다. 하부구조는 또한 네트워크 관리(SNMP)와 서비스(DNS, NFS, NTP, WWW)와 보안(즉, 사용자 권한과 접근 제한 등)을 포함한다.

또한 하부구조는 인간의 실수에 대해 보호할 필요가 있다. 관리자가 호스트를 잘못 배열을 했을 때, 호스트는 가치가 없는 서비스를 제공하게 된다. 이것은 그(기본 서버가 아닌)호스트를 요구하는 사용자에게 영향을 미치고, 그 때문에 영향을 받은 다수의 사용자들이 제한될 것이다. 명확히 이것은 어떤 하나의 호스트에 의존하는 사용자보다 더 많은 수의 사용자가 있을 것이다.

3.4.2 네트워크 보호

네트워크가 공격받기 쉬운 몇 개의 문제점이 있다. 고전적인 문제로 "서비스 부인"공격이다. 이 경우, 네트워크는 합법적인 사용자의 데이터를 더 이상 가져올 수 없는 상태가 온다. 이와같은 방법에는 두 가지가 있다.

- 라우터를 공격하는 것
- 외부로부터의 트래픽이 네트워크에서 범람하도록 하는 것

여기에서 라우터의 의미는 방화벽, 프록시 서버와 같은 구성요소를 포함한 활성화된 네트워크의 상호접속 구성요소 보다 더 큰 종류의 의미로 사용된다.

라우터에 대한 공격은 패킷이 라우터로 향하지 못하도록 하는 것이다. 앞의 경우에는 잘못배열, 위조 라우팅 업데이트의 투입, 혹은 "쇄도하는 공

격"이 원인이 된다. 네트워크에 대해 쇄도하는 공격은 넘치는 패킷이 평상시 유포되는 것을 제외하고 라우터에 대한 쇄도공격과 유사하다. 이상적인 넘치는 공격은 네트워크의 노드들에서 알려진 몇 개의 흠집을 활용하고 패킷을 재 전송하도록 하는 단일 패킷의 투입을 하고, 잘못된 패킷을 생성하고, 이들 각각은 또 다른 호스트에 의해 반복되고 선출된다. 잘 선택된 공격패킷은 전송이 지수적으로 증가하게 된다.

다른 고전적인 문제는 "눈속임"(spoofing)이다. 이 경우, 가짜 경로갱신은 잘못 발송된 패킷을 만들면서 하나 이상의 라우터에 보낸다. 이것은 서비스 거부와 다르다. 서비스거부에서 객체는 라우터를 사용 불가능하게 만들고 이러한 상태는 네트워크의 사용자에 의해서 빠르게 발견된다. 눈속임에서 위조 라우터는 패킷으로 하여금 침입자가 패킷에 있는 데이터를 감시할 수 있는 호스트에 발송될 수 있게 한다. 그런 후 위조 패킷은 다른 목표를 향해 재 발송된다.

이 문제의 해결책은 라우팅 갱신패킷이 사용중에 있는 라우팅 프로토콜에 의해 보내지는 것을 보호하는 것이다(RIP-2, OSPF).

보호에는 세 가지 수준이 있다.

- 읽기힘든 패스워드
- 암호 검사
- 암호화

패스워드는 물리적 네트워크를 직접 접근할 수 없는 침입자로부터 최소한의 보호를 제공한다. 패스워드는 또한 잘못 배열된 라우터에 대해 약간의 보호를 제공한다. 패스워드의 장점은 대역폭과 CPU 소비 등 일반적으로 비용이 매우 적게 든다는 것이다. 체크섬은 위조된 패킷의 투입과 비록 침입자가 물리적인 네트워크에 직접 접근한다 할지라도 보호한다. 순서화된 수로 조합되거나 단일 식별자들로 조합된 체크섬은 재공격으로부터 보호할 수 있다. 재공격은 갱신된 것을 침입자나 부정한 라우터에 의해 전송되는 것이다. 최고의 보안은 순서화된 또는 유일하게 식별될 수 있는 라우팅 갱신의 완전한 암호화에 의해 제공된다. 이것은 침입자가 네트워크의 위상을 결정하는 것을 보호한다. 암호화의 단점은 갱신을 처리하는데 드는 경비가 많다는 것이다.

RIP-2(RFC 1723)과 OSPF(RFC 1583) 둘다 읽기힘든 패스워드를 지원한다. 추가적으로 각각 기본 프로토콜은 MD5 암호화를 지원한다.

