기업 네트워크 보안 "이젠 기업 사활의 문제"

기업 보안문화의 변화…새로운 보안 개념 확립이 관건

해커의 침입은 비즈니스 보안에 중대한 위협임에 틀림없다. 방화벽과 같은 물리적인 예방 조치도 중요하지만 기업 네트워크 보안의 핵심요소는 바로 기업 내부에 존재하고 있다. 가장 주의해야 될 적이 바로 회사내의 직원이라면 그 문제의 심각성은 더해진다. 이제 우리는 새로운 보안 개념의 필요성과 변화에 대한 완벽한 이해가 왜 필요한지에 대해 다시 한번 심사숙고 할 때가 된 것이다.

업계에 관련된 잡지를 단 한 권도 구독하지 않으며, 그 흔한 메일링 리스트에도 가입해 있지 않은 사람이라 할 경우에도 만약 당신이 운영하는 회사에서 어느날 회사 최고의 프로그래머가 해커에게 당했다는 소식을 듣게 된다면 아마도 거의 패닉 상태에 이르게 될지도 모른다.

당신의 안전 수치는 어느 정도인가

초기 해커들은 소위 수법이라 말하는 그들만의 독특한 행동 양식에 사인을 남겼다. 지금도 마찬가지로 모든 하이테크 장애물에도 불구하고 수많은 해커들은 보기 좋게 침투하고 자신들의 명함을 남기곤 한다. 그들의 행위는 그 이유를 떠나 기업 전체를 곤경에 빠트리며, 심지어는 소규모 국가를 파멸 속으로 몰아 넣기도 한다. 단 한 사람이 법망을 교묘히 피해 나가면서 컴퓨터를 조정함으로써 보안상의 악몽을 발생시킬 수 있는 셈이다.

오늘날에 와서는 더 하겠지만 지난해 샌프란시스코 소재 컴퓨터 보안 협회의 보고서는 산업계와 정부를 중심으로 도처에 자행되는 사이버 범죄 행위가 위험 수치를 넘어서고 있음을 경고하고 있다. 보고서에 따르면 많은 수의 기업과 기관으로부터 제공받은 자료를 참고로 하고 있는데, 단지 리스트에 올라온 기관이나 단체 이외에도 수많은 기업과 기관들이 피해를 당하고 있음은 굳이 설명하지 않아도 미루어 짐작할 수 있다.

보고서의 내용의 다음과 같다. 리스트에 포함된 응답자 중 90%가 1년 동안에 걸쳐 컴퓨터 보안상의 침입 행위를 받은 경험이 있으며, 70%가 일반적인 컴퓨터 바이러스나 랩톱 절도, 혹은 직원 자의에 의한 네트워크 공격 이외에 다양한 유형의 침입을 받았다고 밝혔다. 이러한 유형에는 기밀정보 절도, 공금 횡령, 외부인에 의한 시스템 침입, 서비스 거부 공격, 데이터/네트워크 방해/파괴 행위 등이 포함되어 있다.

당했다면 그 피해액은

사이버 범죄에 대해 어느 나라보다 앞서있는 미국의 경우에 비추어 볼 때 한국 역시 해킹에 대해 자신할 수 없을 것이라는 점이 지배적인 견해다.

보고서의 조사 항목 중 보안상의 침해를 받았을 경우 그 피해액에 관한 부분이 있다. 과연 피해액은 어느 정도 이며, 피해액에 대한 정확한 산출은 가능한 것인가. 보고서에 따르면 이 부분에 대해 응답자 중 70%가 컴퓨터 침입에 의해 재정적 피해를 입었다고 밝혔으며, 그 중 42%만이 정확한 피해액을 산출할 수 있었다. 피해액의 산출 결과는 더욱 놀라웠다. 1998년부터의 피해액을 산출한 결과 3억 달러에 이르렀다. 하지만 이 금액은 협회가 조사한 250 여개의 기업과 기관에만 해당되는 것이며, 그나마도 그 중 42%의 경우라고 분석할 때 보안상의 문제로 인해 입은 손실은 기하급수적으로 증가할 것이라는 것은 자명한 사실이다. 이러한 상황을 기본으로 볼 때 국내 상황도 결코 이에 못지 않으리라는 분석이다.

비즈니스의 방어라인은 있는가

해킹은 식성이 특별하지 않다. 모든 것이 해킹의 대상이 된다는 점이다. 즉, 엔터프라이즈 기업의 문제만이 아닌 것

이다. 회사의 인지도 때문에 많은 기업들이나 기관들이 자신들의 해킹 사례에 대해 함구하고 있지만, 거의 대다수의 기업과 기관이 이들 해킹의 공격에서 자연스럽지 않다는 점에는 모두 공감할 것이다. 이러한 범법적인 해킹이 늘어나자 사이버 테러리즘을 예방하고자 하는 움직임이 대두되고 있다.

확실한 사실은 공격의 진원지가 두 곳이라는 점이다. 바로 외부와 내부에서 발생한다는 것이다. 따라서 기업 입장에서 피해를 당하지 않기 위해서는 전방위적인 계획이 필요하다. 즉, 프론트 라인과 백 라인을 동시에 보호하는 이중 방어 전략이 마련되어야 한다는 것이다.

