ICT 융복합 시대의 사이버 보안

작년까지 국내에서 대형 침해사고는 2년마다 발생하였으나, 올해 초 대규모 개인정보 유출 사고가 발생하면서 그 암묵적인 2년 룰은 깨졌다. 연이은 침해사고 발생으로 보안의 중요성은 크게 증대되고 있으며, 사이버 공격기술은 대응기술의 발전을 앞질러 빠르게 고도화되고 있고, 그에 대한 피해 또한 가파른 증가세를 보이고 있다. 이에 전 세계적으로 보안시장은 꾸준한 성장세를 보이고 있으며, IoT를 필두로 초연결 시대로 접어드는 시점에서 그 중요성은 날로 증대되고 있다.

전 세계적으로 특히 국내는 연이은 대형 보안사고를 경험해서인지 모르겠으나, 보안은 비용이라는 인식에서 벗어나, 경제적·사회적 비용 측면에서 꼭 필요한 요소라는 인식이 저변에 확대되고 있으며, 다른 분야에 비해 보안 투자는 꾸준히 증대되는 양상을 보이고 있다. 더 나아가 이제는 보안을 차세대 먹거리 산업으로써 육성하려는 정책이 마련되어 추진되고 있으며, 국가 차세대 ICT 신산업 육성 계획을 검토하는 과정에서도 보안이 꼭 고려되어야 하는 요소로 자리매김하고 있다.

이에 본 특집에서는 최근의 사이버 공격 양상과 국내 기술 및 시장 상황을 간략하게 살펴보고, 빅데이터 보안, APT 공격 대응기술, IoT 보안 등 우리가 글로벌 경쟁력을 가질 수 있는 보안 분야와 표준화 이슈에 대하여 살펴보고자 한다.

임채태 TTA 정보통신표준화위원회 사이버보안 PG(503) 의장
한국인터넷진흥원 침해대응기술팀 팀장

ICT EXPERT INTERVIEW

Question 01

최근 국내외 인터넷 환경을 위협하는 사이버 공격 양상은 어떠한가요?

모바일 산업을 위시한 인터넷 신산업의 성장으로 정보의 집적·활용이 증가하면서 정보탈취, APT, 사이버 사기 등 국민생활과 국가 경제의 안위를 위협하는 다양하고 복합적인 사이버 공격 위협이 증대되고 있습니다. 그 가운데, 최근 가장 큰 사이버 공격 위협은 정보유출이라 할 수 있겠습니다. 개인 및 기업 정보는 금전적 이익을 목적으로 하는 사이버 범죄의 대상으로 부각되면서 전 세계적으로 정보 유출 사고는 크게 증가하였습니다. 2013년 세계는 사이버 공격으로 5.5억 개의 정보가 유출(2012년 대비 62% 증가)되었으며, 온라인 금융사기 등 사이버 범죄로 인한 손실은 117조 원으로 추정되고 있습니다.

국내의 경우, 2014년 초 3개 카드사(KB, 롯데, 농협), KT 등에서 개인정보 유출 사고가 연이어 발생하였고, 카드사의 경우 총 1억 100만 건의 고객정보, KT의 경우는 1,200만 건의 개인정보가 유출되는 등 유례를 찾아보기 힘들 정도로 큰 규모였습니다.

특히 국내의 경우, 유출된 개인정보를 기반으로 MMS를 전송하여 소액결제로 연결되는 스미싱이 급증하였는데, 경찰청에 집계된 스미싱 피해액을 보면 2012년 6억 원(2,182건)에서 2013년 57억 원(29,575건)으로 10배 가량 매우 큰 폭으로 증가하였습니다.

Question

02

국내 정보보호 기술 및 시장 현황을 해외 선진국과 비교해 말씀 부탁드립니다.

국내 정보보호 기술 및 시장현황을 요약하면 기술 경쟁력은 정체 상태이며, 글로벌 경쟁력은 저조하다고 할 수 있겠습니다.

먼저 기술경쟁력 측면에서 살펴보면 국내 기업은 기초·원천기술 부족으로 글로벌 선도 국가인 미국 대비 기술격차 80%로써 2011년부터 2013년까지 지속적으로 80%를 유지하는 모습으로 정체되고 있습니다. 반면 중국의 경우 ICT 전반에 걸쳐 상당히 빠른 속도로 추격하고 있는데, 정보보호 또한 2011년에서 2013년 사이 기술 격차가 2.1% 감소하는 양상을 보이고 있습니다.

