情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

정보보호 컨설팅 방법론과 적용

안 혜 연*

요 약

정보보호 컨설팅 영역은 최근 정보시스템 분야에서 많은 관심을 끌고 있는 일종에 하나로 모든 영역에서의 정보시스템에 대한 의존도가 높아질수록 더욱 중요도를 더하게 될 것이다. 이글에서는 먼저 1장에서 이러한 정보보호 컨설팅에 대한 필요성 및 개념에 대해서 간단히 설명하고 2장에서는 정보보호 컨설팅의 수행 내용에 대한 조금 더 구체적인 정리를 해보았다. 3장에서는 이러한 수행 내용이 효과적으로 진행되기 위해서 필요한 방법론에 대해서 설명하였다. 또한 4장에서는 정보보호 컨설팅이 실제적으로 어떤 형태로 일어나는지에 대한 서비스별 소개를 하고 있다. 이러한 서비스 모델은 단지 예제일 뿐 모든 고객의 상황과 요구가 다양하므로 훨씬 많은 다양한 서비스 모델이 있을 것으로 생각된다.

Ⅰ. 서 론

정보통신 네트워크의 확산과 개방화에 따라 전세계적으로 e-Business 시대가 도래하고 있다. 21세기 정보화 사회는 정보가 재화의 가치로 인정받고 인터넷이 기업 경쟁력의 핵심 요소로서 부각되는 사회로서, 전세계 모든 나라가 인터넷 상에서의 경제적 우위를 선점하기 위해 동분서주하고 있다. 이미 인터넷 뱅킹이나 전자상거래 등을 통하여 인터넷은 기업과 고객간의 경제활동 매개체로서 그 중심에 서게 되었으며, 앞으로 더욱 많은 분야에서 인터넷과 결합된 서비스들이 활성화될 것으로 기대된다. 정보통신 분야에서의 표준화는 정보통신 시장의 국제적인 개방화, 다양화, 경쟁화 추세에 의하여 사용자에게 정보통신기기 및 시스템간의 상호연동을 원활하게 하는 것은 물론 국가 사회적으로 불필요한 중복투자를 방지하여 적은 비용으로 고도의 효율을 획득하기 위한 방법이다. 특히, 정보보호 분야에서의 표준화는 정보의 가치가 점차 높아지고 이들 정보에 대한 보호의 필요성이 커짐에 따라 그 중요성이 부각되고 있으며 선진국에서는 자국의 국가 안보 및 국익을 위해서 국제 표준의 선점을 통한 우위확보 경쟁이 매우 치열한 실정이다.

그러나, 인터넷은 국가발전의 성패를 좌우하는 중요 변수로서의 역할을 하는 한편, 자체적 결함으로 인해 많은 취약성과 위협을 내포하고 있다. 매년, 인터넷의 신분노출, 은폐가능성과 정보 접근의 용이성을 이용하여 많은 해킹 사고가 발생하고 있으며, 컴퓨터 관련 범죄가 기하급수적으로 증가하고 있는 실정이다. 이는 인터넷을 통한 해킹 기술의 개방 및 최첨단 해킹 툴의 개발 증대로 인해 초보자들도 쉽게 해킹할 수 있는 환경이 조성됨에 반하여 많은 중요 정보들이 보호되지 못한 채 인터넷 상에 방치되어 있는 실상에서 비롯된다고 볼 수 있다.

이러한 위협이 전자상거래나 금융 거래에 미치는 영향을 고려해본다면 정보보호의 시급성 및 필요성을 간과할 수는 없다. 정보보호란 데이터 및 시스템을 고의적 또는 실수에 의한 불법적인 공개(노출), 변조, 파괴로부터 보호하는 것이다. 정보보호가 보장되지 않은, 빈약한 전자상거래 환경에서는 고객의 개인정보와 결재 정보, 심지어 계좌 번호나 신용카드 번호까지도 쉽게 유출될 수 있으며, 이로 인하여 발생하는 피해 또한 심각한 수준에 이를 수 있다.

인터넷 기반 사업에서 기업 정보시스템의 신뢰성 확보는 경쟁력 우위 선점과 사업적 성공을 위한 중요 가치를 지닌다고 볼 수 있다. 정보시스템의 신뢰성 문제는 기업들의 정보보호에 대한 많은 관심과 노력을 내포하고 있으며, 점차 심화되고 있는 보안

* (주)시큐어소프트(ahn@securesoft.co.kr)

사고를 줄이고 안전한 인터넷 서비스를 구축하기 위해서는 정보보호에 대한 투자가 필수적이라 하겠다.

