베이징 올림픽을 안전하게

올림픽이나 월드컵과 같은 대규모 국제행사가 개최되면 개최국의 근심거리 중 빠질 수 없는 것이 바로 테러예방이다. 지난 8월 8일 개막된 베이징 올림픽의 열기가 한층 고조되고 있는 가운데, 중국 역시 올림픽 개최에 앞서 테러방지를 위한 보안활동을 강화하고, 또 테러 발생에 대비한 훈련에 많은 노력을 할애하고 있는 것으로 알려져 있다. 하지만 테러는 총이나 폭탄과 같은 무기들로만 이뤄지는 것은 아니다. 오히려 사이버 공간에서 발생하는 침해사고는 우리가 일반적으로 생각하는 테러와는 전혀 다른 엄청난 피해를 안겨줄 수 있다. 요즘처럼 사회적 활동의 많은 부분을 IT에 의존하고 있는 상황에서는 더욱 그러하다. 이런 상황에서 아시아 주요 국가의 CERT가 베이징 올림픽 기간 중 발생할 수 있는 각종 사이버 침해사고에 대비한 공동의 노력을 펼치고 있다.

정보보호뉴스 취재팀

최근 몇 년간 사이버 침해사고 대응을 위한 국가 간 협력의 필요성에 대한 인식이 증가해 APEC, OECD, ITU 등 국제협의체, 또는 관심 국가들 간의 협력을 바탕으로 사이버 침해사고에 공동대응하기 위한 노력들이 지속적으로 이뤄지고 있다.

특히, APEC 내 통신분야 실무그룹인 APEC TEL에서는 하나의 작업그룹에서 다뤄왔던 정보보호 분야를 지난 2006년부터 별도의 워킹그룹인 SPSG(Security Prosperity Steering Group)로 승격시켜 국가 간 침해사고 대응사례를 공유하고 상호협력을 위한 방안을 협의하고 있다. 이런 노력은 OECD에서도 인터넷에서의 악성코드에 대한 이해를 높이고 국가 간 대응방안을 공유 및 협력하는 추세로 이어지고 있는데, 지난 6월 서울에서 개최된 OECD 장관회의에서 인터넷의 미래를 좌우하는 주요 요소로 인터넷 신뢰 확보가 강조됐던 것도 최근의 흐름을 반영한 것이다. 또한 통신분야 국제 협의체인 ITU 내에서도 사이버 보안에 대한 국제협력 방안이 활발히 논의되고 있다.

12개국 13개 CERT 공동 훈련실시

사이버 공격대응을 위한 국가 간 협력이 활발하게 이뤄지고 있는 대표적인 기구로 APCERT(Asia Pacific Computer Emergency Response Team)가 있다. 지난 2003년부터 아태지역 국가들의 침해사고대응팀이 모여 설립한 APCERT는 KISA KrCERT/CC가 APCERT 운영위원으로 참여해 활동을 주도해왔으며, 대표적인 활동으로는 2005년부터 실시되고 있는 아태지역 침해사고 공동대응훈련이 있다. 이 공동대응훈련은 2004년부터 한국 주도로 실시했던 한중일 침해사고 공동대응훈련을 APCERT

회원국으로 확대해 실시하는 것으로, 베이징 올림픽 기간 중 발생할 수 있는 침해사고에 대비한 공동대응훈련도 APCERT 차원의으로 진행됐다.
안전한 올림픽 개최를 위한 공동훈련은 지난 2007년 11월 훈련 시나리오를 작성해 진행했으며, 당시 훈련에 참여했던 팀들은 그 경험을 바탕으로 올림픽 폐막까지 발생 가능한 사이버 보안사고에 대비하고 있다.

실제와 같은 가상훈련

베이징 올림픽 개최에 대비한 이번 사이버 침해사고 공동 대응훈련에는 한국과 중국은 물론 일본, 호주, 싱가폴 등 12개국 13개 CERT가 참여했으며, 여기에 KT, LG데이콤, 하나로텔레콤, 드림라인, 온세텔레콤 등 국내 5개 주요 ISP 사업자들이 참가했다.

▲ 베이징 올림픽 대비 공동 대응훈련 참가 APCERT 회원국

공동대응 훈련은 '이메일을 통한 베이징 올림픽 사칭 사이트의 악성코드 유포'와 '중국 내 특정 웹 사이트에 대한 국내발(發) DDoS 공격대응' 등 크게 2가지 시나리오를 바탕으로 진행됐다. 훈련 시나리오는 훈련시작 전까지 공개되지 않는 불시훈련(Blind Drill) 형태로 진행돼 훈련의 본래 목적인 긴급 상황에서의 대처능력 향상을 유도했다는 점이 특징이다.

가상의 공격에 대한 대응내용을 살펴보면, 아래 그림처럼 이메일을 통해 베이징 올림픽 사칭 사이트에서 악성코드 유포가 이뤄지게 될 경우, 해당 악성메일을 입수해 분석한 후, 국내 ISP에 긴급 상황전파를 통해 악성코드 유포 사이트를 차단하게 되며, 홈페이지 보안공지를 통해 예방 및 대책을 홍보하게 된다.
또 중국내 특정 웹 사이트에 대한 국내발(發) DDoS 공격이 감지될 경우, APCERT로부터 공격 트래픽 정보를 입수하고, ISP를 통해 국제관문국에서 국내발 중국행 DDoS 공격 트래픽을 차단하고, 이와 함께 공격 근원지 IP를 가진 해당 ISP에 통보 및 조치요청을 하는 것으로 대응은 마무리된다. 이외에도 올림픽 기간 중 발생할 수 있는 DDoS, 홈페이지 변조, 피싱메일, 제로데이 취약점 등 다양한 공격 시나리오를 추가해 해외 CERT와 KrCERT/CC가 실제와 동일한 상황 아래에서 훈련을 실시했다.

공격 시나리오	공격 시나리오
이메일을 통한 베이징 올림픽 사칭사이트의 악성코드 유포	중국 특정 웹 사이트에 대한 국내발(發) DDoS 공격 대응
APCERT로 부터 베이징 올림픽 사칭 사이트 관련 악성메일 입수	APCERT로 부터 국내발 DDoS 공격 트래픽 정보 입수
사칭 사이트에 은닉된 악성코드 분석실시	국내 주요 ISP에 긴급 상황전파를 통한 국제관문국에서 국내발 중국행 DDoS 공격 트래픽 차단
국내 주요 ISP에 긴급 상황전파를 통한 악성코드 유포사이트 차단	DDoS 공격 트래픽 분석 및 국내 근원지 IP에 대한 ISP별 분류
홈페이지 보안공지를 침해사고 예방 및 대책안내(이메일 열람 주의 등)	공격 근원지 IP의 해당 ISP에 대한 통보 및 조치요청
언론보도를 통한 대국민 대책 안내	

▲ 공동 훈련 시나리오

공동대응 훈련뿐만 아니라, 각국은 사이버 공격의 모니터링 및 차단과 동시에 긴급연락체계를 구축해 베이징 올림픽이 성공적으로 개최될 수 있도록 지원하고 있다. 특히, 타 국가보다도 사이버 공격에 대한 모니터링 및 차단 시스템이 잘 갖춰진 우리나라의 경우, 국내 취약한 서버나 PC를 경유지로 해 베이징 올림픽 관련 사이트를 공격하는 악성코드나 해킹을 조기에 탐지해 차단함으로써 이웃국가의 성공적인 올림픽 개최에 일조하고 있다. S