디지털산업정보학회 논문지 제4권 제2호 - 2008년 6월

정부 주요기관에 대한 사이버 공격의 대처 방법

이 영 교* · 박 종 순**

A Countermeasures on the Cyber Terror for the National Key Organizations

Lee, Young-Gyo · Park, Joong-Soon

〈Abstract〉

As internet is spreaded widely, the number of cyber terror using hacking and virus is increased. Also the international cyber terror to the national key organizations go on increasing. If the national key organizations is attacked by the attack, the national paper, document and records are exposed to the other nations. The national paper, document and records can give damage to the nation. Especially, the unknown attack can give much damage to the nation. Therefore, this paper suggested a countermeasures on the cyber terror for the national key organizations provided the inner of the organization is safe. The uneffective item and invasion privacy item are included among the countermeasures. However the countermeasures can protect only one cyber terror to the national key organizations.

Key Words : Cyber Terror, Worm, Virus, Hacker, Hacking, National Key Organizations

Ⅰ. 서론

인터넷이 전세계로 활발하게 보급되면서 이제 어디에서든지 세계 곳곳의 정보를 검색할 수 있게 되었다. 또한 인터넷을 통한 각종 온라인 서비스(인터넷 쇼핑, 인터넷 뱅킹, 인터넷 도서관, 이메일 등등)를 편리하게 이용할 수 있게 되었다. 그러나 이러한 편리함과는 정반대의 역효과로 인터넷을 통한 바이러스와 해킹이 전 세계적으로 창궐하게 되었다.

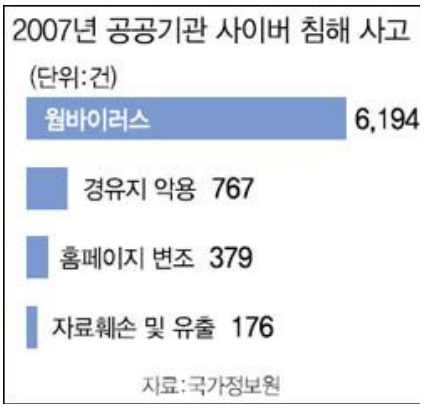
바이러스와 해킹은 일반 사용자는 물론이려니와 기업이나 단체에게도 엄청난 물질적·정신적 피해를 준다. 그러나 보다 치명적인 피해를 받게 되는 곳은 국가의 가장 중요한 기관(청와대, 국가안전보장회의, 국회, 국정원, 국방부 등)들일 것이다. 이들 중요기관에서 다루어지는 자료들은 국가의 정치, 경제는 물론 국가안보 등에 관련된 아주 민감하고 중요한 자료들이다. 따라서 이들 기관의 자료가 바이러스나 해킹에 의해 유출된다면 그 국가적인 피해는 엄청나게 된다. 특히 2007년과 2008년, 정부주요기관의 국제간 해킹 및 바이러스를 통한 정보 유출 시도사건이 빈번해지고 있다. 따라서 본 논문에서는 이들 사건들을 분석하고 그에 대한 대응 방법을 제시하고자 한다. 논문의 나머지 부분은 다음과 같이 구성되어진

* 서일대학 인터넷정보과 전임강사
** 서일대학 인터넷정보과 부교수

다. 2장에서는 정부 주요기관에 대한 해킹 및 바이러스 공격에 대한 공격 사례를 소개하고 3장에서는 해킹 및 바이러스의 공격에 대한 분석을 수행한다. 4장에서는 그에 대한 대처 방법을 제안하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 정부주요기관에 대한 해킹 및 바이러스 공격 사례

국가정보원이 최근 발간한 '2008 국가 정보보호백서'에 따르면 지난해 국내 공공기관에서 발생한 사이버 침해사고는 총 7,588건으로 집계됐다. 2006년(4,286건)에 비해 77%나 증가한 수치다. 작년 민간 부문 해킹 사고가 2만1,732건으로, 2006년(2만6,808건)보다 19% 정도 감소한 것과는 대조적이다[1].



<그림 1> 2007년 공공기관 사이버 침해사고
(국가정보원 제공)

지난 2004년 7월 15일 경향신문에 따르면 국회 69대, 해양경찰청 77대, 원자력연구소 50대, 국방연구원 9대, 국방과학연구소, 해양연구소, 통일연구원, 천문연구원, 중소기업청 각 1대 등 모두 211대의 컴퓨터가 해킹을 당했다. 피해기관에는 국군기무사령부도 포함돼 있다. 해커들이 국회, 국방부 등의 주요기관을 해킹한 사건이 알려지기 시작한 이후 제3국을 근원지로 한 해킹이 매년 증가추세를 보이고 있다. 이에 따라 보안시스템이 강화되고 있지만 최근 들어서는 해커들이 사용하는 해킹툴도 강력해져 보안시스템을 무력화시키고 있다[2].

