제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

사이버 위협에 대한 국내 경보 체계 현황

이도훈*, 백승현, 오형근, 이진석
국가보안기술연구소
{dohoon*, shpaek, hgoh, jinslee}@etri.re.kr

요 약

오늘날 인터넷을 비롯한 정보통신 기술의 발전으로 이에 대한 개인 및 사회 주요 시설의 의존도가 날로 심화되고 있다. 최근에는 인터넷 웜 및 바이러스와 같은 사이버 위협들이 이러한 정보통신 기술 인프라에 내재해 있는 취약성을 악용하여 로컬 PC를 공격하는데서 인터넷과 같은 정보통신 기술 인프라를 공격하는 추세에 있다. 이런 추세에 있는 사이버 위협들은 사회 구성 주체들의 개별적 대응만으로는 한계가 있기 때문에 체계적인 공동대응협력체계가 절실하다. 공동대응협력체계를 구축하기 위해서는 일차적으로 사이버 위협 발생 시 정보통신 인프라에 미칠 영향력을 사전에 분석하고 분석한 정보를 사회 주체 간에 공유하는 일이 필요하다. 이를 위해 본 논문에서는 현재 국내의 관련기관이나 업체에서 사용 중인 사이버 위협의 경보 체계 현황을 조사한 후, 국내 경보 시스템을 산출 범위에 따라 두 부류(정보통신기술 인프라에 대해서는 전역적 경보 체계, 개별 위협에 대해서는 개별적 경보 체계)로 분류한다. 그리고 분류한 결과를 분석하여 국내 경보 체계의 문제점을 지적한 후 이의 해결을 위한 접근 방향을 간략히 제시한다.

The Present State of Domestic Alert Systems for Cyber Threats

Do-Hoon Lee*, Seug-Hyun Paek, Hyung-Geun Oh, Jin-Seok Lee
National Security Research Institute

ABSTRACT

Todays, the more information technologies(IT) like internet is developed, the more main facilities of individuals and social organizations get deeply involved in IT. Also, the trend of cyber threats such as internet worms and viruses is moving from local pc attacks to IT infrastructure attacks by exploiting inherent vulnerabilities of IT. Social organizations has a limit to response these attacks individually, and so the systematic coordinate center for social organizations is necessary. To analyze and share cyber threat information is performed prior to the construction of the coordinate center. In this paper, we survey domestic alert systems for cyber threats of related organizations and companies, and then classify them into two categories by the range of threat assessment: global alert systems for global IT infrastructure and individual alert systems for each threat. Next, we identify problems of domestic alert systems and suggest approaches to resolve them.

1. 서 론

인터넷을 비롯한 정보통신 기술의 발전으로 개인에서부터 민간 기업에까지 정보통신 기술에 대한 의존도가 날로 심화됨에 따라 사회 주요 시설에 존재하는 취약성을 이용한 전자적 침해와 사이버 위협에 대한 위험도가 높아지고 있다. 최근에는 인터넷 웜 및 바이러스와 같은 사이버 위협들이 정보통신 기술에 내재해 있는 취약성을 악용하여 로컬 PC를 공격하는 추세에서 인터넷과 같은 정보통신 기술 인프라를 공격하는 추세로 전환하고 있다[1]. 만약 이러한 사이버 위협으로 인해 인터넷 코어 망과 같은 정보통신 핵심기반구조가 마비된다면 국가경제에 엄청난 파급 효과를 미치게 된다. 2003년 발생한 1.25 인터넷 대란은 국가경제에 있어서 그 파급 효과가 어느 정도 인지를 실감할 수 있게 하였다[2][3].

이런 추세에 있는 사이버 위협들은 사회 구성 주체들의 개별적 대응만으로는 한계가 있다. 그렇기 때문에 이에 대한 체계적인 공동대응협력 체계가 절실히 필요하다[4]. 공동대응협력체계를 구축하는데 있어서 사이버 위협 발생시 정보통신 인프라에 미칠 영향력을 사전에 분석하고 정보호호주체가 신뢰할 만한 대응 요령을 제공하는 경보 체계가 일차적으로 구축되어야 하며, 이에 선행하여 국내 경보 체계 현황을 조사할 필요가 있다.