두 번째, 글로벌 경쟁력 측면에서 살펴보면, 세계 정보보호 시장규모는 2013년 1,900억 불이며, 국내 시장 규모는 2013년 53억 불로 세계시장 2.8%에 불과한 상황입니다. 또한 국외기업은 활발한 M&A를 통한 대형화로 10대 글로벌 기업어 세계시장 25%를 점유하는 등 시장 지배력을 높이고 있으며, 국내 기업은 M&A가 전무하며 매출액 300억 원미만의 업체가 약 92%로 영세 중소기업으로 내수시장에 의존하고 있습니다.

또한, 국내 기업의 수출비중은 490억 원으로 세계 정보보호 시장규모 대비 0.053%로 상당히 저조한 실정입니다. 다만, 최근 국내 몇몇 보안기업이 내수시장에서 눈을 돌려 수출을 확대하려는 노력이 커지고 있는 상황에서 가시적인 성과가 나오기를 기대하고 있습니다.

더불어 긍정적인 신호로써, 보안의 중요성이 커지면서 보안에 대한 투자 증대, 국내 보안제품 및 서비스의 유지보수에 대한 제값받기, 보안 산업이 향후 먹거리 중 하나라는 인식과 함께 정책적인 정보보호 기업 육성 등 다양한 움직임이 국내 정보보호 기술 및 시장을 보다 건실하게 만들지 않을까 기대해봅니다.

Question

03

최근 새로 부각되고 있는 보안 기술 또는 제품은 어떤 것이 있습니까?

다양하고 복합적인 새로운 유형의 APT 공격이 증가함에 따라, 이에 대응하는 기술이 부상하고 있습니다. 이러한 기술의 특성은 특정 사이버 공격 대응보다는 예방 측면에서 다양한 정보를 기반으로 침투 시도 즉, 어떠한 경로로, 어떠한 방법으로 침투를 시도하는지를 탐지·분석하는 기술입니다.

주요 기술들을 살펴보면, 기업·기관마다 다수의 보안장비를 운용함에 따라 대량의 다양한 로그를 통합 관리하고, 다양한 정보를 기반으로 사이버 공격 탐지 기능을 고도화하기 위한 SIEM(Security Informaion and Event Management) 기술이 부상하고 있습니다.

또한, APT 공격의 전초단계인 침투 과정을 선제적으로 탐지·차단하기 위해 네트워크 유입단에서 악성코드 유입탐지, 공격침투 탐지, 침입방지 등 기능을 통합 제공하는 STAP(Specialized Threat Analysis and Protection) 기술이 부상하고 있으며, 이러한 기술들의 특성은 단일 보안 장비로 사이버 공격을 탐지하지 못하는 상황에서 이상징후, 선별, 연관정보 분석 등 분석가를 돕는 기술이라고 하겠습니다.

더불어 아직 가시적인 기술 또는 제품이 드러나지는 않았지만, 스마트카, 원격진료, 스마트 가전 등 ICT 융복합 산업이 급속히 성장하고, 정부에서도 IoT 산업을 적극적으로 육성함에 따라 IoT 보안 등 융합 보안기술이 급부상하고 있습니다. 최근들어, 스마트 카에 대한 불법 운전 제어, 의료장비에 대한 비정상 작동 등 해킹 시연이 빈번하게 이루어지면서, 해당 분야에 대한 보안 기술 및 제품에 대한 요구는 크게 증대되고 있는 상황입니다.

Question 04

우리가 우위 선점할 수 있는 핵심원천기술은 어떤 것이 있습니까?

좋다고 해야할지 나쁘다고 해야할지 모르겠으나, 보안 측면에서 국내 ICT 환경 인프라는 전세계에서 최상의 테스트 베드로 여겨지고 있습니다. 즉 다른 나라에서 경험하기 힘든 고도화된 사이버 공격이 빈번히 발생하고 있으며, 최신의 사이버 공격을 경험할 수 있는 환경이라 하겠습니다. 이에 글로벌 벤더들은 앞다투어 국내시장에 진출하고 있으며, 소스코드까지 제공해야 하는 높은 수준의 CC인증을 획득하려는 움직임까지 있는 상황입니다. 이러한 환경에서 국내 보안담당자들은 많은 어려움을 겪고 있으나 반대로 이를 기회로 삼는다면, 즉 다양한 경험을 바탕으로 선도적인 보안기술 또는 서비스를 개발하거나, 최신의 사이버 공격 대응 노하우를 적극 활용한다면 국제적으로 우위를 선점할 수 있다고 생각됩니다.

더불어 차세대 신산업으로써 국가적으로 상당한 역량을 투입하고 있는 IoT 등 융·복합 기술 및 서비스는 전 세계적으로 동일선상에 있거나 일부 분야에 있어서는 앞서가고 있습니다. 이러한 신규 융합산업의 성장과 발맞추어 핵심 보안 원천 기술/제품 및 서비스를 적시에 마련한다면 국제적으로도 경쟁력을 지닐 수 있을 것으로 판단됩니다. 여기서 보안은 융·복합 산업과 별개로 존재하지 않고, 상호 윈윈할 수 있는 관계이며, 보안이 선결되어야 융·복합 산업이 원활하게 성장할 수 있다는 인식을 가지고 상호 협력한다면 국내 ICT 산업 전반에 좋은 영향을 미칠것이라 생각됩니다.