2005년 7월 과기부 산하 43개 기관의 보안시스템을 감시하는 한국과학기술정보원(KISTI)의 원장 홈페이지가 해킹당한데 이어 '리니지 명의도용' 사건이 일어났다. 2006년에 들어서는 KISTI의 홈페이지가 해킹당했으며 유명 게임회사인 넥슨사가 운영하는 '마비노기' 게임의 해킹 사건이 일어났으며 EBS, 아시아문화산업교류재단, 씨네타운 등의 홈페이지가 해킹당해 접속자의 개인정보를 빼내는 악성코드가 유포되기도 했다. 특히 육군 내 컴퓨터 전산망 바이러스 침투 및 해킹이 2005년부터 2007년까지 3년간 4,500여건(해킹 145건, 바이러스 침투 4,400건)에 이르렀다.

2008년 4월 22일 한국일보에 따르면 새 정부 출범을 며칠 앞둔 지난 2월 중순, 국가기관의 심장 격인 청와대 전산망에 외부 해커들이 침입, 상당량의 중요한 정보들을 빼내간 것으로 21일 확인돼 충격을 주고 있다. 더욱이 청와대와 국가정보원은 3월 말까지 해킹 사실조차 알지 못했으며 그 이후 총체적인 점검에 들어갔으나 아직까지도 어떤 자료가 유출됐는지조차 정확히 파악하지 못하고 있어 국가기관의 전산망 관리는 물론 국가안보 차원의 보안 관리에 치명적인 문제점을 드러냈다[3].

청와대와 국정원에 따르면, 이들 해커들은 정상적 절차 없이 시스템에 다시 접근할 수 있도록 하는 백도어(back door) 프로그램을 설치하는 치밀함을 보였다. 따라서 국정원 등의 추정대로 해커들이 상업적 목적이 아닌 국가안보 차원의 기밀을 노리는 중국이나 북한의 정보기관이라면 즉각적으로 국가기관 전산망에 대한 총체적 점검에 들어가 보안망을 철저하게 구축해야 할 상황이다.

해커들은 최근 청와대 전산망을 다시 노렸다. 4월 19일 오전 청와대로 향하는 인터넷망에 정체를 알 수 없는 접속이 폭주했다가 방화벽에 막혀 봉쇄됐다. 청와대는 이 해킹 시도를 국가안보 차원의 중대사건으로 간주, 국

정원과 사정당국에 조사를 지시했다.

2008년 4월 1일 세계일보에 따르면 이명박 정부의 장·차관, 실·국장 등 고위 공직자의 이메일을 겨냥한 해킹이 시도된 사례가 적발돼 파문이 일고 있다. 고위 공직자를 겨냥한 해킹 메일은 채용 응시자처럼 인사말과 사진을 보내고 여기에 자신을 소개하는 파일을 첨부하는 방식으로 돼 있다. 첨부파일을 열면 이메일과 컴퓨터 안의 자료가 해킹당하는 것으로 알려졌다[4].

특히 해킹 이메일은 중국 등 국내가 아닌 제3국에서 한글로 작성돼 유입됐으며, 고위 공직자의 이메일을 통해 궁극적으로 정부 전산망을 해킹하려고 한 것으로 추정되고 있다. 국정원 한 관계자는 "최근 모 부처의 고위 공직자에 대한 이메일이 이 같은 해킹 이메일에 노출된 적이 있으며, 해커들이 노리는 것은 궁극적으로 정부 전산망인 것으로 보인다."고 말했다.

국정원은 또 최근 해킹 이메일인 '이명박 대통령 순방 일정 이메일'을 주의하라고 각 정부부처에 당부하기도 했다. 이 메일에는 "대통령 비서실입니다. 첨부 파일은 대통령 출국 방문 일정입니다. 받아주십시오"라는 내용이 들어 있었다.

Ⅲ. 해킹 및 바이러스 공격에 대한 분석

인터넷이 활발히 보급되지 못했던 1980년대만 하더라도 바이러스는 외국여행을 갔다 오는 산업체와 학계의 연구진의 디스켓 등을 통해 국내로 유입이 되었으며 국내에서의 전파도 디스켓 등의 오프라인 매체로 이루어지다보니 대체적으로 느린 편이었다. 또한 국제간 해킹은 거의 이루어지지를 못하였다. 그러나 인터넷이 활발하게 보급되기 시작한 2000년 전후부터 디스켓, CD ROM, DVD 등의 오프라인 매체를 이용한 바이러스의 전염보다도 인터넷을 통한 바이러스 전염이 더욱 많아지게 되었다. 또한 인터넷을 이용한 국제간의 해킹도 점차 늘어나게 되었다.