본 논문에서는 국내의 경보 체계 현황을 파악하기 위해, 먼저 공공기관차원에서의 경보 체계 현황을 조사하고 이를 정리한다. 둘째, 민간부문으로 보안 관련 산업체에서의 경보 체계 현황을 조사하고 이를 정리한다. 그리고 이를 기반으로 경보 체계를 위협 대상의 범위에 따라 전역적 경보 체계와 개별적 경보 체계로 분류한다. 마지막으로 국내 경보 체계에 대해 비교 분석한 후 현재 국내 경보 체계의 문제점과 해결 방안에 대해 간략히 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 공공기관의 경보 체계에 대해 먼저 설명한 후 3장에서 민간산업체에서의 경보 체계에 대해 설명한다. 그리고 4장에서 조사한 국내 경보 체계들을 비교 및 분석하여 국내 경보 체계 현황에 대해 언급한 후, 5장에서 본 논문의 결론을 맺는다.

2. 공공기관의 경보 체계

2.1. NCSC

국가사이버안전센타(National Cyber Security Center: NCSC)는 민간, 공공 등 국가 전 분야의 사이버 위협에 대한 효율적인 사전 예방과 사고 발생 시 신속한 대처를 위해 2003년 12월에 설립된 범국가적 사이버 테러 대응 센타이다[5]. NCSC에서는 현재의 사이버상의 위협 상황을 판단하여 사이버테러경보를 발령하는 전역적 경보 체계를 가지고 있다. 예보는 '정상' 단계에서 국내외 신종 컴퓨터 바이러스의 출현 정보, 최신 해킹 기법, 그리고 보안취약점 등의 발표로 피해가 우려되는 경우 발령한다. 그리고 경보는 국내외 실제 공격이 발생하여 각급 기관 및 통신 업체 등으로부터 이상 징후 또는 피해 상황이 접수될 경우 관련 상황을 종합 분석하여 발령한다.

NCSC의 전역적 경보 체계에서 사이버테러 경보 단계를 정상, 주의, 경고, 위험의 4단계로 나누어 범국가적으로 사이버 위협 상황에 따라 경보를 발령하고 그에 맞는 대응 요령을 제공하고 있다[6]. NCSC의 사이버테러 경보 단계 발령 기준은 다음과 같다.

- 1단계(위험): 국가적 차원에서 네트워크 사용 불가능하거나 주요 정보통신기반시설에 대한 공격으로 인해 심각한 피해가 발생한 경우로 국가적 차원에서 공동 대처해야할 필요성이 있는 상황
- 2단계(경고): 주요 정보시스템에 대한 공격으로 피해가 발생하고 그 범위가 여러 기관에 걸쳐서 나타나는 경우로 다수 기관의 협조가 필요한 상황

- 3단계(주의): 정보시스템에 대한 공격으로 국내외 피해가 발생하거나, 시스템이 악의적 목적으로 도용되거나, 네트워크 트래픽이 급격히 증가한 경우로서 피해의 범위가 단일 시스템 및 단일 조직에 해당하고, 정보시스템 전반에 걸쳐 보안태세 강화가 필요한 상황
- 4단계(정상): 모든 분야에서 정상적인 활동이 가능하지만 국내외 신종 컴퓨터 바이러스의 출현, 최신해킹기법, 보안취약점 발표로 피해가 우려되는 경우로서, '예보'가 발령될 수 있는 상황

2.2. KrCERT

인터넷침해사고대응지원센타(Korea Computer Emergency Response Team: KrCERT)는 인터넷침해사고의 조기탐지, 분석, 예경보를 통해 피해 확산 방지와 상시적인 정보공유를 위한 민간부문의 침해사고대응지원센타이다[7]. KrCERT는 민간 부문의 침해사고 분석 및 기술 지원과 대응협력체계를 구축하고 있다.

KrCERT는 국내 인터넷 소통현황에 따라 경보 단계를 정상, 주의, 경고, 위험의 4단계로 나누어 발령하고 그에 맞는 대응요령을 일반사용자, 네트워크/서버 관리자, IDC/ISP별로 제공한다. 각 등급에 대한 발령 기준은 아래와 같다.

