보안관제시장 혼전 '차별화·신뢰성 확보' 勝敗 좌우

100억원대 규모 시장 선점위한 경쟁 치열 … 보안시스템 구축후 지속적인 관리 중요

A기업은 최근 오랫동안 연구를 거쳐 새로운 제품을 개발했다. 이 제품은 세계 최초로 혁신적인 제품으로 평가받고 있다. 그러나 A기업의 B사장은 요즘 새로운 고민거리를 갖게 됐다.

B사장의 고민거리는 다름 아닌 주변의 경쟁사들이 새로 개발한 제품의 소스를 알아내기 위해 열을 올리고 있기 때문에 제품 소스에 대한 보안을 걱정하고 있는 것이다.

따라서 B사장은 보안 시스템을 구축하기로 마음먹고 최고가의 보안제품을 급하게 구입하여 구축하기 시작했다.

침입차단시스템, 침입탐지시스템, 각종 인증 및 암호 시스템을 구축하고 나서야 B사장은 마음을 놓을 수가 있었다.

그러나 불과 몇 주 후 유통망이 구축되어 판매가 시작되어야 할 시점에 신제품 소스가 유출 된 것이다.

고생 끝에 개발에 성공한 A사는 망연자실하여 하늘만 바라보고 이젠 법정과 보험사만을 찾아 다녀야 할 판이 됐다.

이러한 원인은 A사의 B사장이 한가지 간과한 것이 있었던 것이다.

바로 좋은 보안 시스템을 구축하기는 했지만, 그 시스템을 운영하고 감시할 관리자를 생각하지 못한 것이다. 그제야 B사장은 보안에 관해 시스템을 구축하는 것보다 구축 후 지속적인 관리가 더 중요하다는 것을 깨닫게 된 것이다.

물론, 위의 상황은 가상이다. 그러나 이러한 상황은 치열한 경쟁 사회에서 있을 법한 일이다. 따라서 무엇보다도 자신의 중요 정보를 지키는 것은 자신이 앞장서야 한다는 것만은 사실이다.

과거 비해 보안인식 높아져

우리나라에도 정보 보안에 관한 인식이 이젠 과거와는 달리 많이 높아지고 있는 실정이며, 그래서 과거의 시스템 구축만으로 보안을 끝이라고 아는 인식보다는 보안은 사후 지속적인 관리가 더 중요하다고 인식하는 사례가 증가하고 있는 실정이다.

이에 따라 구축해 놓은 보안 시스템을 24시간 감시해주고 모니터링 해주는 관제서비스 분야가 서서히 두각을 나타내고 있다.

그러면 올 상반기 보안 관제 서비스 시장은 어떠하였으며, 하반기 시장은 어떠할 것인가?

결론부터 말한다면 현재까지는 어둡다고 말할 수 있다. 물론, 아직 올해가 다 지나간 것은 아니다. 그렇다고 해서 하반기에 접어들면서 그 수요가 급격하게 늘어날 것이라고 기대하는 업체는 그리 많지 않다.

올해 상반기 보안 관제 서비스 시장이 어두운 것에 대해 업계에서는 우선 무엇보다도 전반적인 경기침체와 그에 따른 닷컴 몰락, 그리고 IDC(Internet Data Center)의 경기침체에 기인한 것으로 꼽고 있다.

또한 관제서비스가 보안 시장에서 새로운 영역으로 자리를 잡아가자 많은 보안 기업에서 보안 관제 서비스 사업을 주력하려 하는 경향에 따라 시장이 성숙되기도 전에과당 경쟁이 서서히 일어나고 있는 것도 하나의 원인으로 꼽고 있다.

업계 한 관계자는 "보안 관제 서비스 시장이 성숙되기도 전에 서비스 품질이 아닌 저가 정책으로 시장이 단순한 가격 경쟁의 양상을 띄기 시작했다"고 설명하고, 이와 관련하여 "모 보안 업체에서 5만원에 관제 서비스를 제공한다는 광고를 하고 있다"고 말하고, "이는 어떠한 형태로든 시장에 영향을 주는 것"이라고 덧붙였다.

시장, 과당경쟁으로 치달아

따라서 이러한 영향에 의해 연초 예상과 달리 보안 관제서비스 시장은 활성화 되지 못하고 있는 것이 사실이다.

