한국컴퓨터정보학회 동계학술대회 논문집 제21권 제1호 (2013. 1)

단계별 프로젝트 보안 방안

장대현°, 이양원*, 표성배**
°*군산대학교 컴퓨터정보공학과
**인덕대학교 컴퓨터소프트웨어과
e-mail:daijang@sk.com°, ywrhee@kunsan.ac.kr*, pyosb@induk.ac.kr**

The Step-by-step Security Plan

Dai-Hyun Jang°, Yang-Won Rhee*, Sung-Bae Pyo**
°*Dept. of Computer Information Engineering, Kunsan National University
**Dept. of Computer Software, Induk University

● 요 약 ●

현재는 수많은 기업체들이 사이버공격을 받아 회사의 기밀 정보와 개인정보를 유출당하는 피해 사례가 속출하고 있다. 그리고 금전상의 이득이나 사회적으로 커다란 혼란을 유발시키는 등의 목적으로 계획되거나 모의된 해킹사례가 나날이 늘고 있다. 본 논문에서는 IT서비스 기업체들이 다양한 방면으로 수행하는 프로젝트의 각 단계별 주요 보안 활동 사례를 알아본다. 사례를 파악하여 실제 프로젝트에 단계별로 적용할 수 있는 보안 방안을 제시하고자 한다.

키워드: 사이버공격(Cyber Attack), 기밀 정보(Secret), 해킹(Hacking), 보안방안(Security Plan)

I. 서 론

수많은 기업들의 회사의 운명과 전체적인 사업 기능을 완료하는데 컴퓨터의 이용과 정보 처리는 필수 불가결한 요소이다. 이러한 컴퓨터의 보안 관리 문제로 우리는 종종 고위 관리 및 컴퓨터 자원의 보호를 모색하고 기타 기관들의 무엇보다 소중한 자산을 보호하는데 광범위 하고 포괄적인 보안 관리 대책의 필요성에 효과적으로 보호하고 있다.

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[1].

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

II. 단계별 프로젝트 보안 활동

현 시대의 소프트웨어 개발이란 프로그림을 짜는 개념에서 보다 확대되어 시스템 개발이라는 용어로 사용되기도 한다. 소프트웨어의 제작 공정 다시 말해서, 소프트웨어 탄생 과정에서 폐기 절차까지의 여러 단계에서 나타나는 소프트웨어의 형상을 가시화(Visualize)한 것을 SDLC 모델이라고 한다.

소프트웨어를 개발 할 때 SDLC 모델의 적용은 아래와 같은 효과를 발휘한다.

1) 개발 프로젝트 비용 산정과 개발 계획수립의 기본이 되는 골격-일정 계획, 예산, 인원, 기타 자원의 배분 역할을 수행하는 도구
2) 용어의 표준화: S/W 개발자 사이와 개발자와 관리자 사이의 합의를 함께 구성
3) S/W 개발 진행 상황 파악: 개발의 지연, 비용의 초과 등의 사태에 대하여 예방하거나 대처하는 기능
4) 개발 프로젝트의 충실한 진행: 다양한 문서(산출물)를 작성하는 시기와 검토하는 시기를 제시함

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

보안 SDLC 활동으로는 크게 네 가지로 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 않은가?

셋째, 보안 소스코드 검토(자가 점검, 툴 활용 등)활동은 수행하고 있는가?

넷째, 단계별 보안성 적용 점검 부족으로 뒤늦은 결함이 발견되지 않는가? 이다.

전사적인 프로세스 활동으로 크게 두 가지로 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 그림1과 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 위험평가를 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 시큐어 코딩 가이드 등의 정의된 보안 교육을 실시하고, 보안 요건 적용을 검토하여 체크리스트를 구축한다. 단위 업무 시스템별 구성요소에 대해서 보호대상을 개별적으로 식별하고, 단위 업무시스템은 표 1의 예시와 같이 업무시스템이 설치되는 시스템 노드(서버 시스템), 노드의 특정 디렉토리에 설치되어 구동되는 어플리케이션 모듈, 모듈간의 통신을 위한 인터페이스로 구분하여 식별한다.

표 1. 보호대상 정의(예시)
Table 1. Definition of Protection Subject(Example)

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)

세 번째, 구축단계에서는 자가 점검을 통하여 소스코드를 검토하고 전 단계에서 정의된 보안 구축을 검토하고 확인하는 절차가 필요하다. 암호화 솔루션을 적용하지 않을 경우, 프레임워크 단에서 보안적용을 통해 보안성 강화를 고려할 필요가 있다. J2EE프레임워크의 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 요건 ID별 상세요건으로 세분화하여 구현 프로그램에 기능이 반영되었는지 점검하여야 한다.

네 번째, 테스트 단계에서는 보안요건이 구현되었는지 검토하고, 취약성 점검 및 프로젝트 수행사의 최종 검토와 고객사의 보안요건 최종 확인이 필요하다. 표 2는 테스트 단계의 진단 항목의 예시이다.

표 2. 테스트 단계-진단 항목(예시)
Table 2. Test Step-Diagnosis Item(Example)

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
취약한 인증 취약점	상
불필요한파일 취약점	하
CSRF(Cross Site Request Forgery) 취약점	중
검증되지 않은 리다이렉트와 포워드	중

※ "2011년06월 금융회사 공개용 서버 침해 사고 및 취약점점검기준"으로 한 11대 취약점 점검항목

마지막으로 보안의 이행 활동 단계로서 보안 활동을 실행하는 단계이며, 운영지침 수립과 주기적인 위험 평가 및 감시를 수행한다.

보안요건 적용 점검 체크리스트를 정의하여 점검 방법과 반영 여부에 대한 점검으로 사용자 인증과 입력 값 검증을 통해 점검해야 한다. 또한, 해커의 입장으로 가정하여 Target 시스템에 대한 불법 침입을 시도하고, 내부 망에서의 모의해킹과 외부 망에서의 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.

보안 취약점을 진단하기 위한 웹 모의 테스트 진단 도구로 사용하는 도구들은 주로 자체 개발시스템 취약성 점검스크립트로 계정 및 패스워드, 시스템파일 설정, 네트워크 서비스 설정, RootKit, 백도어 점검, 시스템파일 무결성 점검, 프로세서 및 네트워크 점검 등의 종합적인 시스템취약성 점검을 위해 사용된다.

III. 결 론

논문에서는 IT서비스 기업체들이 다양한 방면으로 수행하는 프로젝트의 각 단계별 주요 보안 활동 사례를 알아보았다. 실제의 예

제를 파악하여 실제 프로젝트에 단계별로 적용할 수 있는 보안 방안을 제시하였다. 본 연구를 통하여 프로젝트 단계별 주요 보안 Activity를 이해할 수 있었고, 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.

참고문헌

[1] Won-Hee Nam, Dea-Woo Park, "A Study on Cloud Network and Security System Analysis for Enhanced Security of Legislative Authority," *The Journal of the Korean Institute of Information and Communication Engineering*, Vol. 15, No. 6, pp. 1320-1326, 2011. 6