3.1 바이러스에 의한 공격 분석

국내에서 바이러스가 크게 번지게 된 것은 1980년경 국내의 모 컴퓨터 잡지사가 동남아시아에서 퍼지던 바이러스에 대한 기사를 게재하면서 바이러스 프로그램의 소스를 소개했기 때문이다. 그 이후로 이를 모방한 바이러스가 국내에서도 급속히 생겨나기 시작했다. 이렇게 모방해서 생기게 된 바이러스들은 대부분 자신을 알리기 위한 홍보용이나 장난으로 만들어진 것들이었다. 이 시기의 바이러스들은 컴퓨터의 메인 메모리나 하드디스크 혹은 디스켓 등의 보조 기억장치나 응용 프로그램에 잠복해 있다가 다른 컴퓨터나 파일을 감염시키는 부트, 파일, 부트/파일 바이러스들이 주종을 이루었으며 그 피해도 초기에는 컴퓨터의 메모리 공간을 낭비시키거나 컴퓨터의 처리 속도를 느리게 하는 등의 피해만을 주었으나 점차 파일을 파괴하는 등의 피해를 주게 되었다. 또한 국산 바이러스가 외산 바이러스보다 많았으며 그 감염 속도는 현저히 느렸다.

그러나 인터넷이 급속도로 보급되기 시작한 2000년을 전후로 하여 인터넷을 통한 이메일, 공유 폴더 등의 네트워크를 이용한 바이러스가 증가하게 되었다. 자기 복제가 가능한 악성코드를 웜 바이러스라고 하는데 인터넷을 통하여 감염되므로 전파속도가 빨라 24시간 이내에 전세계로 전파되어 그 피해가 더욱 크게 되었다. 웜 바이러스는 컴퓨터가 부팅되지 않도록 하거나 하드 디스크가 인식되지 않도록 하는 등의 시스템 파괴를 할뿐만 아니라 네트워크를 통하여 새로운 알고리즘이나 중요 자료들을 유출시키기도 하고 네트워크의 속도를 저하시키기도 한다. 또한 감염된 컴퓨터에서 주소록을 이용하여 다시 전파되도록 하는 지능적인 수법을 사용하기도 한다[5, 6, 7].

3.2 해킹에 의한 공격 분석

컴퓨터 크게 보급되기 이전인 1970년대까지만 해도 해커라고 하면 컴퓨터광을 총칭하는 의미로 사용되었다.

컴퓨터를 전반에 걸쳐 깊이있게 배우는 사람들로써 이들은 컴퓨터 시스템의 오류나 취약점을 찾아내어 이를 수정하도록 도와주곤 했다. 1980년대에 접어들어 개인용 컴퓨터가 학교, 사무실, 가정 등에 급속히 보급되자 해커들의 숫자도 늘기 시작했으며 이들은 다른 시스템에 불법으로 접속하여 정보를 빼내어 판매하기 시작하였다. 1990년대 들어서는 이해관계에 따라 정부 기관의 홈페이지를 공격하는 등 자국 혹은 상대국을 대상으로 정치적 활동도 하였다. 2000년을 전후로 하여 인터넷이 급속도로 보급되면서 국내에서의 해킹은 물론 국제간의 해킹도 급격히 증가하게 되었다. 또한 해커가 제작한 해킹 프로그램이 인터넷을 타고 급속히 번져 나가게 되어 수많은 해커를 양성하게 되었다. 특히 최근에는 컴퓨터 시스템에서 유용한 정보를 빼가서 이를 이용하여 금전을 요구하는 국제적인 범행이 이루어지고 있으며 국가의 중요 문서를 해킹하는 등의 국제적인 사이버 테러도 발생하고 있다[5-10].

3.3 해킹과 바이러스의 기술 통합

과거에는 컴퓨터 바이러스는 생물 바이러스처럼 타인의 컴퓨터에 감염되고 증식되어 자신을 알리거나 타인을 괴롭히는 실행 프로그램이 주종을 이루었다. 해킹은 서버에 침입하여 관리자 권한을 획득하여 필요한 정보를 빼가거나 데이터를 파괴하였다. 그러나 정보보호 기술이 발전하여 직접적인 공격이 어려워지자 바이러스의 형태를 띤 해킹 기술인 웜 바이러스 형태로 발전하고 있다. 사실상 초기에는 바이러스의 기술과 해킹 기술이 전혀 상이했지만 발전하면서 점차 비슷해져서 이제는 바이러스인지 해킹인지를 구분 할 수 없게 되었다. 대표적인 웜 바이러스에는 코드레드, 님다 등이 있다. 과거에는 바이러스와 해킹이 단순한 개인적인 목적으로 만들어지거나 행하여 졌지만 점차 정치, 사회적 목적을 가지게 되었으며 이익을 위하여 경쟁사나 상대국을 대상으로 이루어지고 있다는 것이다. 특히 앞장에서 살펴보았듯이 사이버 공격이 최근에는 국가의 주요기관을 상대로 이루어지며 국가의 주요 기밀문서를 목적으로 한다는 것이다.