- 위험: 국내 인터넷 전 분야에 소통장애가 발생하여 정상적인 서비스가 어렵거나 주요 정보통신기반시설의 피해로 인하여 대국민 서비스가 지장을 받는 경우로, 국가적 차원에서 공동 대처해야 할 필요성이 있는 상황
- 경고: 인터넷 소통장애가 전국적으로 확산 조짐이 있거나 발생되고, 해킹/웜 공격으로 주요 정보통신기반시설의 피해가 발생하는 경우로서 ISP, IDC 및 정보보호업체 등의 공동대응이 필요한 상황
- 주의: 해킹/웜 공격으로 일부 사용자의 인터넷 사용 장애가 발생 및 예상되거나 국지적인 인터넷 소통장애가 발생하여 인터넷서비스에 지연이 발생 및 예상되는 경우로서, 일반 PC사용자, 서버 관리자, 그리고 ISP 등의 보안태세 강화가 필요한 상황
- 정상: 인터넷 소통에 지장이 없는 상태

3. 민간산업체의 경보 체계

3.1. 안철수연구소

안철수연구소(www.ahnlab.com)는 1995년 3월 창립된 국내 안티-바이러스 전문 기업이다[8]. 안철수 연구소에서는 정보 통신 전반에 대한 전역적 경보 체계를 가지고 있지는 않다. 그러나 안철수 연구소는 새로운 바이러스 및 악성코드가 발견되는 경우 감염시 위험도와 확산 가능성들을 산출하고 현재 확산 정도 및 피해 정도에 따라 고객들이 신종 바이러스를 주의할 수 있도록 경고 서비스를 제공하고 있다. 그리고 개별 바이러스의 감염시 위험도와 확산시 위험도를 산출하여 등급을 정하고 이를 알리는 개별적 경보 시스템을 자체적으로 갖추고 있다. 개별적 경보 시스템은 바이러스 정보뿐만 아니라 이를 치료할 수 있는 엔진의 업데이트, 인터넷에서의 바이러스 진단 서비스와 그에 맞는 대응요령을 모두 지원하고 있다.

안철수 연구소에서는 발견된 악성코드의 감염시 위험도와 확산 위험도에 따라 각각 5가지 등급으로 나누어 긴급 바이러스 정보를 나타낸다. 먼저 감염시 위험도는 해당 악성코드가 실행되어 시스템이 감염되었을 경우, 시스템에 미치는 증상에 따른 등급이다. 활동일 바이러스의 경우에는 활동일에 미치는 증상을 기준으로 선정한다. 감염시 위험도에 따른 등급 산정 기준은 다음과 같다.

- 1등급(파괴): 운영체제 부팅 불가(시스템 파일 손상, 하드디스크 파괴 및 포맷 등)
- 2등급(위험): 다수의 파일 삭제 혹은 복구하기 어려운 손상
- 3등급(위해): 파일 감염시 내부 정보 손상(프로그램 실행 불가능 발생), 부분파일 삭제, 백

도어, 지속적인 재부팅으로 인한 시스템 부팅 불가, CMOS 파괴, 시스템속도 저하

- 4등급(대비): 특정파일 삭제, 프로그램 변경 (실행은 가능)
- 5등급(주의): 문자나 소리 출력 등 실질적인 피해 없음

확산 위험도는 해당 악성코드가 지니고 있는 확산 잠재 가능성에 대한 등급이다. 악성코드가 지니고 있는 감염경로의 특성에 의해 등급을 선정한다. 확산위험도에 따른 등급 산정 기준은 다음과 같다.