기업 정보시스템의 신뢰성을 보장하고 안전한 e-business 환경을 조성하기 위해서는 기업 네트워크, 시스템, 어플리케이션 등 다양한 측면에서 효율적인 정보보호 체계를 구축하는 것이 최우선 과제이다. 허가받지 않은 사용자의 네트워크 접근을 막고 전송 데이터의 기밀성 보장 및 변경 방지를 위해서는 네트워크 보안을 확립해야 하며, 저장된 중요 정보의 기밀성을 방지하고 불법 사용자에 의한 정보의 변경이나 파괴를 방지하기 위해서는 시스템 보안을 수립해야 한다. 또한, 어플리케이션상의 데이터들에 대한 기밀성, 무결성 등을 확보하기 위해서는 어플리케이션 보안이 수행되어야 한다.

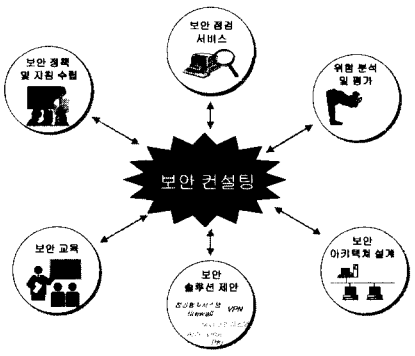
Security func. / Target	Authentication	Access Control	Confidentiality	Integrity	Non Repudiation
N/W	• ID / Password • OTP	• IP filtering • Protocol filtering • Monitoring	• IP Tunneling	• IP Tunneling	
System	• ID / Password • Smart card • Biometrics	• Role-based access control • Security attribute setup • Pattern Decton	• File encryption • Secure DBMS	• File Integrity Check • Secure DBMS	
Appl.	• ID / Password • Smart card • Digital Certificate • Biometrics	• User-type based access control	• Data encryption	• Digital Signature • CheckSum • MAC	• Digital Signature

〔그림 1〕 보안 구현 기술

이와 같이 보안이 필요한 각 영역별로 여러 다른 보안 기능을 구축하기 위한 기술들을 그림 1.과 같이 정리해보았다. 예를 들어, 기업 정보시스템의 비인가된 접근을 막기 위해서는 일회용 패스워드(OTP, One Time Password), 스마트 카드, 바이오메트릭스와 같은 사용자 인증 기술이 요구되며, 허가되지 않은 정보 접근을 차단하고 정보의 무결성을 보장하기 위해서는 접근통제(Access Control) 기술, 침입차단시스템(firewall), 그리고 침입탐지 시스템 등이 필요시된다. 또한, 전자상거래나 금융거래 시 네트워크를 통해 전송되는 금융정보의 기밀성 보호 및 부인방지를 위해서는 PKI를 중심으로 한 사용자 인증, 암호화, 전자서명 등의 암호 기술이 필요하다고 할 수 있다.

이에 따라 국제적으로 정부 및 민간기관을 중심으로 정보보호 기술에 대한 표준화 요구가 급증하면서 정보보호에 관한 표준화 작업이 활성화되고 있다.

이러한 측면의 대표적인 국제적 노력으로 ISO/IEC JTC 1 SC27, ITU-T, IETF(Internet



〔그림 2〕 보안 구현 기술

Engineering Task Force) 등에서 구체적인 정보보호 표준화 작업이 진행되고 있으며 전자상거래, 인터넷 보안을 위한 정보보호 표준화를 활발하게 추진중이다[1][2][3][4][5]. 특히 IETF는 인터넷의 통일성과 표준을 유지하기 위해 설립된 조직으로 인터넷 표준의 개발 및 선정을 목적으로 정부기관, 업계, 학계 등 다양한 분야의 연구개발자들로 구성된 개방된 형태의 국제단체이다. IETF에서는 정보보호 분야를 포함하여 표준화 분야별로 워킹그룹을 결성하여 표준화 활동을 수행하고 있다[6][7][8][9].

국내에서도 정보화 추진과 더불어 다양한 정보통신망이 상호 연동되고 정보보호 서비스가 구축되어감에 따라 정보보호기술 표준화에 대한 필요성이 급증하였고 핵심 기술과 응용 기술 분야에 대한 표준화를 추진하고 있다. 정보보호 기술 표준화는 국제 표준 동향을 수용하면서 국내에 적합한 방식으로 이루어져야 한다. 국내에 적합한 표준화 체계 확립과 표준 제정을 위해 국제 표준화 동향 분석은 필수적이라 하겠다.

본고에서는 인터넷 보안 표준화의 핵심 기구인 IETF의 조직구조 및 표준화 절차를 소개하고 정보보호 분야의 워킹그룹에서 수행하고 있는 표준화 활동을 소개한다.