불행히도, 무차별 공격과, 네트워크에 넘치는 잘못된 호스트와 라우터에 대한 적당한 보호책은 없다. 다행히도 이 공격의 형태는 공격이 일어난 때와 종료할 때가 명확하다.

3.4.3 서비스 보호

서비스의 종류는 다양하며 각각은 자신의 보안 필요조건을 가지고 있다. 이러한 필요조건은 예정된 서비스의 사용에 대한 것이다. 예를 들어, NFS와 같이 사이트내부에서 사용될 서비스는 외부에서 사용 가능한 서비스와는 다른 방어메커니즘을 요구한다. 이것은 외부접근으로부터 내부서버를 보호해야 한다. 그러나 WWW서버는 내장 방어책을 제공한다. 즉, 서비스/프로토콜/서버는 비 권한접근과 웹 데이터베이스의 수정을 막을 수 있어야 한다.

일반적으로 내부서비스와 외부서비스는 이미 기술된 것과 다른 보호자격을 가지고 있다. 그러므로 서버 호스트컴퓨터의 한 집합체인 내부서비스와 다른 집합체인 외부 서비스는 별개로 존재하게 해야된다. 많은 사이트들이 외부로부터 접근가능한 서브넷집합과 사이트 안에서 접근할 수 있는 또 다른 집합을 갖는다. 물론 이 부분들을

연결하는 방화벽이 있다. 최고의 보호는 방화벽과 같은 것이 적절한 동작을 보장하는 것이다.

최근 많은 조직에서 인트라넷의 사용에 대해 관심이 증가하고 있다. 일반적으로는 외부와 내부를 구별하지만, 인트라넷을 사용하는 사이트들은 서비스를 설계·제공할 때 세 가지의 분류를 고려하여 개별의 행동을 취할 필요가 있다. 인트라넷이 제공한 서비스는 공개적인 것도, 단일 조직의 부 단위 서비스와 같이 완벽하게 개인적인 것도 아니다. 그러므로 서비스를 지원하는 내부·외부서비스와 네트워크가 분리된 시스템이 필요하다.

외부서비스의 한 형태로 익명 혹은 게스트 접근이 있다. 이것은 익명의 FTP 또는 게스트(비권한적인) 로그-인이라고 할 수 있다. 익명의 FTP와 게스트 로그-인의 사용자ID는 외부사용자가 유지하는 파일 시스템과 임의의 호스트로부터 격리되어야 한다. 또 다른 익명의 영역으로는 읽기 가능한 접근이 있다. 사이트는 법적으로 공개된 유용한 정보의 내용에 대해 책임을 져야한다. 그래서 익명의 사용자가 맡긴 정보를 감시하는 작업이 있어야 한다.

여기에서 name service, password/key service, 권한/대리 서비스, 전자우편, WWW, 화일전송, NFS등의 가장 인기 있는 몇 개의 서비스에 대해 생각할 수 있다. 이 서비스들은 자주 사용될 뿐만 아니라 주 공격대상이다. 그리고 이 서비스에 대한 공격이 성공하게 되면 기본서비스의 무결성을 보장할 수 없게 된다.

3.4.4 DNS & NIS(+)

인터넷은 호스트와 네트워크의 주소해결을 하기 위해 DNS를 사용한다. NISD와 NIS(+)는 전체 인터넷에서 사용되지는 않지만 DNS 서버와 같은 위험에 당하게 된다. Name-to-address 해결책은 임의의 네트워크의 운용을 안전하게 하는 데에 결정적인 영향을 준다. DNS 서버를 통제하거나 구현할 수 있는 침입자는 보안책을 파괴하고 재발송 트래픽을 할 수 있다.

기관(조직)은 보조 네임서버로서 행동하고 필터링 라우터를 사용하여 서비스 공격부인으로부터 DNS마스터를 보호하기 위한 사이트를 생성해야한다.

전통적으로 DNS는 분산능력이 있다. 특히 질문으로부터 반환된 정보가 수정되었는지, 네임서버로부터 온 것인지 명확하지 못하다. 프로토콜에서의 작업은 무결한 정보를 가져온 프로토콜 안에서 디지털신호를 통합하는 것이다.

3.4.5 패스워드/키 서버(NIS(+) and KDC)

일반적으로 패스워드와 키 서버는 암호화 알고리즘을 가지고 정보를 보호한다. 그러나 단방향 암호화된 패스워드는 사전공격(dictionary attack; 일반단어가 저장된 암호와 일치하면 확인해서 공격하는)으로 결정된다. 그러므로 이 서버들이 서비스를 제공할 계획이 없는 호스트는 접근할 수 없다는 것을 보장해줘야 한다.

