Robert Lowe

기업 CERT의 가장 큰 문제는 '준비부족'

기업마다 국가마다 정보보호에 대한 문화 차이는 존재하기 마련이다. 하지만 그 차이가 크다고는 볼 수 없다. 다양한 공격기법에 대한 대응방안 마련, 기업 정보보호의 방향 수립, 정보보호 교육방식 등 기업 보안 조직이나, 국가 CERT의 관심과 고민이 비슷하기 때문이다. 이런 생각은 호주 침해사고대응팀(이하: AusCERT)에 몸담고 있는 Robert Lowe와의 인터뷰에서 더욱 잘 알 수 있었다. AusCERT는 우리와 같은 고민을 어떻게 풀어가고 있는지 소개해 본다. Robert Lowe는 AusCERT의 침해사고 분석 전문가로 활동했으며, 현재는 AusCERT의 교육 및 컨퍼런스 책임자로 활동하고 있다.

정보보호뉴스 취재팀

▲ Robert Lowe
(Team Leader, Training and Conference, AusCERT)

Q. 기술적으로 혹은 관리적인 측면에서 AusCERT가 호주 내 기관이나 기업들에게 특별히 권고하는 것이 있다면.

A. 보안에 대한 관심 정도가 다를 수 있겠지만 본질적으로 정보보호에 대한 중요성은 모든 국가나 기업이 다 공유하고 있다고 생각한다. 최근 AusCERT에서는 호주 기업들이 그들의 정보자산에 대한 가치를 이해하기 위한 위험관리 기반의 접근방식을 비즈니스에 적용할 것을 장려하고 있다. 이와 함께 우리가 주목하는 것은 기관 혹은 기업의 임원진이 가지는 보안에 대한 관심 정도다. 기업의 정보보호 이니셔티브가 성공적으로 이뤄지기 위해서는 보안에 대한 최고 결정권자들의 인식이 높여져야 한다.

Q. 한국에서는 정보보호 전문가의 중요성이 강조되고, 직업으로서 유망한 분야로 인식되고 있다. 호주에는 정보보호 분야로 진출하려는 인력이 충분하다고 생각하나. 또 미래의 정보보호 전문가들에게 무엇이 가장 필요하다고 생각하나.

A. 지금까지의 경험과 보안 담당자들의 의견을 분석해 볼 때, 현재 호주의 정보보호 기술 인력에 대한 수요는 매우 높은 상황이다. 불과 10년 전만해도 대학 내 정보보호 학과가 개설되지 않았던 것은 물론이고, 지금은 빈번하게 등장하는 정보보호 이슈들이 당시에는 두드러지게 나타나지 않았다. 하지만 최근에는 대부분의 대학이 정보보호 과정을 다루는 것은 물론, 정보보호에 대한 내용 전체를 다루는 교육기관도 많이 있다. 이것은 불과 10년 사이에 생긴 변화들이다. 그럼에도 불구하고 나는 정보보호 전문가가

되기 위해 특정 분야에서 경력을 쌓아야 한다는 식의 필수조건은 없다고 본다. 다만 정보보호의 중요성에 대한 인식과 새로운 것에 유연하게 대처하는 능력을 가지고 있다면 더욱 뛰어난 정보보호 전문가가 될 수 있을 것이다.

Q. 정보보호는 끊임없는 교육이 필수지만 정보보호 전문가를 위한 재교육은 쉽지 않은 문제다. 정보보호 분야의 전문가를 위한 재교육 프로그램은 어떻게 구성해야 한다고 생각하나.

A. 많은 교육기관에서 이뤄지는 정보보호 교육은 말 그대로 각양각색이다. 호주 내 기업 정보보호 담당자들을 위한 지속적인 교육에 있어서도 '이것이 최선이다'라는 교육 커리큘럼과 방식은 없다. 하지만 교육 커리큘럼의 다양성은 필요하다. 호주의 많은 기업들이 직원 교육을 위해 별도의 예산을 편성해 놓고 있고, 이렇게 배당된 예산을 가지고 직원들 스스로가 자신들에게 필요한 교육 옵션을 선택하도록 하고 있다. 반면 정보보호 교육에 있어 좀 더 짜임새 있는 접근은 아마도 대규모 사업(Massive Undertaking)이 될 것이다. 이는 정보보호 분야 내에서도 업무의 종류가 매우 다양하기 때문에, 그리고 개인에게 적합한 훈련을 선택하는 것이 필요하기 때문이다. 그러나 이런 방식의 교육은 다양한 역할을 한꺼번에 수행하는 사람이 받기에는 그 양이 방대하고 내용 또한 복잡하기 때문에 적절하지 않을 수 있다는 점 또한 염두해 둬야 한다.

Q. 기업 내 보안인식 제고(Security Awareness)를 위해 기업들이 보안교육을 수행하고 있음에도 불구하고 정보보호 교육 효과에 대한 의문을 가지고 있다. 기업이 보안교육의 실효성을 입증하는 방법은 무엇이라고 생각하나.

A. 정보보호 분야의 다른 모든 상황이 그렇듯, 정보보호 인식제고 교육에 대한 투자 수익률을 계산하고 이를 수치화한다는 것은 정말 어려운 일이다. 기업이나 기관이 Malware에 감염된 PC 수를 수치화하고 그 원인을 분석할 수는 있다. 하지만 이런 통계자료들은 다양한 보호 메커니즘에 의해 나타난 결과물이라는 것을 감안할 때 기업 구성원들의 높은 보안의식은 필수적이다. 하나의 관리체계, 혹은 하나의 통제수단으로 기업 보안이 완성될 수 없다. 눈에 보이는 숫자와 결과물이 나타나지 않더라도 체계적이고, 협동적으로 이뤄지는 보안교육은 기업 보안의 저해 혹은 위협 요소들에 대한 지각, 탐지 그리고 대응능력을 향상시켜 기업의 손실을 예방한다는 점을 경영진에게 강조해야 한다.