이에 따라 보안 관제 서비스 업체들은 상반기에 활발하게 추진했던 M&A나 전략적 제휴, 통합보안관제기술 개발 등에 포커스를 맞추고 하반기에 이에 대한 결과가 가시적으로 나타나주기를 기대하고 있는 실정이다.

반면, 상반기에 나름대로의 성과도 있었다. 보안시장의 위축에도 불구하고 IDC 센터의 수익성을 차별화 하기 위해 보안 서비스 SLA(Service Level Agreement)를 특화 하는 등 다각적인 노력을 보이기도 했다.

일반적으로 현재 국내 보안시장과 미국의 보안시장을 비교해 볼 때, 제품 또는 기술면에서 3~4년 차이가 있으며, 그 외의 활용적인 측면과 특히 서비스 차원에서 본다면 5~6년 정도 차이가 난다고 전문가들은 설명하고 있다.

특히 미국의 보안관제를 전문으로 하는 회사 Counterpane이 2000년 연말에 엄청난 액수의 투자를 유치한 점으로 미루어 볼 때, 보안 관제 시장의 확대는 분명한 사실로 다가오고 있다고 보여진다.

현재 국내의 보안 관제 서비스 시장은 IDC와 파트너 관계를 맺고 있는 상황에서 향후 전망을 예측하기 어려운 상황이며, 또한 IDC의 M&A 소리가 나오고 있고 일부는 현실화되고 있는 상황을 볼 때 하반기는 혼전이 예상되고 있는 실정이다.

이러한 혼전은 향후 IDC의 M&A 진행과정 및 파트너의 보안 서비스 수준에 만족하지 못하는 IDC 내부의 불만으로 다시 한번 짝짓기가 예상되어 혼전이 가중 될 것으로 보인다.

특히 IDC에 입주한 대형 고객과 같은 경우 IDC와 협정을 체결한 보안 서비스 파트너와의 업무 협정도 가능할 것으로 전망되고 있다.

하반기 시장 '半信半疑'

보안 업계에서는 아직은 올해 하반기 시장에 대해 아직은 두려움 반과 기대 반으로 하반기 시장에 맞이하고 있다.

현재 긍정적으로 하반기 시장을 전망하는 입장은 우선 경기 침체 환경에도 불구하고 보안 아웃소싱에 관한 필요성 인식은 증가하고 있는 추세이며, 기업체의 보안 마인드가 향상되고 있다는 것을 손꼽고 있다.

이에 따라 보안업계는 하반기에는 보다 안정적인 서비스를 제공하려는 업체의 노력과 그에 따른 시장의 확대를 기대하고 있다.

또한 보안 관제서비스가 대기업, 정부, 금융권을 중심으로 한 보안SI 프로젝트, 정보통신기반보호법과 관련한 보안 컨설팅 프로젝트와 연계되는 것도 하나의 원인으로 꼽고 있다.

그러나 하반기 시장이 과연 상반기의 그늘을 모두 덮어버릴 만큼의 밝은 햇살이 비춰질지도 의문이다.

업계에서는 밝은 기대와는 달리 현재의 상황을 하반기에도 연속선상으로 보는 견해가 적지 않다.

업계 한 관계자는 "오히려 하반기에는 상반기보다 더욱 어려워질 것으로 전망된다"며 "이는 주요 고객들이었던 닷컴 기업들이 재무 상태가 악화되기 때문"이라고 설명했다.

따라서 "주요고객 사이트를 일반 기업으로 많이 선회해야 할 것"이라고 덧붙였다.

이렇게 하반기 시장에 대해 의견이 갈리고는 있지만, 대부분의 많은 기업들이 하반기 시장에 대해 긍정적으로 바라보고 있는 실정이다.

이러한 기대는 연초의 큰 성장세를 이룰 것이라는 기대에 대한 보상심리와 함께 실제 하반기 들어 전반적인 경기 침체가 조금씩 풀리는 것에 따라 공공시장과 대기업의 대규모 프로젝트를 포함한 수요가 늘 것으로 예상하기 때문이다.

기술력 특화로 수요 창출해야

지난해 보안 관제 서비스 시장은 업계 추정으로 50억원에 이르렀다고 한다.

연초 올해 보안 관제 예상 시장규모에 대해 많은 업체들이 150억원까지 말한 바 있으나, 현재로서는 많은 업체들이 100억원 정도로 내다보고 있다.

분명한 것은 당초보다는 작은 규모이지만 보안 관제 서비스 시장은 지속적으로 커나가고 있다는 것이다.