공격 방법도 무척 다양해지고 있다. 구글이나 네이버 등의 검색 엔진을 이용하여 개인정보를 획득한 후 이를 이용한 해킹방법도 등장하였으며 보안이 취약한 웹사이트를 해킹해 그곳을 방문한 네티즌들을 대상으로 악성코드를 무차별적으로 유포시키는 신종 해킹수법도 유행하고 있다[5, 7]. 따라서 인터넷에 연결되어 있는 수만개의 웹사이트들이 가해자이자 동시에 피해자가 되기도 한다. 수많은 컴퓨터들이 자신의 의지와는 상관없이 사이버 범죄자들에게 악용당하기도 한다는 것이다. 최근에는 웜, 바이러스, 해킹 등 사이버 공격기술이 돈을 얻기 위한 협박에 이용되면서 점점 더 수법이 교활해지고 있다. 개인정보나 기업의 정보유출로 사생활 노출은 물론 재산상 심각한 피해를 입고 있는 것이다. 정부는 2003년 1월에 있었던 인터넷의 접속 불능 사태의 재발을 막기 위하여 인터넷침해사고대응지원센터(KISC : Korea Internet Security Center)를 운영하고 있다[11]. 그러나 현재 국내 보안정책이나 기술은 신종 사이버 공격에 대한 대비가 되어 있지 않다.

Ⅳ. 제안하는 대처 방법

사이버 공격자들의 공격수법은 점점 지능화, 복잡화되는 등 첨단의 기술을 이용하는 반면, 이를 막기 위한 보안 기술은 이를 뒤쫓아 가기에 바쁜 상황이다. 기존의 보안 기술로는 검출이 안되는 신종 바이러스, 웜, 트로이 목마 등의 악성코드가 계속적으로 발견되고 있으며 이를 막기 위한 사전 조치가 아니라 사후 조치에 머무르고 있는 상황이다.

<그림 1>는 2005년에 4대 기업 모범 사례에서 소개된 기업의 기술유출 방지 및 보안 시스템 사례이다. 반도체, 휴대폰, 자동차, 조선 기술과 같이 기업의 중요한 기술에 대한 기술유출의 방지 및 보안대책은 기업 생존의 사활

이 걸려 있다. 또한 국가간의 사이버전을 대비한 방안도 그안도비슷하거나 더 중요한 레벨일 수 있다. 그래서 군의 사이버전 수행체계에 관한 연구도 이루어지고 있다[6]. 그리고 중요핵심기반시설에 대한 보안관리 연구도 제시된 바가 있다[12]. 따라서 이와 같이 군이나 기업체에서 시행하고 있는 보안 대책 및 시스템은 정부주요기관의 보안 대처 방법과 그 목적 및 유형에서 비슷하다고 하겠다.

구 분	내 용	기업별 운영제도
기준, 프로세스의 정형화	○ 출입 관리	통제구역 출입권한 제한 PC 및 카메라류 등 회사 반/출입 금지 품목 지정관리 ※ 서울반도체 : 보안층괄제 도입 및 보안담당 조직의 재편성
	○ 인적 보안	보안서약서 징구, 핵심인력 관리
	○ 문서(우편물) 보안	비밀등급 관리, 문서분류 체계 등 ※ 한국IBM : 기밀정보 폐기함, 상세하게 정의된 기밀서류 파기 절차, 테러예방과 연계된 우편물 보안 강화
	○ 시스템 보안	PC 보안프로그램, 방화벽 설치, 비업무용 사이트차단 등
	○ 위반시 신상필벌 지침	※ 서울반도체 : 내부신고제(4등급, 최고 1억원), Best 부서와 Worst 부서 선정 : 포상, 대책 ※ 삼성종기원 : 철저한 信賞必罰 (一罰百戒)
	○ 외부 방문객 관리지침	회사□통제구역 방문 사전 예약제 등 ※ 삼성종기원 : 내방객의 PC 및 카메라류, 카메라폰 반입금지 (프로세스 미준수시 출입불가)
보안 시스템 구축	○ 방문객 관리	외부방문객과 사무, 제조공간 분리
	○ 보안구역 출입 통제 시스템	사원증, 생체인식, RF-ID 시스템 등 구축
	○ 인프라 구축 (Server, DRM, S/W, H/W, N/W관리 등)	※ 삼성종기원: 보안통합관리센터 운영(One Stop Service) ※ 에스원 : SNC(삼성 네트워크컴퓨팅) 시스템
임직원 보안 의식 제고	○ 지속적인 홍보, 교육	※ 서울반도체: 보안유출사례/캠페인 제작□배포 ※ 삼성종기원 : 사이버 보안교육 과정 개설 및 월간 Hil Security 발행
	○ 보안감사	※ 삼성종기원 : 보안지킴이 (부서단위 보안조직), 보안어사제 (주기적인 보안점검) 운영