3.4.6 인증/프록시 서버(SOCKS, FWTK)

프록시 서버는 보안강화에 증대를 가져왔다. 이것은 사이트에 특정호스트가 내부구조를 감시하고 서비스가 집중되는 것을 허용한다. 서비스의 집중은 침입자의 공격목표가 된다. 프록시 서버를 요구한 방어유형은 대개 사용중인 프록시 프로토콜과 프록시 서비스에 의존한다. 서비스를 필요로 하는 호스트와 서비스를 그 호스트만 접근하도록 한 제한규칙은 방어의 시작점이다.

3.4.7 전자 우편

전자우편 프로토콜이 가장 오래된 서비스로 가장 널리 배치된 서비스이기 때문에 전자우편 시

스템은 오랫동안 침입의 근원지가 되어 왔다. 또한 그 특성에 의해 전자우편 서버는 외부세계에 접근을 요구하므로 대부분은 임의의 근원지에서 입력을 받아들인다. 전자우편 서버는 일반적으로 송수신 에이전트와 프로세싱 에이전트 두 부분으로 구성되어 있다. 전자우편이 모든 사용자에게 배달되고 항상 개인적이기 때문에 프로세싱 에이전트는 전형적으로 특권을 가진 루트(root)시스템에 우편을 배달하도록 요구한다. 대부분의 전자우편 구현은 수신 에이전트가 시스템의 특권을 가지는 것을 의미하는 서비스를 실행한다. 이것은 여기에서 언급하지 않는 몇몇 보안허점이 발생한다. 두 에이전트를 분리하는 구현방법들이 있다. 이런 구현방법은 일반적으로 안전한 것으로 생각되지만, 문제가 발생되지 않게 신중하게 설치해야 한다.

3.4.8 WWW

웹은 사용이 쉽고 정보서비스를 집중하기 때문에 지수적으로 증가하고 있다. 몇몇 프로그램들은 보안을 제공하지 않아 보안구멍을 만들어낸다. 만약 인터넷 단체에 유용한 웹 서버라면 비밀정보가 같은 호스트상에 위치하지 않는 것이 특히 중요하다.

많은 사이트들은 WWW서버와 함께 FTP서비스를 같이 배치하기를 원한다. 그러나 단지 정보를 제공하는 익명의 FTP에서만 사용된다. WWW와 조합된 익명의 FTP를 사용하게 되면 위험이 증가하게 되고 자체에 있는 각각의 서비스가 상이한 점을 고려해서 보안을 제공해야 한다.

3.4.9 파일 전송(FTP, TFTP)

FTP와 TFTP 모두 사용자에게 점대점 방식에서 파일을 받고 보내는 것을 허용한다. 그러나 TFTP가 아무 것도 요구하지 않는 반면에 FTP는 인증을 요구한다. 이런 이유로 TFTP는 가능한 한 사용하지 않는 것을 권장한다.

부적절하게 배열된 FTP서버는 침입자에게 파일 복사와 재배치, 삭제를 허용하므로 서비스를 정확하게 배열해야 한다. 암호화된 패스워드에 접근하는 것과 독점 데이터, 트로이목마의 침입은 서비스가 부정확하게 배열되었을 때 일어날 수 있는 보안구멍이다. FTP서버는 그들 자신의 호스트에 존재한다. 두 프로토콜이 공통의 보안대책을 갖은 이후로 몇몇 사이트들은 웹 서버와 FTP를 같이 배치하는 것을 선택하기도 한다. 그러나 실행은 권고되지 않는다. 특히 FTP서비스가 파일의 저장을 허용할 때는 그러하다. 앞서 언급한 것과 같이 사이트에 내부적으로 제공된 서비스들은 외부적으로 제공된 서비스와 함께 배치되지 않도록 하고 각각 자신의 호스트를 갖게 해야된다.

TFTP는 FTP와 같은 기능을 제공하지 않기 때문에 보안이 되지 안는다. 이 서비스는 내부 사용에 대해서만 고려를 했고 그런 후 제한방법을 배열해서 서버가 이미 결정된 파일의 집합에만 접근할 수 있다. TFTP는 자신의 호스트에 존재하고 외부 FTP나 웹 접근을 지원하는 호스트에는 설치되지 않아야 한다.

