ISP의 능동 대응 서비스 제공 방안

이 승 민, 남 택 용
한국전자통신연구원 네트워크보안구조연구팀
전화 : 042-860-1775 / 팩스 : 042-860-5611

A Deployment Strategy for ISP's Active Response Service

Seungmin Lee, Taekyong Nam
Network Security Structure Research Team, ETRI
E-mail : todtom@etri.re.kr

Abstract

Because of great damages by illegal hacking, demand for security of the public network as well as the private is seemingly limitless. This critical requirement is leading ISPs to deploy new security services for their customers.

In this paper, we present active responses for the security of a ISP's network, and describe the deployment of a new security service using the network secured by that responses.

I. 서론

인터넷과 전자상거래의 급속한 확산과 함께 불법 해킹이나 바이러스 등으로 시스템과 네트워크 자원의 손상을 막을 수 있는 해결책 중의 하나로서 등장한 보안 솔루션은 단순한 제품 위주에서 점점 종합적인 보안 서비스 중심으로 변해 가고 있는 추세에 있다. 즉, 정보보호 컨설팅 및 교육에서부터 시스템 구축과 관리의 대행, 그리고 정보보호 컨설팅을 비롯한 취약점 점검 및 리포팅, 시스템 점검, 데이터 복구, 통합보안관리 시스템 운영 등의 종합 정보보호서비스로 발전해 가고 있다. 이러한 움직임은 정보보호전문업체 내부에서도 찾아볼 수 있으나, 최근 자사의 기존 보안 솔루션을 확대하거나 종합 정보보호서비스를 제공하고자 하는 ISP에서 보다 주도적으로 전개되고 있다.

이와 같이, 최근 ISP 입장에서 보안 서비스 분야가 중요한 사업영역으로 인식됨에 따라, 앞으로는 외부 침입에 대하여 자사의 망을 경유한 공격자에 대하여 능동적 대응 방안이 고객의 보안 서비스 선택에 중요한 변수가 될 것으로 보인다.

본 고에서는 ISP가 제공하는 보안 서비스 현황과 외부 공격에 대하여 현실적으로 대응할 수 있는 능동적 대응 방안에 대하여 살펴본다. 나아가서 이러한 능동적 대응이 하나의 독립된 보안 서비스로서 발전할 수 있는 가능성에 대해서도 알아보기로 한다.

II. ISP의 보안 서비스 현황

기존 ISP의 보안 서비스는 장비 임대 및 VPN 등이 주력이었으나, 최근 보안 관제 서비스 뿐만 아니라 컨설팅 및 솔루션 구축에 이르는 다양한 서비스를 제공하고 있다.

자사의 망을 보유한 인터넷서비스제공자들은 표 1에서 열거한 보안 서비스를 선택적으로 제공하고 있다. 즉, 기존의 보안 전문업체 중심으로 전개 되어온 보안 서비스에 비해서, 보다 다양한 종류를 가지고 자사의 전략에 맞게 주 서비스나 부가 서비스 형태로 제공하고 있다.

현재 ISP가 제공하는 서비스는, 자체 인력을 보유하

고 서비스를 제공하는 경우와, 전문업체와 제휴하여 서비스 제공은 ISP가 담당하고 실제 보안 솔루션은 제휴한 업체에서 제공하는 경우가 있다. 이와 같이 기존의 보안 전문업체가 독자적으로 제공하는 형태에 비하여 ISP 중심으로 등장한 보안 서비스는 기존의 인터넷 서비스와 결합하여 다양한 묶음의 서비스로 고객에게 다가갈 수 있다는 점과, 자체 인력을 보유하고 있는 경우에는 자사의 인터넷망을 이용하여 보다 저렴하게 보안 서비스를 제공할 수 있다는 이점이 있다.

국내의 경우, D사는 최근 17개의 보안 업체와 제휴하여 종합 정보보호 서비스를 제공하고 있으며, K사의 경우 보안 업체와 제휴하여 IDC(Internet Data Center) 중심으로 서비스를 시작하였다.

외국의 NTT사의 경우에는 기존의 Managed Network Service의 부가 서비스 형태로 등급별 Managed Security Service를 제공하고 있으며, AT&T, Worldcom 등도 Managed Security Service 위주의 보안 서비스를 제공하고 있다. 현재 ISP가 제공하고 있는 보안 서비스는 표 1과 같이 요약할 수 있다[1].