II. 정보보호 컨설팅의 수행 내용

1. 정보보호 정책 수립

보안 정책은 조직의 정보자산을 어떻게 관리하고 보호할 것인가에 대한 지침 및 절차를 기술해 놓은 문서이다. 보안 정책은 조직의 정보자산을 안전하게 보호하고 효율적으로 관리하기 위해 최우선적으로

수립해야 하는 항목으로, 모든 정보보호 행위의 기반이 된다.

보안 정책 수립시에는 기업의 사업적 목적 및 서비스 운영환경과 보안 요구사항과의 관계를 고려하여 기업의 보안 요구사항을 식별해야 하며, 기업이 보유하고 있는 기존의 보안 정책이 기업의 현황에 적합한지 실제로 일관성 있게 적용되는지를 평가해야 한다.

2. 보안 점검 서비스

보안 점검 서비스는 기업의 정보시스템이 안고 있는 취약점을 진단 및 분석하여 이에 대한 해결책을 제시하고 향후 기업의 안전한 정보 보안이 유지될 수 있도록 지원하기 위한 것이다. 이는 두 가지 방법으로 수행될 수 있다. 첫번째 방법은 취약점 분석 도구를 이용하여 네트워크, 시스템, 데이터베이스, 어플리케이션의 취약성을 점검 및 분석하는 것이다. 이의 결과는 취약점 분석 도구의 성능에 의존되지만 분석이 객관적이고 용이하다는 장점을 가진다. 두번째 방법은 보안 전문가에 의한 모의 침입 테스트로서, 실제로 기업 정보시스템 침입을 시도하여 시스템 관리자의 공격 탐지 및 대응 능력을 평가하고 네트워크 감사 및 모니터링의 효율성을 진단한다.

상호 보완적인 이 두 가지 방법을 병행할 때 더욱 정확한 정보시스템의 취약점 점검을 수행할 수 있을 것이다.

3. 위험 분석 및 평가

위험 분석은 위협분석, 취약성 분석, 기존 보안 대책 분석을 통해 보호되어야 할 정보시스템의 위험 수준을 판단하고, 이에 대한 대응책을 도출하여 정보보호 수준을 향상시키기 위한 것이다. 위험 분석은 Check List를 통하여 보안 점검을 수행하는 기본통제(baseline control)를 이용하거나 위험 분석 도구를 통하여 기업의 위험 수준을 평가할 수 있다.

4. 네트워크 보안 아키텍쳐 설계

기업 인프라를 통하여 기업의 중요 정보가 관리되고 분배됨에 따라 기업의 현황 및 사업 목적을 고려한 최적의 네트워크 보안 아키텍쳐의 구현은 필수적이라고 볼 수 있다. 따라서, 웹 기반 또는 클라이언트/서버 환경에서 기업 정보시스템의 신뢰성 향상을 위해 네트워크 자원의 효율적인 확장 및 변경 관리를 지원하는 과학적인 솔루션이 제공되어야 한다. 즉, 컴퓨터 환경 및 서비스 환경 변화에 따라 네트워크 아키텍쳐 및 보안시스템의 재구축이 용이하도록 확장가능하고 효율적인 네트워크 보안 아키텍쳐가 설계되어야 한다.

5. 보안 솔루션 제안

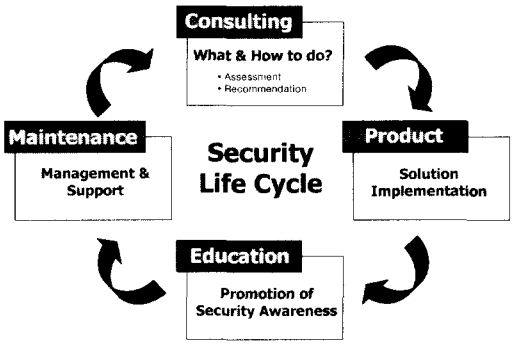
기업은 각기 다른 정보시스템을 구성하고 있으며 사업적 환경이 상이하다. 각종 보안 솔루션을 평가하여 기업의 사업적 및 보안적 요구사항과 예산에 적합한 보안 제품을 선정하는 것은 안전한 기업 인프라를 구축하기 위해 매우 중요한 요소라 할 수 있다.

6. 보안 교육

부주의나 고의에 의한 보안 사고를 최소화시키고 사원들의 정보보호에 대한 인식 제고를 위해서는 보안 교육을 실시해야 한다. 보안 교육은 일반 사원을 대상으로 하는 보안 기본 교육과 시스템 관리자 및 보안 관리자를 대상으로 하는 보안 전문 교육으로 분류될 수 있다. 보안 기본 교육은 사원들의 보안 수준향상을 도모하기 위한 것으로, 정보보호의 이해와 보안 정책 및 보안 책임 관련 사항에 대한 내용을 다루며, 보안 전문 교육은 보안 시스템 관리 및 유지 보수 등에 관한 사항으로 필수적이고 전문적인 보안사항을 다루게 된다.

