금융분야의 관리적·기술적인 정보보호 강화를 위한 정보보안요구사항 분석

김관겸*, 박진섭*, 이기정*
*대전대학교 컴퓨터공학과
e-mail:karud@hanmail.net

Analysis of Information Security Requirements for Strengthening Administrative·Technical Information Security in Financial Field

Gwan-Gyeom Kim*, Jin-Sub Park*, Ki-Jung Lee*
*Dept of Computer Engineering, Daejeon University

요 약

금융권 정보보안 강화를 위해 관리적·기술적 측면의 정보보안 요구사항을 분석하였다. 금융분야는 IT법규 준수가 중요하기 때문에 기반시설의 취약점 진단을 위해서 사용되는 정보보호수준평가의 통제분야에 IT법규 중 법률 및 정보보호활동 내역을 포함되어야 하며, 자산보호 및 서비스 연속성 보호를 위해 웹 애플리케이션의 취약점을 보호해야 한다.

1. 서론

정보통신 기술이 급속도로 발전하고 있는 지금 정보화 역기능 피해도 날로 심각해지고 있다. 해킹, 바이러스, 피싱/파밍, 불법 스팸 DDOS등 다양한 형태로 나타나고 있으며, 개인의 프라이버시와 기업의 정보 및 정보시스템과 같은 자산들이 위협받고 있다.

2009년 인터넷이용실태 조사에 따르면 이용자의 41.2%가 인터넷 뱅킹을 통해 금융 서비스를 받고 있는 것으로 조사되었다. 전자거래가 일상생활에서 보편화되고 있는 지금 금융권에서는 전자거래의 안전성을 강화하기 위해 금융감독위원회 허가 하에 금융보안 연구원을 설립하였으며, 「전자금융거래법」을 강화하여 전자금융 범죄에 대응하고 있다.

금융권의 보안 실태는 제 1금융권, 제 2금융권은 모두 정보통신기반시설로 지정돼 있으며, 기반보호 법에 따라 정보보호 전문업체 등을 통해 기반시설 취약점 진단을 실시한다. 이때 관리적인 측면은 정보보호수준평가를 통해 평가되고, 기술적인 측면은 정보보호 전문업체의 취약성 분석도구를 이용한다.

하지만 정보보호수준평가는 다양한 특성을 지닌 기반시설 지정이 확대됨에 따라 각 기관 특성별 정보보호 수준을 평가 하는데 한계점이 있으며, 기술적인 측면은 새로운 위협이 나타남에 따라 지속적인 관리가 필요하다.

2. 관리적 정보보안 요구사항 분석

2007년 1월 1일부로 「전자금융거래법」이 시행되면서 「전자금융감독규정」도 전면 개정됨에 따라 전자금융거래에 대한 법률관계가 보다 명확해졌다.

「전자금융감독규정시행세칙」을 보면 금융분야의 정보보호 요구사항을 보다 명확하게 파악할 수 있다. 시행세칙 내에는 정보통신망, 공개용 웹서버 등에 대한 해킹 및 장애에 대한 감독규정이 명시되어 있고, 전자금융업무 및 정보기술부문의 안전성 확보를 위해 인력(조직, 위부위탁), 시설(전산실), 정보기술부문(단말기, 전산자료, 정보처리시스템)등에 대한 정보보호활동내역이 수록되어 있다.

전자금융은 그 특수성과 복잡성으로 때문에 전자금융감독규정 해설서 및 검사 매뉴얼을 읽을 필요가 있으며, 회계관련 규정이 필요한 경우 해외에서 요구하는 바젤II 및 GLBA, SOX 등도 참고해야 필요가 있다. 특히 IT검사 매뉴얼은 주요정보통신기반시설에 대한 평가에 용이한 자료가 포함되어 있다.

다음의 <표 1>은 정보보호수준평가의 평가항목 중 IT법규 준수를 위해 평가되어야 할 항목들과 통제분야의 맵핑표이다.

<표 1> 정보보호수준평가 통제분야와 금융법률 및 매뉴얼

1. 정책 및 절차수립	제15조(정보화 계획 수립 및 운영)
4.유지보수	○ 제10조(정보처리시스템 보호대책) ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 3.시설 및 장비, 장비의 유지보수 ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 6.통신망, 통신망 구축현황관리
5.매체보호	○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 4.운영통제, 출력자료 분배통제 ○ 제9조(전산자료 보호대책)

