사례를 통한 프로젝트 단계별 보안 방안에 대한 연구

신성윤* · 장대현* · 김형진**

*군산대학교

**전북대학교

A Study on The Step-by-step Security Measures of Project through Cases

Seong-Yoon Shin* · Dai-Hyun Jang* · Hyung-Jin Kim**

*Kunsan National University

**Jeonbuk National University,

E-mail : {s3397220}@kunsan.ac.kr

요 약

유수의 기업체가 사이버공격을 받아 개인정보를 유출당하는 피해 사례가 속출하고 있다또한 금전이득의 획득이나 사회적 혼란 유발 등을 목적으로 계획된 해킹사례가 지속적으로 증가하고 있다 본 논문에서는 IT서비스 기업들이 수행하는 프로젝트 단계별 주요 보안 활동 사례를 파악한다 이를 통하여 실제 프로젝트 단계별로 적용할 수 있는 보안 방안을 제시하고자 한다

ABSTRACT

Leading companies has led to the victimization being leaked to accept personal information by the cyber attack. Also planned hacking cases on purpose such as acquiring monetary gain or social distracting is constantly increasing. In this paper, we identify examples of the project step-by-step leading IT services companies to perform security activities. Real-world projects step-by-step through security measures that can be applied are presented..

키워드

Ⅰ. 서 론

국제통화기금(IMF) 전산망 해킹('11.6) 세계군수업체인 록히드 마틴('11.4), 현대 캐피탈 해킹 사건('11.4), 농협 전산망 장애사건('11.4) 등 국내외 유수의 기업체가 사이버 공격, 전문 해커집단에 의한 해킹 등 정보시스템의 해킹으로 인한 피해 사례가 속출하고 있다. 이러한 환경에도 불구하고 국내 민간기업의 81.4%가 IT예산의 1%도 정보보호에 투자를 하지 않고 있는 실정이다. 정부는 현행 정보보호 관련 법령으로 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 기본법으로 하여 분야 및 적용대상에 따라 산발적인 개별법규를 두어 각 분야별, 적용대상별로 정보보호를 위한 규율을 실시하고 있다.

* 본 논문은 군산대학교 공학연구소의 연구지원에 의하여 수행되었으며, 이에 감사드립니다.

본 논문에서는 IT서비스 기업들이 수행하는 프로젝트 단계별 주요 보안 활동 사례를 통하여 실제 프로젝트 단계별로 적용할 수 있는 보안 방안을 제시하고자 한다.

Ⅱ. 본 론

현재 IT서비스 기업의 주요 보안 SDLC 활동은 보안 SDLC(분석/설계/구축/테스트)와 전사 프로세스를 통한 활동으로 크게 두가지로 구분할 수 있다.

그림1. 프로젝트 단계별 주요 보안 Activity

보안 SDLC 활동으로는 크게 네가지로 분류할 수 있다. 첫째, 보안 법제도에 근거한 보안요건 정의 및 설계/구현 추적은 잘 되고 있는가? 둘째, 보안 설계/코딩 표준 가이드가 적시 활용이 어렵고, 개발자의 기존 코딩 습관을 답습하고 있지 않

은가? 셋째, 보안 소스코드 검토(자가점검, 툴 활용 등)활동은 수행하고 있는가? 넷째, 단계별 보안성 적용 점검 부족으로 뒤늦은 결함이 발견되지 않는가? 이다.

전사 프로세스 활동으로 크게 두가지로 분류할 수 있다. 첫째, 보안성 관련 세부 Task 정의 및 관련 투입공수는 적절한가? 둘째, 단계별 보안 Activity에 대한 Best Practice는 공유/활용되고 있는가? 이다.

프로젝트 단계별로 주요 보안 Activity를 보면 그림 1과 같다. 프로젝트는 분석, 설계, 구축, 테스트, 이행의 다섯 단계(SDLC)의 Activity로 각 단계별로 보안 Activity활동을 전개한다.

첫 번째, 분석단계에서는 고객사의 환경 분석과 보안 요건을 분석하고 정의를 한다. 법, 제도, 규정 등을 검토하고 패키지 보안기능 및 통합 보안계획을 수립하여 보안 위협 시나리오 기반의 위험 평가를 통한 보안 요건을 정의 한다. 어플리케이션 보안 요건 영역으로 익명에게 공개를 목적으로 하는 프로그램을 제외한 모든 어플리케이션은 사용 전 반드시 인증과정을 거쳐야 하며 사용자 권한에 따른 통합인증관리를 지원하도록 설계해야 한다.