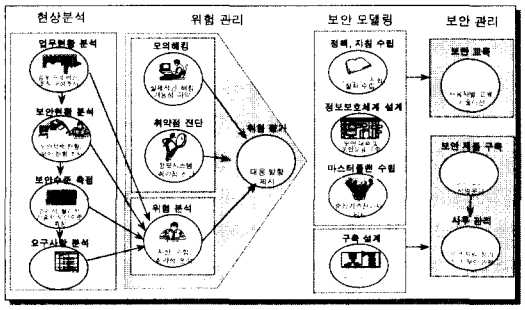
III. 정보보호 컨설팅 방법론

개방 네트워크 환경에서 조직이 효과적인 정보보호를 수행하기 위해서는 우선 보안 컨설팅을 수행하여 기존의 조직 정보시스템에 대한 총체적 진단 및 분석을 실시해야 한다. 그 다음에, 보안 컨설팅에 의해 권고된 사항을 기반으로 안전한 조직 정보시스템을 구축하고 정보보호에 대한 인식을 제고하며 지속적으로 보안이 유지될 수 있도록 지원 및 관리해 주는 행위가 요구된다(그림 3). 특히 인터넷을 이용한 서비스 체계를 구축하고 있는 조직에서 정보보호의 중요성은 더욱 부각되고 있는 실정이며 조직 정보시스템에 대한 위험을 최소화하기 위해 보안 컨설팅이 필연적으로 수행되어야 된다고 볼 수 있다.



〔그림 3〕 효과적인 정보보호 체계

보안컨설팅은 그림 4에서 보여지는 바와 같이 현상분석, 위험 관리, 보안 모델링, 보안관리의 네 단계로 수행된다.

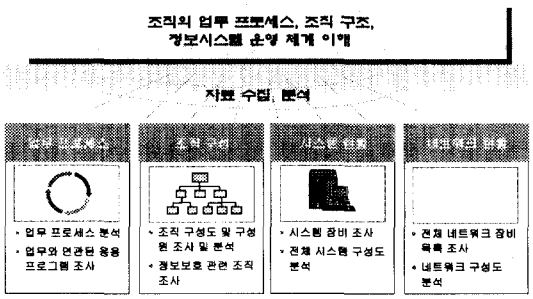


〔그림 4〕 정보보호 컨설팅 단계

1. 현상 분석

보안 현황 분석은 보안컨설팅에서 가장 우선적으로 수행해야 하는 단계이다. 이는 이 후 단계의 기초가 되는 자료 수집, 현황 조사, 요구수준 파악 등을 포함하는 단계로, 조직의 환경에 꼭 맞는 보안 컨설팅을 수행하기 위해 필수적으로 요구되는 과정으로 볼 수 있다.

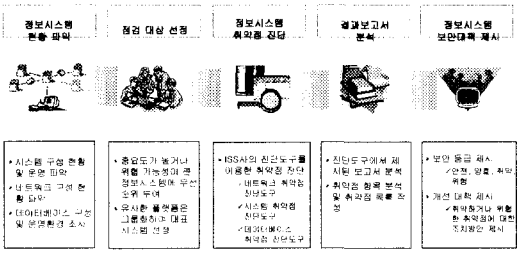
이 단계는 업무현황 분석, 보안현황 분석, 보안수준 측정, 요구사항 분석 단계로 분류된다. 업무 현황 분석 단계에서는 조직의 일반적인 업무 상황을 파악하고, 조직의 업무 프로세스 및 보안 관련 조직을 조사한다. 보안 현황 분석 단계에서는 조직의 전반적인 보안 현황을 조사한다. 보안 수준 측정 단계에서는 선행된 두 단계에서 수집된 자료 및 설문을 통한 조직의 보안 수준을 측정한다[10]. 요구사항 분석 단계에서는 조직의 보안 요구사항 분석 및 조직 환경에 적합한 보안 우선순위를 식별한다.



〔그림 5〕 현황 분석 단계

2. 위험 관리

조직의 보안현황 및 보안 요구사항이 파악되면 조직의 응용 서비스 및 정보시스템에 대한 위험을 분석하고 취약점을 점검하여 조직 전산망 안고 있는 문제점을 파악한다.