따라서 업계에서는 업체간의 지나친 서비스 요금 과당 경쟁은 피하고, 각자 경쟁력 있는 기술력을 특화하고 이를 바탕으로 한 수요 창출을 하기 위한 노력이 필요할 것이다.

2001년 하반기 시장에서는 무엇보다도 중요한 것은 업체 스스로의 노력에 따라 '되찾아오느냐' 아니면 찾은 것을 '빼앗기느냐'의 싸움이 될 것이다.

"보안은 지속적인 사후관리가 중요"

관제 기술 향후 3~4년내 급성장 가능성 보여

약 력

포항공과대학원 전기공학 석사

코코넛 서버보안/인증/통합관제 팀장

코코넛 기술본부 팀장

이정훈

최근 들어 구축해놓은 보안 시스템에 관한 관제 서비스를 요하는 기업이 늘어나고 있다. 이는 그동안 제품만 들여놓았다고 보안이 끝나는 것이 아니라는 것을 기업체에서 서서히 인식해가고 있는 결과이기도 하다. 그러나 실제로 보안 관제라는 것이 그리 쉬운 기술만은 아니다. 현재 보안 관제서비스 분야에서 여타 다른 기업보다 발빠른 행보를 걷고 있는 코코넛의 보안 관제 전문가를 통해 관제서비스에 관해 기술적인 설명을 들어본다. 〈편집자 주〉

보안관제서비스를 설명하기 위한 아주 쉬운 비교 대상이 바로 물리적 보안 대행업체이다.

이 업체들은 도둑을 막기 위해서 건물에 각종 센서를 설치하고 이 센서에서 보고되는 자료를 중앙에서 관리하다가 특이 사항이 발생되게 되면 즉시 출동하여 특이 사항이 무엇인지 확인하고 해결하는 역할을 한다.

인터넷 보안관제 업체 역시 서비스의 원리는 이와 매우 흡사하다. 고객의 인터넷을 이용한 해커의 침입을 차단, 탐지하기 위해서 침입차단시스템, 침입탐지시스템, 각종 인증 및 암호화 시스템을 설치하고 중앙관제센터에서 이를 24시간 감시하고 있다가 특이사항이 발생하게 되면 바로 인터넷을 이용하여 원격에서 대응하거나 직접 고객의 서버 위치로 출동하게 된다.

보안 관제인력 적고 인건비 높아

실제로 모든 상점들이나 건물이 물리적 보안대행업체를 이용하지는 않는다.

일부 대형건물은 자체적으로 물리적 보안시스템과 관리 인력을 유지하기도 한다. 이는 인터넷 보안관제서비스에도 비슷하게 적용된다.

즉, 어떤 업체는 보안 전문 업체에게 관제서비스를 의뢰하기도 하고, 또 보안에 대한 투자를 많이 하는 일부 업체는 자체적으로 보안시스템 관리자를 두어 자사 시스템의 보안을 유지하기도 한다. 여기서 중요한 것은 비용과 인력이다. 보안시스템을 충분히 관리 할 수 있는 인력을 보유하고 값비싼 보안시스템을 도입할 수 있는 예산이 갖추어졌다면 굳이 보안관제 서비스를 받을 이유는 없다. 하지만 여건상 대부분의 업체에게 이는 이상에 그칠 수밖에 없다.

현재 정보 보안 인력시장에서 보안시스템을 안정적으로 유지할 수 있는 능력을 소유한 인력은 극히 소수이고, 설사 그런 인력을 구할 수 있다 하더라도 인건비가 상당히 비싸다. 또한 설비 역시 만만치 않다.

값비싼 보안시스템이 도입이 네트워크의 복잡성에 비례하여 증가하고 이를 통합적으로 관리해야 할 통합관제 시스템도 구입해야 한다. 이 통합관제 시스템은 구매는 경우에 따라 보안시스템 자체 보다 더 큰 비용이 소모 될 수도 있으므로, 결국 배보다 배꼽이 더 큰 경우가 될 수도 있다.그렇다면 굳이 왜 이렇게 어렵고 비싼 보안 관제 기능을 갖추어야 하는가 라는 의문이 제기될 수 있다.

사용자들은 방화벽과 같이 보안 시스템만 도입하더라도 어느 정도의 보안성은 담보되는 것이 아닌가라는 의문을 끊임없이 제기할 수 있다.