표 1. ISP 보안 서비스

구분		내용
보안관제 (Managed Security Service)	Managed F/W	F/W임대, 모니터링 및 접근 통제 관제 서비스
	Managed IDS	IDS임대, 모니터링 및 침입탐지 관제 서비스
	Managed VPN	VPN 구축 및 관리 서비스
	Managed Anti-virus	Virus-wall 설치/임대, 모니터링, 주기적 업데이트 제공 등
	서버보안	서버 F/W, CA 이용서비스, PKI솔루션 등
	기타	메일보안, 데이터 백업 등
보안 컨설팅		취약성 분석, 정보보호 수준평가, 정보보호 정책수립, 정보보호 교육 등
솔루션 구축		통합보안(ESM)구축, 전사적 PC보안 자원관리

III. ISP 망 보안의 중요성

예전의 특정 서버들에 대한 선별적인 해킹과는 달리 최근에는 Worm을 이용한 무차별적인 DoS(Denial of Service) 성의 공격이 빈번하고 있다. 이는 어느 한 국가나 기관 또는 단체에서 해결 할 수 없으며, 인터넷을 이용하는 모든 사용자가 적극적으로 대처해야 한다[2]. 여기서, DoS와 같은 유형의 공격 특성에 대해서는 이미 개별 고객들에게 트래픽이 흐르고 나면 고객측에서의 조치는 별의미가 없으므로 ISP가 망차원에서 대처하는 것이 가장 바람직하다고 볼 수 있다.

이러한 점에서, 망차원에서 일부 불량고객에 대해서는 망으로 들어오는 트래픽을 차단하려는 움직임이 일어나고 있으며, 실제로 외국의 사례를 보면 Codered나 Nimda에 감염된 고객의 인터넷 접속을 막는 적극적인 조치를 취하기도 한다.

국내 ISP에서도 자신의 서버 뿐만 아니라 네트워크를 보호하기 위하여 통합보안관리를 수행하고 있으며, 특히 정보통신기반보호법이 제정됨에 따라 사이버 공격에 따른 망 자원의 위협에 대하여 네트워크 차원의 보안에 관심이 증가하고 있다. 일부 ISP에서 국제 Gateway나 IX(Internet eXchange) 등과 같은 인터넷 망의 접점에 IDS를 설치 운용하기 시작한 것도 이 때문이다.

따라서 향후에는 고객이 보안 서비스를 선택함에 있어서, 비슷한 네트워크 품질을 제공하는 ISP들 가운데 ISP 망의 보안성이 중요한 변수가 될 것으로 보인다. IV 절에서는 ISP를 경유하는 사이버 공격에 대한 능동적 대응 방안을 통하여 자사의 IP 백본망의 보안성 확보는 물론, 나아가서 고객에게 하나의 보안 서비스로 전개할 수 있는 구체적인 방안에 대하여 기술한다.

IV. 능동 대응 서비스 제공 방안

그림 1은 ISP 망을 경유하여 공격하는 예를 나타낸 것이다. 백본망을 소유하고 있는 ISP가 대응할 수 있는 방법은 공격시점을 기준으로 크게 공격 경로를 따라서 사전에 대응하거나 반대로 사후에 적절한 대응을 할 수 있는 경우로 나눌 수 있다.

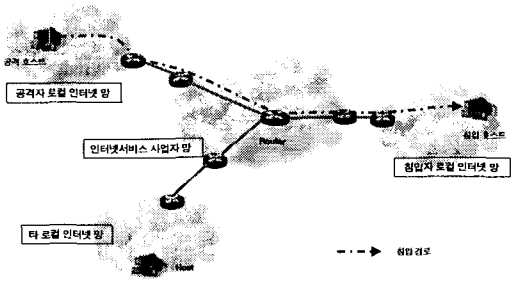

그림 1. ISP를 경유한 공격 경로 예

표 2. 능동 대응 방안

사전 대응 방법	사후 대응 방법
Ingress Filtering IDS 설치 NMS 연동	IDS 로그분석 및 대응 역추적 및 차단

Ingress Filtering[3]

Ingress Filtering을 적용하여, ISP 망 가장자리에 위치한 라우터에서 외부로부터 들어오는 패킷에 대하여 ingress filtering을 수행하면서, 미리 지정한 영역의 IP 블럭이 아닌 패킷에 대해서는 폐기 시켜서 사전에 IP Spoofing 공격등에 대처한다. 또한, 불량고객 리스트를 관리하여 해당되는 IP에 대해서는 사전에 폐기시켜서 망 보안을 유지한다.

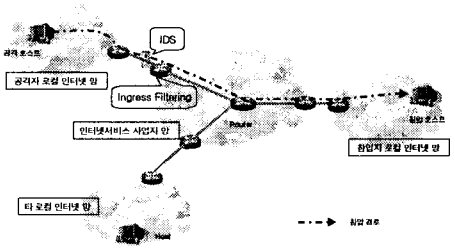

그림 2. Ingress Filtering 및 IDS 적용

IDS 및 Firewall 설치

그림 2과 같이 ISP 백본망의 가장자리로서 국제 Gateway나 타 ISP와의 접점 및 일반 고객으로부터의 인입점에 IDS장비를 설치하여, 외부로부터 들어오는 패킷을 감시하면서 일상적인 트래픽이 아닌 것에 대해서는 그 원인을 분석하여 침입을 사전에 방지하고 탐지한다. 이는 침입차단시스템과 연동하여 실시간으로 외부 트래픽을 차단할 수 있다.