〔그림 6〕 위험 관리 단계

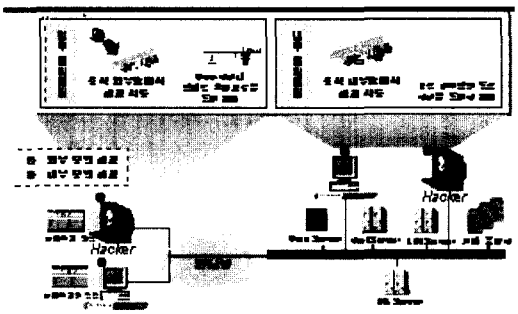
2.1 모의 해킹 및 취약점 진단

모의 해킹 및 취약점 진단 단계에서는 조직의 네트워크, 시스템, 데이터베이스의 취약점을 진단하고 분석하는 것으로서, 취약점 분석 도구를 이용하는 방법과 해킹 전문인력을 이용한 실제 침입시험 방법의 두 가지 방법으로 수행될 수 있다.

네트워크 취약점 진단은 네트워크 장비의 취약점을 진단하여 DDOS(Distributed Denial Of Service) 공격을 포함한 다양한 공격에 대한 위험을 최소화할 수 있는 방안을 마련하는데 도움을 줄 수 있으며, 시스템 취약점 진단은 시스템 운영체제의 수많은 부분을 점검하여 호스트 내부의 취약점을 점검하고, 데이터베이스 취약점 진단은 데이터베이스 시스템이 노출하고 있는 잠재적인 보안 위험을

자동으로 검증하여 조직 응용 서비스의 취약점 대응 방안을 모색하는 것을 지원할 수 있다.

또한 조직 정보시스템에 대한 모의 해킹인 실제 침입 시험을 수행하여 네트워크 및 시스템에 대한 감사기록, 모니터링, 침입탐지, 대응 상황을 점검한다. 이 실제 침입 시험을 통하여 조직 정보시스템 안전성을 평가할 뿐만 아니라 시스템 관리자가 공격을 효과적으로 탐지하고 대응할 수 있는 능력을 평가하고 및 보안시스템의 효율성을 분석할 수 있다.



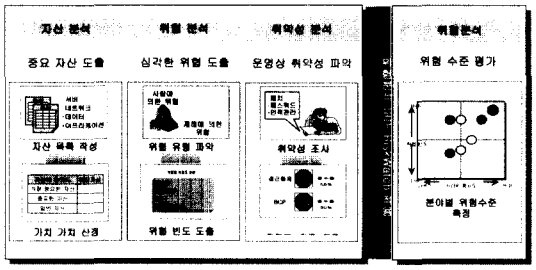
〔그림 7〕 모의 해킹

2.2. 위험 분석 및 위험 평가

위험 분석 단계에서는 조직의 중요 정보시스템과 그 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대하여 조직의 정보시스템의 취약성을 분석하고 이로 인해서 예상되는 손실을 분석한다.

위험 분석은 IT 자산을 식별/분류하고 자산가치를 평가하는 자산분석 단계, 위협 식별/분류 및 위협 발생가능성과 손실크기를 측정하는 위협분석 단계, 취약성을 점검하고 취약성 수준을 평가하는 취약성 분석단계를 통하여 보호되어야 할 정보시스템의 위험 수준을 판단하고 이에 대한 대응책을 도출함으로써 조직의 정보보호 수준 향상을 도모한다.

자산 분석은 보호해야 할 전산자원을 식별하고 체계적으로 분류함으로써, 소유하고 있는 자산들의 가치를 평가하는 기본 단계로, 조직의 자산 가치를 확인하여 정량화하는 작업을 수행한다. 위협 분석 단계에서는 조직의 정보 자산에 대한 위협을 식별하고 분류해서 발생빈도와 손실크기를 측정한다. 취약성 분석 단계에서는 각 자산에 대한 취약점을 파악하고 분류하여 위협을 감소시키는 것을 목적으로 하며, 이 단계에서는 식별된 각 정보 자산들에 대하여 구체적인 취약성을 조사, 분석한다



〔그림 8〕 위험 분석 단계

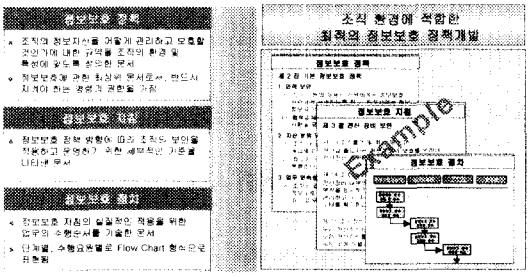
위험 평가단계에서는 모의해킹, 취약성 분석, 위험 분석을 기반으로 조직의 위험 수준을 평가하고, 위험도를 산출한다.

