신규 서비스 구축 및 개선 시 보안성 검토에 관한 사례분석 및 연구

천인혁O, 최 혁*
OST Unitas,
*서울시립대학교 컴퓨터과학부
e-mail: sorisera@naver.comO, chyuk@uos.ac.kr*

Case analysis and research on security review when building and improving new services

In-Hyoek CheonO, Hyuk Choi*
OSecurity Team, ST Unitas,
*Dept.of Computer Science, University of Seoul

● 요 약 ●

금융회사는 신규서비스 구축과 서비스의 시행 전에 보안성 심의를 받아 기준을 충족한 경우 실 운영이 가능 했으나, 기업 자체적으로 검토를 진행하고 보안수준을 스스로 유지 하도록 변경 되었다. 금융회사를 포함한 서비스 제공자는 실제 서비스를 오픈하기 전 보안성 검토를 자체적으로 이행하고 있으나 클라우드 등 회사 자산의 다양한 환경변화와 조직 내 각 부서의 세부적인 요구사항을 충족하기에는 현실적인 한계가 따른다. 기존 연구는 전문가 및 실무자를 통해 보안성 검토 체크리스트의 항목을 개선하고 효과를 검증하는데 노력 하였다. 하지만 실질적인 결과를 바탕으로 한 연구는 부족한 실정이다. 따라서 본 논문은 실 운영 중인 시스템 및 서비스의 기획에서 운영까지의 전체 프로세스를 대상으로 보안성 검토를 수행한 결과를 분석하여 보안 실무자 입장에서의 적절한 검토 방안을 제안한다.

키워드: 보안정책(Security policy), 보안성 검토(Security Review)

I. Introduction

금융회사(전자금융거래법에 명시된 회사 및 전자금융업자, 전자금융보조업자)는 신규서비스 구축과 연관된 서비스의 시행전 유관기관(금융보안원)에 보안성심의를 받고 심의기준에 충족하여야 했다. 하지만 핀테크 사업 활성화로 심의 해야할 대상이 늘어남에 따라 보안성 심의를 기업 자체적으로 진행하고 보안수준을 스스로 유지 하도록 변경되었다. 따라서 각 기업에서는 신규 서비스에 대한 보안성검토를 자체적으로 이행하고, 자체 판단이 어려운 경우에는 유관기관(금감원)에 문의하여 "비조치의견서"를 통해 답변을 확인 받고 있다. 그러나 기술의 발전에 따른 내 외부적 환경변화는 기업이 지속적으로 해결 보완해야할 가치로 존재 하였다. 또한 회사의 각 조직의 이해가치와 실무자 관점에서의 다양한 보안 요구사항을 충족하기에는 현실적인 한계가 존재해 왔다. 이를 해결하기 위해 기존 연구는 보안성검토 개선을 목적으로 체크리스트 및 중요항목을 변경 또는 추가하고 전문가 또는 실무자의 조사(설문)를 실시하여 효과성을 입증을 꾀한 경우가 대다수이다. 따라서 실제 서비스를 기준으로 한 보안성검토에 관한 연구는 미흡하다. 본 논문에서는 운영 중인 시스템 및 서비스에 대한 보안성검토 결과를 도출 하였다. 또한 기획 단계에서부터 오픈까지의 전체 서비스 프로세스별로 보안성 검토를 진행하였으며 조직 내 유관부서의 역할에 따라 구분한다. 2장은 기존 연구를 분석하고 실 운영 서비스의 보안성검토결과를 분석한다. 3장은 적절한 검토방안을 제안하며 4장에서 결론을 맺는다.

II. Preliminaries

1. Related works

1.1 기존 연구

사내 보안 관리 방안에 관한 연구에서는 대부분의 개인정보 유출 등의 보안 사고는 악의적인 공격자와 내부자(임직원 및 협력사직원)를 통해 발생하며 대부분이 내부자에 의해 유출되고 있어 사내보안관리방안 가이드를 제시하여 보안수준 향상을 목표로 한다. 내부자 정보유출을 방지하기 위해 6개 항목의 사내보안 관리방안을 제시한다. 외부자보안, 임직원보안 수칙, 물리적보안, 기술적보안, 사내정보 관리, 보안기획으로 구성된다. 외부자 보안은 관리적 기술적 물리적 보안통제로

