인터넷 침해 대응을 위한 제언

박 치 항[1)]

목 차

1. 서 론

올 해를 맞이하면서 겪었던 1.25 인터넷 대란과 2.18 대구 지하철 참사는 우리들에게 커다란 충격과 함께 시스템 구축시 안전에 대한 고려가 얼마나 심도있게 다루어 져야 하는가를 피부로 느낄 수 있게 했으며 사고 대응과정에 대해서도 많은 시사점을 제공하고 있다. 통신과 교통 분야에서 발생한 이번 사건은 직접적인 피해는 물론 후유증과 간접적인 피해도 심각한 상태이다. 두 사건 모두 사건 발생 이후 유사 사건이 계속되어 전국민을 불안하게 하였을 뿐만 아니라 국가 신인도에도 상당한 영향을 미친 것으로 관측되고 있다. 이 두 사건은 전혀 다른 환경에서 발생한 사건이지만 안전에 대한 일반적인 인식 즉, 어떠한 환경에 대해 안전성이 유지되기 위해서는 어느 정도까지 가정하고 준비해야 되는가, 사건이 발생하면 어떠한 안전수칙이 어떠한 절차를 거쳐 지켜져야 하는가, 원인규명과 사건처리를 위해서는 어떤 장치와 대응태세가 요구되는가 등 여러 면에서 매우 유사한 관점을 발견하게 된다. 다시 말하면 하나는 사이버 세계에서, 다른 하나는 실세계에서 발생한 같은 범주의 사건이라는 것이다.

사회가 복잡해지고 일반인과 가까이 접하고 있는 기술이 급속도로 고도화되면서, 수반되는 역기능과 사고도 같은 비중으로 급속하게 대규모화되고 빈번해 지고 있다는 사실을 주목할 때이다. 이번 인터넷 사고에 유독 우리나라만 심각한 피해를 입게 된 배경에는 세계 최고를 자랑하는 우리의 초고속 인터넷 환경이 네트워크 장치를 마비시키는 데에도 초고속으로 작용하면서 미처 대응할 시간을 갖지 못했기 때문이기도 하다. 문제는 이러한 사고가 언제 재발할 지 모른다는 것이다. 내일 또 다시 유사한 아니면 새로운 인터넷 침해사고가 발생하지 않을 것이라고 어느 누구도 예단할 수 없으며 이러한 사고가 반복될 경우 발생하게 될 사회적 혼란과 손실은 실로 엄청날 수 있는 것이다. 최근의 인터넷 사고시에도 일부에서는 인터넷 대안론까지 제기했던 예는 예사롭게 넘길 일이 아니다. 어렵게 일구어 낸 세계 최고의 인터넷 환경을 유지하기 위해서는 고속화와 병행하여 최강의 보안시스템 개발이 필수적임을 우리는 1.25 인터넷 대란을 통해 깨닫게 되었으며 아울러 이번 사

1) 한국전자통신연구원 정보보호연구본부 본부장

건을 통해 아래에서 언급되는 바와 같은 인터넷 침해사고에 관한 몇 가지 중요한 초기 대응전략을 발견할 수 있게 된 것은 불행 중 다행이라고 생각한다.

2. 폭주 트래픽 차단

인터넷에 DDOS형 공격과 같은 이상 상황 발생 시에도 망의 마비상태를 방지하여 정상적인 기능을 유지하기 위해서는 원인규명과 발원지 추적에 우선하여 폭주 트래픽을 적절히 차단하는 방안이 필요하다. 인터넷 노드에 유입되는 모든 트래픽을 무차별하게 차단하게 되면 이용자 입장에서는 인터넷이 동작불능 상태가 되므로, 유사시 우선순위나 QoS에 의해 트래픽을 차단할 수 있는 기술 개발이 요구된다. 이를 위해서는 평상시 각각의 인터넷 노드에서, 유입되는 인터넷 트래픽 유형에 대한 분석이 이루어지게 한다면 트래픽 폭주와 같은 비상시 정책(Policy)이나 규칙(Rule)에 근거하여 효율적으로 트래픽을 제거할 수 있게 될 것이다. 또한 비상시에만 예외적으로 적용 가능한 트래픽 모니터링 기법을 개발하여 트래픽 양에 따른 단계적 패킷차단 전략을 구사하면 더욱 효과적일 수 있을 것이다.