한가지 알아두어야 할 점은 방어 시스템은 곧 하이테크를 통한 보안 기술이라는 생각에서 벗어나야 한다는 점이다. 가장 중요한 방어 시스템은 튼튼한 방화벽도, 소프트웨어 암호화도, 백업 시나리오도 아니다. 가장 강력한 방어 무기는 바로 직원들이다.

이러한 생각은 기존 컴퓨터 업계에서 간과되고 있는 부분이었으나, 최근 경향으로 볼 때 사이버 침입으로부터 조직을 보호하는 싶은 생각이 제대로 있는 기업일수록 직원이라는 핵심 요소에 대한 철저한 분석에 대한 요구가 높아지고 있다.

이러한 요구는 결코 직원에 대한 차별성의 문제가 아니다. 바로 채용기준의 재검토를 말하는 것이다. 오늘날 기업들은 채용기준이 매우 다양하기 때문에 다소 현실성이 결여된 듯이 보일 수 있다. 하지만 리스크를 감수 없이 모든 것을 얻을 수는 없다는 점도 간과해서는 안될 것이다.

기업이 갖추게 될 첫 번째 기술적 방어막은 신입 사원들이 이해할 수 있고 충분히 지각할 수 있는 것이라야 한다. 즉 프로세스에 대한 제어권을 가져야만 한다. 채용팀은 잠재적 사원의 기본 소양을 알아볼 수 있어야 하며, 향후 법적 소송에 대비한 법률적 사항을 주지시킬 수 있어야 한다는 것이다. 이러한 문제는 국내에서도 비일비재하게 일어났던 점을 감안한다면 다시 한번 재고해 볼 필요가 있다.

직원 채용

많은 전문가들은 직원 채용과 관련해서 알아 두어야 할 기본적인 사항을 권한 위임, 보수적 성향, 통합 부분 등 3가지로 밝히고 있으며, 그 내용에 대해 다음과 같이 설명하고 있다.

첫째, 권한 위임 부분은 권한을 위임 받은 직원들은 조직 내에서 좋은 실적을 달성하려고 노력하지만, 그 권한에 따르는 책임을 반드시 주지시켜야만 한다. 둘째, 보안 직원은 다소 고리타분 하더라도 완고해야만 한다. 정치적인 보수적 성향을 말하는 것이 아니라 기술에 대한 접근 태도가 보수적인 사람을 채용해야 한다. 새로운 생산시스템의 최신 기술에 대해 아무에게나 거리낌 없이 말해 대는 보안 직원은 절대 필요치 않다. 셋째, 보안팀은 통합/상호교류 지향적이어야 한다. 유지보수를 위해 방화벽의 가동을 중지 시키거나 IP를 변경하는 작업을 담당하는 직원들간에는 상대방의 작업에 대한 충분한 의사 전달이 필요하다.

보안은 곧 전투다

보안에 있어 완벽한 요약 리스트는 꼭 필요한 존재다. 기업 보안에 있어 마치 볼트와 너트 같은 요약 리스트를 만들어야 하는 것이다. 먼저 기업 시스템은 액세스 권한을 얻으려는 모든 사용자를 확인할 수 있어야 한다. 만약 그들이 기업에 우호적인 입장이라면 기꺼이 들여보내고, 그렇지 않은 입장이라면 그들의 통행을 막아야만 한다.

방화벽의 사용은 이러한 보안 장비를 배치하는 것만큼이나 중요하다. 흔히 생각하는 바로는 외부에서 들어오는 모든 것들은 패스워드 인증을 받고 라우팅 되며, 데이터는 몽땅 백업되고 바이러스 검색도 끝났다. 모든 것이 OK. 하지만 과연 그럴까라는 의문이 필요하다.

대기업에서 중소기업까지 모든 기업은 비즈니스를 격리해 둘 필요가 있다. 그리고 내부적으로 한번 더 격리되었을 때 우리는 OK라는 말을 할 수 있는 것이다. 또한 중요한 시스템은 필수적으로 많은 장치(자물쇠, 열쇠)로 보호 받아야만 한다. 어느 누군가 기업에 불만을 가진 외부 혹은 내부의 사람으로부터 공격 받을 수 있다는 사실을 간과해서는 안된다.

전체적 관리 필요

이상의 모든 사항이 준비되었다면 전체적 관점에서의 관리가 필요하다. 지리학상으로 여기저기로 확장되어 가고 있는 오늘날 기업들의 경우 이러한 확장성을 제어하기 위해 필요한 컨셉과 애플리케이션의 양도 똑같이 증가하게

된다. 따라서 분산된 모든 지점으로부터 하드웨어와 소프트웨어를 모니터링하기 위해 필요한 운영지침을 만들어야 한다. 이 같은 지침에 따른 작업에 소요되는 경비는 만만치 않으므로 지침을 처음 만들 때 정확한 판단력이 요구된다.