3.4.9 NFS

네트워크 파일 서비스는 호스트에 공통 디스크를 사용할 수 있도록 한다. NFS는 자주 기억장소를 디스크서버에 전부 의존하는 디스크 없는 호스트를 사용하곤 한다. 불행히도 NFS는 적절한 보안책이 없다. 그래서 NFS 서버는 서비스를 위해 사용되는 호스트에만 접근이 가능하게 한다. 이것은 파일 시스템이 호스트에 제공하는 것과 어떤 방식(읽기 전용, 쓰기 전용 등)을 제공할 것인지를 명시함으로써 수행된다. NFS서비스가 외

부적으로 접근할 수 있는 것을 요구하면 파일 시스템들은 지역네트워크 외부에 있는 임의의 호스트에 그 기능을 제공하지 않는다. 따라서 NFS서비스에 대한 외부접근은 방화벽에 의해 중지된다.

3.4.10 보호책을 보호

사이트가 공격에 대해 보안서버 자체를 열어놓으면 보안상 가장 명백한 취약점이 된다. 따라서 이미 거론된 관점에 따라 다음사항이 지켜져야 한다.

- 보안서버는 off-site로부터 접근이 불가능하다.
- on-site의 사용자에게 인증을 제외한 최소한의 접근을 제공해야 한다.
- 그리고 임의의 서버와 함께 배치되지 않아야 한다.
- 서비스 자체에 접근하는 모든 노드에 대해서는 추적을 제공하면서 로그 할 수 있어야 한다.

3.5 방화벽

인터넷 사용에서 가장 널리 알려진 공식화된 보안도구 중 하나가 방화벽이다. 방화벽은 많은 인터넷 보안문제에 일반적인 만병통치약의 호평을 받아왔다. 그러나 그렇지가 않다. 방화벽은 시스템 보안탐구에 대한 또 다른 도구일 뿐이다. 방화벽들은 보호의 확실한 단계를 제공하고 일반적으로 네트워크 수준에서 보안정책을 구현한 방법이다.

방화벽을 기반으로 한 라우터는 사용자 인증을 제공하지 않는다. 따라서 더 향상된 보안을 위해서 방화벽을 기반으로 한 방어거점(Bastion)호스트를 두어 다음과 같은 종류의 인증을 제공할 수 있다. 방화벽 정책은 다음절에서 간략히 언급한다.

- 사용자 이름/패스워드 : 그정보가 반복 시행으로 노출될 수 있기 때문에 가장 취약한 종류이다.
- 1회용 패스워드 : 소프트웨어나 하드웨어 토큰을 사용한 1회용 패스워드는 매 세션마다 새로운 패스워드를 생성한다. 이것은 과거 패스워드가 재사용 될 수 없어 노출되거나 도둑맞을 염려가 없음을 의미한다.
- 전자서명 : 공개키 암호를 사용하여 생성된 서명을 사용한다.

4. 방화벽 보안정책

방화벽이 인터넷 패킷의 경로선택 혹은 중계자로서의 여부가 명확하게 정책에 기술되어야 한다. 이것은 라우터가 패킷 필터링 게이트웨이로 작용하는 경우에는 방화벽(이 경우에 라우터)은 옵션 없이 단지 패킷을 라우트 한다.

일반적으로 응용 게이트웨이 방화벽을 외부 인터페이스와 내부 네트워크 인터페이스 사이에 임의의 트래픽을 라우트하기 위해서만으로 구성하지는 않는다. 왜냐하면 이것은 보안통제를 피할 수 있기 때문이다. 모든 외부의 내부연결은 응용 프록시(Proxy)를 통과 해야만 한다.

4.1 방화벽 타입

방화벽은 다양한 방법으로 구현될 수 있다.

표 1 은 다양한 방화벽 구조를 나타내며 그 등급은 "낮음", "중간", "높음"이라는 위험처리 환경으로 분류된다.

4.1.1 패킷 필터링 게이트웨이

패킷 필터링 방화벽은 소스 주소, 목적지 주소와 포트를 기반으로 접근을 승인하거나 거부하는

표 1

방화벽 구조	"높음" 위험 환경 예 : 병원	"중간" 위험 환경 예 : 대학	"낮음" 위험 환경 예 : 꽃집
패킷 필터링	0	1	4
응용 게이트웨이	3	4	2
복합 게이트웨이	4	3	2

4	recommended choice
3	effective option
2	acceptable
1	minimal security
0	unacceptable

패킷 필터링 규칙을 가지는 라우터를 사용한다. 이것은 매우 저가격의 최저 보안을 제공하고 "낮음" 위험환경에서 선택될 수 있다. 이것은 빠르고 유연성이 있으며 투명하다. 필터링 규칙은 라우터 상에서 쉽게 유지되지 않는다. 따라서 규칙을 유지하고 생성하는 일을 간단히 하기 위해 툴(Tool)이 존재한다. 필터링 게이트웨이는 타고난 위험을 가지고 있다. 즉, IP 패킷 헤더에 포함된 소스, 목적지 주소와 포트가 유일한 정보로 내부 네트워크에 트래픽 접근을 허용할 것인지 여부를 결정한다.