NMS 연동

ISP 인터넷망을 관리하는 망관리시스템(NMS)에서 트래픽의 추이를 감시하여, 갑자기 트래픽이 급증하거나 트래픽의 변화가 없어도 Codered 처럼 작은 사이즈의 패킷이 다량 발생하여 PPS(packets per second)의 급속한 증가가 있는지 탐지한다. 이와 같이 진행중인 외부 공격에 대하여 실시간으로 침입 정보를 반영하여 대처할 수 있다.

IDS 로그 분석 및 대응

IDS의 로그를 분석하여 바이러스에 감염되거나 침입된 서버 IP를 찾아서 해당 고객에게 해킹 사실과 치유 방법을 통보한다.

역추적

ISP망을 경유하여 공격한 경로를 역추적하여 인입점에서 차단하고, 타 ISP를 경유하였다면 상호 협력하여 근원지를 찾아낸다. 이를 위하여 ISP 가장자리에 위치한 라우터에 로그저장 기능과 로그 분석 기능을 구현하여 중앙의 매니저에서 그림 3과 같이 역추적 할 수 있다[4]. 아래 그림은 역추적을 위한 하나의 시나리오이다.

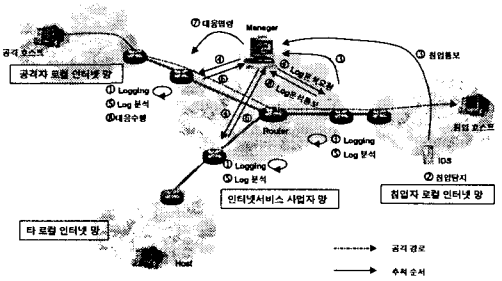

그림 3. 역추적 방안

① 에지 라우터에서 로그정보를 저장한다.
② 침입사실을 탐지한다.
③ 침입정보를 매니저시스템으로 통보한다.
④ 에지 라우터로 로그분석을 요청한다.
⑤ 로그를 분석하여 공격패킷이 지나왔는지 조사한다.
⑥ 분석결과를 통보한다.
⑦ 적절한 대응명령을 통보한다.
⑧ 에지 라우터에서 대응기능을 수행한다.

지금까지 ISP에서 구체적으로 적용하여 자사 망의 보안과 고객에게 보안 서비스로 제공 가능한 방안에 대하여 살펴보았다. 크게 외부 공격을 사전에 방지하기 위한 방법과 공격 후에 대응 할 수 있는 방법으로 구분하였다. 실제로 개개의 방법을 적용함에 있어서는, ISP 마다 처한 상황과 기존 서비스의 운용환경에 맞게 활용할 수 있으며 특히, 역추적의 경우 그림 3과 같은 시나리오를 구현함에 있어서는 자사에 맞는 다양한 연구가 필요하리라고 본다.

V. 결론

지금까지 현 ISP의 보안 서비스와 ISP 망 보안의 중요성 그리고, 이를 확보하기 위한 현실적인 대응 방안의 필요성에 대하여 살펴보았다. 나아가서, 현재 ISP의 보안 서비스가 보안 전문업체의 서비스와 차별화 되고 고객입장에서 보다 매력적인 망 차원의 보안 서비스를 제공하기 위한 구체적인 방안을 제시하였다.

향후, ISP 입장에서는 현재 자사가 제공하는 다양한 종류의 보안 서비스를 ISP 망 차원의 능동적 대응 방안과 결합하여 전략적인 핵심 사업영역으로 전개해 나간다면, 기존 보안 전문업체에서 독자적으로 제공하고 있는 보안 서비스와 차별화 된 능동적인 서비스로 발전할 수 있을 것으로 기대된다.

참고문헌

[1] ISP Planet, www.isp-planet.com/technology /msssp /mssp_survey.html

[2] 구자현, "ISP 보안관리 사례 및 사고 대응 방안," www.kisa.or.kr/K-trend/KisaNews/200111/special-report_03.html, 2001. 11.

[3] P. Feguson and D. Senie,"Network Ingress Filtering : Denial of Service Attacks Which Employ IP Source Address Spoofing," RFC2267, Jan. 1998.

[4] 이승민 외, "인터넷에서 에지 라우터의 로그 정보를 이용한 공격자 역추적 방법," NCS2001, 2001. 12.