메이저 업체치고 자체적인 원격 관리 툴을 가지고 있지 않는 곳은 거의 없다. 직원 채용 때화 마찬가지로 제품 역시 완벽한 제품을 사용해야만 한다. 그리고 이러한 제품이라도 설치 후 다시 테스트를 통해 완벽성을 재검토 해야만 한다. 또한 기업이 관리하길 원하는 하드웨어의 종류에 신경 쓰지 않도록 크로스 플랫폼과 OS 의존 소프트웨어 환경을 구현하는 것이 좋다. 이러한 환경을 고려하지 않았을 경우 조만간 '후회하는 날'을 맞보게 될지도 모른다는 많은 전문가들의 조언에 다시 한번 신경을 쓰는 것에 인색할 필요는 없을 것 같다.

오늘날 기업들은 급속히 번창하는 사이버 테러에 맞서 싸우고 있다. 침입, 웜즈, 바이러스, 보안 위협과 같이 보다 다양화 되고 강력해진 최근의 사이버 테러 양상으로 인해 그 반대 세력도 힘이 점점 커지고 있다. 웬만한 기업이라면 모두 방화벽을 설치하고 있을 것이다. 하지만 이것은 최선책이 아님을 명심해야 한다. 이미 밝혔듯이 기술적 방어와 더불어 적절한 관리와 채용 관행을 유지한다면 더욱 완벽한 보안을 유지할 수 있다. 하지만 여기에는 꼭 집고 넘어가야 할 문제점이 도사리고 있다.

끝없는 노력 있어야

많은 전문가들은 이러한 보안 정책이 매우 큰 대기업체만이 할 수 있다는 점에 초점을 맞추고 있다. 즉, 기술적 방어책과 함께 인사 방어책을 동시에 실시할 수 있는 대상이 극히 한정되어 있다는 것이다. 소규모 기업을 운영하는 입장에서는 너무 큰 비용이 창출된다는 것이다.

이 부분에 대해 전문가들이 내어 놓은 방법은 다음과 같다. 소규모 기업 운영하고 있고 동시에 보안상의 취약점이 산재해 있을 경우 아웃소싱을 선택할 것인가, 아니면 자체적인 해결할 것인가라는 부분에 대해 자체적인 평가를 해야 한다는 것이다. 물론 이러한 문제는 결정하기 어려운 부분이다. 그렇기 때문에 많은 전문가들은 양자택일이라는 극단적인 방법을 제시한다. 리스크를 감수하고 전쟁에 뛰어 들던지 반대로 안전한 수익 창출을 위해 그럴 마음과 자신이 없다면 e-비즈니스나 새로운 하이테크 세계에 존재하는 기능에 관심을 애초에 갖지 않아야 된다고 말한다.

이들이 말하는 하나의 원칙은 불변이다. 바로 보안에 대한 방어 조건은 변하지 않는다는 것이다. 즉, 성숙된 직원, 침입자를 막기위한 하드웨어와 소프트웨어, 그리고 해커, 크래커, 조이라이더와 같은 사이버 범죄자들의 테러 행위를 감내할 수 있는 지구력이 필요함과 동시에, 조직 전체 내에 일정에 보안정신이 심어져야 한다는 것이다.

정말로 끝이 없는 작업임에 틀림없지만, 기업은 내/외부 범법 행위에 대한 회사정책에 대한 지속적인 검토와 갱신 작업을 필요로 한다는 것이다. 기업과 해커가 친구가 되거나, 타협을 통해 서로 원만한 관계를 유지할 수 있는 방법이 나오기 전에는 이러한 끝없는 노력은 어쩔 수 없는 일이다.

전문가가 조언하는 보안에 관한 질문과 답

- **가장 두려운 것은**
  → 현재 업계 전반에 걸쳐 가장 큰 두려움의 대상은 인증 받지 않은 액세스다.
- **보안시장 동향은**
  → 업계 동향에 따르면 보안 비즈니스의 수익은 2003년 경이면 약 20억 달러 규모가 될 것이라 분석되고 있다.
- **공격의 진원지는**
  → 모든 공격은 출입구와 관련이 되어 있다. 외부로부터 침입을 받거나 내부에서도 공격이 이루어 진다. 하지만 중요한 점은 그 공격의 진원지가 아니고 그 공격으로 인한 피해가 너무 엄청나다는 점이다.
- **해커의 공격 루트는**
  → 해커는 인터넷을 통해 공격한다는 점을 누구나 알고 있다. 조금만 유심히 찾아 본다면 손쉽게 발견할 수 있는 해킹용 스크립 툴이 무궁무진하게 존재하기 때문에 해커들의 극성은 날로 더해지고 있다.
- **내부 공격은 어느 정도**
  → 보안 조사 결과를 보면 모든 공격 행위 중 60% 이상이 내부에서 자행되고 있다.
- **보안 기술 발전을 통한 해결책은**
  → 보안산업의 기술적인 발전은 항시 해커들의 기술을 발전시키는 하나의 연습장이 되어가고 있다. 보안 기술의 1단계 발전에 대비 해커들은 2-3단계 발전을 거듭하고 있는 것이 사실이다. 기존의 해커들이 최고의 보안요원으로 변신하는 것은 결코 우연이 아니다.