과거 방화벽만으로 보안 끝

일반적으로 보안 전문가들의 보안지침의 첫 번째로 중요하게 생각되는 것이 보안은 지속적인 관리가 핵심이라는 것이다.

즉, 침입차단시스템, 탐지시스템을 도입하는 것이 중요한 것이 아니라 이 시스템 설치 후에 이 제품의 정책 등에 대해 지속

적으로 관심을 가져야 하고, 쉴새 없이 쏟아내는 로그에 대한 감시가 더욱 중요한 것이라는 것이다.

몇 년 전만 하더라도 침입차단시스템 하나로 모든 회사의 보안이 끝났다고 생각해도 무방한 시대가 있었다. 하지만 지금은 단순히 침입차단시스템뿐만 아니라 다양한 보안요소를 만족시키기 위한 더욱더 다양한 보안시스템이 출현했고, 네트워크의 복잡도가 증가함에 따라 같은 보안제품도 여러 개가 설치되는 수준에 이르렀다.

지금과 같은 상황에서는 보안통합관제 툴과 같은 보조 툴이 없다면 관리 자체가 힘들어지게 됐다는 것이다. 이렇듯 시장의 요구사항이 변화하는 것은 과거 SMS(System Management System)의 등장했던 시장 배경과 매우 흡사하다. 또 실제로도 보안관제시장에서 기존의 SMS 툴이 그 나름의 기능을 발휘, 일정 부분 선점을 하고 있다. 이에 대해서는 뒷부분에서 다시 언급될 것이다.

다시 보안 관제 기능으로 돌아가서, 앞에서 보안 시스템을 간략하게 언급했던 보안 관제의 기능들 보안 시스템을 감시하고 이상이 발생하게 되면 출동한다 에 대해 중요한 기능 위주로 몇 가지 좀 더 자세히 살펴보겠다.

통합관제 툴은 크게 보안정책의 수립, 적용, 보안상황의 감시, 대응, 및 리포팅, 시스템 관리 등의 기능이 필요하다. 하나하나 세밀하게 짚어보자.

보안정책 수립 중요

▲보안 정책 수립 - 첫 번째로 중요한 것이 보안정책의 수립 부분이다. 현재의 모든 보안시스템은 자체내의 보안정책 수립 툴을 가지고 있으며 이를 통해 보안시스템의 정책을 정의할 수 있다. 여기서 관리의 문제점이 하나 등장한다. 같은 침입차단 시스템이라 하더라도 제품마다 보안정책의 정의 방법과 툴이 각각 다르다는 것이다. 실제로 통합 관제 툴이라면 침입탐지시스템에 대한 표준화된 정책수립 툴을 제공하여 침입차단시스템의 종류에 관계없이 일관된 정책수립 방법을 제공해야 한다.

▲보안 정책 적용 - 보안정책의 적용은 앞서 얘기한 정책의 적용이다. 각각의 보안제품은 각각의 고유 프로토콜과 스크립트 언어로서 정책을 실제 보안시스템 모듈에 적용한다. 통합관제툴은 각각의 보안시스템의 종류에 관계없이 중앙의 콘솔에서 손쉽게 보안 정책의 적용이 될 수 있도록 지원해야 한다.

▲보안상황 감시 - 보안상황의 감시는 관리되는 보안시스템 또는 일반 시스템의 보안관련 로그를 취합하여 관리자가 쉽게 보안상황을 확인할 수 있도록 하는 기능이다. 이 기능에서는 보안시스템 자체도 네트워크의 한 시스템이기 때문에 시스템의 정상 작동여부도 감시해야 한다.

▲보안 상황 대응 - 보안상황의 대응은 관제 기능에서 매우 중요시되는 기능중의 하나이고, 또 최근에 관제서비스 업체들이 속속 등장하면서 많이 활성화되고 있다. 통합 관제툴이 제공하는 기능중의 강력한 기능이 바로 이것이다. 통합 관제툴은 여러 보안시스템의 로그를 분석하여 그 보안상황을 더욱 더 정확히 탐지하고 이에 대한 대응을 여러 보안시스템이 협동하여 할 수 있다는 것이다. 일례로 침입탐지시스템에서 침입을 차단하고 이를 침입차단시스템에 통보하여 침입차단시스템이 이를 차단하는 것이 바로 이의 가장 간단한 한 종류이다.

