금융권 정보보안과 물리적 망 분리 솔루션

(주) 에프네트 김 영 근 사장

정보통신기반보호법이 7월 1일자로 시행되고, 금융권에 대해 인터넷 뱅킹과 관련한 전자금융거래 표준약관이 9월 시행을 앞두면서 정보보호에 대한 관심이 높아지고 있다.

이러한 정책의 시행은 해당 업계의 발전을 이끌면서 더욱 향상된 정보보호 솔루션과 서비스를 제공할 수 있도록 하는 밑거름이 될 것이라고 판단한다.

또 이같은 정책 시행 목적은 해당 기업이나 시설이 적절한 수준의 정보보안을 실행함으로써 전자적인 침해로부터 발생할 수 있는 사회적인 피해에 대비한다는 측면이 있다.

이를 위해서는 정보보안정책을 지원하는 적절한 솔루션 선택과 보안정책의 엄격한 운용이 중요하다.

특히 요즘 외부로부터의 전자적 침해에 대응하는 것이 갈수록 중요해지고 있는 추세인데 이에 대응하기 위해서는 다양한 보안 솔루션이 조화를 이루어 보안 환경을 구성하는 것이 필요하다.

이 글에서는 외부로부터의 침입에 대응하는 솔루션, 특히 물리적 망 분리 솔루션에 대해 소개하고자 한다.

인터넷 시대에서 보안의 중요성

인터넷은 기존 경제의 흐름을 바꿀 혁명적인 기술로 인정 받고 있다. 많은 사업과 활동이 인터넷에 접속하여 경제활동과 일상활동을 전개하고 있다.

정보보안의 문제가 부수적인 업무가 아닌 기본적인 업무로 등장하기 시작하는 것도 이 인터넷의 대중화에 근거하고 있다. 정보의 기밀성, 가용성, 무결성 등에 대한 위협은 내부자 또는 외부자에 의한 시스템 침입, 정보유출 · 변경 · 훼손, 불법적인 사용 · 복제 등과 지진, 자연적인 재난 등 다양한 측면이 있으나 최근에는 외부로부터의 위협, 특히 해킹이 규모나 심각성에서 점점 더 커지고 있고 사회적으로도 중요한 과제가 되고 있다.

사실 더 많은 네트워크가 인터넷에 접속될수록 또 정보기술이 더욱 대중화 될수록 해킹과 같은 외부로부터의 위협이 늘어날 것이라고 예상할 수 있다.

해킹을 익히기 쉽고, 해킹 도구도 더욱 강력해지면서, 사용하기 쉬워지는 추세는 마치 컴퓨터가 개선되고 대중화되고 더욱 사용이 편리해지는 과정과 같다고 볼 수 있다. 게다가 단순히 해킹에 그치는 것이 아니라 크래킹과 같은 악의적인 범죄 발생이 늘어나는 것도 우려할 만한 일이다.

한국정보보호진흥원의 발표에 따르면 2001년 상반기 해킹 피해는 작년에 비해 275% 늘어난 2,710건이며, 피해 대상의 50%이상이 기업이다.

기업의 피해가 늘고 있다는 것은 기업에 관련된 이해당사자가 많다는 측면에서 우려할 만한 사항이며, 특히 사회적으로 중요한 기능을 하는 금융권 같은 기업이 정보유출이나 서비스 장애 등으로 인해 입는 피해는 해당 기업 뿐만 아니라 사회에도 큰 타격을 주게 된다.

현실적으로 최근 벌어진 중 - 미 사이버 전쟁은 정보침해 현상이 심각한 수준으로 벌어질 수도 있음을 보여주는 사례라고 할 수 있다.

그러나 기업이나 금융권이 이러한 상황을 이해하고 있음에도 불구하고 정보보안을 제대로 구현하는 데는 아래와 같은 어려움이 있다.

첫째, 보안솔루션은 복잡하다. 기본적인 보안지식 뿐만 아니라 개별 시스템에 대해서도 상세한 지식이 필요하다.

