인터넷 침해사고 동향 변화에 따른 대응 정책

정보통신기반보호대응팀 연장길

I. 서론

1994년 말 각 정부부처에 산재되어 있던 정보통신 관련 기능을 통합하여 정보화의 주무부처로 정보통신부를 신설하여 정보화사업을 추진한 이래 우리나라는 인터넷 이용자 3천만 명, 초고속인터넷 가입자 세계 1위 등과 같은 세계최고 수준의 IT 인프라를 자랑하게 되었다. 이러한 정보통신 인프라의 고도화는 일반 기업에게는 비용절감과 생산성 향상을 가져왔으며, 일반 국민에게는 인터넷 금융거래 및 대정부 서비스 등을 통한 삶의 질을 향상 시켜왔다.

그러나 정보통신 인프라가 고도화되고 정보통신 의존도가 높아질수록, 그 역기능 또한 증가하고 있다. 우리는 2003년 1월 슬래머웜으로 인하여 전국적으로 네트워크가 마비되는 사상 초유의 사태를 경험한 바 있다. 정보통신부에서는 이를 계기로 2003년 12월 인터넷침해사고대응지원센터를 개설하여 인터넷 침해사고에 대해 사전 대응활동을 펼치고 있으며, 기 발생 사고에 대해서는 즉각적인 대응을 통하여 피해 확산 방지에 이바지하였다.

최근 인터넷 침해사고 유형의 변화는 사이버 침해사고 대응체계의 틀을 변화시키고 있다. 과거의 인터넷 침해사고는 주로 시스템 파괴나 네트워크 마비 등을 목적으로 웜바이러스를 대량으로 유포시켰으나, 최근 들어 금전적 이득을 목적으로 특정집단을 은밀하게 공격하고 있다. 과거의 침해유형은 자료 백업이나 시스템 보안패치 등을 통하여 충분히 방어할 수 있었으나, 최근의 침해유형은 이러한 과거의 대응으로는 근본적인 방어책이 될 수 없다.

이에 정보통신부에서는 시스템, 네트워크에 대한 침해행위뿐 만아니라 대상물을 지정해 발생하는 개별적 해킹행위에 대해서도 조기에 발견하여 대처할 수 있는 정책 및 기술개발을 강화하고자 한다. 또한 최근 해킹 행위는 고도화, 복잡화의 양상을 띠고 있는 바, 이를 적절히 대처하고자 자동화된 프로그램을 개발하여 대응하고자 한다.

II. 본론

사이버침해사고의 최근 경향에 대응하기 위하여 정보통신부에서는 네트워크 모니터링을 고도화하고, 인터넷 이용자의 정보보호를 강화하며, 안전한 웹사이트 환경조성 및 침해사고 대응기반을 확대하고자 한다. 다음 각 절에서 자세한 내용을 살펴본다.

1. 네트워크 모니터링 고도화

네트워크 환경은 음성 · 데이터, 유 · 무선, 통신 · 방송 융합형 멀티미디어서비스를 지원하는 광대역통합망(BcN) 환경으로 발전하고 있으며, 이로 말미암아 가까운 미래에는 IPv6 환경이 일반화 될 것이다. 이러한 IPv6 환경에서도 인터넷 이상징후를 파악할 수 있는 시스템을 개발운영하는 것은 필수 불가결한 문제이다. 정보통신부는 우선 IPv4과 IPv6의 혼용망에서 이상징후를 모니터링할 수 있는 시스템을 개발하고자 한다. 더불어 IPv6망 환경에서 발생할 수 있는 웜 · 바이러스에 대한 분석이 가능하도록 테스트베드를 개발할 것이다.