Question 05

정보보호 표준화 측면에서 시급하거나, 중요한 과제는 무엇이 있을까요?

최근 어느 정도 규모가 있는 기관 및 기업에서 적용하여 운영하고 있는 보안장비는 상당한 수준에 이르고 있습니다. 하지만, 세계 1위 바이러스 백신조차도 50% 정도의 탐지율을 보이는 상황에서 단일 보안 솔루션으로 APT와 같은 고도화된 사이버 공격에 대응하기 어려운 상황입니다. 최근 부상하는 보안기술에서 알 수 있듯이, 다수의 보안장비에서 생산되는 대량의 로그를 연관분석하거나, 사이버 공격을 위한 침투 징후 등 보안 위협정보를 공유하는 요구가 상당히 커지고 있습니다. 사실 정보공유에 대한 요구는 그전에도 있었고 ITU-T, IETF 등 다수의 국제 표준화 그룹에서도 정보공유 방법 및 프로토콜 등이 다뤄졌었으며 일부는 표준안으로 제정되어 있습니다. 하지만, 현실에서는 이러한 표준들이 국내외 보안장비에 제대로 적용되지 않고 있으며, 상호 연동 또한 미진한 상황입니다. 최근 고도화되는 사이버 공격 위협을 사전에 탐지·분석한다는 측면에서 대상이 되는 보안정보를 정의하고, 이를 공유하기 위한 방법 등 현실을 반영한 표준화가 필요한 시점이라 하겠습니다. 또한, IoT 산업의 급속한 성장과 함께 다양한 사물 통신기술들이 등장하는 상황에서, 데이터 보호, 인증, 키 관리 등 상호 연동이 가능한 보안기술 표준 마련이 시급한 상황입니다. 이는 전 세계적으로 부상하는 분야로써 국제 표준화를 선도하는 측면과, 국내 IoT 산업의 원활한 성장을 견인한다는 측면에서 국가 경쟁력 및 위상을 제고할 수 기회를 부여하고 있으며, 여기서 표준화의 역할이 크다고 하겠습니다.

Question

06

사이버 보안 강화를 위해 협력되어야 할 서비스 영역 또는 분야에 대한 전망을 말씀해 주신다면?

고도화되는 사이버 공격위협에 대응하기 위한 전형적인 사이버 보안 기술 및 서비스 개발도 물론 중요하지만, 협력 측면에서 살펴본다면 아무래도 글로벌로 대등한 위치에서 시장선점이 가능한 분야를 집중 육성하는 정책이 경쟁력 확보에 도움이 될 것으로 생각됩니다. 그 분야로써는 첫째, IoT 등 융합분야 및 빅데이터, 클라우드 등 인터넷 신산업 분야와 둘째, 공공기간망, 전략망, 지능형 교통망 등 정부 주도의 신 정보통신망 인프라, 마지막으로 5G, SDN(Software Defined Network) 등 미래 통신기술 분야가 해당될 것입니다.

이제는 보안이 경제적, 사회적인 비용 측면에서 반드시 필요하며, 원활한 서비스 성장을 위해서도 없어서는 안될 분야로 인식이 개선되고 있어서 전에 비해 협력이 수월할 수 있을 것으로 기대합니다. 여기서 한발 더 나아가, 개발 과정부터 보안을 적용하는 경우 보안취약점이 50~60% 감소한다는 통계에서 알 수 있듯이 새로이 구축·개발되는 과정부터 충분히 보안이 고려된다면, 이는 비용과 경쟁력 측면에서 효과적인 동시에, 두 산업 모두 경쟁력을 향상시킬 수 있는 수단이 될 수 있을 것입니다.

이러한 인식공유와 함께, 협력을 유도한다는 측면에서 정부의 산업 육성 정책 및 타 분야에 대한 R&D 계획에 보안을 일정 부분 이상 고려하도록 하는 방안이 검토될 수 있을 것입니다. 그러나, 무엇보다 중요한 것은 보안에 종사하시는 분들 모두 앞서 제시한 분야를 포함하여 타 분야에 적극적인 관심을 가져야 할 것이며, 해당 분야 전문가들 또한 열린 마음으로 보안을 고려하는 노력이 필요할 것입니다. ICT 전반에 걸쳐 상호 협력하는 문화가 정착되어 향후 보안을 포함한 국내 ICT 산업이 글로벌 우위를 선점할 수 있기를 고대해 봅니다.