<그림 2> 기술 유출 및 방지를 위한 기업보안 시스템

그러나 보다 문제가 되는 것은 사이버 공격에 의해 아무런 흔적이 없이 정보가 유출되는 '알려지지 않은 공격'이다. 정부 주요기관이 이러한 공격을 받는다면 한 국가의 주요 정책이나 결정이 고스란히 상대국에 노출되고 그 사실을 인지하지 못하게 되는 상황에 이를 수 있다. 따라서 본 장에서는 시스템 내부는 안전하다는 전제 하에 외부에서 인터넷을 통하여 들어오는 단한번의 인식 가능 및 불가능한 사이버 공격을 막는 대처 방법을 제시하고자 한다.

(1) 온라인 PC와 오프라인 PC를 별도로 운영

일반적으로 우리는 컴퓨터에 인터넷을 연결하여 웹 사이트를 검색하고 이메일을 체크하며 문서를 작성하여 저장하는 등의 컴퓨터 관련 업무를 한대의 PC에서 수행한다. 그러나 이러한 방식은 컴퓨터가 바이러스에 걸려 고생을 해본 사람이면 누구나 상당히 위험한 방식이라는 것을 알고 있다. 한번 바이러스에 걸리게 되면 컴퓨터를 복구하는 데에 시간적, 경제적인 노력이 소요되며 하드디스크에 저장되어 있던 정보가 100% 완전히 복구되지 않는다. 다른 저장 매체에 백업을 받아 놓았다면 다행이지만 백업 작업도 번거로운 작업임에 틀림없다. 그러나 보다 중요한 문제는 중요 문서가 노출될 수도 있다는 것이다. 포트차단을 이용한 네트워크 침해사고의 기술적인 대응 방법들이 많이 제안되어 있으나[8, 13, 14] 해킹의 기술도 그에 따라 발전하고 있으며 단 한번의 정보 노출을 막기 위해서는 정부 주요기관 내에서는 인터넷을 연결하여 웹 검색 및 이메일 체크 등을 수행하는 온라인 PC와 문서 작업 등의 업무를 수행하는 PC를 별도로 운영함으로써 인터넷을 통한 정보 유출이나 파괴를 일단 차단해야 한다.

(2) 이메일에 파일 첨부를 자제하여야 한다.

발신자의 신원이 확실치 않은 이메일에 첨부된 파일을 열어보는 것은 상당히 위험한 행위이다. 일부 바이러스들이 이를 통하여 감염되기 때문이다. 심지어 넘다 바이러스와 같이 첨부 파일을 열어보지 않고 수신된 이메일을 읽기만 해도 감염되는 바이러스도 존재하기 때문이다. 따라서 주요기관 내에서는 이메일에 파일을 첨부하는 것을 금하거나 자제하도록 하여 수신자가 파일이 첨부된 이메일 자체를 열어보지 못하도록 하여야 한다. 뿐만 아니라 이메일에 파일을 첨부하여 발송하는 것은 중요 자료가 외부로 유출될 수 있는 경로를 제공하기 때문이다.

(3)수신된 이메일의 사전 검색

불특정 다수에게 뿌려지는 스팸 메일은 대부분 제목이나 발신자를 보면 걸러내어 읽어보지 않고 삭제할 수 있다. 이에 따라 스팸 메일은 점점 교묘한 제목을 달아 수신자가 열어보도록 유혹하고 있다. 뿐만 아니라 이메일을 통해 전파되고 있는 웜 바이러스들도 그 제목이나 발신자를 교묘하게 표시하여 수신자를 유혹하고 있다. 특히 정부 주요기관 내에서 '이명박 대통령 순방 일정'과 같은 제목의 이메일은 정보보안 전문가조차도 속을 수 밖에 없다. 따라서 주요기관들마다 그 특성을 파악하고 있는 보안전문가들을 두어 수신되는 이메일들을 메일서버에서 걸려내고 발신자에게 이메일 발송 여부를 다른 통신 매체(유선전화, 휴대폰, 문자 등)를 이용하여 확인하거나 격리된 컴퓨터에서 열어 보는 등의 사전 검색을 거친 뒤 안전한 이메일들을 수신자에게 전달하여야 한다.

(4) 주요기관 내에서는 사적인 일은 자제해야 한다.