- IP 혹은 DNS 주소 속임수에 대해 방어하지 못한다.
- 공격자는 방화벽에 의해 일단 승인되면 내부 네트워크에 접속된 어떤 호스트로의 접근도 가능하다.
- 강력한 사용자 인증은 패킷 필터링 게이트웨이에서 대부분 지원되지 않는다.
- 아주 미미한 로깅을 제공한다.

4.1.2 응용 게이트웨이

응용 게이트웨이는 방화벽 상에서 수행하는 서버 프로그램(Proxy)을 사용한다.

이들 프록시는 외부의 요청에 대하여 그들을 시험하고 적절한 서비스를 제공하는 내부 호스트에 적법한 요구를 전달한다. 응용 게이트웨이는 사용자 인증과 로깅 같은 기능을 제공할 수 있다. 응용 게이트웨이가 비교적 안전한 방화벽으로 여겨지기 때문에 이 구성은 "중간-높음"의 위험 사이트에 많은 장점을 제공한다.

- 방화벽이 네트워크 외부에서 볼 때 단지 하나의 호스트 주소로 구성된다.
- 다양한 서비스를 위한 프록시들의 사용은 불안전하거나 잘못 구성된 내부 호스트를 가진 기업을 보호하기 위하여 내부 네트워크 상에 있는 서비스를 직접 접근하지 못하도록 방어한다.
- 강력한 사용자 인증이 응용 게이트웨이에 장착될 수 있다.
- 프록시는 응용수준에서 자세한 로깅을 제공할 수 있다.

응용 게이트웨이 방화벽을 통하여 지원되는 각 서비스(FTP, HTTP 등)마다 프록시를 요구한다. 프록시에 의해 지원되지 않는 서비스가 요청될 때 그 기관(조직)은 3가지 선택이 가능하다.

- 안전한 프록시를 방화벽 공급자가 공급할 때까지 서비스를 거부하는 방법
- 사용자가 프록시를 개발하는 방법
- 방화벽을 통과시켜 서비스를 제공하는 방법

"낮음"

프록시에 의해 지원되지 않는 인터넷 서비스가 방화벽 통과를 요구할 때 방화벽 관리자는 요구

된 서비스를 허락할 구성과 플러그를 정의해야만 한다. 방화벽 공급자로부터 프록시가 제공될 때는 그 플러그를 제거하고 프록시가 운용하게 한다.

"중간-높음"

방화벽의 프록시 소프트웨어에 의해 인터넷 서비스가 처리되어야만 한다. 만약 새로운 서비스가 요청된다면 그 서비스는 프록시가 확보되고, 관리자에 의해 테스트 될 때까지 보류하여야 한다.

4.1.3 복합 게이트웨이

복합 게이트웨이는 앞서의 방화벽 형태를 두 개 이상 결합한 것이며 병렬이 아닌 직렬의 형태로 구현된다. 직렬로 연결된다면 보안은 더욱 강화된다. 반면에 병렬로 연결된다면 네트워크 보안 척도는 가장 낮은 보안 척도의 방화벽으로 보호될 것이다. "중간-높음"의 위험 환경에서 복합 게이트웨이는 이상적인 방화벽 구현이 될 수 있다.

4.2 방화벽 관리

다른 네트워크 장치와 마찬가지로 방화벽은 누군가에 의해 관리되어야 한다. 보안정책은 방화벽 관리책임이 누구인지 언급해야 한다. 두명의 방화벽 관리자(주, 보조)는 정보보안 부서장에 의해 지명될 수 있다. 주 관리자는 방화벽을 변경할 수 있고, 보조 관리자는 단지 주 관리자 유고시에만 조작해야 하며 동시에 접근해서는 안된다. 각 방화벽 관리자는 거주지 전화번호, 삐삐번호, 휴대폰 번호, 기타 번호나 코드로 지원이 요청될 때 접속할 수 있어야 한다.