- 1등급: 반복적인 메일 발송, 네트워크 공유폴더, P2P, 메신저, 보안취약점, 파일실행 중 2개 이상 중복된 감염경로를 가지는 경우
- 2등급: 반복적인 메일 발송, 네트워크 공유폴더, P2P, 메신저, 보안취약점 중 1개의 감염경로를 가지는 경우
- 3등급: 1회 메일발송이나 메신저를 이용한 수동발송(파일첨부 등의 동작을 사용자가 선택하도록 유도하는 경우) 중 1개의 감염경로를 가지는 경우
- 4등급: P2P를 이용한 감염경로를 가지는 경우
- 5등급: 감염파일을 실행함으로써 감염시키는 감염경로를 가지는 경우

안철수 연구소에서는 확산 위험도와는 별개로 해당 악성코드가 현재 확산되어 있는 정도를 등급으로 표현한 현재 확산도 기준이 있다. 해당 악성코드의 현재 확산정도는 일정시간동안 안철수 연구소로 접수되는 피해신고수를 기준으로 정해진다.

3.2. 하우리

하우리는 컴퓨터 바이러스 백신 및 데이터 복구 프로그램 개발 전문업체이다[9]. 안철수연구소와 마찬가지로 하우리에서도 전역적 경보 체계를 가지고 있지 않지만 개별 바이러스의 출현으로 인한 확산과 피해에 따라 고객들에게 상황을 알리는 서비스를 하고 있다.

하우리에서는 바이러스 대응 상태를 단계별로 나타내주는 경보 시스템을 운영하고 있다. 그러나 개별 바이러스의 확산 및 피해에 근거하여 대응 상태를 결정하기 때문에 정보 통신 전반에 대한 전역적 경보 체계라 하기에는 무리가 있다.

하우리에서는 CODE 1,2,3,4의 총 4단계로 바이러스 대응 상태를 구분하여 발표하고 있으며 직원들에 대한 비상대응 근무 기준도 함께 제시하고 있다. 각 상태의 발령 기준은 다음과 같다.

- CODE 1: 확산으로 인한 피해가 네트워크 마비 수준으로 증가 중이어서 대처 방법 및 피해 복구에 대한 문의가 가능한 상황으로 전 직원 24시간 비상대기 상태
- CODE 2: 감염이 확산 중으로서 대처 방법에 대한 문의가 가능한 상황으로 전직원 비상대기 상태
- CODE 3: 확산 가능성이 높아 감염이 우려되는 상황으로 전직원 전화 대기 상태
- CODE 4: 평상시 예, 경보 수준으로 신종 바이러스가 출현할 수 있기 때문에 백신을 최신 엔진으로 업데이트 할 것을 권유

하우리의 개별적 경보 체계는 개별 위협의 파괴도와 확산도에 따라 각각 5등급으로 구분하여 등급을 산정하고 있다. 파괴도의 등급 산정 기준은 다음과 같다.

- 1 등급: HDD 파괴로 인한 부팅 불가, 전문적 복구 필요
- 2 등급: 시스템 운영에 영향을 미치는 시스템 파일의 치명적인 손상으로 인한 부팅 불가, HDD 자체 복구 가능
- 3 등급: 시스템 운영에 영향을 미치지 않는 시스템 파일 손상, 정상적인 시스템 운영 가능(예: winsock.dll 손상, 그러나 전자우편 실행 정상)
- 4 등급: 일반 파일 삭제
- 5 등급: 버그로 인한 파괴 루틴 실행 실패

확산도의 등급 산정 기준은 다음과 같다.

- 1 등급: 두 개 이상의 확산 경로 지님(예: 메일, 네트워크, p2p, 메신저 등)
- 2 등급: 한 개의 확산 경로
- 3 등급: 한 개의 확산 경로를 가지지만 부분적 확산(예: 아웃룩 일부 주소로 전자우편 발송))
- 4 등급: 기본 확산 경로(예: 실행 파일 감염)
- 5 등급: 버그로 인한 자동 확산 루틴 실행 실패

4. 국내 경보 체계 현황

4.1. 국내 경보 체계의 비교

이상 살펴본 국내 경보 체계의 각 항목별 비교 및 정리 결과 자료는 [표1]에 나타나 있다.