3. 트래픽 차단 공조체제

어느 한 인터넷 노드 관점에서 볼 때, 유입되는 폭주 트래픽에 대한 차단 기능만으로는 계속해서 끊임없이 유입되는 트래픽 폭주 상황을 벗어날 수가 없게 되기 때문에 유입되는 트래픽 양을 줄일 수 있는 방법이 모색되어야 한다. 라우터의 경우를 예로 들면 인접한 라우터에게 트래픽 폭주 상황을 알리고 트래픽 유출을 억제 시키도록 요구하면 요구 받은 라우터는 트래픽 모니터링 장치를 통해 상황을 점검한 후 적절한 대응 수단을 취하게 될 것이며 다시금 인접 노드에 상황을 전달하는 트래픽 차단 공조체제를 유지함으로써 망 차원의 트래픽 양을 점차적으로 감소시킬 수 있게 된다. 이러한 공조체제가 효율적으로 수행되기 위해서는 ISP나 일정 범위의 네트워크를 단위로 네트워크 침해 종합분석 시스템을 두어 관할 구역의 인터넷 노드로부터 이상 정보를 수집하여 종합 분석함으로써 트래픽 폭주 발원지나 유형에 대한 판단을 가능하게 할 수 있어 결과적으로 비상상황에 대한 효과적 대응방안을 강구할 수 있게 될 것이다. 또한 네크워크 침해 종합분석 시스템은 필요시 ISP나 국가 단위의 비상 경보시스템과 연계됨으로써 국가차원의 비상사태 예방에도 효과적으로 활용될 수 있게 된다.

4. 별도 제어망 필요

인터넷은 전화망에서 사용하는 것과 같은 신호망을 별도로 가지고 있지 않고 일반 정보나 제어 정보 모두 동일한 망을 통해 전달되기 때문에 트래픽 폭주와 같은 비상상황이 발생하여 망에 긴급 조치가 필요한 경우 긴급 제어 정보를 효과적으로 전달할 수 있는 방법이 없어 트래픽 폭주로 인한 망의 비상사태로부터의 회복을 어렵게 만든다. 따라서 현재의 인터넷 구조를 그대로 유지하면서 제어 정보를 효과적으로 전달할 수 있는 논리망 개념을 인터넷에 도입할 필요가 있다. 간단하게는 앞 절에서 언급한 우선순위에 의한 폭주 트래픽 차단 정책을 사용하여 제어 정보는 가장 높은 우선 순위를 부여하여 어떤 상황에서도 차단되지 않도록 하는 방법을 사용할 수 있을 것이다.

5. 모니터링장비/보안장비 심사 강화

이번 인터넷 대란을 겪으면서 얻게 된 또 하나의 중요한 교훈은 네트워크 모니터링 장비나 보안 장

비 설계시 비상시의 이상 상황에서의 동작에 대한 보다 철저한 검증이 요구된다는 사실이다. 구체적으로 말하면, 평상시에는 정상적인 데이터 흐름이 주류이고 가끔 비정상적이거나 정체가 불명확한 데이터가 발생하기 때문에, 이들 비정상 데이터에 대해 충분한 시간을 갖고 다양한 분석과 검토과정을 수행하게 되겠지만 비상시 이상 데이터가 폭주하는 경우에는 이들 모니터링 시스템이 제대로 동작하지 못할 수 있을 뿐만 아니라 이상 데이터 분석을 위해 또 다른 다량의 데이터를 발생시켜 네트워크 트래픽 폭주 현상을 더욱 악화시키는 결과를 초래할 수 있다는 사실이다. 따라서 모니터링 장비나 보안 장비 제조업체에서는 설계시 이러한 상황에 대한 면밀한 분석이 요구되며 장비인증기관에서도 장비인증시 시험항목 및 인증을 위한 시험절차에서 이러한 상황에 대한 철저한 검증이 요구된다 하겠다.

