원전에 대한 사이버 공격

원전에 대한 사이버 공격이 날로 늘어나고 있는 현 상황에서 원전업계가 스스로 이를 방어해 낼 수 있는 방법은 무엇인가? 한 조직이 혼자서 자기의 사이버 영역에 대한 공격에 대비할 수는 없다. 그런 식으로는 언제나 사이버 공격보다 한 발 늦을 뿐이다. 이 싸움은 일종의 군비 경쟁 같은 것이기 때문에 서로 간의 협력을 통해 우리를 위협하는 사이버 공격자들보다 유리한 고지를 선점하고 있어야 하는 것이다.

5년 전 이란의 복합 원자력 시설의 컴퓨터에 바이러스가 침입한 적이 있었다. 정교하고 복잡한 악성 소프트웨어인 Stuxnet을 사용한 공격은 이란의 우라늄 농축용 원심분리기를 가동시키는 컴퓨터를 목표로 삼았는데 Stuxnet은 아마 최초로 밝혀진 사이버공격용 소프트웨어였을 것이다.

2015년에 나온 한 보고서에 따르면 북한의 핵개발 프로그램을 공격하기 위해서 Stuxnet과 유사한 소프트웨어가 개발되었다고 한다. 이 사이버 공격용 소프트웨어는 제대로 설정된 한글 환경의 컴퓨터와 접속하게 되면 작동이 되도록 설계되었지만 해커들이 평양의 핵개발 시설에 있는 컴퓨터에 바이러스를 심는 데 성공하지 못하는 바람에 공격은 실패로 끝났다고 한다.

2014년 12월에는 한국의 원자력발전소 운영 회사인 한국수력원자력(KHNP)의 컴퓨터가 해킹을 당해 정보가 절취되는 사태가 벌어졌는데 이 사이버 공격으로 악성 코드를 담은 5,986개의 피싱 메일이 5일간에 걸쳐 3,500명의 종업원들에게 뿌려졌다고 한다.

그러나 한수원은 그 도난 정보들은 원전의 제어 시스템에는 영향을 끼치지도 않는 이미 공개된 프로그램들이었기 때문에 원전 가동에 아무런 문제가 없었다고 해명했다.

그런데 해킹 공격에 사용된 인터넷 주소를 조사한 결과 북한의 소행이라는 것이 밝혀졌지만 북한은 관련 사실을 전면 부인하였다. 그러나 서울의 중앙지검은 이번 해킹에 쓰인 데이터 처리 방식의 코드가 이전에 북한의 해커들이 'Kimsuky' 사이버 공격 작전에서 사용한 것과 동일한 방식과 구성으로 된 코드였다고 주장했다.

증가하는 사이버 공격

규모가 커지면서 기술적으로도 날로 정교해지고 있는 사이버 공격은 단지 외부로부터의 공격만을 의미하지는 않는다. 관련 업무에 종사하는 사람이 뜻하지 않은 실수를 하거나 작업을 서두르다가 내부적인 사고로 발생하기도 한다.

한 조사에 의하면 사이버 공격의 약 3분의 1은 외부로부터 이루어지지만 전체의 80% 가까운 사고는 의도적이

사이버 공격 위험을 방지할 수 있는 가장 좋은 방법은 우리가 공격의 목표가 될 가능성이 있는지, 우리에게 사이버 공격을 해 올만한 동기가 무엇인지를 미리 인식하고 있는 것이다. 그러면 공격이 가능한 기술과 어떻게 공격을 시도할 것인지에 대한 단서나 징후를 감지할 수 있다. 또 국제적 협력을 통해 각 나라의 정보 기관, 정부, 통신 당국, 그리고 경찰과의 협조가 필요한 것은 물론이다.

지 않은 것이라고 한다. 그렇지만 점점 더 많은 사람들이 컴퓨터를 다루는 능력을 갖추게 되면서 사이버 공격의 발생 사례는 늘어나고 있다.

사이버상에서 발생하는 사고의 범위와 그 규모가 증가함에 따라 세계적으로 원전에 대한 사이버 공격에 대한 취약성과 사이버 공격의 발생 가능성이 증대되고 있을 뿐 아니라 실제적으로 공격을 당할 위험성도 증가하고 있다.

이에 따라 IAEA는 지난 2015년 6월에 원전 시설에 가해지는 사이버 공격의 위험에 대처하기 위한 국제적인 대응 방안을 이끌어내려고 시도한 바 있다. IAEA의 유키야 아마노 의장은 핵시설의 컴퓨터 보안에 관한 제1회 국제 회의에서 "테러리스트나 범죄 집단들이 국제적인 조직망을 갖추고 활동하기 때문에 전 세계 어느 곳이라도 공격할 수 있으므로 이제는 우리의 대응도 국제적인 공조 체제를 갖추어야 한다."고 말했다. 또한 "작년에만도 악성 소프트웨어로 원전에 무작위 사이버 공격을 가한 경우가 여러 차례 있었는데 그때 공격을 당한 원전들은 특히 조심해야 한다."고 덧붙였다.