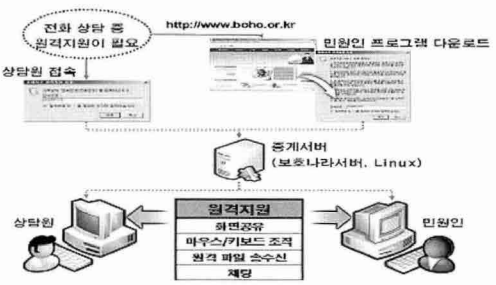
또한, 현재 운영 중인 네트워크 모니터링 시스템의 정보수집 범위를 확대할 필요가 있다. 네트워크 모니터링 수집대상 기관을 작년 50개 기관에서 금년에는 총 80여개 기관으로 확대하여 정보를 수집할 계획이다. 이 경우 국내 민간 인터넷 대역폭을 기준으로 96%범위의 트래픽을 모니터링할 수 있어 수집정보의 정확성 및 신뢰성을 제고하게 된다.

2. 인터넷 이용자 정보보호 강화

1) 사이버 침해사고 원격지원서비스 실시

정보통신부는 산하기관인 한국정보보호진흥원에 해킹 · 바이러스 상담지원센터(Cyber 118)를 개설하여 2000년 4월24일부터 일반인을 대상으로 해킹 및 바이러스 등에 대하여 신고 접수 및 상담업무를 해오고 있다. 그러나 전화를 통하여 보안패치, 바이러스 치료 등을 설명하는 방식은 민원인의 컴퓨터 지식이 낮을 경우 상대적으로 효과가 낮을 수도 있는 문제점이 발생하였다.

정보통신부에서는 민원인의 컴퓨터 지식이 낮을 경우에도 효과적인 서비스를 제공하기 위하여 의뢰인의 동의하에 의뢰인의 PC에 원격으로 접속하여 해킹툴, 웜바이러스, 스파이웨어 등 악성코드를 제거해 주며, 또한 감염 원인을 파악하여 향후 비슷한 사고발생시 대응할 수 있는 방법을 알려주는 서비스를 무료로 실시할 계획이다. 또한, 민원인에게 평가판 백신 사용유도 및 정품 백신사용을 권장하는 한편 정보보호 실천 수칙 홍보를 통해 정보보호에 대한 국민들의 관심을 고취시킬 예정이다.

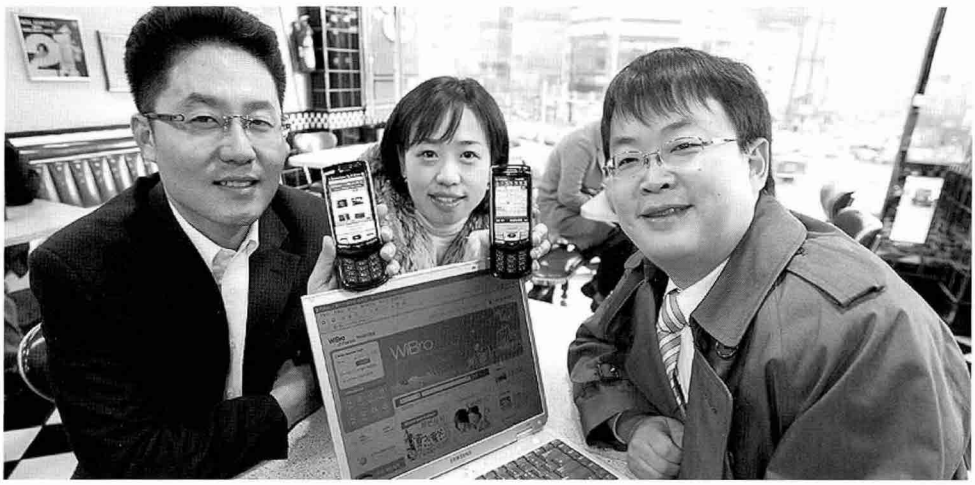


▶사이버 침해사고 원격지원서비스 개요도

본 서비스가 활성화될 경우, 년 2,000~3,000명의 민원인을 수용할 수 있을 것으로 추정되며, 경제적인 이유 등으로 ISP(Internet Service Provider) 등으로부터 보안서비스를 받지 못하고 있는 취약계층에게 도움이 될 것으로 예상된다.