구분되어 있으며 네트워크구성도 등 내부 문서관리, 대외제공 문서관리를 하여야 한다.[1]

소명을 이용한 내부정보유출 방지 관리 방안에 대한 연구에서는 보안솔루션이 운영되는 중에 내부자 실수로 인한 보안위반행위를 소명하도록 함으로써 소명절차를 이용한 내부정보 유출방지 관리방안을 연구 하였다. 기업 내부에서 사용자가 어떤목적 또는 업무로 보안행동에 위배하였는지 명확하게 소명을 하고 상위 결재권자에게 결재요청을 함으로써 정보의 접근 사실과 위험행동에 대한 근거를 마련 한다. 내부정보유출 경로는 인터넷, 저장장치, 프린터, 모바일기기반출, 스마트폰을 통한 유출로 구분한다. 예를 들어 미승인USB를 사용한 경우 누가, 언제, 어떤 파일을 사용하였는지를 소명하고 요청부서가 검토 요청 후 담당부서에서 승인한다.[2]

사례 분석을 통한 IVN의 필수 보안 요구사항 도출에서는 자동차에 모든 보안대책을 적용 하는것이 좋으나 비용대비 현실적 적용한계성을 이해하여 차량 사이버 보안을 보장하기 위해 필수로 적용해야 하는 보안요구 사항을 제시한다. 이때 실제 공격 취약점을 분석하여 자산 위협을 식별하고 보안목표를 도출하여 위험평가 기반으로 차량에 필수적으로 적용되어야 할 보안요구사항을 도출한다. 위험분석을 통해 보안자산식별, 각 자산별 보안목적 정의, 위험도 평가를 수행하였고, 보안자산은 차량에 저장된 개인정보, ECU소프트웨어, ECU간 통신데이터를 포함한다. 취약점 및 공격사례를 기반으로 식별한 보안자산은 ECU소프트웨어, 통신데이터, 유저데이터이고, 보안목적은 기밀성, 무결성, 가용성, 인증, 최신성으로 정의한다.[3]

안전한 전자금융거래를 위한 보안등급 기준마련 및 사례연구에서는 금융위원회가 보안성심의를 폐지하고 자체 금융기관(기업) 내 보안성 심의로 보안수준 점검의무를 갈음 하는것으로 변경됨에 따라 심도 있는 보안성 검토를 위해 기존의 CIA기반의 보안등급에 인증(A)과 개인정보(P) 지표를 추가하여 CIAAP 보안등급을 제안한다. 보안등급 지표의 추가를 위해 인증과 개인정보에 대한 중요성, 도입필요성, 실제 사례를 나타내었고 특히 개인정보의 경우 경제적인 부분과 프라이버시 보호 측면으로 하여 지표를 구분 하였다. 신용카드 현금서비스 거래화면과 계좌이체 거래화면을 CIA와 CIAAP 보안등급을 비교하고 실제사례를 나타내었으며 특히 기존 CIA 기준 검토시 도출되지 않은 추가인증과 개인정보보호를 통해 보안이 강화되었다고 볼 수 있다.[4]

모바일 금융서비스 보안성검토를 위한 보안점검 항목 개발에 관한 연구에서는 실제 기업 내에서 보안성검토를 자체 진행할 인력, 여력이 현실적으로 부족하고 이를 위한 구체적인 항목 및 기준이 없는 문제점이 있어 모바일 금융서비스를 중심으로 보안성검토를 진행하기 위한 구체적인 항목을 연구 하였다. 연구 방법은 기존연구사례를 분석하고 새로운 항목을 도출하여 전문가를 통한 검증과 테스트를 함으로써 제안하는 방법의 근거를 제시 하였다. 기존 보안성심의는 사전보안성검토, 보안대책 수립 및 적용의 적정성 검토, 소스코드 취약점 점검, 관리 물리 기술 분야 적정성검토로 구성되며, 제안한 방식은 금융당국 보안성심의 기준, 행자부 모바일 전자정부 서비스 보안기준, OWASP Mobile TOP 10 등 국내외 모바일 서비스 보안진단 기준을 조사하고 위협분석을 통해 개선방안 연구 후 전문가 인터뷰 및 테스트를 통해 효과성을 검증 하였다. 특히 점검 방법은 감독기관 기준, 관련논문, 국내외관련 기준. 가이드(컨설팅회사)를 통해 점검항목을 도출하였다.[5]

기존 연구는 보안성 심의 기준에 일부항목을 추가하여 기준 수립과 제시한 기준의 적절성을 평가하는데 주력 하였다. 또한 일부 시스템에 대한 실제 검토를 하였으나 더 많은 연구가 필요하다.