이메일의 사전 검색은 상당히 개인의 프라이버시를 침해하는 방법이다. 그러나 한 국가의 가장 중요한 기관이라면 개인적인 행동은 충분히 자제되어야 하는 사항이다. 물론 어느 누구도 자신의 가족, 친지, 친구 등에게 이메일을 보내거나 받을 수 있다. 그러나 그로 말미암아 수신된 이메일의 발신자와 제목으로 스팸이나 웜 바이러스를 걸러내기가 어렵게 될 수 있다. SirCam 바이러스와 같은 경우는 감염된 컴퓨터에서 무작위로 선택된 파일명을 메일 제목과 첨부 파일명으로 사용하며 아웃룩이나 채팅 프로그램의 주소록을 이용하여 제 3자을 감염을 시키기 때문이다. 따라서 이런 경우에는 이메일의 발신자가 가족, 친지, 친구 등으로 표시되므로 보안전문가는 물론 본인도 바이러스 이메일을 걸러낼 수 없게 된다. 따라서 기관 내에서는 사적인 메일을 금하여 이러한 사적인 메일을 통하여 들어오는 사이버 공격을 근원적으로 차단해야 한다.

(5) 불필요한 파일의 다운로드나 프로그램의 설치

주요기관의 컴퓨터에서는 MP3, JPEG 파일, 동영상, 영화, 쉐어웨어 등의 파일을 무료로 다운로드받는 일을 삼가야 한다. 무료로 다운로드받는 이러한 파일들중에 악성코드들이 삽입되어 있는 경우가 종종 발생하기 때문이다. 또한 여러 웹 사이트에 방문하면서 그곳 사이트에서 제공하는 보안프로그램, Active X 또는 코덱 등을 설치하는 것도 조심하여야 한다. 이러한 대응 방안은 이미 성재모 등이 제안한 논문에서 기제안된 것이기도 하다[5]. 특히 최근 UCC(User Created Content) 동영상이 인터넷을 통하여 널리 제공되면서 이를 보기위한 호기심을 이용하여 신뢰할 수 없는 Active X 또는 코덱 등을 설치하도록 하고 있다. 이 또한 악성코드가 자신의 컴퓨터에 무단히 설치하도록 하는 문을 열어 주게 되는 것이다. 성인용 사진이나 동영상을 이용한 악성코드 침투는 이미 널리 알려진 사실이기도 하다.

(6) 문서의 전달은 구식 방법을 이용

이메일에 파일을 첨부하지 않으면 어떻게 문서를 관련 부서에 전달할 수 있을까? 기관내에 직원이 100 여명정도라고 가정한다면 시간적, 공간적으로 출력된 문서를 직접 사람이 전달하기도 힘들다. 이메일에 문서를 첨부하지 않는다면 팩시밀리를 이용한 문서 전달이 가장 효과적인 방법이다. 팩시밀리는 인터넷이 원활히 보급되기 직전까지의 과도기에 널리 사용되었던 문서 전달 장비이다. 전화선을 이용한 팩시밀리 장비가 인터넷에서 노출될 수 있는 디지털 데이터를 근원적으로 차단할 수 있다. 그러나 워드 프로세서에 내장되어 있는 팩스 보내기 기능은 사용하지 말아야 한다. 이 기능은 인터넷을 통하여 팩스 보내기를 제공함으로 이메일에 문서를 첨부하는 것과 같이 인터넷에 정보를 유출시킬 수 있다. 따라서 오프라인 PC에서 작성한 문서를 일단 프린터로 출력하고 이를 전화선을 이용한 팩시밀리를 통하여 수신자에게 전달하여야 한다.

(7) 종이 문서에 대한 보안 강화

중요한 문서에 대한 작성 및 보관 그리고 전달 작업을 온라인에서 배제시켰으므로 인터넷을 통한 유출은 막을 수 있다. 반면 출력되는 문서가 늘어나므로 하드 카피된 문서에 대한 보안을 강화해야 할 필요가 있다. 팩스를 보내기 위하여 출력된 문서는 팩스 송신 후 바로 분쇄기를 이용하여 폐기하여야 한다. 또한 폐기되지 않고 외부로 유출될 가능성을 막기 위하여 부서의 출입구마다 EM(Electro Magnetic)이나 RFID(Radio Frequency IDentification) 태그 검출기를 설치하여 허가받지 않은 종이 문서의 외부 유출을 이중, 삼중으로 철저히 막아야 한다. 물론 그러기 위해서는 특수 제작된 출력용지를 사용해야 한다. 노트북, 카메라(필름 카메라, 디지털 카메라), 이동식 디스크, USB 메모리 등의 저장 매체에 대한 출입구 검색은 당연히 이루어 져야 한다.