두 번째, 설계단계에서는 보안 표준과 가이드를 수립하여 프로젝트 투입인력을 대상으로 시큐어코딩 가이드 등의 정의된 보안 교육을 실시하고, 보안 요건 적용을 검토하여 체크리스트를 구축한다. 단위 업무 시스템별 구성요소에 대해서 보호대상을 개별적으로 식별하고, 단위 업무시스템은 업무시스템이 설치되는 시스템 노드(서버 시스템), 노드의 특정 디렉토리에 설치되어 구동되는 어플리케이션 모듈, 모듈간의 통신을 위한 인터페이스로 구분하여 식별한다.

표 1. 보호대상 정의(예시)

구성요소	설명
시스템 노드	어플리케이션 모듈이 설치될 IP주소를 가진 물리적 시스템을 의미함. 특정 업무시스템 식별할 때 해당업무에 포함되는 시스템 및 상호 통신을 하는 타 시스템을 포함함
어플리케이션 모듈	시스템 내부에 설치되는 어플리케이션 모듈 중 해당 업무시스템의 구성요소에 포함되는 어플리케이션 모듈을 의미함
인터페이스	어플리케이션 모듈 상호간의 정보교환을 위한 모든 통신방식을 포괄하여 의미함(예:FTP), DB-Link, EAI, SOCKET, HTTP, rhost)

보안속성 설계로는 개별 업무시스템별로 보호대상 정의 테이블에서 식별된 보호대상 노드, 모듈은 분석단계에서 정의 된 보안기준에 따라 보안속성을 설계한다. 보호대상 정의 테이블에 보안속성 설계를 추가하여 보안 속성 설계로 상세화 한다. 보안 속성으로는 보호대상, 엑세스 허용대상, 접근통제 영역, 식별 및 인증 영역, 암호화 영역으로 크게 다섯 가지로 분류할 수 있다.

행정안전부는 정보시스템SW개발운영자를 위한 "소프트웨어 개발보안 가이드" ('11.9월 2판 발행)을 통하여 정보시스템 개발단계에서 고려해야할 주요 보안 취약점에 대한 소스코드 레벨에서의 대응조치에 대한 가이드를 제시하고 있다.

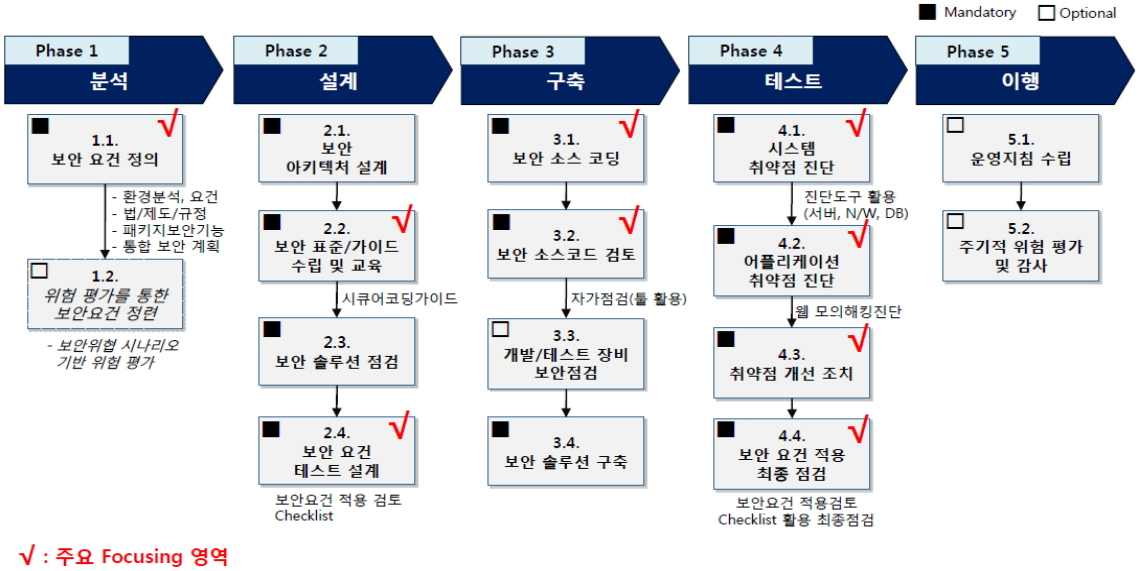

그림 1. 프로젝트 단계별 주요 보안 Activity

설계단계의 검증은 구체적인 시스템의 구현 산출물이 나오기 전이므로 문서검토의 방식으로 진행되며 어플리케이션의 보안설계에 초점이 맞추어져 있다.