Table 1. 보안성 검토 사례

NO	제목요약	검토사항
1	서버 구성	네트워크 : AD서버존 별도 구성 통신제어 : 방화벽 통한 IP및 포트 제어 시스템 보안 : 백신최신화, EOS여부확인, 호스트방화벽 시스템 간 접근통제 : 분리된 존의 각 서버 간 통신제한 접속이력 보관 : 법적기간 준수(1~2년) 주요정보 접근제한 : 인사DB접근 금지 서버접근제어 및 이력관리 : 서버접근제어솔루션을 통해 접속로그 및 행위이력 기록
2	판매 목적 상품정보 전송	외부통신 : 아웃바운드제한, 특정IP 제한 전송구간 보안 : 암호화, SFTP 사용
3	타 서비스 연동 API	외부통신 : 아웃바운드 제한 개인정보 제공 동의 및 제공처, 동의거부 권리, 거부시 불이익 웹취약점 조치 전송구간 암호화
4	DataPipeline 개선 (IDC <-> 클라우드)	네트워크 : 별도 보안영역구성, 구간암호화 개인정보 비식별화 ※ AWS Direct connect, VPC Peering
5	업무용 메신져 구축 및 개선	통신 : 외부기기에서 내부시스템 접근제한 단말기 : 외부기기(휴대폰 및 모바일기기) 책임추적 : 내부시스템 접속이력 보관 및 위변조 관리 : 접속로그보관, 검토(월1회)
6	외부업체 업무위탁	위탁업무(개인정보)의 문서화 손해배상 관련 법적 책임 명기 업무 본연의 목적을 위한 서약
7	제휴업체 회원정보 제공	개인정보 수집 목적 및 동의 개인정보 3자 제공 목적 및 동의 개인정보 제공 시 보안 : 암호화
8	서비스 취소 수수료 차감 방지를 위한 증빙기능	계약관계 확인 개인정보 동의 : 본인 증빙 서류 수집 개인정보파일 암호화 : 안전한 방식으로 암호화 개인정보 파기 : 목적 달성 시 파기
9	비회원 구매 확대	개인정보 파기 및 분리보관 개인정보 위탁 및 제3자 제공 개인정보 암호화
10	외부파견 근무자의 내부시스템 접근	안전한 접속수단 : VPN 단말기 보안 및 고정IP 사용 책임추적 : 접속기록 보관 및 검토 추가인증수단(OTP) 적용 파일보안검사 및 개인정보보유 현황검사 사용기간 및 서버연결시간 제한 불필요 파일 삭제

1.2 보안성검토 실 사례 및 결과

본 장에서는 회사가 운영 중인 시스템 및 서비스의 보안성 검토 실제 사례를 나타내고 결과를 분석한다. 또한 검토 결과를 바탕으로 보안성 검토 대상을 분류하고, 검토 시 주요항목을 도출한다. [표 1]

에서와 같이 총 10개의 사례를 선별 하였으며 선별 기준은 보안부서로 요청된 사항 중 개시 전에 서비스가 종료되거나 검토 후 보안이슈 및 사업성, 계약관계 등으로 서비스를 하지 않게 된 사례는 제외 하였다.

보안성 검토 대상은 [표 2] 에서와 같이 신규 서비스를 개발 하는 경우, 기존 운영 중인 서비스에 기능을 추가 및 변경하는 경우, 외부 서비스와 연계하는 경우, 개인정보를 수집 또는 노출 변경하는 경우로 구분할 수 있다. 분류한 기준은 실제 보안성 검토를 수행한 결과를 바탕으로 하였으며 최빈수는 운영중인 서비스 및 그와 연관된 인프라 시스템의 추가 구축이나 변경으로 나타났다. 보안성 검토 사례를 분석한 결과 주요 검토 항목은 [표 3]에서와 같이 총 7가지로 항목을 구분 할 수 있다. 네트워크 및 통신, 단말기 및 시스템, 책임추적, 개인정보, 컴플라이언스 및 계약, 데이터 보안, 관리로 분류 할 수 있으며 이는 보안성검토를 진행하면서 결과에 따라 분류 하였다. 특히 검토결과를 현업부서에 가이드 할 때 취약점 및 보완조치를 이행하는데 연관성이 있어 부서별 상호 내용공유가 필요한 내용을 한 항목으로 정리 하였다.(a, b, e, g)