2) 온라인게임 해킹방지

국내 온라인게임이 중국 등 외국에서도 크게 인기를 끌면서 국내 게이머들의 아이템을 노린 해킹 피해가 확산됨에 따라 피해를 최소화하기 위한 대책이 요구된다. 최근 국내 사이트 해킹, 인터넷 검색 등을 통해 취득한 타인의 명의를 도용하여 국내 온라인게임에 가입하거나 피싱사이트, 악성코드를 이용하여 게임 계정을 탈취하는 등 온라인게임 사용자들의 피해



가 빈번하게 발생하고 있는 실정이다.

지난 2월28일 정보통신부는 문화관광부, 경찰청, 온라인게임업체, 국내 주요 ISP들이 참석한 가운데 인터넷 명의도용 사건과 최근 해킹 관련 대책회의를 개최한 바 있으며, 이날 정부와 관련 기관/업체는 다각적인 방면에서 대책을 수립 추진키로 하였다.

우선 '게임정보보호협의회'를 구성하여 최신 해킹 기법, 보안대책 등 정보를 수시로 공유할 것이다. 본 협의회는 온라인게임업체를 비롯하여 정통부, 검·경, 한국정보보호진흥원, 인터넷진흥원, 소프트웨어 진흥원 등 관계기관들이 참여할 예정이다.

둘째, 온라인게임 사이트 등 국내 상위 주요 사이트 방문시 자동으로 윈도우 보안 패치 프로그램을 설치하는 방안을 지속적으로 추진할 계획이다. 이 경우 현재 평균 38% 수준에 머물러 있는 윈도우 보안 패치율이 80%이상으로 높아질 것으로 보인다. 윈도우 보안 패치를 적용한 시스템은 자동으로 전파되는 악성코드의 위험성에서 벗어날 수 있으며, 악성코드 감염으로 인한 게임 계정정보 유출의 효과적으로 방어할 수 있다는 점에서 큰 의미를 갖는다.

셋째, 국외에서 국내 시스템을 경유하여 국내 게임 업체로 접속을 시도하는 트래픽을 지속적으로 적발하여 차단할 것이다. 국외 게이머에 의한 불법 게임아이템 매매가 폭발적으로 증가함에 따라 일부 게임 업체에서는 국외로부터의 접속을 차단하고 있으나, 일부 국외 게이머는 국내 서버를 경유하여 접속하는 사례가 빈번하게 발생하고 있다. 이에 ISP 등과 공조를 통해 불법적인 우회 IP에 대한 국내 접속을 차단해 나갈 것이다.

넷째, 국내 웹서버와 개인 PC 보안 강화를 위하여 경제적인 이유로 상용 웹 방화벽 도입이 어려운 중소규모의 웹서버에 적용할 수 있는 공개 웹방화벽을 무료 배포할 예정이다.

▶악성코드 은닉사이트 탐지 및 조치 개요

끝으로 주민번호 대책수단 이용을 의무화하는 등 인증 강화 정책을 추진하고 있으며, 국내 주민번호가 국외 사이트에서 검색되지 않도록 외국 유관기관에 협조 요청할 계획이다. 또한 게임사이트와 이용자 보안 강화를 위하여, '온라인게임 해킹대응가이드북' 제작·보급할 것이며, 주요 홈페이지 제작자 및 게임 이용자 PC 대상으로 한 보안 교육을 연중 지속적으로

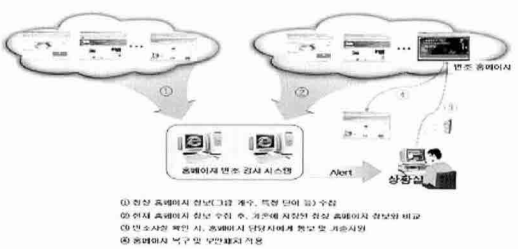
실시할 계획이다.