또 소프트웨어적인 버그나 보안 정책 등 보안 관련 취약점이 계속 새로 발생하며, 개선되는 해킹 기술을 따라잡기도 만만치가 않다. 표준화가 되어 있지 않기 때문에 다양한 보안 솔루션간의 연계성도 문제가 된다.

둘째, 조직적인 지원이 미흡하다. 정보보안은 경영자의 의지가 뒷받침되어야 하며, 보안 전담 조직도 필요하다.

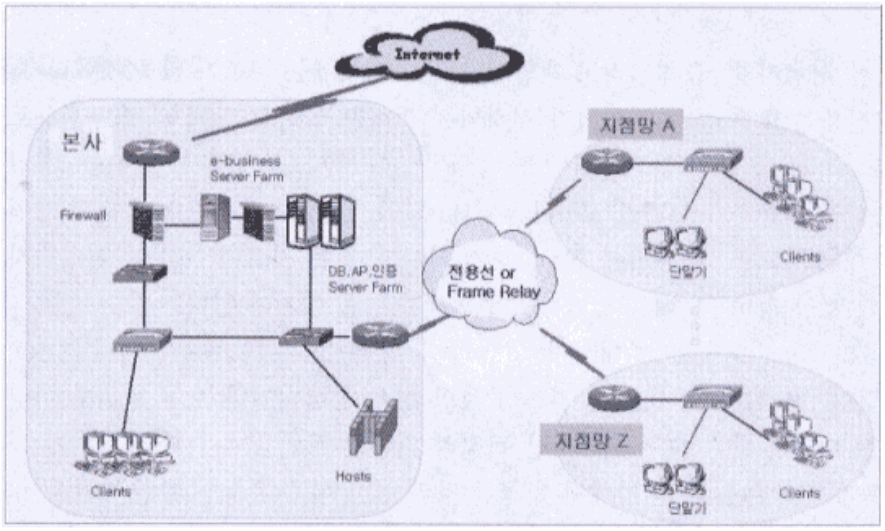
셋째, 지식정보화 사회에서 정보보안이 필수적인 요소

이기는 하지만, 비용효과적이어야 한다는 측면도 무시할 수가 없다는 것이다. 어느 기업도 정보보안 비용이 자신의 부담능력(이익)을 넘어서는 것을 바라지는 않을 것이다. 세계적인 컨설팅 업체인 PwC 자료에 따르면 작년에 해커, 컴퓨터 바이러스를 물리치기 위해 기업이 쏟아부은 돈이 무려 3000억 달러(약 360조원)에 이른다.

이러한 측면에서 최근 은행을 중심으로 관심을 보이고 있는 물리적인 망 분리 솔루션인 넷스위치는 장비는 위와 같은 어려움을 해소하는데 다소 도움을 줄 수 있다.

다른 모든 보안 솔루션과 마찬가지로 이 물리적인 망 분리 솔루션도 그 자체로 완벽한 것은 아니다. 그러나 다른 보안 솔루션들과 조화를 이루어서 더 완벽하면서도 간단하게 보안을 구현해준다고 볼 수 있다.

그림 1 금융권 네트워크 구성도



금융권 네트워크의 특성과 물리적 망 분리 솔루션 활용 방안

금융권의 일반적인 네트워크 구성은 그림1과 같다.

인터넷 뱅킹과 같은 인터넷 비즈니스와 내부 사용자들의 인터넷 사용으로 인해 사설망이 인터넷과 연결되는 것은 선택의 여지가 없는 추세이다. 금융권에서는 전자적 침해로부터 내부 자원을 보호하기 위해 방화벽, 침입탐지 시스템 등을 도입하고 있다.

그러나 해킹 기술이 항상 보안 장비를 앞서는 경향이 있기 때문에 소프트웨어적인 보안 방식은 불의의 침해로부터 100% 안전하다고 볼 수 없다. 물리적 망 분리 장비를 사용할 경우에는 그림 2와 같이 인터넷과 내부망이 분리가 된다.