		NCSC	KrCERT	안철수연구소	하우리
전역적 경보 체계	단계	4개 단계: 정상>주의>경고>위험		없음	없음
	산정기준	피해범위 출현→ 단일기관→ 여러기관→ 국가적차원	인터넷소통 정도 원활→ 일부장애→ 확산조짐→ 전국적장애		
	대응요령	상황별 대응요령을 매우 상세하게 제공	일반사용자, 관리자, ISP/IDC별 대응요령 제공		
개별적 경보 체계	등급	없음	3개 등급: C,B,A	감염시위험도 5개 등급: 주의,대비,위해,위험,파괴 확산위험도 5개 등급: 5,4,3,2,1	피해도 5개 등급 확산도 5개 등급
	산정기준		공개안됨	피해/확산정도	피해/확산정도
	대응요령	바이러스 정보와 함께 제공			
특이사항		동향 분석 정보 제공	인터넷 소통 현황 정보 제공	신종 바이러스에 대한 주의 경고 제공, 개별 바이러스에 대한 현재 확산도 정보 제공	신종 바이러스의 피해/확산 정도에 따라 바이러스대응상태 제공

[표 1] 국내 경보 체계 비교

이들로부터 다음과 같은 특징을 알 수 있다. 첫째, NCSC와 KrCERT와 같은 국가공공기관은 사이버 위협이 발생했을 경우 상황에 따른 정보통신기술 인프라 전역에 관련된 전역적 경보 체계를 가지고 있지만, 안철수 연구소와 하우리는 전역적 경보 체계가 없거나 미미하다. 그렇지만 개별 위협에 대해서는 매우 상세한 정보와 대응요령 및 이를 치료할 백신 프로그램을 전문적으로 제공하고 있다.

둘째, 전역적 경보 체계와 관련하여 전체적인 사이버 위협 상황에 대한 판단을 개별 컴퓨터의 피해도보다 네트워크 서비스에 대한 피해도를 보다 우선시 한다. [표 ?]에서 보는 것과 같이 NCSC와 KrCERT는 등급 산정 시 위협이 어느 정도의 국가 조직 및 주요 네트워크 인프라에 피해를 끼치고 있는 지를 기준으로 한다.

셋째, 개별적 경보 체계와 관련하여 안철수 연구소와 KrCERT이 개별 위협에 대해 확산도와 피해도를 나누어 등급 산정하는 것을 알 수 있다. 이는 일차적으로 과거의 바이러스 확산이 단순 파일 복사 및 실행에만 의존하지 않고 인터넷이 보편화 되면서 메일, 메신저를 통한 확산 등 확산 경로가 다양화되는데 있다. 또한, 개별 PC에서 네트워크 인프라로의 공격 대상이 변경한 것도 확산 정도가 주요한 산정 기준이 되는 원인이 된다.

4.2. 문제점 및 접근 방안

본 논문에서 조사한 국내 경보 체계는 현재 초기 대응 체계를 구축하는 수준에 있다. 본 절에서는 이러한 국내 경보 체계의 문제점을 지적

하고 이를 해결하기 위한 접근 방안을 간략히 제시한다.

● 경보 발령 기준의 모호

각 상황별 경보 단계가 모호하게 구분되어 있어서 유사한 상황이라 할지라도 경보를 발령하는 주체의 주관적인 기준에 따라 다른 단계의 경보를 발령할 수 있다. 예를 들어, 확산 가능성의 기준을 달리 가지고 있는 경보 발령 주체들이 어떤 기관들(혹은 지역들)에 피해가 발생(혹은 인터넷 소통 장애)한 경우 어떤 주체는 '주의'를 어떤 주체는 '경고'를 발령할 수 있다. 이의 해결을 위해 정보통신 기술 인프라에 위해 가능성이 있는 위협 요소를 식별하고 분류하는 위협 식별 및 분류 모델과 자산을 분류하고 우선순위에 따라 보호 대상을 선정하는 자산 도출 모델의 개발이 필요하다.