▲리포팅 및 시스템 관리 - 통합관제툴의 본연의 기능은 아니지만 관리자를 도와주기 위한 부가적인 기능으로 리포팅 기능과 시스템 관리 도구이다. 리포팅 기능은 이를 통하여 네트워크 및 서버의 보안 위배 및 리스크 정보를 판단할 수 있기 때문에 효율적인 리포팅 기능은 보안성 향상에 도움을 준다. 시스템 관리 기능은 첫번째로 보안과 관련된 시스템의 관리 기능과 두 번째로 SMS의 기능을 일부 가지고 있어야 한다. 보안관리도 일종의 시스템 관리이기 때문에 이 두 부분은 실로 완벽히 이분화 하기는 쉽지 않다.

보안정책 수립 · 적용 표준 전무

간략하게 보안관제 툴의 기능에 대해 정리해 보았다. 짐작컨대 실제로 이 글을 읽는 현업 보안관리자나 시스템 관리자들은 앞서 정리한 기능들에 대해서 공감하지만 그 기능들은 구현하기가 쉽지 않음에 또한 힘들어하고 있을 것으로 예상된다. 여기서 잠시 기업의 보안을 담당하시는 실무자들이 직면해 있는 통합관제의 어려움에 대해서 몇 가지 언급을 하겠다.

우선 무엇보다도 보안 정책의 수립 및 적용을 일관되게 할 수 있는 표준이 전혀 없다는 것이다. 만약 자신이 보안시스템의 종류가 5개라면 5개에 대해서 모두 다른 정책 수립 및 적용 모듈이 필요하게 된다는 것이다. 또한 각 제품마다 플랫폼도 상이하여 이 모든 것을 고려해야 한다.

보안 상황의 감시에서는 일차적으로 각 보안시스템에서 쏟아내는 로그의 분석 모듈이다. 만약 보안시스템의 수 십대 이상이라면 이의 로그를 실시간으로 분석하여 정말로 중요한 사항에 대

해서만 보고하는 모듈이 나올 수가 없다. 그렇기 때문에 실력 있고 경험 많은 보안 전문가에 의해 실제로 보안 관제툴을 대규모 시스템에서 운영해 본 경험이 필수인 것이다. 실제 경험이 없이 보안로그만을 모아 놓게 되면 그 많은 양 때문에 실시간 대응보다는 사고 후 원인분석에만 적용할 수밖에 없을 것이다.

보안 위배 사항에 대한 대응은 앞의 정책 수립, 적용, 감시가 제대로 되어야만 이루어질 수 있는 분야이다. 마지막으로 개발자의 관점에서도 통합 관제툴은 대규모의 시스템과 연관되어 확장성 및 안전성이 단 시간내 확보되기 힘들며 수많은 플랫폼, 네트워크 관련 작업 집중 등으로 인하여 개발 및 설치 초기에 많은 애로사항이 발생하게 된다. 그렇다면 현재 통합 관제 시장의 기술 현황은 어떠한가? 현재 통합관제 시장을 살펴보면, 고객의 잠재 수요는 빠른 속도로 확장되고 있지만 이를 만족시킬 만한 안정성과 기능을 가지고 있는 완성도 높은 제품은 거의 없다.

고객 만족할 완성도 높은 제품 없어

이 시장에서의 초기 선두 주자는 유명한 SMS 도구인 Tivoli나 Unicenter와 같은 제품인 것이 현실이다. 이 툴들은 시스템 관리 툴로써 초기부터 여러 시스템 관리의 프레임워크를 만들어 놓고 추가 기능만을 계속 업데이트하는 제품이다. 이 중 하나의 추가기능이 바로 보안관제 기능이다. 하지만, 보안관점에서 접근한 제품이 아니고 비용과 초기 설치면에서 상당한 부담을 주기 때문에 보안 관제시장에서 보편적으로 널리 보급되고 있지는 않다. 또한 앞부분에서 언급한 통합 관제툴이 가져야 할 기능을 다 포함하고 있지도 않는 것이 현실이며, 주로 로그 처리에 초점이 맞추어져 있다. 이런 상황에서 많은 보안 업체들이 틈새 시장을 노리며 통합 관제 툴을 잇따라 내놓고 있다.

