정보 공유 프레임워크가 필요하다

Keisuke Kamata, JPCERT/CC

■ ■ ■ 최근 발생하는 침해사고의 경향을 분석해 보면, 동일한 공격기법이라도 악성코드 유포방법과 공격대상은 대륙별로 국가별로 조금씩 차이를 보이고 있다. 다양하고 빠르게 변화하는 공격방식에 대응하기 위해서는 무엇보다 강력한 정보공유 체계가 전제되어야 한다. 우리나라와 지리적으로

먼저 JPCERT/CC에서 분석한 2008년 일본의 침해사고 특징을 간단하게 설명해 준다면.

▪ 일본에서 실제로 피해를 입힌 사건들을 분석해 보면 SQL 인젝션을 빼놓을 수 없으며, USB 메모리를 통한 바이러스 감염, 그리고 특정 대상을 겨냥한 공격유형이 두각을 나타냈다. 아울러 JPCERT/CC가 주목하고 있는 이슈들을 나열해 보면, 'Maccolo'를 통한 스팸 메일의 감소, Google의 Street View와 관련된 주제들, 무선 랜 암호화 기술, 웹 애플리케이션 취약점, DNS 캐시 포이즈닝 취약점, 오픈 SSL 패키지 이슈 등이 있다.

2008년 한국에서는 DDoS 공격과 협박이 큰 이슈였다. 일본 역시 DDoS 공격에서 자유롭지 않았을텐데, JPCERT/CC 차원의 대응책은 무엇이었나.

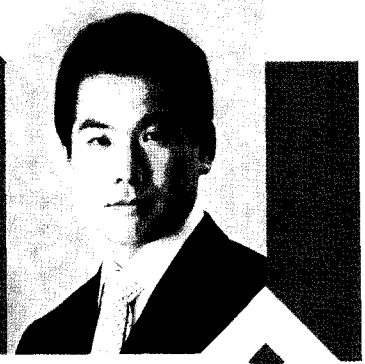
▪ 일본 내 ISP에서 빈번하게 DDoS 공격이 발생했던 것으로 알고 있다. 지금으로써는 표준화된 대책이 없는 상황이며, 때문에 DDoS 공격은 일본 내 기업이 스스로 처리하기 어려운 사고 유형으로 남겨져 있다. 다만, 아직까지 금전을 목적으로 특정 기업을 겨냥한 DDoS 공격과 협박에 대한 사례는 접수되지 않고 있다.
JPCERT/CC가 개별적인 DDoS 관련 사건을 자주 다루지는 않았지만 일부 회사에서는 우리에게 조언을 구하고 있으며, 한국과 일본 사이에서 있었던 DDoS 공격에 대해서도 KrCERT/CC와 JPCERT/CC가 상호협력을 통해 성공적으로 대응한 사례도 있었다. 일본에서는 DDoS 공격 대응 기술에 대한 연구는 'Trace Back'을 통해 장려되고 있다.

Trace Back에 대해 조금 더 자세히 소개해 준다면.

▪ IP Trace Back은 패킷 자체가 스푸핑되어 있다고 할지라도, 해당 패킷의 근원과 경로를 찾아내는 기술이다. 현재 일본 내 ISP들과의 협조를 통해 실제 인터넷 환경에서도 적용할 수 있는 단계에 와 있다. 이를 통해 DDoS 공격에도 대응할 수 있는데, 스푸핑된 소스 주소를 가지고 익명의 DDoS 흐름을 역추적해 공격의 근원지를 감지해 차단할 수 있게 된다.

가장 가까운 국가 중 하나인 일본의 JPCERT/CC의 활동은 그런 의미에서 훌륭한 참고사례가 될 수 있다. 이번 호에서는 JPCERT/CC에서 사고처리, 네트워크 트래핑 모니터링 업무를 담당했고, 최근에는 감시 및 경보 그룹의 매니저를 맡고 있는 Keisuke Kamata와의 인터뷰를 통해 일본의 침해사고 현안을 들어보고자 했다. 특히 KISA KrCERT/CC와도 협력활동을 펼친 바 있는 Kamata의 견해는 2009년 침해사고에 대비하고 있는 국내 정보보호 전문가들에게 큰 도움이 될 수 있으리라고 믿는다.

| 정보보호뉴스 취재팀 |



일본과 한국은 중국으로부터 출발한 사이버 공격으로 피해를 입고 있다. 국제적인 협력이 강조되고 있지만 아직까지 그 효과는 크지 않은 실정인데, 중국으로부터 발생되는 공격을 효과적으로 차단할 수 있는 방법은 무엇이라고 생각하나.