4.2.1 방화벽 관리자 자질

일상적 방화벽 관리를 위해 일반적으로 두 명의 경력자를 권고한다. 이와 같은 방법으로 방화벽 관리기능의 가용성은 극대화된다.

사이트 보안은 그 기관의 매일 매일 업무행위에 중요하다. 그러므로 방화벽의 관리자는 네트워크 개념과 구현에 대한 이해가 요구된다.

4.2.2 원격 방화벽 관리

방화벽은 공격자에게 보이는 1차 방어선이다. 방화벽은 일반적으로 직접 공격하기가 어렵다. 공격자는 종종 방화벽에 대하여 종종 관리계정을 목표로 한다. 관리 계정의 사용자 이름/패스워드는 엄격히 보호되어야 한다. 이러한 형태 공격으로부터 가장 안전한 보호방법은 방화벽 호스트 주위의 강력한 물리적 보안을 하는 것이며, 단지 접속된 터미널로만 방화벽 관리를 허용하는 것이다. 그러나 운영상 종종 방화벽 관리가 원격 접근 형식으로 이루어진다. 이때 강력한 인증없이 비신뢰 네트워크를 통해 방화벽에 대한 원격접근이 되어서는 안된다.

또한 도청을 예방하기 위하여 세션 암호화가 원격 방화벽 연결시 사용되어야 한다.

4.2.3 사용자 계정

방화벽은 결코 일반 서버목적으로 사용되어서는 안된다. 단지 방화벽에 대한 사용자 계정은 방화벽 관리자와 백업 관리자에게만 주어져야 한다. 또한 단지 이들 관리자들은 시스템 수행을 갱신하거나 기타 시스템 소프트웨어에 대한 권한이 주어진다.

"방화벽 관리자와 백업 관리자에게만 회사 방화벽에 사용자 계정을 준다. 방화벽 시스템 소프트웨어의 수정은 방화벽 관리자 혹은 백업 관리자에 의해서만 수행되어야 하고 네트워크 서비스 관리자의 인가를 요구한다."

4.2.4 방화벽 백업

고장이나 자연재해 발생시 복구하기 위해 다른

네트워크 호스트와 마찬가지로 방화벽은 시스템 백업을 정의하는 어떤 정책을 가지고 있어야만 한다. 시스템 구성 파일과 마찬가지로 데이터 파일은 방화벽 고장의 경우에 백업 계획을 가질 필요가 있다.

방화벽(시스템 소프트웨어, 구성 데이터, 데이터 파일 등)은 일일, 주간, 월간 백업이 되어야만 하며, 시스템 고장의 경우에 데이터와 구성파일이 복구할 수 있어야 한다. 백업파일은 읽기전용 매체에 안전하게 저장되어야 하며, 저장된 데이터는 부주의에 의해 덮어쓰기가 되지 않도록 해야 하며, 단지 적절한 사람에게만 접근되어야 한다.

또 다른 백업은 현재의 방화벽 고장시 안전하게 운용할 수 있도록 또 다른 방화벽을 더 구축하는 것이다. 이와같은 백업 방화벽은 앞서의 방화벽 고장시, 고장 수리시간 동안에 대체될 수 있다.

4.3 기타 방화벽 정책

방화벽은 네트워크와 호스트 보안과 밀접한 관계를 가지고 있기 때문에 보안정책에 있어서도 밀접한 관계를 가진다.

간단히 요약하면 다음과 같다.

- 네트워크 신뢰관계
- VPN
- 시스템 무결성
- 문서화
- 물리적 보안
- 방화벽 사고처리
- 서비스의 복구
- 방화벽 업그레이드
- 방화벽 정책의 개정과 갱신
- 로그와 감사추적

5. 인터넷 서비스 정책 예

인터넷 접속은 인터넷 사용자에게 폭 넓은 서비스를 제공하고 외부 사용자에게 폭 넓은 시스템 접근을 제공한다. 업무의 필요성 혹은 기관의 역할에 따라서 정책은 내부, 외부 네트워크 각각에 어떤 서비스를 허용할 것인지의 여부를 명백히 문서로 작성하여야 한다. 인터넷 서비스는 다양하지만 가장 보편적인 서비스만을 언급하고자 한다.

rsh, rlogin, rcp 등과 같은 BSD의 "r" 명령은 원격 시스템에서 명령을 UNIX 시스템 사용자에게 허용되도록 설계되었다. 대부분은 인증이나 암호화를 지원하지 않아 인터넷 상에서 사용은 많은 위험이 있다.