표2. 보안속성 설계 – 식별 및 인증 영역(예시)

속성	설명	예시
ID	보호대상으로 접근하는 모든 엑세스 허용 모듈의 ID 형태 또는 고정된 ID일 경우 ID의 텍스트	Key파일, ID
PW	엑세스시 패스워드 인증의 수행 여부	O,X
기타	ID, PW 인증 이외에 추가적인 인증 방법 적용시 해당 방법을 구체적으로 기술	인증서, 토큰

구축단계에서는 자가점검을 통하여 소스코드를 검토하고 전단계에서 정의된 보안 구축을 검토하고 확인하는 절차가 필요하다. 암호화 솔루션을 적용하지 않을 경우, 프레임워크 단에서 보안적용을 통해 보안성 강화를 고려할 필요가 있다. J2EE 프레임워크의 경우, JDK에서 제공하는 보안관련 패키지, 클래스, 라이브러리, 설정파일 등을 식별/활용이 가능하다.

소스코드 보안취약점을 점검하기 위해서는 입력값 검증 등 소스코드 보안 취약점 점검 수행 절차를 정의하여 점검하여야 한다.

보안 요건 정의서에 제시된 각 보안 요건ID별 상세요건으로 세분화하여 구현 프로그램에 기능이 반영되었는지 점검하여야 한다.

표3. 설계단계 보안 – SW보안 취약점 유형

구분	SW보안 취약점 유형
입력데이터검증및표현	- 프로그램 입력값에 대한 검증누락 또는 부적절한 검증이나 사용되는 데이터의 잘못된 형식 지정 - XSS,SQL 삽입, 버퍼오버플로우, 운영체제 명령어 삽입 공격 등
API 악용	- 의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생 - Get(), J2EE:System.exit()함수 등
중략...	
코드품질	- 복잡한 소스코드로 인해 관리성 유지보수성, 가독성이 저하되어 SW 개발 및 유지보수시 타입변환 오류 자원(메모리 등)의부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안취약점 - 자원의 부적절한 반환 등
캡슐화	- 중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때 인가되지 않은 사용자또는 시스템에게 데이터 누출이 가능해지는 보안 취약점 - 제거되지 않고 남은 디버거코드, 시스템데이터 정보 누출 등

테스트 단계에서는 보안요건이 구현되었는지 검토하고, 취약성 점검 및 프로젝트 수행사의 최종 검토와 고객사의 보안요건 최종 확인이 필요하다.

표4. 테스트 단계 – 진단항목 예시

점검항목	위험도
SQL Injection 취약점	상
XSS(Cross Site Scripting) 취약점	상
디렉토리 목록 노출 취약점	하
관리자 페이지 노출 취약점	중
파일업로드 취약점	상
파일다운로드 취약점	상
파라미터변조 취약점	상
취약한인증 취약점	상
불필요한파일 취약점	하
CSRF(Cross Site Request Forgery) 취약점	중
검증되지 않은 리다이렉트와 포워드	중

주1) “2011년06월 금융회사 공개용 서버 침해사고 및 취약점점검기준”으로한 11대 취약점점검항목

보안요건 적용 점검 체크리스트를 정의하여 점검 방법과 반영 여부에 대한 점검으로 사용자 인증과 입력값 검증을 통해 점검해야 한다. 또한, 해커의 입장으로 가정하여 Target 시스템에 대한 불법 침입을 시도하고, 내부망에서의 모의해킹과 외부망에서의 모의해킹 방식으로 진단을 한다. 침입자의 목적은 인터넷에 오픈되어 있는 대상 시스템으로의 침입 후 대상 시스템의 관리자 권한 및 데이터를 얻어내는 것과 내부망의 금융정보 또는 고객 관련 데이터를 획득할 수 있는 보안 취약점을 발굴하는데 목적이 있다.

III. 결 론

본 연구를 통하여 프로젝트 단계별 주요 보안 Activity를 이해하고, 보안요건 항목 및 세부 요건 Best 사례를 습득하였으며, 프로젝트 각 단계별 보안 방안 Guide 및 사례를 통하여 SDLC 전 영역에 걸친 Seamless 한 보안성 검증 및 테스트 역량을 확보할 수 있었다.