▪ 모니터링 시점에 따라서 JPCERT/CC에서는 중국에 기원을 둔 사이버 공격의 수를 다르게 산정하고 있으며, 실제로 사이버 공격은 중국에서만 오는 것이 아니라 다른 다양한 국가들로부터 발생되기도 한다. 때문에 중국에 기원을 둔 공격만을 위해 JPCERT/CC가 별도의 대책을 마련할 계획은 갖고 있지 않다. 중요한 것은 전체적인 상황을 관찰하고 포괄적인 이해와 함께 각각의 사고를 개별적으로 다뤄야 한다는 것이다. 이를 위해서 각국의 CSIRT(Computer Security Incident Response Team)끼리 긴밀하게 협력하는 것이 필요하며 중국으로부터의 발생되는 공격의 경우, 일본은 CNCERT/CC와의 더욱 깊이 있는 그리고 강화된 협력관계 구축을 통해 해결해 나갈 것이다.

일본과 한국 사이버 대응 협력체계에 있어 개선해야 할 부분이 있다면 무엇이라고 생각하나.

▪ 현재 KrCERT/CC와 JPCERT/CC는 한국과 일본 두 국가간에 발생되는 주요 국제 사건들을 다루는 데에 협력하고 있는데, 만약 정보 공유 프레임워크를 시스템화할 수 있다면 사고에 대응하는 시간과 비용을 더욱 절약할 수 있는 것이라고 믿는다. 사이버 대응 협력 시스템이 존재한다고 해서 각국의 CSIRT 활동을 제한하는 것은 아니기 때문에, 우리는 이 시스템에 정부와 민간부문 등 다양한 계층의 참여가 필요하다고 생각한다.
또한, JPCERT/CC는 현재 아시아-태평양 지역의 주요 인터넷 활동을 감시할 수 있는 시스템인 'TSUBAME'를 구축하고 있는데, 이 시스템은 아시아-태평양 지역 국가들에 센서를 장착해 이 지역 전체의 인터넷 상황을 이해하는데 도움을 줄 것이다. 현재 시스템 운영을 위한 센서들은 이미 장착돼 가동을 시작했다. 비록 TSUBAME를 통해 얻어지는 정보는 인터넷 공간 전체에서 발생하는 사건사고의 일부분에 불과하겠지만, 이 정보공유 플랫폼이 아시아-태평양 국가들의 실시간 상황을 교류하고 이해하는 역할을 해줄 것으로 기대하고 있다.

많은 일본 기업들은 정보보호 관리체계(Information Security Management System) 인증을 획득하고 유지하고 있는 것으로 알고 있다. 한국의 상황과 비교해 볼 때 부러운 부분인데 많은 기업들이 ISMS를 획득하고 유지할 수 있는 배경은 무엇이라고 생각하나.

▪ 그 원인은 다양하게 분석될 수 있지만, 일본 회사들이 빠른 속도로 ISMS를 획득했던 가장 큰 요인은 이 같은 사업이 일본 정부의 주도로 진행됐다는 점이다. 또한 IT 분야에서 아웃소싱의 영역이 점점 증가하고 있다는 점도 크게 작용했다고 본다. 즉, 아웃소싱을 관리하는 기업들은 각 아웃소싱 수행 기업들로부터 발생할 수 있는 사고를 예방하기 위해 정보통제가 필요한데, 이를 ISMS를 통해 해결하고 있다.

ISMS가 정부 주도로 진행돼 왔다면, 그에 따른 정부 차원의 인센티브도 있었을 텐데.

▪ ISMS를 보급하는데 있어서 정부 차원의 금전적인 혜택은 없었다. ISMS의 확산은 일본 IT 산업계가 SI 벤더들에게 ISMS 인증획득을 요구해 각 기업들이 자발적으로 획득하기 시작한 결과이기도 하다. 예를 들어, 특정 SI 벤더가 ISMS 인증을 받지 않았다면 새로운 사업에 참여할 수 있는 기회는 줄어든다. 이와 같은 예는 일본에서 쉽게 찾아볼 수 있다.

최근 일본에서는 신원 확인과 관련된 위조 건수를 줄이기 위해 'JukiNet'(기본 거주인 등록 네트워크)이라고 불리는 카드에 암호화한 사진을 포함시킬 것이라는 뉴스를 접한 바 있다. 이런 변화는 1차적으로 위조 방지에 도움이 되겠지만 추후에 프라이버시 침해와 같은 새로운 문제가 제기될 가능성이 있는데.