인터넷과 연결될 필요가 없는 호스트와 서버는 내부망에 위치하게 되고 내부 사용자는 인터넷을 이용할 때는 내부망에 접속할 수 없으며, 또 내부망을 이용할 때는 인터넷에 접속 할 수 없다. 즉, 외부의 해커는 내부 사용자 PC를 경유하거나 내부 네트워크를 경유하여 호스트나 서버 자원에 접근하는 것이 불가능하다는 의미이다.

전산보안 관리자의 입장에서는 물리적 망 분리 장비를 설치함으로써 간단하게 해킹 경로를 차단했다는 것이 큰 도움이 될 수 있다. 개인 PC와 웹 서버의 보안 문제가 남아 있지만, 핵심적인 데이터를 확실하게 보호할 수 있는 수단이 마련된 것이다.

그러나 여기에도 변수가 있는 데, 그림에서도 볼 수 있듯이 인터넷 뱅킹과 같이 내부 자원과 연동되지 않으면 안되는 e-business가 속속 등장하고 있다는 점이다.

인터넷 뱅킹을 담당하는 웹서버는 내부 DB서버와 금융결제원의 인증서버와 통신하여 고객에게 서비스를 제공하게 된다. 즉, 네트워크의 물리적인 측면에서 보면 인터넷 서비스를 하는 쪽이 논리적으로 내부망과 인터넷을 연결시키기 때문에 일종의 백도어처럼 되는 것이다.

따라서 사용자와 연결된 내부 네트워크의 물리적인 망 분리가 의미가 없다고 평가할 수도 있다.

그러나 정보보안은 최대한 침해의 가능성, 즉 불법적인 침투의 확률을 줄여나가는 과정이다. 내부 사용자와 연결된 네트워크는 내부 사용자가 웹 서버 구역보다 다양한 인터넷 서비스를 이용하게 되므로 외부 침입에 더 취약할 개연성이 높다고 볼 수 있다.

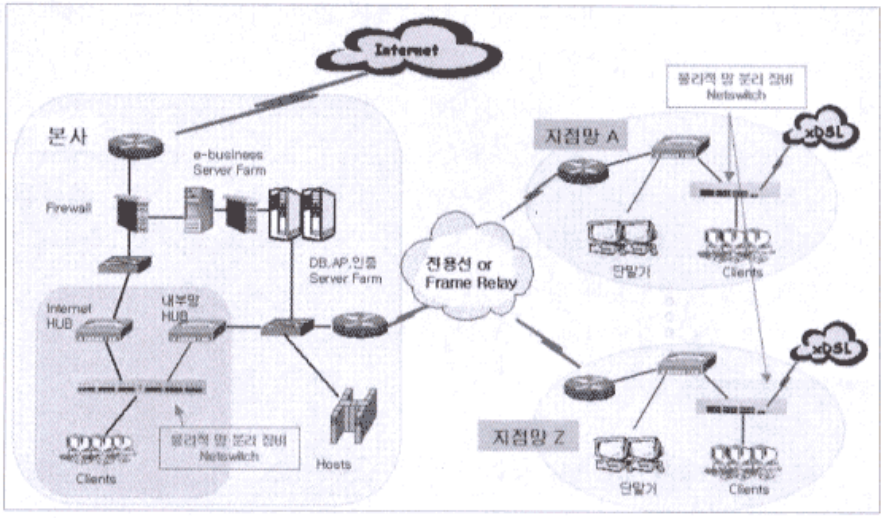
또 점점 더 복잡해지고 많은 서비스가 제공될수록 보안 정책과 수단은 복잡해지고, 비용 부담 뿐만 아니라 논리적 허점이 드러날 가능성이 높아진다.

따라서 정책과 수단을 최대한 단순화 시키고 통제의 범위를 좁히는 것이 중요해진다.

보안 관리자의 입장에서는 핵심 자원에 대한 외부의 침투 가능 경로를 줄여 특정 경로에 대응을 집중하는 것이

전자적 침해의 가능성을 줄이는데 도움이 될 것이다. 물리적 망 분리 솔루션은 자신의 경계에서는 원천적으로 침입을 차단하여 주므로 핵심 내부자원에 대한 정보 보안의 범위를 인터넷 비즈니스와 연관된 경로로 제한할 수가 있다.