사이버 안전의 개선

국가적으로 중요한 인프라 시설들에 공격을 가함으로써 이득을 얻고자 하는 범죄 집단의 사이버 공격 가능성이 높아짐에 따라 사이버상의 위험성에 대한 기본적인 의식은 높아지고 있다.

대부분의 국가 기관들은 중요한 시설의 안전에 대해 위기 관리 계획을 수립해 놓고 있지만 일반적인 위기 관

리 계획에서처럼 미리 나와 있는 대응 시스템은 물론 사이버 공격을 시도할 만한 범인들의 신원이나 범행 동기 등을 파악하게 해주는 데이터가 없기 때문에 그런 위기 관리 계획들을 사이버 안전 업무에 그대로 적용하기에는 무리가 있다.

2014년 독일의 연방정보기술국은 이름은 밝히지 않은 한 독일 제철소에 대한 사이버 공격 상황을 공개했는데 피싱 이메일로 제철소의 정보 시스템을 교란시켰다는 내용이었다. 그 정보 시스템은 제철소의 제어 시스템과 회사전체의 정보망이 상호 연결되도록 설계되었기 때문에 제철소의 제어 시스템에 대한 공격이 가능했던 것이다. 결국 제철소는 그 사이버 공격에 의해 제어 시스템과 생산 설비의 전원이 끊겨서 용광로가 적절한 폐로 과정을 거치지 못하는 바람에 재앙적 수준의 결과를 맞게 되고 말았다.

영국 Lancaster 대학의 보안문제연구센터 부소장인 Daniel Prince 박사는 그 독일 제철소 제어 시스템에 사용된 소프트웨어의 취약성을 조사중이라고 밝혔다. "결국은 시스템 구조와 설계의 문제이다. 제철 회사의 다양한 업무 분야 전반에 걸쳐 회사와 제철소의 제어 시스템 구조를 다각도로 분석하는 조사 작업을 하게 되는데 시스템 사이의 위기 관리를 어떤 방식으로 하며 사용자와 시스템의 상호 작용은 어떻게 이루어지고 있는지 조사한다. 또한 링크를 잘못 클릭하거나 작업 중 발생하는 실수 등에 의해 방어벽이 뚫려 제철 설비나 제어 시스템에 손상을 초래할 취약한 부분이 어디인지도 조사한다."

Prince 박사는 또 위험은 급속히 증가하기 마련이라고 말하면서 "위험성을 인식한다는 측면에서 우리는 항상 최첨단에 자리잡고 있어야 한다."고 강조했다. 위험을 방지할 수 있는 가장 좋은 방법은 우리가 공격의 목표가 될 가능성이 있는지, 우리에게 사이버 공격을 해올만한 동기가 무엇인지를 미리 인식하고 있는 것이다. 그러면 공격이 가능한 기술과 어떻게 공격을 시도할 것인지에 대한 단서나 징후를 감지할 수 있다. 또 국제적 협력을 통해 각 나라의 정보 기관, 정부, 통신 당국, 그리고 경찰과의 협조가 필요한 것은 물론이다.

Prince 박사는 "악성 소프트웨어 Stuxnet 사건은 사이버 공격에 눈을 뜨게 해준 사건이다. 우리가 그런 특정 제어 시스템 쪽으로 눈을 돌릴 수 있게 해 주었다. 분명하고 제대로 잘 수립된 대책을 확보하여 사이버 공격이 발견되면 어떻게 대처할 것인지 언제나 경계심을 유지할 필요가 있다."고 말했다.

다시 말하자면 위험을 미리 감지할 수 있는 관점을 확보하고, 위험 요인의 유형에 대한 이해를 제고하며, 확산되는 위험 요소를 직시해야 하는 것이다. 박사는 또 "궁극적으로 우리는 해커의 입장에서 생각할 필요가 있으며 그래야 효율적인 방어가 가능하다."고 말했다.

공격을 기다리는 입장에서 미리 관측하고 적절히 대응하면서 미래의 공격을 방어하는 등 사이버 공격자보다 우위에 서 있기란 매우 어려운 일이다. Prince 박사에 의하면 가장 좋은 방법은 Cyber Information Sharing Partnership 같은 방식을 통해 관련 당사자들끼리 연대하고 정보를 공유하는 것이다.

그는 "한 조직이 혼자서 자기의 사이버 영역에 대한 공격에 대비할 수는 없다. 그런 식으로는 언제나 사이버 공격보다 한 발 늦을 뿐이다. 이 싸움은 일종의 군비경쟁 같은 것이기 때문에 서로 간의 협력을 통해 우리를 위협하는 사이버 공격자들보다 유리한 고지를 선점하고 있어야 하는 것이다." 라고 말을 맺었다.