3. 보안 모델링

3.1 정책, 지침 수립 및 체계 설계

정보보호 정책 수립 단계에서는 조직의 정보 자산을 어떻게 관리하고 보호할 것인가에 대한 구체적인 행위를 규정하는 정보보호 정책, 지침, 절차를 제시한다.

정보보호 체계설계단계에서는 현상 분석 단계와 위험관리 단계에서 도출된 관리적, 물리적, 기술적 이슈들을 분류하고 각 분야별 보안대책 방안을 제시함으로써 조직의 정보보호체계를 수립한다.

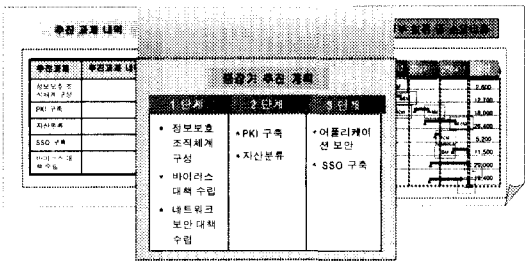


〔그림 9〕 정보보호 정책 및 지침 수립 단계

3.2 마스터플랜 수립 및 구축 설계

마스터플랜 수립 단계에서는 보안 대책 및 보안 모델에서 제시한 정보보호체계 구축을 위한 중장기적인 계획을 수립한다.

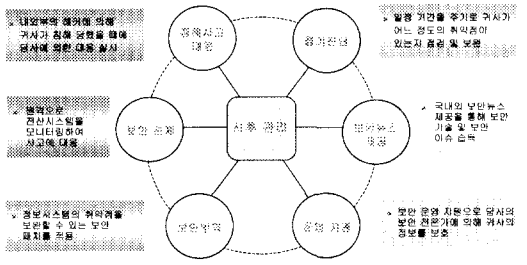
구축 설계 단계에서는 정보보호체계 구축을 위한 보안 솔루션 평가 기준을 제시하고 조직의 실정에 맞는 보안 시스템 구축을 지원한다.



〔그림 10〕 마스터 플랜 수립 단계

4. 보안 관리

보안 관리 단계에서는 보안대책이 정상적으로 유지되는지의 관리 여부, 시스템 및 환경의 변화에 보안 요구 사항의 변경관리 체계의 구축과 보안 계획에 따른 보안 수준의 유지와 모니터링 구축, 보안 사고에 대한 대응체계구축 등 유지보수 확인과 고객사에 대한 보안교육, 보안 기술 이전 및 사후관리를 실시한다.



〔그림 11〕 사후 관리

IV. 정보보호 컨설팅의 적용

1. 보안 컨설팅 서비스 유형

현재 컨설팅 업체에서 제공하고 있는 컨설팅 서비스를 유형을 고객에게 제공되는 서비스 내역의 관점에서 살펴보면 취약점 진단 서비스, 어플리케이션 보안 모듈 설계, 전자상거래 보안, 취약점 분석 및 안전한 인트라넷 설계, 통합 보안 모듈 구축 등의 다섯가지로 나누어 볼 수 있다.

2. 취약점 분석 서비스

2.1 정의

취약점 분석 도구를 이용하여, 정보시스템이 안고 있는 보안 취약점을 진단 및 분석하여 문제 해결책을 제공하며, 또한 향후의 안전한 정보보호 유지를 위한 제안한다. 또한, 보안 전문가들이 정보시스템에 대한 실제 침입 시험을 수행하여 고객들이 실제로 취약성 및 피해가능성을 인식하도록 하며, 네트워크 및 시스템에 대한 감사기록, 모니터링, 침입탐지, 대응 상황을 점검하여 고객의 정보시스템의 보안 상황을 파악한다.

2.2 기대 효과

내부환경 측면에서는 네트워크 장비 및 중요 시스템의 취약성 점검으로 더욱 신뢰적인 보안 시스템 운영 환경을 지원할 수 있고, 대외환경 측면에서는 신뢰성있는 전산자원으로 대외 경쟁력을 확보하고, 사이버 테러에 대비하여 기업의 정보시스템에 대한 보안 강화를 기대할 수 있다.

3. 어플리케이션 보안 모듈 설계

3.1 필요성

인터넷을 이용한 서비스의 활성화와 E-business의 도래로 인터넷은 기업의 핵심 요소로서 기업 서비스 향상을 도모하고 기업과 고객간의 유대관계를 활성화시키는 반면, 네트워크를 통한 범죄는 증가하고 있다. 따라서 고객들은 제품 및 서비스에 보안 기능을 요구하게 되었다. 그러나, 어플리케이션 개발자들은 보안 관련 지식의 부족으로 고객들의 요구에 맞는 제품 및 서비스를 개발하는데 어려움이 따르는 것이 현실이다.