6.보안인식과 교육	○ 제3조(인력 및 조직 관리) ○ 제19조(비상대책 수립·운용)
7.업무연속성	○ 제9조(전산자료 보호대책) ○ 제14조(IP주소 관리대책) ○ 제19조(비상대책 수립·운용) ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공), 6, 통신망, 통신망 장애관리
8. 물리적보안	○ 제8조(단말기 보호대책) ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 3.시설 및 장비, 물리적환경 ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공), 5.보안, 물리적보안
9.인적보안	○ 제3조(인력 및 조직 관리) ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 1.IT서비스제공/자원 관련 조직 및 요원, 직무분리 ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 1.IT서비스제공/자원 관련 조직 및 요원, 인적자원 및 자질
10.사고대응	○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공) 3.시설 및 장비, 장비의 유지보수 ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 6.통신망, 통신망장애관리
11.감사 및 책임추적성	○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공, 4.운영통제,처리통제
12.시스템 및 통신보호	○ 제11조(해킹 방지대책) ○ 제13조(홈페이지 등 공개용 서버 관리대책) ○ 제20조(정보처리시스템의 성능관리) ○ 제28조(이용자 비밀번호 관리) ○ IT검사 매뉴얼, 504.체크리스트(시스템), 1. 시스템 개발, 도입, 유지보수 관련 조직 및 요원, 직무분리 ○ IT검사매뉴얼, 604.체크리스트(IT서비스제공), 4.운영통제, 시스템성능관리 ○ IT검사 매뉴얼, 604.체크리스트(IT서비스 제공) 5.보안, 논리적보안

위와 같은 사항들이 정보보호 수준평가에 포함된다면 금융권 보안관리 시 최우선으로 고려되어지는 IT 법규들을 준수할 수 있다.

또한 개인정보보호법, 신용정보보호법, 전자금융거래기본법, 전자서명법 등을 참조한다면 금융분야의 업무시 발생하는 대부분의 IT 보안위험을 관리하여 자산을 보호할 수 있다.

3. 기술적 정보보안요구사항 분석

금융권에서는 정보의 무결성이 가장 중요하게 요구되어진다. 계좌 금액이나 거래내용 위변조와 같은 사례가 발생할 경우 해당 금융기관의 경제적 피해가 크기 때문이다.

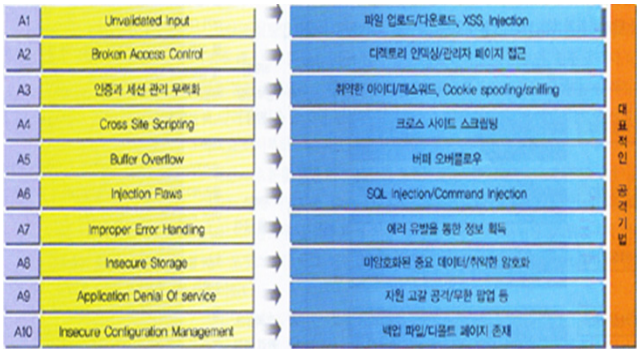
또한 전자금융에서 거래액 비중이 높은 증권 같은 경우 네트워크 장애를 통해서 발생하는 개인 및 기관들의 피해는 막대하다. 그래서 보안성 상실시 서비스 영향 정도를 고려해야 한다.

금융분야	무결성>가용성≥기밀성

(그림 1) 정보보호 목표

위의 (그림 1)과 같이 자산보호는 무결성이 중시되며, 서비스의 연속성을 보장하기 위해서는 가용성이 중요시 된다. IT 자산을 보호하기 위해서는 민감한 자원에 대한 접근제어가 필수적이다. 보호가 요구 되는 자원에는 기본적으로 애플리케이션 접근, 웹서비스, 중요 시스템 파일 및 데이터베이스, 중요 시스템, 사용자 계정 등이 있으며, 자산에 대한 물리적/논리적 통제가 필요하다.

서비스 연속성을 보장하기 위해서는 바이러스 , 스팸, 침입시도, 스파이웨어, 서비스 거부 공격, 키 입력저장, 악성 프로그램, 시스템 취약성 등의 위협으로부터 보호되어야 하며, OWASP(Open Web Application Security Project)에서 주장하는 (그림 2)와 같이 가장 심각한 웹 애플리케이션 취약점을 보호해야 한다.



(그림 2) OWASP TOP 10

4. 결론

금융권의 보안위협으로부터 자산을 보호하기 위해서는 금융분야에 적합한 업무적 특성을 고려해야 한다. 특히 금융 부분은 법규준수가 중요하기 때문에 전자금융 시 준수되어야 하는 법규를 파악해 준수여부를 파악해야 하며, 새로운 기술적 보안 위협으로부터 자산을 보호하기 위해 웹 애플리케이션 취약점을 파악하고, 지속적인 관리를 통해 보안위험을 완화해야 한다.

참고문헌

[1] 김정덕, 홍기향, "정보보호거버넌스 이슈 및 연구과제", 정보보호학회지, 2007.8
[2] 한국정보보호진흥원, 정보보호대책 프레임워크 수립연구, 2004.10
[3] 한국정보보호진흥원, 주요정보통신기반시설의 정보보호수준평가 방법론 개발, 2005.11
[4] OWASP, OWASP TOP 10 Korean Version, 2007
[5] 한국 인터넷진흥원, 2009년 인터넷 이용실태조사 요약보고서, 2009.9
[6]http://www.kisa.or.kr
[7]http://www.owasp.org