Q. 과거 침해사고 분석가로 활동하면서 다양한 사례를 경험했을 것이다. 침해사고 대응에 있어 기업 CERT들이 공통적으로 범하는 실수는 무엇인가.

A. 예기치 못한 사고에 대응하는 기관 및 기업들을 돕는 과정에서 경험한 바에 따르면, '준비부족'이 가장 크다. 많은 기관이나 기업들은 수사를 원활히 진행하기에 충분한 로그 정보나 기타 원천 정보들을 보관하지 않았고, 심지어 무엇이 사고의 원인이었는지 조차 이해하지 못하고 있는 경우도 있었다. 사고가 일어난 시점에서 이와 같은 정보들이 미비하다면 사고에 대한 대응은 매우 어려워지기 마련이다.

Q. 그와 같은 실수를 하지 않기 위해서 그리고 사고 발생시 원활한 대응을 하기 위해서 기업이 필수적으로 준비해야 하는 것이 있다면.

A. 많은 기업이나 기관들은 실제로 사고가 일어났을 때를 대비해 계획 혹은 절차를 마련해놓고 있어야 한다. 물론 사고의 유형이 무척 다양하기 때문에 그 유형들에 일일이 맞춰 대응계획을 수립하기란 어려울 수 있겠지만 적어도 최소한의 예방책, 예를 들면 '사고 발생 시 어떤 시점에서 국가 CERT 혹은 법 집행기관에 연락을 취해야 할 것인가?'와 같은 문제에 대해 고민하는 것 정도는 충분히 가능하다. 이와 같은 질문에 대한 답을 찾아가는 과정과 정부의 정책을 실행에 옮기는 과정을 통해 기업이나 기관에서는 사고가 일어났을 때 우왕좌왕하지 않고 합리적이고 효율적인 결정을 빠르게 내릴 수 있게 될 것이다. 마지막으로, 침해 사고 담당자들은 사고가 일어났을 때 침착함을 갖추고 있어야 한다. 만약 그들이 당황하게 된다면, 성급하게 잘못된 결론을 내릴 수 있을 뿐더러 사고의 본질을 잘못 판단할 수 있다. 또한 증거를 훼손하거나 잘못 취급할 수도 있고 자신들의 대응이 어떤 영향을 미칠 지에 대해 미처 생각하지 못해 상황을 악화시킬 수도 있을 것이다. 어떻게 사고에 대응할지에 대해 침착하게 객관적인 태도로 생각하고 행동에 옮기는 것은 사고의 피해를 최소화하는 데에 도움을 줄 수 있다.

Q. 2008년 한 해동안 한국에서는 봇넷과 DDoS 공격이 가장 큰 이슈였다. 호주의 정보보호 이슈는 무엇이었고, 오는 2009년 전 세계가 관심있게 봐야 할 정보보호 이슈를 하나 꼽는다면.

A. AusCERT의 관점에서 봤을 때, 클라이언트 시스템에 영향을 끼치는 악의적 목적의 Malware가 여전히 주요 이슈 중 하나였다. 말웨어는 봇넷을 확보하거나, DDoS 공격을 개시하거나, 개인 정보를 훔쳐내거나, 스팸을 보내거나, 혹은 금전적 이득을 얻기 위한 다른 공격들을 시행할 때 사용된다. 올해에는 웹 애플리케이션 공격과 결합된 악의적인 소프트웨어 또한 목격된 바 있다. 이런 공격은 이용자들이 단순히 웹 브라우저를 띄우는 것만으로도 감염되게 하는 고약한 것이다. 이와 같은 Malware 이슈는 2009년에도 지속될 것으로 보인다. iPhone 등 모바일 기기가 금융거래 등 점차 다양한 분야에서 활용됨에 따라 Malware의 활동영역은 더욱 넓어질 것으로 예상된다.

Q. 다양한 공격기법이 등장하면서 소수의 인력들로는 대규모 공격에 효과적으로 대응할 수 없다. 특히, 봇넷을 이용한 DDoS 공격은 기업이 감당하기에는 큰 규모의 공격이며, 기업 정보보호 부서의 노력만으로는 이들 공격을 적절히 막기 어렵다. 기업은 무엇을 해야 하나.

A. 보통 보안팀은 적은 인원으로 구성되는데, 기업 임직원은 이 보안팀이 적은 인원으로도 다양한 보안 사고에 능수능란하게 대응하기를 기대한다. 이런 여건 속에서 보안팀들은 어떤 사고에 먼저 대응해야할 지를 선택해 우선순위를 매겨야 한다. 그래서 사업 경과와 정보 자산에 대한 완벽한 이해가 매우 중요하다. 또한 봇넷으로 제어되는 DDoS 공격으로 어려움을 겪는 기관들은 위험을 완화시키기 위해 도움을 요청할 필요가 있다. 이럴 경우 ISP에서 도움을 줄 수 있을 것이며, 국가 CERT는 공격에 사용된 봇넷이 어떤 종류인지를 밝혀내는데 도움을 줄 수 있을 것이다. S