이와 같이 이유로 어플리케이션 보안 모듈 설계에 있어서 보안 전문가에 의한 컨설팅이 필요하다.

3.2 어플리케이션 보안 모듈 설계

어플리케이션 보안 모듈 설계가 필요한 서비스는 가용성 및 신뢰성 보장이 요구되는 서비스와 암호, PKI, 접근통제, 그 외 보안 기능을 필요로 하는 어플리케이션 서비스, 해킹, DOS(Denial of Service) 공격을 비롯한 컴퓨터 범죄에 민감한 인터넷 서비스가 있다.

어플리케이션 보안 모듈 설계는 서비스에 대하여 안전한 방안을 제시하고 보안 모듈을 설계하여 서비

스의 안전성을 확보하는 데 있으며 고객이 제품 및 서비스 개발시에 보안 기능을 고려하여 설계를 할 수 있도록 컨설팅을 수행한다.

3.3 어플리케이션 보안 모듈 검토

어플리케이션 보안 모듈 검토란 이미 운영되고 있는 어플리케이션이 안전하게 운영되고 보안 기능을 충분히 수행하는지 검토하는 것으로서 어플리케이션의 기능적 요구사항(functional requirement)에 대한 보안성 검토와 어플리케이션의 보안 모듈에 대한 타당성을 검토한 후 적절한 대책을 제시해 주는 것이다.

4. 전자상거래 보안

4.1 전자상거래 보안 컨설팅

인터넷의 활성화와 정보화 사회의 진전으로 다양한 서비스에 대한 요구가 증가하고 있다. 기존의 사회에서 이루어지는 모든 서비스가 사이버 공간으로 이동함에 따라 발생하는 것으로서 개인식별, 인증, 전자서명, 전자결재, 전자화폐, 전자지불, 전자투표 등 다양한 기능을 요구하게 되었다.

전자상거래 보안 컨설팅이란 PKI(Public Key Infrastructure) 기술을 사용하여 전자상거래에서 요구되는 서비스를 제공하는 것을 말한다.

PKI 솔루션은 다양한 PKI 제품과 서비스, 사업의 요구사항에 따라 복합적인 적용이 이루어져야 하며, 비즈니스 모델에 맞는 최적의 PKI를 적용해야 한다.

4.2 PKI 서비스의 내용

PKI 서비스의 단계별 내용은 기업의 목적에 맞는 PKI을 구축하기 위한 비즈니스 요구사항 분석하고, 적절한 PKI 구축 방법과 범위, 절차, 우선순위, 정책 등 제시한다. 또한 빠른 사업 환경의 변화와 기술의 변화에 쉽게 적용할 수 있는 모듈화 되고 유연성이 있는 PKI 솔루션을 개발하며 고객에게 가장 적합한 최적의 솔루션을 제시하고, PKI 제품을 평가하고 고객의 어플리케이션과 상호작용에 대한 평가와 확장성에 대해 테스트한다.

5. 취약점 분석과 안전한 인트라넷 설계

5.1 취약점 분석 및 안전한 인트라넷 설계

취약점 분석 및 안전한 인트라넷 설계 패키지는 취약점 분석을 통하여 고객 정보 시스템의 취약점을 진단 및 분석하며 실제 고객의 요구사항을 분석하여 보안 솔루션 선정부터 보안 아키텍쳐 설계 및 구현에 이르는 최적의 인트라넷을 구축할 수 있는 서비스를 제공한다.

5.2 안전한 인트라넷 구축

안전한 인트라넷 구축이란 네트워크, 시스템, 데이터베이스 취약점 점검 및 분석 내용을 기반으로 조직의 안전한 인트라넷을 구축하는 것이다. 이것은 조직의 요구사항을 최대한 수용하여 비용 효율적이고, 조직의 환경에 적합한 보안 대책 방안을 수립한다.

안전한 인트라넷 구축 방법은 기업의 환경에 적합한 최적의 보안솔루션을 제시하는 것과 중요 정보시스템 및 네트워크의 보안 체계를 구축하는 보안 아키텍쳐 설계 및 구현이다.

5.3 보안 솔루션 선정 및 제안

조직의 사업 및 보안적 요구사항과 예산에 적합한 보안 제품을 선정하고 제안함으로써 안전한 인트라넷을 구축하는 것이다.

5.4 보안 아키텍쳐 설계 및 구현

비용 대비 효율, 보안요구사항, 사용 편리성을 고려하여 최적의 보안 아키텍쳐를 설계하고 구현하는 것이다.

