



까지 차단할 수 있는 3세대 방지 기능을 포함해야 한다”며 “Blacklist 방식과 Whitelist 방식, 또한 기술적 탐지 기술의 병행이 필요하다”고 조언했다.

특히 “Whitelist를 통한 정상도메인 검증의 활성화가 필요하다”고 강조했다.

이에 앞서 ‘침해사고 예방 및 대응능력 강화를 위한 정부정책 방향’이라는 주제로 발표한 정재훈 방송통신위원회 네트워크안전과 사무관은 “정부는 최근 범죄형 해킹이 늘고 불법 불건전 유해정보도 확산되고 있다”고 전제한 뒤, “인터넷 이용환경의 안전성을 제고하는 동시에 인터넷 경제의 신뢰 기반을 확충하는 쪽으로 관련 종합대책 추진 전략을 마련했다”고 밝혔다.

그는 또 침해사고 예방과 관련 대응체계 강화를 위해 정부가 최근 마련한 구체적인 대책을 설명했다.

정 사무관은 아울러 “우리나라가 IT 인프라 구축의 선도국 가임에도 인터넷 활용을 위한 신뢰기반 미비로 세계적인 인터넷기업 배출에는 한계가 있다는 평가가 있었다”며 정부의 인터넷 정보보호 종합대책이 침해사고 등 인터넷의 역기능

을 줄이는 데 도움을 줄 것이라는 뜻을 밝혔다.

## 중국발 해킹 심각한 보안 이슈

이주호 CN시큐리티 중국지사 관리팀장은 ‘중국 해커의 한국 해킹 최신 동향’이라는 B트랙 마지막 주제발표에서 “중국발 해킹은 최근 심각한 보안이슈로 대두되고 있으며 기존 보안체계로 해킹시도 자체를 원천 봉쇄할 수 없기 때문에 더 빠른 정보와 능동적인 보안체계를 구축해야 한다”고 말했다.

그는 “정보통신기술의 발달로 사이버 세계가 제2의 생활공간이 되어가면서 해킹에 의한 피해가 점차 증가하고 있는 추세이며, 이 중 중국발 해킹 시도는 전체 비중의 50%를 상회하고 있다”며 “최근 매스컴을 통해 알려진 중국발 해킹의 경우 국가기관, 자치단체, 대기업, 언론기관 등 국내 유수의 기관과 기업에 해킹을 시도하고 있으며 해킹 기술 자체가 고도화되고 지능화 되면서 보안 시스템 자체를 무력화 시키고 있다”고 강조했다.



또한 중국도 인터넷 사용이 급격히 증가하면서 이러한 중국발 해킹은 지속적으로 증가할 것으로 파악하고 있다고 경고하기도 했다. 한편, B 트랙 두 번째 강연자로 나선 자끌린 피터슨-자비스(Jacqueline

Peterson-Jarvis) 마이크로소프트 APAC 보안 관리 매니저(Security&Management Manager)는 “취약성 사고 중 50%가 심각하고 아주 높은 위협이며 이로 인해 보안 담당자들은 밤새 일 할 수 밖에 없는 상황이고 이로 인해 금융업계가 가장 큰 피해를 입고 있다”고 밝혔다.

그는 또 “물리적 위협, 사회 공학적 위협, 사이버 크라임 등 의 위협이 증가하고 있는 상황에서 안전하고 빠른 속도의 프로세스를 제공하는 것이 보안 솔루션의 가장 핵심”이라고 주장했다. 이와 관련해 마이크로소프트는 다양한 제품을 다루고 있는 기업인만큼 이와 관련한 다양한 보안 솔루션과 서비스를 제공하고 있다고 덧붙였다.

또한 그는 “취약성의 완전 제거는 불가능한 일이기 때문에 마이크로소프트는 새로운 취약성이 발견되면 최대한 빨리 고객들에게 이를 공개하고 최대한 빨리 새로운 취약성 위협에 대응할 수 있도록 노력하고 있다”고 강조했다.

## 내부정보 유출방지 절실

ISEC 2008이 성대하게 막을 내린 직후인 지난 달 초, 한 유명 정유업체의 고객 개인정보 천백만여 건이 내부 직원에 의해 유출된 것으로 알려져 큰 파문이 일었다. 그러나 해당 사건 이전에도 내부자에 의한 정보유출 사건이 심심치 않게 발생해왔기 때문에 이번 ISEC 2008을 찾은 각 기업의 보안 실무자들 대다수는 내부정보 유출방지를 주제로 한 강연에도 큰 관심을 보일 수 밖에 없었다.

특히 최근 보조 기억매체에 대한 내부정보 유출로 인한 피해가 빈번한 가운데 USB 메모리 등 보조기억매체에 대한 보안이 이슈가 되고 있다.

이에 첫 날 B 트랙의 발표자 중 한 명이었던 김상진 세이퍼존 본부장은 ‘내부정보 유출방지의 심각성과 보안USB를 이용한 효율적 통제 방안’이라는 주제발표를 통해 “최근 IT기술의 급속한 발전과 더불어 정보유출의 증가로 인해 피해 사례가 증가하고 있다”며 “사용자의 PC에 저장되어 있는 자료를 보조기억매체를 통해 외부로 유출되는 것을 체계적으로 관리하고 모니터링 해야 한다”고 밝혔다.

특히 ‘국정원 USB메모리 등 보조기억매체 보안관리 지침’을 만족하는 보안USB의 도입으로 이러한 보조기억매체를 이용한 내부정보 유출방지 대책이 절실하다는 것이다.

김 본부장은 “세이퍼존이 개발한 보안USB DefCon Secure USB는 ‘국정원 USB메모리 등 보조기억매체 보안관리 지침’을 만족하는 제품으로, 사용자 인증 식별 및 인증 기능과 저장데이터의 암·복호화, 저장된 자료의 임의 복제를 방지 기능 등 사용자들의 편의성을 고려한 다양한 기능을 제공하고 있어 보조기억매체를 체계적으로 관리하고 모니터링할 수 있다”고 강조했다.

한편, 정보보호에 대한 관심이 내부 데이터에 대한 보안으로 확대되고 있는 가운데, 암호를 이용한 DB보안에 관심이 집중되고 있다.

이와 관련해 C 트랙 두 번째 강연자로 나선 펜타시큐리티시스템의 김덕수 부장은 “무엇보다 내부자에 의한 정보유출사고가 전체의 80%를 넘어서고 있고 사고의 60% 이상이 발견되지 않아 내부 보안 정책의 중요성은 말로 표현할 수 없다”며 “현재 DB보안은 접근제어를 통해 이뤄지는 경우가 많으나 여기에는 한계가 있다”면서 “DBMS 암호 등 다양한 기술을 이용한 다각적인 보안체계가 필요하다”고 역설했다. 그는 특히 DB보안의 접근제어를 보완하는 기술로써 DBMS 암호가 주목받고 있으며 벤더의 보안 결함을 이용해 접근