POP(Post Office Protocol)은 서버로부터 E-메일을 검색하기 위한 클라이언트-서버 프로토콜이다. POP은 인증에서 APOP이라고 하는 재사용되지 않는 패스워드 사용을 지원하는 TCP 기반 서비스이다. 암호화 검색 E-메일을 제공하지 않는 POP은 도청에 취약점이 있다.

NNTP(Network News Transfer Protocol) 은 Usenet 뉴스그룹을 지원하기 위해 사용된다. NNTP는 축적-전송 프로토콜을 구현한 TCP 기반 서비스이다. NNTP가 상대적으로 간단한 프로토콜이기 때문에 공공 NNTP 서버 소프트웨어에 대한 공격이 최근에 발생되고 있다. NNTP 서버는 방화벽에서 수행되지 않지만 표준 프록시 서비스는 NNTP 통과를 가능하게 한다.

핑거(Finger)와 whois는 유사한 기능이다. 핑거는 시스템 사용자에 대한 정보를 검색하는데 사용된다. 핑거는 종종 필요이상의 정보를 주기 때문에 대부분의 기관에서 핑거는 방화벽에 국한하거나 금지되어야 한다. whois도 매우 유사하며

방화벽에 국한하거나 금지되어야 한다.

UNIX 원격 프린팅 프로토콜 lp와 lpr는 원격 호스트가 다른 호스트에 접속된 프린터를 사용하여 프린트하는 것을 허용한다. lpr은 축적-전송 프로토콜이다. lp는 원격 프린팅을 제공하기 위해 rsh 기능을 사용한다. 일반적으로 lp와 lpr은 공급자가 관련 프록시를 제공하지 않는 방화벽에서는 금지되어야만 한다.

Real Audio는 TCP/IP 네트워크로 디지틀 오디오를 전달해준다.

WWW의 멀티미디어 능력에 대한 장점을 취하기 위해서 많은 신규 서비스가 개발되고 있다. 어떤 인터넷 서비스가 허가되고 거부될 것인지는 기관의 필요에 따라야 한다. 전형적 기관에 의해 요구되어질 수 있는 이러한 인터넷 서비스들에 대한 보안 정책 예는 <표 2>에 나타낸다.

표 2. 인테넷 보안정책 예

서비스	정책				정책 예
	내부에서 외부로		외부에서 내부로		
	상태	인증	상태	인증	
FTP	Y	N	Y	Y	FTP접근은 내부 네트워크에서 외부로 허락된다. 외부로 부터의 접근은 강력한 인증이 요구된다.
Telnet	Y	N	Y	Y	Telnet접근은 내부에서 외부로 허락된다. 외부에서 내부로 접근은 인증이 요구된다.
rlogin	Y	N	Y	Y	외부로부터 회사 호스트에 rlogin은 NSM 으로부터 서면 허가가 요구되며 강력한 인증이 요구된다.
HTTP	Y	N	N	N	외부사용자접근이 예정된 모든 WWW서버는 회사 방화벽 외부의 호스트에 있어야 한다.
SSL	Y	N	Y	Y	SSL 세션은 SSL세션이 회사 방화벽을 통과할 때 고객서명이 요구된다.
POP3	N	N	Y	N	회사 POP서버는 회사 방화벽 내부에 위치해야한다. APOP의 사용이 요구된다.
NNTP	Y	N	N	N	NNTP 서버에 대한 외부 접근은 허용되지 않는다.
Real Audio	N	N	N	N	현재 회사 방화벽을 통과해야하는 오디오 세션 지원 업무 요구는 없다. 그러한 지원을 요구하는 사업장은 NSM과 협의 해야한다.
Lp	Y	N	N	N	lp 서비스는 회사 방화벽에서 제거된다.
finger	Y	N	N	N	finger 서비스는 회사 방화벽에서 제거된다.
gopher	Y	N	N	N	gopher 서비스는 회사 방화벽에서 제거된다.
whois	Y	N	N	N	whois 서비스는 회사 방화벽에서 제거된다.
SQL	Y	N	N	N	외부호스트에서 내부 DB로의 연결은 NSM의 허가가 필요하며 인증된 SQL 프록시 서비스가 요구된다.
Rsh	Y	N	N	N	rsh 서비스는 회사 방화벽에서 제거된다.
기타 (NFS 등)	N	N	N	N	언급하지 않은 기타 서비스 접근은 거부한다.