앞서 언급한 바와 같이 보안시스템의 증가로 수요가 증가하는 것을 단적으로 보여주는 사례라고 할 수 있다. 그러나 이 제품들은 아직까지 시장을 주도하고 있지는 못하다. 대부분의 통합 관제툴이 자사의 보안제품의 통합에만 관심이 있을 뿐 타제품과의 연동 부분에서는 완벽하지 못하기 때문이다. 또 다른 통합관제의 예는 가장 유명한 통합 관제툴의 제작도구인 OPSEC(Open Flatform for Security)에서 볼 수 있다. 침입차단시스템으로 유명한 Firewall-1의 제작 회사인 Checkpoint사가 주도한 것이다. 이 제품의 특징은 자사의 제품을 기반으로 한 통합을 주장하고 있다는 것이다. 자신의 침입차단시스템과 연동할 수 있는 API를 공개함으로써 많은 제품들이 시장의 주도 제품인 Checkpoint사의 침입차단시스템과 연동기능을 제공하게 되는 것이다. 이 외에도 자사 제품과 연동 가능하도록 API를 공개하는 다른 몇 개의 제품이 있지만 워낙 시장점유율이 높은 제품이 주도 하고 있기 때문에 크게 시장에서 영향은 미치지 못하고 있다.

표준화 작업 진행…향후 개선 보여

향후 통합관제제품은 SMS의 보안기능 강화와 보안을 고려하고 가볍게 만든 보안통합툴, 그리고 OPSEC과 같이 특정 솔루션 벤더의 제품을 중심으로 이끌어 가는 보안통합툴 등 세 종류가 각축을 벌일 것으로 보인다.

필자의 생각으로는 보안을 위한 틈새 시장으로 보안 통합 관제툴이 당분간은 확대하고 유지할 것으로 생각된다. 이 제품시장에서 또 하나의 큰 영향을 미칠 요소가 있다. 앞에서 언급했듯이 다양한 제품을 연동할 표준이 없다는 사실인데, 사실 지금 IETF(Internet Engineering Task Force)에서는 침입 로그 표준화에 대해 draft가 나와 있으며, 국내의 ISTF(Internet Security Technology Forum)에서도 침입탐지 및 차단시스템에 대한 로그형식 표준이 2001년 5월에 제정되었다. 지금 사항들이 역시 가장 하기 쉬운 로그 형식에 맞추어져 있으나 IDEF(Intrusion Detection Exchange Format)라고 하여 침입탐지 및 대응 시스템간에 데이터 공유를 위한 데이터 포맷과 기능들을 정의하는 과정에 있다.

따라서 근일 내에 완성되기는 어렵겠지만, 앞에서 말한 표준이 없다는 문제점은 점차적으로 개선될 것으로 전망된다. 표준에 대한 시장의 변화에 따라 통합 보안 관제툴은 또 한번의 큰 변혁기를 가질 것으로 보인다. 지금 몇몇 보안 업체들은 이 보안 표준을 리드하기 위해 활발한 활동을 보이기도 한다. 지금까지 개략적으로 보안관제서비스의 기능, 어려움, 현재의 기술력 등에 대해서 얘기를 해 보았다. 지금은 제품의 완성도도 미흡하고 시장의 수요가 많은 편은 아니지만 짧은 시간 안에 제품의 완성도와 시장의 수요도가 급격히 증가하리라고 본다. 중요한 것은 완벽한 보안을 위해서는 관리가 핵심이라고 모든 보안전문가와 관리자가 동의하고 있다는 사실이며, 그 관리의 핵심역할을 할 것으로 기대되는 완성도 높은 통합보안 관제 툴의 발전에 따라 보안 관제 서비스의 발전 역시 기술적으로나 시장 현장에서나 향후 3-4년 내에 무궁한 발전 가능성을 지니고 있다고 보여진다.

Interview

"고객 위한 관제서비스 다각화 이루어져야"

시큐어소프트 보안관제센터장 김창민

현재 보안 시장 상황은

시장이 무르익기도 전에 이미 업체가 너무 많이 생겨서 과당경쟁이 일어나고 있는 실정이다. 이는 굳이 관제 서비스 분야만이 아니라 보안시전 전체의 분위기이다. 작년부터 수요에 비해 공급이 많아지고 있다. 관제서비스는 올해부터 업체가 서서히 늘어나고 있다. 또한 관제서비스 시장은 IDC 타격에 의해 침체된 상태이다. 관제서비스는 IDC 연계가 많은 분야이기 때문에 IDC 경기 영향을 많이 받게 된다. 서비스 질이 향상되기 이전에는 가격 경쟁이 심화될 것이다. 서비스 가격은 제품의 수입가와 인력, 초기투자 등이 함께 결정되는데 심하게는 월 5만원에 계약이 이루어지기도 한다. 무엇보다도 경쟁력을 갖추기 위해서는 서비스 질을 높여야 한다. 많은 사이트에 서비스를 하는 것보다 높은 서비스를 해야 한다.