그림 2 물리적 망 분리 솔루션



지점망의 물리적 망 분리 솔루션

금융권 지점망의 경우 보안 뿐만 아니라 비용 절감, 인터넷 이용의 활성화 측면에서 물리적 망 분리 솔루션을 도입할 만 하다.

맨 처음의 그림2와 같이 지점에서는 본점을 통해 인터넷을 사용하게 된다. 사용자들의 인터넷 사용량이 늘어날수록 지점 사용자들의 인터넷 접속 속도에 대한 불만이 커지고 전용선 또는 F/R의 대역폭 확대에 대한 압박이 높아진다.

두번째 그림과 같이 물리적인 망 분리 솔루션을 적용하면 저렴한 xDSL망을 지점에 연결하여 사용자들에게 불만 없는 인터넷 이용을 제공할 수 있고 별도의 보안 장비 없이 본사 내부망은 100% 보호된다.

본사와 지점간 회선 대역도 늘릴 필요가 없다. 오히려 기존의 인터넷 트래픽이 줄어들기 때문에 회선 대역을 줄일 수도 있다. 다만 본점과 마찬가지로 사용자들의 PC 보안이 문제가 된다. PC에도 중요한 자료가 보관되는 경우가 많기 때문에 이에 대한 대안이 필수적이라고 할 수 있다.

PC용 보안 S/W를 설치하는 것도 대안이 될 수 있고, 자료를 PC가 아닌 서버에 보관하도록 정책을 수립하는 것도 의미가 있다.

그러나 더 적극적이고 미래지향적인 대안은 SBC (Server Based Computing)를 적용하는 것이다.

물리적인 망 분리 솔루션과 더불어 SBC를 적용하면 회사 업무와 연관된 주요 프로그램이 서버에서 동작되고, 데이터도 서버에 저장되게끔 하여 개인 PC에 저장됨으로써 생기는 해킹,바이러스, HDD의 물리적 손상에 의한 위협을 제거할 수도 있다.

물론 서버의 자료를 개인 PC에 복사 · 저장하지 못하게 할 수도 있다. 그렇게 하면 개인 PC가 침해 사고를 당하더라도 개인적인 자료 이외에는 피해가 없을 것이다.

데이터가 저장되는 서버는 물리적 망 분리 솔루션으로 인터넷과 단절되기 때문이다. 여기서 PC 대신 WBT(Windows Base Terminal)를 적용하게 되면 개인 단말에 HDD가 없어지고 모든 자료가 서버에 저장되기 때문에 단말조차 피해를 입을 여지가 없다.

여태까지 언급한 물리적 망 분리 솔루션이나 SBC, WBT은 기존의 보안 방식이 아니거나 보안 장비도 아니다. 그렇지만 적절히 기존의 보안 솔루션과 결합하게 되면 앞에서 언급한 것과 같이 아주 훌륭한 보안 수준을 구현할 수 있다. 게다가 높은 수준의 정책이나 관리 수단이 필요한 것도 아니기 때문에 관리자들이 집중하여 보안 정책을 구현할 수 있도록 도와준다.

금융권을 예를 들어 설명했으나 정부기관, 연구소나 군, 기업에서도 적용 가능한 솔루션이라고 할 수 있다.

물리적 망 분리 솔루션을 활용하는 것이 예기치 않은 전자적 침해로부터 핵심 자원을 보호하는 주요한 방법이 될 수 있다. 그러나 처음에도 언급했지만 하나의 솔루션이 모든 문제를 해결해줄 수는 없다.

특히 정책이 뒷받침되지 않는 보안 솔루션은 그 기능을 제대로 발휘할 수가 없다. 이제는 기존의 낡은 개념으로부터 탈피하고 근본적인 보안 정책을 수립하여 인터넷 비즈니스 환경에 대비할 때이다.