* 상태 (Y/N) : 사용자가 그 서비스를 사용할 수 있는지 여부
* 인증 (Y/N) : 그 서비스가 사용되기 전에 인증(강력 혹은 기타)형태 여부

6. 결 론

인터넷의 폭발적인 성장과 더불어, 조직(기관) 내의 인트라넷 등을 통한 업무에 필수적 요소로 자리잡고있는 전자우편, 내부결재시스템 등 업무 환경이 복잡해지고 광범위하게 변하고 있다. 따라서 내·외부의 정보보안문제도 심각해지고 있는 양상을 보이고 있다. 대부분의 조직이 정보보안을 위해 방화벽등을 도입하여 운영하고 있으나 그 실효성은 생각했던 것보다 미흡한 것으로 보고 있다. 이는 시스템이 개방형으로 전개됨에 따라 정보가 조직에 산재하게 되고 전자우편등을 통한 신속한 이동 등의 문제도 있지만 조직내부에 의한 정보 누설이 더욱 심각한 통계가 있다. 따라서 좀더 포괄적이고 종합적인 정보보호정책 수립이 필수 불가결한 요소가 된다고 볼 수 있다.

국내의 경우 몇몇 조직에서 외국의 자문으로 정보보호정책이 만들어져 운용중에 있으나 국내의 실정에 많은 부분에서 비현실적인 문제점을 안고 있어 전면적이고, 강제적인 운용이 안되고 있다. 혹은 필요한 서비스를 보안문제로 인하여 차단함으로써 불편함과 업무효율을 저하시키고 있음에 비추어 볼 때, 각 조직에 맞는 효과적인 정보보안 정책 수립이 요구된다고 본다. 본 고에서는 개략적인 정보보호정책의 개념과 수립단계, 고려요소 등을 소개하였다.

참 고 문 헌

[1] S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer Communication Review, Vol 19, 2, pp. 32-48, April 1989.

[2] G. Howard, "Introduction to Internet Security: From Basics to Beyond", Prima Publishing, Rocklin, CA, 1995.

[3] NCSA, "NCSA Firewall Policy Guide", 1995.

[4] NCSA, "Firewalls & Internet Security Conference '96 Proceedings", 1996.

[5] C. Pfleeger, "Security in Computing", Prentice-Hall, Englewood Cliffs, NJ, 1989.

[6] M. Ranum, "An Internet Firewall", Proceedings of World Conference on Systems Management and Security, 1992.

[7] W. Stallings, "Internet Security Handbook", IDG Books, Foster City CA, 1995.

[8] W. Stallings, "Network and InterNetwork Security", Prentice Hall, , 1995.

[9] "Site security Handbook", RFC-1244, Internet Draft Network Working Group, IETF, 1997.

[10] Barbara Guttman, Robert Bagwill, "INTERNET SECURITY POLICY : A TECHNICAL GUIDE", DRAFT, NIST Special Publication 800-xx, July 21, 1997.

[11] C. C. Wood, "Information Security Policies Made Easy-A Comprehensive Set of Information Security Policies ver. 5", IISCBS,Inc. 1996

[12] ETRI,"초고속정보통신기반 안전성 정책연구", 1997.11.

[13] 박진섭 외 6인, "인터넷 방화벽 보안정책", 제 7권 1호, CISC'97, 1997.11

[14] KISA, "Firewall 시스템 총서", 1996.10.

[15] KISA, "방화벽 FAQ", 기술문서 CERT-KR-TG-96-002, 1996.

[16] KISA, "전산망 정보보호-접근통제기술-", 1996. 12

[17] KISA, "정보보호총서",1996.12.

[18] KISA, "안전한 전산망운영을 위한 보안기술지침서 연구 및 개발",1997.12.

[19] SERI, "인터넷 관리자를 위한 보안 지침서", ver. 2.0, CERT-Korea, 1997.1

[20] German Information Security Agency, "IT Baseline Protection Manual", May. 1996.

박 진 섭

- 중앙대 컴퓨터공학과 학,석사,박사(공학)
- 한국기계연구원 연구원(수치제어센터)
- 연암대학 전자계산과 조교수
- (현)컴퓨터침해사고 대응협의회 보안정책 및 지침연구회 의장
- (현)대전대학교 컴퓨터공학과 부교수
- (현)대전대학교 대학원 교학부장
- 관심분야 : 컴퓨터통신 및 네트워크 모델링, 성능평가, 시뮬레이션 컴퓨터 보안정책