(8) 원격지에서의 자료 다운로드 자제

이제 우리는 인터넷 접속이 가능한 곳에서 세계 어느 곳의 정보라도 수집할 수 있게 되었다. 또한 출장 시에 준비한 PPT, PDF 파일 등의 디지털 자료 이외에 추가적인 자료를 자신이 속한 기관의 홈페이지에 접속, 검색하여 다운로드받을 수도 있다. 물론 이러한 원격지에서의 자료 이용이 무척 편리한 방법이지만 반면에 해킹이나 바이러스에 의한 표적이 될 수도 있다는 것이다. 로그인 시나 파일을 다운로드받을 때에 본인 확인을 위해 패스워드를 입력하도록 하지만 이런 보안 정책은 최근의 사이버 공격을 막기에는 역부족이다. 따라서 필요한 데이터는 사전에 반드시 보조 저장매체에 휴대하도록 하고 원격지에서 온라인으로 자료를 다운로드받는 일은 피해야 한다. 불가피한 경우에는 기관 내에 잔류하는 직원과 통화하여 잠시 자료를 올렸다가 다운로드 후에는 제거하여야 한다. 인터넷 상에 자료가 계속적으로 존재하는 것 자체가 해커에게 자료를 해킹해가라고 하는 상당히 위험한 행위이기 때문이다. 또한 공유 폴더를 운영하는 것 역시 매우 위험한 일이므로 피해야 한다. 편리해서 최근의 사용이 증가하고 있는 웹하드의 사용시에도 패스워드를 설치함은 물론이려니와 장기간 자료를 올려두지 말고 필요시에만 잠시 자료를 올렸다가 즉시 삭제하도록 해야 하겠다.

(9) 웹 사이트와 데이터베이스의 분리 운영

여러 정보를 유, 무료로 제공해주는 ISP(Internet Service Provider)뿐만 아니라 기업, 공공기관, 은행, 국세청, 법원 등 정부의 여러 기관 및 주요기관이 홍보 및 창구 업무를 위한 인력을 줄이기 위하여 웹 페이지를 이용한 온라인 홍보 및 서비스를 제공하고 있다. 이들 기업체나 기관이 운영하는 웹페이지에는 다양한 소개 자료 및 검색 기능을 두어 이용자가 원하는 자료들도 열람할 수 있도록 하고 있다. 한 서버에 웹페이지와 데이터베이스를 같이 운영하기도 하고 대형 기관에서는 별도의 서버로 운영하기도 한다. 그러나 결과적으로 인터넷으로 연결되어 있다는 측면에서는 동일한 결과를 낳게 한다. 사용자가 편리하게 온라인으로 해당 업체 혹은 기관에서 원하는 자료를 얻을 수 있는 만큼 해커도 쉽게 자료를 획득해갈 수 있기 때문이다. 따라서 사용자들이 이용하기가 다소 불편하더라도 모든 자료를 웹페이지와 연결하지 말아야 한다. 문서에 대한 등급을 나누어 3등급 자료는 온라인으로도 열람 가능, 2 등급은 사내에서만 열람 가능 그리고 1 등급 자료는 사내의 지정된 보안룸에서만 가능하도록 하는 등의 조치가 필요하다.

(10) 보조 저장매체의 보안

앞에서 살펴본 것들은 인터넷을 이용한 자료 전달을 기피하도록 하여 해킹이나 바이러스 공격에 의해 쉽게 정보가 노출되는 것을 막도록 하는 방법들이다. 대신 CD ROM, DVD, USB 메모리 등의 오프라인 매체의 사용이

증가하게 된다. 이러한 매체들의 외부 출입을 철저히 통제하여야 하고 출장 등의 목적으로 적합한 절차에 의해 외부로 가지고 나갈 경우라도 분실할 경우를 대비하여 매체에 대한 보안을 강화해야 한다. 점차 보조 저장매체의 대용량화 및 소형화에 따라 한번에 저장되는 정보의 량은 늘어나고 휴대하기는 편리해지고 있다. 반면 파손이나 분실할 경우 그 피해도 따라서 증가하게 된다. 따라서 보조 저장매체에 저장되는 파일들을 암호화하여 적법한 사람만이 파일을 열어볼 수 있도록 하여야 한다. 이렇게 함으로써 보조 저장매체를 분실한 경우에 이를 습득한 사람이 악의적 혹은 우연히 국가의 비밀 정보를 열람하거나 이를 제3자에 판매하는 등의 행위를 막을 수 있다. 그러나 한편으로 보안 기능이 취약한 PC에 USB 메모리를 연결하는 경우에 악성코드에 감염시키는 웜이나 바이러스 등이 있어 자칫 USB 메모리가 악성코드의 전파 수단이 될 수도 있다. 따라서 'USB Guard'와 같은 프로그램을 설치하여 USB에서 바이러스가 자동으로 실행되는 것을 차단하여야 한다.