관제서비스가 나오게 된 배경은

현재 보안 제품이 많이 등장했다. 업체들은 사용하고 있는 보안제품 들을 관리를 해야하는데 비용이 많이 들고, 전문적인 관리 능력을 갖고 있지 못해 모니터링을 대행사에 의뢰하게 되다보니 아웃소싱 관제서비스가 나오게 됐다. 따라서 관제서비스를 이용하는 기업들은 편안하게 업무를 볼 수 있게 됐다.

기업에서 관제 서비스 아웃소싱을 멀리하는 이유는

일반 기업에서는 외부에 관제 서비스를 요청하는 것을 꺼려하고 있다. 특히 이러한 현상은 대기업에서 더 강하게 나타나고 있다. 이는 대부분의 기업이 자사의 소스가 오픈되는 것을 우려하기 때문이다. 또한 각 기업에서 보안을 담당하는 전산 담당자들이 업무가 과중하다보니 주가 여타 다른 업무가 되고 부가 보안업무라고 인식하게된다. 따라서 정보를 안전하게 보호하고 인프라를 구축해야 하는데 이 순서가 뒤바뀌게 되는 것이다. 이에 따라 보안에 대한 필요성을 인식하지 못하게 되는 경우도 있다.

향후 예상되는 시장 변화는

작년까지만 해도 관제서비스는 IDC쪽 서버가 많았다. 일반 기업의 관제서비스는 미흡한 상태이다. 앞으로는 IDC 고객만이 아니라 ISP업체와 대기업들에게도 서비스제공과 장비 임대 등의 서비스의 다각화를 이루어야 한다. 현재 관제 서비스뿐만 아니라 보안시장 전체의 동향은 기술이 우선시 되던 분위기에서 제품을 만들어 판매하고, 다음으로 솔루션을 제공하다 이제는 서비스 제공으로 흘러가고 있다.

관제 서비스의 사업 다각화에 대한 시각은

관제서비스 업체가 다른 방향으로 사업 다각화를 하는 것은 보안 서비스와 솔루션의 통합을 이루어나가는 것으로 보아야 할 것이다. 그래서 부정적으로만 바라보는 것은 바람직하지 않다. 그러나 관제 서비스 회사가 수익이 없다고 해서, 경영이 악화된다고 해서 사업을 다각화시키는 것은 결국은 또 다른 질 낮은 제품을 양산하는 것에 불과하다.

국내 관제서비스 기술력의 수준은

아직은 걸음마 단계의 수준이다. 또한 관제서비스를 받고 싶어하는 기업에게 가격 산출의 근거가 없다. 이는 자꾸 서비스 영역을 넓히고자 하기 때문이다. 앞으로의 관제 서비스의 기술 수준은 주먹구구식이 아니라 질이 중요하다. 이는 곧 고객의 만족으로 나타날 수 있다.

관제서비스의 필요성과 기업이 요구하는 관제서비스의 수준은

아웃소싱의 하나로 고객의 욕구가 날로 증가하고 수준이 높아지고 있다. 이젠 시스템의 전문적인 운영이 필요하고, 구축된 시스템을 정확하게 운영해야 한다. 기업이 요구하는 수준은 대기업들에게서 통합보안매니저먼트(ESM)까지 요구하는 사례가 늘어나고 있다. 이는 기업 자체에서 직접 모든 것을 해결하고 하기 위함이다. 그 외 나머지 기업들은 아직은 보안에 대한 마인드가 되어 있지 않아 그저 모든 것을 대행 업체에 맡기는 경우와 보든 사항에 대해 리포팅을 원하는 기업들이 절반씩 차지하고 있다.

현재 관제서비스의 어려운 점은

무엇보다도 보안 인식의 결여이다. 따라서 보안 교육이 필요하다. 또한 고객들은 관제 서비스를 대행해 주는 업체의 담당자가 직접 와서 얼굴을 보이기를 바란다. 관제 서비스 업체들은 대부분이 적은 인원이기에 어려움을 느낀다.