또한 보안성 검토 요청이 많거나 검토결과 반복적으로 도출되는 내용은 별도의 항목으로 구분 하였다.(c, d, f)

(e, g)의 경우 관리적인 측면에서의 보완활동이 지속적으로 필요한 경우로 계약서, 서약서, 협약서 및 약정서, 정기점검결과보고서 등 대외비 문서를 관리하는 부서와 서비스 운영 부서와의 협업이 필요하다. (c, d, f)의 경우 보안성 검토 요청이 많거나 보안성 검토 결과 취약점으로 자주 등장하여 중점적으로 관리 하여야 한다. 특히 개인정보 및 책임추적의 경우 미 조치시 법위반, 보안인증 시 결함, 사고 시 소명 등 다양한 측면에서 위험이 있어 서비스 오픈 후에도 지속적으로 관리가 필요하다.

Table 2. 보안성 검토 대상 분류

NO	항목	내용
I	신규 서비스 개발	기존 서비스 외 신규 개발
II	주요 서비스 기능 추가 및 변경	기존 서비스에 기능 추가 및 변경 개발기간이 장기간 소요되는 경우
III	외부 서비스 연계	개인정보, 금융정보, 민감정보 등 내부 보유 정보 연동 개발
IV	개인정보 수집 또는 노출 변경	수집 항목 변경에 따른 개발

Table 3. 보안성 검토 결과 및 주요 항목

NO	항목	내용
a	네트워크 및 통신	외부통신, 전송구간, 존구성 및 분리, 접속수단, 망간통신
b	단말기 및 시스템	취약점, 백신, 보안설정, 접근통제, 추가인증
c	책임추적	접속 및 행위 로그 보관
d	개인정보	수집, 저장, 이용, 제공, 파기
e	컴플라이언스 및 계약	서비스 계약, 손해배상
f	데이터 보안	암호화, 접근제한
g	관리	정보보호서약, 협약 또는 약정, 감사

Table 4. 보안성 검토 결과 분석

NO	보안성 검토 대상 분류				주 검토항목						
	I	II	III	IV	a	b	c	d	e	f	g
1	●				√	√	√			√	
2		●			√						
3		●	●		√	√		√			
4		●			√			√			
5	●			●	√	√	√				√
6				●				√	√		√
7		●		●				√			
8		●		●				√	√	√	
9		●		●	√				√	√	
10	●				√	√	√	√			

[표 4]는 보안성 검토 결과를 분석한 것으로 보안성 검토 대상 분류 측면에서는 기존 서비스에 기능을 추가하거나 개인정보 관련 서비스의 검토가 다수임에 나타났다. 또한 주 검토 항목에서는 네트워크 및 통신과 개인정보 부문이 다수로 나타났다. 특히 사업 특성상 분류한 대상이 통합 되었을 경우 심도 있는 보안성 검토가 필요하다. 예를 들어 외부서비스와 연동되어 개인정보를 API등을 통해 처리할 경우 계약 및 법적부문, 네트워크 및 시스템, 개인정보 등 다방면의 검토가 수반 되어야 한다.

III. The Proposed Scheme

본 절에서는 전체 서비스 및 보안성검토 프로세스를 살펴보고 실무 중심의 검토방안을 제안한다. 보안성 검토 프로세스는 [그림 1]과 같다. 고객 또는 경영진에 의해 신규서비스 또는 기존서비스의 개선사항의 목적이 발생되고 실질적인 기획단계에 돌입한다. 이때 기획부서 뿐 아니라 보안, 법무, 개발, 시스템 등 유관부서가 각 업무 룰에 맞는 요구사항을 도출하고 보안 및 법무부서에서 법, 관리, 기술적 기준으로 전반적인 검토를 수행한다. 검토결과에 따라 미흡한 사항을 보완하고 완료 시 서비스를 오픈한다.