▪ JPCERT/CC 입장에서 이에 대해 프라이버시적인 시각이 아닌 기술적인 시각으로 보는 것이 적절하다고 생각한다. 다시 말해 자칫 JukiNet 시스템의 취약점으로 나타날 수 있는 정보의 수집 및 공유, 그리고 유관 기관들과의 협력이 포함된다. 아직까지는 JukiNet 채택 비율이 낮아 이로 인해 심각한 문제가 발생되거나, 주의를 기울일 정도는 아니라고 본다.

향후에는 더 복잡한 애플리케이션과 더 많은 소프트웨어들이 다양한 형태로 등장하겠지만, 이들 애플리케이션과 소프트웨어의 보안성을 검증하는 일은 점점 더 어려워지고 있다. 어떻게 대비해야 하나.

▪ 우리가 할 수 있는 일들은 웹 어플리케이션의 개발 단계에서 보안 코딩, 웹 애플리케이션의 보안 검증, SOC, IDS 등을 이용한 웹 서버 모니터 등이다. 이런 일련의 과정을 거치게 되면 실제 사고에 대한 이해와 CSIRT들 간의 협력 프레임워크를 효과적이고, 효율적으로 운영하게 하는 기반이 될 것이다. 이 과정에서는 정보 공유 프레임워크를 촉진하는 것이 매우 중요한데, 일본은 웹 애플리케이션, 소프트웨어, 하드웨어, 그리고 다른 관련된 제품들의 취약점을 보고하는 프레임워크를 가지고 있다. JPCERT/CC는 조정 센터로서의 역할을 통해 이 프레임워크의 한 축을 담당하고 있다.

국내외 정보보호 전문가들은 해커 그룹이 마피아처럼 점점 더 조직화되고 치밀해 질 것이라고 예상하고 있다. 참으로 두려운 현상인 것만은 분명하다.

▪ 사이버 범죄에 대응하기 위해서는 우선, 법 집행기관이 범죄자에 대한 적극적인 검거가 필요하고, 범죄자들의 체포를 위해서는 사이버 범죄를 규정할 수 있는 명확한 법률 제정이 우선되어야 한다. CSIRT 관점에서 대응방안은 CERT들간 혹은 다른 외부기관과의 정보 협동 프레임워크 구축과 조정 프로세스를 개발하는 것이 필요하다. 물론 이를 위해서는 각각의 CSIRT들의 능력이 향상되어야 하며, 동일한 수준의 대응능력을 보유하고 있어야 한다. 이런 협력체계는 특정 국가 내부에서만 존재한다고 해결되는 것은 아니며, 국가대 국가 차원에서도 동일하게 적용된다. CSIRT 조직이 만들어지지 않고 있거나, 활동이 미흡한 국가들에게도 지속적인 지원이 필요한 이유다. 한국과 일본이 펼치고 있는 다양한 노력들이 효과적인 국제 협력활동으로 이어질 것이라고 믿는다.

크래커들의 기술은 빠르게 변화하는 반면, 정보보호 담당자들의 기술력은 상대적으로 뒤따라가는 경향이 많다. 이를 개선하기 위해서는 정보보호 담당자를 위한 유용한 재교육 프로그램이 마련될 필요가 있는데, 일본 내에서는 재교육이 어떻게 이뤄지고 있나.

▪ 정보보호 전문가의 교육과 관련해서는 여러 가지 측면에서 고려되고 있는데, 일본 내에서는 사실 보안 전문가 자체가 부족한 실정이다. 따라서 일본에서의 정보보호 인력 개발과정은 정보보호 전문가를 많이 양성하는 것에 초점이 맞춰져 있다. 물론 일본의 일부 정보보호 기업들은 전문적인 자체 교육 프로그램을 통해 직원들을 교육시키고 있는 것으로 알고 있다.

마지막으로 2009년 대두될 위협요소는 무엇이라고 예상하고 있는가.

▪ 특정 대상을 겨냥한 공격과 엔드 유저뿐만 아니라 웹 애플리케이션과 같은 상위 레이어를 겨냥한 공격들이 2009년에는 더욱 증가할 것으로 예상된다. 그리고 이것은 공격 기술과 말웨어의 복잡성을 이끌어내게 될 것이다. 또한 2008년 DNS 해킹사고를 겪었던 만큼, 인터넷 인프라에 영향을 미치는 이슈들에 부딪치게 될 가능성도 충분히 있다고 생각한다. IPv6도 고려대상이 되고 있다. **S**