● 통합 경보 발령체계 부재

각 주체별로 경보 발령 기준이 통일되어 있지 않아 같은 상황에서 서로 다른 경보를 발령하여 상황 판단 및 대응에 혼란을 줄 수 있다. 예를 들어, 단일기관에서 문제가 발생하였지만 인터넷 소통에는 문제가 없는 경우, NCSC에서는 '주의' 경보를 발령하는 반면에 KrCERT에서는 인터넷 소통이 원활하기 때문에 '정상' 경보를 발령할 수 있다. 이의 해결을 위해 각 주체별로 경보 발령을 위한 정보를 공동으로 수집하고 분석하여 상호 정보 교류를 통한 공통 경보 발령 체계 수립에 대한 연구가 이루어 져야 한다. 구체적으로 경보 발령을 위해 적합한 정보 포맷과 여러 주체들로부터 수집할 정보의 요구 사항을 정의한다.

● 공동 대응 협력 체계 부재

NCSC, KrCERT, 안철수 바이러스 연구소, 하우리는 사이버 위협 발생 시 그 대응이 개별적으로만 이루어져 왔고 그 대응 협력체계가 정의되어 있지 않아 중대한 사이버 위협 발생 시 경제적으로 엄청난 피해를 받을 수 있다. 이의 해결을 위해 공동대응협력체계를 위한 관련 법 제정과 같은 제도적 차원의 뒷받침이 필요하다. 기술적으로 보안 이벤트 및 로그 포맷 표준화를 비롯한 보안 정보 공유 프레임워크 구축이 이루어져야 한다.

5. 결론

본 논문에서는 사이버 위협으로 인한 체계적이고 신속한 상황 판단 및 대응을 위하여 국내의 경보 체계들을 전역적 경보 체계와 개별적 경보 체계로 분류하여 조사 및 분석하였다. 먼저 국가기관차원에서 NCSC와 KrCERT의 경보 체계 현황을 조사하였고 민간 산업체 차원에서 안철수연구소와 하우리의 경보 체계 현황을 조사하였다. 그리고 이를 바탕으로 국내 경보 체계들을 비교하고 비교한 자료로부터 경보 발령 기준의 모호, 통합 경보 체계 부재, 그리고 공동대응협력체계 부재를 문제점으로 지적하고 그에 대한 해결방안을 간략히 제시하였다.

참고문헌

[1] 정관진, 이희조, "인터넷 웜과 바이러스의 진화와 전망," *정보처리학회지 제10권 2호 pp. 27-37*, 2003년 3월.

[2] Robert Lemos, "Counting the Cost of Slammer," CNet News.Com, *http://zdnet.com.com/2100-1104-982955.html?tag=nl*,, Jan. 31, 2003.

[3] 정태명, "인터넷 침해사고 원인과 대책," *정보처리학회지 제10권 2호 pp. 22-26*, 2003년 3월.

[4] 박상서, 박춘식, "정보전 개념과 주요 동향", *정보처리학회지 제10권 2호 pp. 47-57*, 2003년 3월.

[5] 국가사이버안전센타, *http://www.ncsc.org/*

[6] 국가사이버안전센타, *국가사이버안전매뉴얼*, 2004년 3월

[7] 인터넷침해사고대응지원센타, *http://www.krcert.or.kr*
[8] 안철수연구소, *http://www.ahnlab.co.kr*
[9] 하우리, *http://www.hauri.co.kr*

이 도 훈
1989년 한양대학교 전자계산학과 졸업(공학사)
1991년 한양대학교 대학원 전자계산학과 졸업 (공학석사)
1991년~2000년 국방과학연구소(선임연구원)
2000년~현재 국가보안기술연구소(선임연구원)

백 승 현
1999년 한동대학교 전산전자공학부 졸업(공학사)
2001년 한국과학기술원 전산학과 졸업(공학석사)
2001년~2003년 (주)아이디스(전임연구원)
2004년~현재 국가보안기술연구소(연구원)

오 형 근
1998년 순천향대학교 전산학부 졸업(공학사)
2000년 순천향대학교 대학원 전산학과 졸업 (공학석사)
2000년 2월~8월 한국사이버페이먼트(선임연구원)
2000년 8월~현재 국가보안기술연구소(선임연구원)
2003년 9월~현재 고려대학교 정보보호대학원 (박사과정)

이 진 석
2000년 한남대학교 대학원 컴퓨터공학과 졸업 (공학박사)
1986년~1999년 한국전자통신연구원(선임연구원)
2000년~현재 국가보안기술연구소(책임연구원)