조직의 현황 및 사업 목적을 고려한 최적의 네트워크를 설계 및 구현하고, 네트워크 아키텍쳐 보안에 대한 점검하며, 네트워크 자원의 효율적인 확장 및 변경 관리를 지원하는 과학적인 솔루션을 제공하게 된다.

또한 웹서버, DB서버를 비롯한 조직의 중요 서버 보안체제 구축하고, 전산환경 변화에 따른 네트워크 및 보안시스템 재구축하게 된다.

6. 통합 보안 모델

통합 보안 모델이란 보안 컨설팅의 모든 것이라 할 수 있다. 보안 정책부터 교육까지 기업에서 요구하는 모든 보안 요소를 다루는 것이다.

통합 보안 모델은 일관성 있게 보안을 적용/유지할 수 있는 정책의 수립, 조직의 요구사항 분석과 위험 분석을 통한 보안 대책 수립과 보안 시스템의 지속적인 운영을 유지할 수 있는 교육을 포함한 솔루션을 제공하는 것이다.

VI. 결 론

지금까지 현황 분석, 위험 관리, 보안 모델링, 보안 관리로 이어지는 보안 컨설팅의 방법론과 적용에 대하여 살펴보았다.

보안 컨설팅은 조직의 신뢰성 보장을 위해 조직이 무엇을, 어떻게 해야 하는가에 대한 해결책을 제시하는 것이다. 즉, 이는 조직의 보안현황 및 요구사항을 파악하고 정보시스템에 대한 위험을 진단, 분석, 평가하여 조직이 취해야 하는 최적의 보안 대책 및 통합 보안 체계를 제시하며 지속적으로 보안 체계를 유지할 수 있는 방안을 제시하는 것이다.

보안 전문 인력에 대한 요구는 몇 년간 급속도로 증가해 왔지만 보안 담당자의 수는 크게 증가하지 않았으며, 이것이 보안 컨설팅의 수요를 촉진시키는 가장 큰 이유라 할 수 있다.

앞으로, 보안 컨설팅은 보안산업의 주요 분야로 급부상하게 될 것이다. 이는 금융이나 전자상거래를 비롯한 많은 사회 활동들이 사이버 세계로 전이되면서 대규모 데이터 센터의 구축이 활성화되고, 이의 신뢰성 및 가용성 보장을 위해 체계적이고 통합적인 정보보호 체계 확립이 필요하기 때문이다. 기업들 및 주요기관들은 안전한 정보 인프라 구축을 위한 선행과제로서 보안 컨설팅을 인지할 것이며, 기업 정보시스템 보안 관리를 위해 지속적으로 보안 전문 업체에 의뢰하는 추세가 될 것이다.

참 고 문 헌

[1] ISO/IEC JTC1/SC27, TR 13335-1, Guidelines for the Management of IT Security(GMITS): Part 1 - Concepts and Models for IT Security, 1996

[2] ISO/IEC JTC1/SC27, DTR 13335-2, Guidelines for the Management of IT Security(GMITS): Part 2 - Managing and Planning IT Security, 1997

[3] ISO/IEC JTC1/SC27, DTR 13335-3, Guidelines for the Management of IT Security(GMITS): Part 3 - Techniques for the Management of IT Security, 1998

[4] ISO/IEC JTC1/SC27, DTR 13335-4, Information technology - Security techniques - Guidelines for the management of IT security(GMITS) - Part 4: Selection of safeguards, 1999

[5] ISO/IEC JTC1/SC27, WD 13335-5, Guideline for the Management of IT Security(GMITS) - Part 5: Safeguards for External Connections, 1999

[6] IETF RFC 1281 Guidelines for the Secure Operations of the Internet, 1991

[7] IETF RFC 1421 Privacy Enhancement for Electronic Mail, 1993

[8] IETF RFC 1244, Site Security Handbook, 1995

[9] IETF RFC 2196 Site Security Handbook, 1997

[10] CSI IPAK(Information Protection Assessment Kit) Checklist

〈著者紹介〉

안 혜 연 (HYE YEON AHN)

정회원

1981년 2월 : 이화여자대학교 수학과 학사

1983년 2월 : 이화여자대학교 대학원 수학과(전산전공) 석사

1994년 2월 : 메사츄세츠주립대학 전기전산기공학 박사

2000년 1월 ~ 현재 : (주)시큐어소프트 기획본부장 겸 연구소장

1994년 5월 ~ 1999년 12월 : 삼성 SDS 수석연구원

1982년 12월 ~ 1987년 6월 : 한국데이타통신 주식회사(DACOM) 연구원

1995년 ~ 현재 : (사)한국여성정보인협회 이사

1998년 ~ 1999년 : 정보보호산업협회 이사

관심분야 : 정보보호 컨설팅, 무선 PKI, 통합보안관리