3. 안전한 웹사이트 환경 조성

1) 국내 악성코드 은닉사이트 점검

작년부터 중국 등 국외 해커의 소행으로 보이는 악성코드 유포사례가 지속적으로 발생하고 있으며, 현재까지 3천여 개의 국내외 홈페이지가 악성코드 유포에 악용되어 악성코드 삭제 및 접속 차단을 한 바 있다. 이중에는 언론사, 포탈업체 등을 방문자 수가 많은 국내 주요 홈페이지가 악성코드 유포지로 악용된 경우도 있다.

홈페이지를 악용한 악성코드 감염 경로를 살펴보면, 해커는 국내 홈페이지를 해킹하여 악성코드 숙주 사이트에 접속하도록 경유지 사이트로 만들며, 이러한 경유지 사이트를 접속한 일반 사용자는 자신도 모르게 자동으로 악성코드 숙주 사이트로 접속하여 악성코드에 감염된다. 이러한 악성코드는 주로 국내 주요 온라인게임의 계정과 비밀번호를 유출하는 행위를



▶홈페이지 변조 탐지 및 조치 개요

하나, 감염되는 악성코드에 따라 어떠한 악의적인 행위도 가능하다.

한국정보보호진흥원에서는 홈페이지가 악성코드 유포로 악용되는지를 점검하는 프로그램을 개발하여 작년 6월부터 국내 홈페이지를 점검하고, 악성코트가 은닉된 사이트에 대해서는 해당기관, 사법기관 및 백신업체 등에 통보하여, 해킹을 시도한 범인검거 지원 및 신속한 백신 업데이트 권고를 시행하고 있다. 현재 국내 7만여 개의 국내 중요사이트에 대하여 매일 해킹 점검을 실시하고 있으며, 향후 점검 대상을 확대 실시할 계획이다.

2) 홈페이지 변조 실시간 감시 시스템 가동

홈페이지 변조행위는 '05년 초에 비하면 현저히 감소하였으나, 금년에도 매달 수백 건 이상이 지속적으로 발생하고 있는 상황이다. 국외 해커로 인하여 발생되는 국내 홈페이지 변조는 해당 기관/업체의 업무 장애 및 신임도 하락에 크게 영향을 끼친다. 또한, 해당 시스템에 존재하는 보안취약점은 홈페이지 변조 행위에 그치는 것이 아니라 피싱사이트 개설, 악성코드 전파 사이트 및 해킹 경유지로 악용 등의 불법 행위가 일어날 수 있다는 점에서 그 심각성은 크다 할 수 있다.

정통부에서는 홈페이지 변조 여부를 자동으로 탐지할 수 있는 시스템을 개발하여 포털, 언론사, 정부기관 등 국내 주요 사이트 1,000여개에 대한 홈페이지 변조 현황을 조기 탐지하고 대응할 계획이다.

3) 휴면 홈페이지 정리 캠페인 실시

인터넷 상에는 다수의 홈페이지가 업체/기관의 폐쇄 또는 영업 정지, 관리 소홀 등으로 인하여 보안관리가 되지 않은 채 방치되어 있다. 이러한 홈페이지는 해킹에 무방비로 노출되어 있으며, 해킹 경유지로 악용될 우려가 있다. 또한, 관리자의 부재로 관련 사실 통보 및 조치가 사실상 불가능하다.

따라서 주인 없이 방치되고 있는 각종 홈페이지에 대하여 대대적인 청소 작업을 추진하여 국내 해킹 피해를 감소시키고자 한다. 우선 IDC, 서버 호스팅 업체 등과 공동으로 장기 방치 홈페이지에 대한 실태조사를 실시하고 이를 바탕으로 해당 홈페이지의 자진 폐쇄 및 보안조치 강화를 유도하는 캠페인을 전개할 것이다. K

※알림※
이 원고는 2회에 걸쳐 연재되고 있으며, 두 번째 원고는 정보화사회 07~08월호 에 게재될 예정입니다.