6. 취약지구 특별관리

1.25 인터넷 대란의 직접적인 원인은 MS-SQL 서버 2000 및 MSDE 2000 시스템의 버퍼 오버플로우의 취약점을 이용한 슬래머 웜의 감염에 의한 것으로 밝혀졌다. 이 취약점에 대한 보안 패치를 적용하지 않은 시스템은 자체 서비스 제공 불능은 물론 본의 아니게 다른 컴퓨터를 공격하고 네트워크 트래픽을 폭발적으로 증가시키는 상황을 유발하였다. 그런데 이 감염과정에서 주목하여야 할 사항이 있다. 감염시스템은 대학, 연구소, 기업 등에서 골고루 발생하였지만 근본적인 취약지구는 대학과 연구소라는 것이다. 대학이나 연구소는 일상업무에 활용되는 업무용 시스템도 있지만 테스트 환경을 위한 다량의 개발장비용 시스템이 존재한다. 이들 시스템은 일반적으로 조직 내 보안관리 대상에서 제외될 뿐만 아니라 보안패치 미적용 등 갖가지 취약점에 노출되어 있다. 따라서 향후에는 보안 취약지구에 대한 검토를 통해 이러한 취약지구에 대해서는 의무적으로 특별관리체제가 갖추어 질 수 있도록 하는 방안이 요구된다. 예를 들면 기관이나 조직 내 모든 시스템을 업무용과 개발용으로 분류하여 개발용으로 사용되는 시스템은 반드시 등록된 IP만 접속할 수 있도록 의무화하는 것도 한 방안이 될 수 있다.

지금까지 1.25 인터넷 대란을 통해 네트워크 차원에서 조속히 행해져야 할 주요 기술개발 방향 및 조치사항을 살펴보았다. 하지만 서두에서 언급했듯이 보안이란 기본적으로 보안장비의 성능이나 기능 측면의 개선만으로는 소기의 목적을 달성할 수 없으며 보안 담당자의 자세와 일반인의 보안의식에 크게 의존하게 된다는 것을 알 수 있다. 미국의 경우 사이버 보안을 국가 안보차원에서 다루고 있을 뿐만 아니라 사이버 공간 보호는 정부 단독으로 이룰 수 없음을 환기시키고 모든 국민이 자신의 사이버 공간을 보호할 수 있도록 다음과 같은 국가전략을 제시하고 있다.

6.1.16가지 수단(Tools)

인식과 정보(Awareness and Information), 기술과 도구, 훈련과 교육, 역할과 협력, 연방정부 지도력, 조정과 위기 관리

6.2.15개 대상(Levels)

일반 사용자 및 자영업자, 대기업, 중요분야 (연방정부, 지방정부, 대학, 정보통신 산업체), 국가적 우선과제 (사이버 공간 보안에 관련되는 기술개발, 제도개선, 시장창출 등), 국제적 이슈

6.2.13개 조치사항(Agenda)

권고(Recommendation), 현재 시행중인 프로그램(Programs), 논의가 필요한 사항(Discussions)

이러한 수단(Tools)이 적용되는 정도와 범위는 대상(Levels)에 따라 차이가 나며 조치사항(Agenda)에서는 현재 시행되고 있는 프로그램(Programs)을 확인하여 향후 추진할 사항을 권고(Recommendation)로 정리하고 좀더 구체적인 검토가 필요한 사항은 논의사항(Discussions)으로 분류하였다.

7. 결 론

우리도 이와 유사한 또는 이를 참조하여 우리에게 맞는 국가적 차원의 전략이 요구되는 시점이 도래하였음을 인터넷 사건을 계기로 실감하게 된다. 세계 최고의 초고속 인터넷 국가에 이어 세계 최강의 인터넷 보안 강국으로 다시 태어날 때 우리는 비로소 명실상부한 인터넷 최강국임을 자부할 수 있게 될 것이며 인터넷 기반의 지식정보사회로의 순조로운 진입과 세계적 수준의 지식정보산업을 이끌어 갈 수 있게 될 것이다.

저자약력

박 치 항

- 서울대학교 응용물리학과 졸업(이학사)
- 한국과학원 전산학과 졸업(이학석사)
- 파리 6대학 전산학과 졸업(공학박사)
- 미국 오레곤 주립대학 객원 교수 역임
- 멀티미디어 컴퓨터 개발 사업책임자 역임
- 고속병렬컴퓨터(주전산기 IV)개발 총괄책임자 역임
- 한국전자통신연구원 컴퓨터연구단 단장 역임
- 현재 한국전자통신연구원 정보보호연구본부 본부장

관심분야 : 멀티미디어, 분산시스템, 그룹웨어, 네트워크 컴퓨팅, 에이전트 아키텍쳐, 차세대 인터넷

이 메 일 : chpark@etri.re.kr