Ⅴ. 결론

해킹과 바이러스를 비롯한 다양한 형태의 사이버 공격이 국가의 주요기관들을 상대로 극심해지고 있다. 그 공격수법은 점점 지능화, 복잡화되는 등 첨단의 기술을 이용하는데 이를 막기 위한 보안 기술은 이를 뒤쫓아 가기에 바쁜 상황이다. 기존의 보안 기술로는 검출이 안되는 신종 바이러스, 웜, 트로이 목마 등의 악성코드가 계속적으로 발견되고 있으며 이를 막기 위한 사전 조치가 아니라 사후 조치에 머무르고 있는 상황이다. 특히 문제가 되는 것은 사이버 공격에 의해 아무런 흔적이 없이 정보가 유출되는 '알려지지 않은 공격'이다. 정부 주요기관이 이러한 공격을 받는다면 한 국가의 주요 정책이나 결정이 고스란히 상대국에 노출되는 상황에 이를 수 있게 된다.

따라서 본 논문에서는 정부의 주요기관에서 시스템 내부는 안전하다는 가정 하에 외부에서 인터넷을 통하여 들어오는 사이버 공격을 막는 대처 방법을 제시하였다. 제시된 대처 방법들은 첨단 기술을 이용한 방법들이 아니고 컴퓨터 관련 업무에 종사하면서 보안 의식이 있는 사람이라면 누구나 생각해낼 수 있는 방법들이다. 제시된 방법들 중에는 처리 시간 및 비용이 증가하는 비효율적인 방법도 있으며 개인의 프라이버시를 침해하는 방법들도 있다. 그러나 국익을 위해서라면 이러한 사항은 충분히 감내할 수 있는 것들이다. 이러한 대처 방법들을 통하여 단 한 번의 정보 유출도 용납할 수 없는 정부 주요기관에 대한 사이버 공격을 차단할 수 있으리라 사료된다.

참고문헌

[1] 국정원, 2008 국가정보보호백서.

[2] 경향신문, http://www.hankooki.com.

[3] 한국일보, http://www.khan.co.kr.

[4] 세계일보, http://www.segye.com.

[5] 양형규, 이강호, 최종호, "국내 검색엔진을 이용한 개인정보 해킹에 관한 연구", 한국컴퓨터정보학회 논문지, 제12권 제3호, 2007.7, pp.195-201.

[6] 김귀남, "국가 사이버전 대비방안 연구", 정보보안 논문지, 제6권 제4호, 2006.12, pp.141-151.

[7] 성재모, 노봉남, 안승호, "최근 주요 해킹 피해 동향과 대응 방안", 한국정보보호학회 논문지, 제16권 제1호, 2006.2, pp.80-84.

[8] 김태훈, 최호성, 김성은, 김주현, "전통적인 네트워크 해킹 기법과 기술적 대응방안", 한국정보보호학회 논문지, 제16권 제1호, 2006.2, pp.75-79.

[9] 정현철, "국내 해킹.바이러스 사고 현황 및 해킹기술 동향", 디지털 행정, 행정자치부 정부전산관리소, 2001.12, pp.37-47.

[10] 임채호, "국내.외 행정정보시스템 해킹사례 ", 행정

과 전산, 총무처 정부전산계산소, 2000.6, pp.36-45.
[11] 정태인, 강준구, 이두원, “인터넷 침해사고 조기탐지 및 대응 체계 운영 현황”, 정보보호학회 논문지, 제15권 제1호, 2005.2, pp.9-16.
[12] 김인중, 정윤정, 고재영, 원동호, “중요핵심기반시설(SCADA)에 대한 보안 관리 연구”, 한국통신학회 논문지, 2005.8, pp.838-848.
[13] 신영선, 박진섭, 박정진, 이희성, “침해사고 대응을 위한 서비스 제어전략에 관한 연구”, 한국컴퓨터정보학회 논문지, 제12권 제4호, 2007.9, pp.127-136.
[14] 안정철, “침입방지시스템과 역할기반 보안정책을 이용한 정부기관 정보보호 시스템 설계”, 한국정보보호학회 논문지, 제14권 제6호, 2004.12, pp.91-103.

논문접수일 : 2008년 5월 18일, 수 정 일 : 2008년 6월 7일(1차)
게재확정일 : 2008년 6월 13일

■ 저자소개 ■

이영교
Lee, Young Gyo

2008년 3월~현재
서일대학 인터넷정보과 교수
2006년 8월 성균관대학교
전기전자컴퓨터공학부 (공학박사)
1999년 2월~2001년 6월
LG정보통신 중앙연구소
선임연구원
1993년 3월~1998년 9월
대우통신 종합연구소 선임연구원
1991년 8월 한양대학교 전자공학과 (공학석사)
1986년 2월 한양대학교 전자공학과 (공학학사)

관심분야 : 정보보안, PKI, 암호이론
E-mail : younggyo@seoil.ac.kr

박종순
Park, Jong Soon

1993년 ~ 현재
서일대학 인터넷정보과 부교수
2005년 한국외국어대학교 (경영학박사)
1990년 한국외국어대학교 (경영학석사)
1985년 성균관대학교 (행정학사)

관심분야 : 웹기반 정보시스템, 정보기술
E-mail : jsoonpark@lycos.co.kr