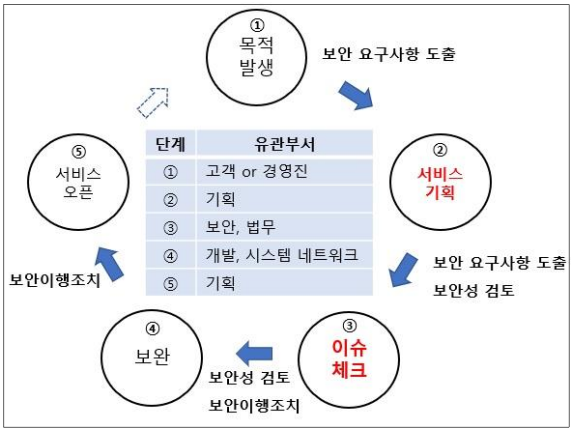

Fig. 1. 서비스 및 보안성검토 프로세스

제안하는 보안성 검토 방안은 법 및 관리 기술적 관점으로 검토를 실시하되 회사내부 비용, 자원, 인력 리소스 등 내부자원을 최소화 하는 방향으로 가이드 해야 한다. 예를 들어 [그림 2]와 같이 타사 서비스와의 연동으로 고객에게 서비스를 제공 할 경우 별도 API 등을 통해 내부자산과 직접적인 통신을 제한하고 추가인증수단 적용하는 등 다양한 관점으로 검토가 필요하다. 이때 제공하는 서비스의 주체 및 활용자산의 경중에 따라 가급적 타사의 인력 및 자원 리소스를 활용하여 개발토록 하는 것을 권고한다. 추가로 회사의 영업 및 기획부서에서 계약상의 갑을 관계에 따라 보안상 예외사항 또는 회사보안지침과 일부 상이한 경우가 발생할 경우 해당부서 품의 등을 통한 위험수용 또는 전가가 요구된다. 또한 개발 및 시스템, 네트워크 등의 타부서에서 신규 회선구축, 장비구매, 추가개발이 동시에 요구되는 경우 오픈 전까지 별도 관리적인 방안으로 대체할 수 있는지를 검토하여야 한다.

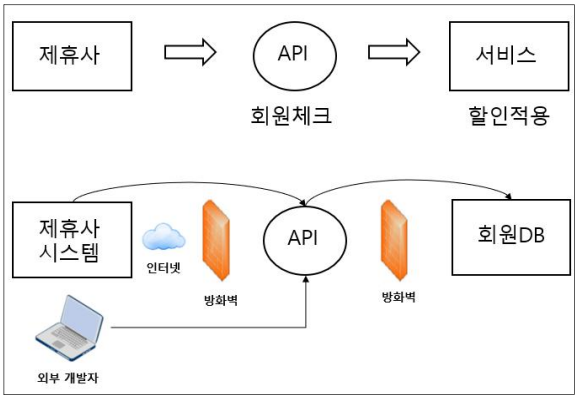

Fig. 2. 타사와의 연동을 통한 고객 서비스

IV. Conclusions

본 논문은 보안성 검토에 관하여 기존 연구와 실제 운영 중인 시스템 및 서비스를 위주로 검토 결과를 분석 하였다. 전체 서비스 프로세스를 기준으로 검토한 결과 검토대상은 기존 서비스에 기능을 추가하는 경우가 많았고 검토내용은 네트워크 및 통신과 개인정보에 대한 사항이 두드러지게 나타났다. 또한 최초시점부터 기획, 운영, 개발, 시스템, 네트워크, 법무 등 유관부서와의 논의가 필요하고 회사의 자원을 최소화 하는 방안을 도출 하는 것이 실무자로써의 역할임을 인지한다. 마지막으로 본 논문의 실 사례는 각 기업의 특성 및 서비스에 일반화 할 수 있도록 추가 연구가 필요하다.

REFERENCES

[1] A Study on a Methodology of the Internal Security Management Korea Information Processing Society 2015 Fall Conference, pp.726 - 729

[2] A Study on The Management Plan for Prevention of Information Leak by Using Call-out Korea Information Processing Society 2014 spring academic presentation Competition, pp.431 -434

[3] Deriving Essential Security Requirements of IVN through Case Analysis The journal of the Korea institute of intelligent transport systems, 2019, pp.144 - 155

[4] Establishing Security Level Standards and Case Studies for Safe Electronic Financial Transactions Korea Information Security Association, pp. 729 - 741, 2018

[5] A study on developed security check items for assessing mobile financial service security, Chung-Ang University Graduate School 2017