한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

정보보호 활동 (분석단계)

신성윤[O], 이현창[*]
[O]군산대학교 컴퓨터정보통신공학부
[*]원광대학교 정보전자상거래학부
e-mail: s3397220@kunsan.ac.kr[O], hclglory@wku.ac.kr[*]

Information Security Activity(Analysis Phase)

Seong-Yoon Shin[O], Hyun-Chang Lee*
[O]School. of Computer Inf. & Comm. Eng., Kunsan National University
[*]Div. of Inf. and E. Com., (Ins. of Conv. & Cre.), Wonkwang University

● 요 약 ●

SDLC 중에서 분석단계는 정보시스템의 개발을 준비하는 단계로서 정보기술 체계의 분석과 사용자의 요구 사항 도출 및 예측되는 위험 요소에 대한 평가도 함께 수행하였다. 정보보호의 요구사항은 도출은 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에서 하였다.

키워드: 분석 단계(Analysis Phase), 정보 보호(Information Security), 정보 기술(Information Technology)

I. Introduction

개발 단계별 정보보호에 관한 연구로는 도서관 개인정보 가이드라인(안)을 제안하여 도서관 종류를 구분하지 않고 어느 도서관에서나 적용 가능하도록 하였으며 개개 도서관은 이 가이드라인(안)을 기반으로 도서관의 현실에 맞게 교정하여 사용할 수 있도록 한 연구[1], 원자력발전소와 연관된 규제요건과 기술표준문서를 바탕으로 원자력발전소의 S/W 구축 생명주기(SDLC) 단계별로 사이버보안 활동과 평가 항목들을 도출하여 S/W 구축 생명주기 단계별로 사이버보안 평가가 가능한 방법을 제시한 논문[2], 그리고 공공기관들의 정보시스템 운영 단계에서 필요한 개인정보보호 관점의 운영감리 점검 항목을 개발한 논문[3]이 있다.

II. Information Security Model

ISO 표준, 국내 표준, NIST, 그리고 KISA의 자료 등에 따라서 개발의 기본 단계를 분석, 설계, 구현, 시험의 4단계로 정의하였다. 그리고 각 단계에 따른 13개의 파생되어 도출된 정보보호 활동을 기본으로 하였다. 그림 2과 같이 한국정보보호 진흥원의 『정보시스템 구축단계별 정보보호 가이드라인』에서 제시한 방법론 모델을 기본으로 하고 있다.

III. Information Security Activity

정보시스템을 개발할 때 일반적으로 정보보호의 요구사항은 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에서 나온다. 자세한 정보보호 요구사항의 내용은 아래와 같다.

기밀성은 정보시스템 내부의 비밀정보를 분류, 정보시스템 내부의 기능에 대한 제한 등을 포함한다.

무결성은 정보시스템 내부의 정보를 변경할 수 있는 개인이나 업무의 식별, 정보시스템 자체의 무결성, 정보시스템의 변경 기능에서의 무결성 보장 등을 포함한다.

가용성은 정보시스템의 모든 구성요소의 가용성 요구사항을 식별할 필요가 있고, 정보시스템 구성요소간의 의존성과 상호작용을 파악하고 네트워크 등의 인프라의 가용성 요구사항을 식별해야 한다.

책임 추적성은 사용자 식별 및 인증과 정보보호의 사고를 조사할 때 필요한 정보를 제공하기 위해 감사에 대한 요구사항을 포함한다. 위험평가의 경우에서, 개발과정 중의 위험평가는 아직 대상 정보시스템이 구현되기 이전 상태이므로 취약성 평가에 의미가 없으므로 위험평가는 예상되는 위협을 바탕으로 이루어진다.

IV. Examples

S사를 대상으로 분석단계의 정보보호를 구현하였다. 일반적으로 정보시스템을 개발할 때 나오는 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에 대한 요구사항들을 정밀 분석하였다.

그림 1의 결과는 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에서 정보보호 활동을 추가하여 나타나는 보안성이 더 증가하는 것으 알 수 있다.

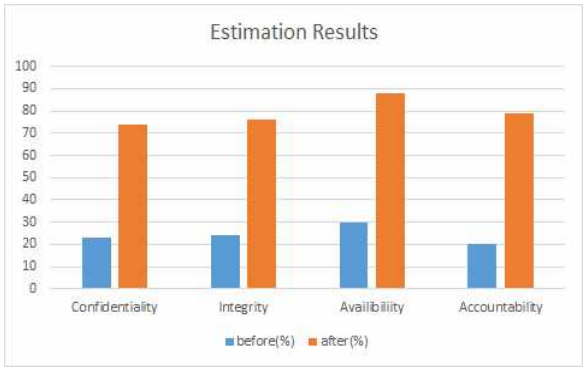

Fig. 1. Estimation Results

그림 2는 분석단계의 정보보호 활동을 추가하여 평가한 매출의 실적이다. 이 매출 실적 또한 소폭으로 상승한 것으로 나타났다.

Fig. 2. Sales Results

V. Conclusion

SDLC 중에서 분석단계는 정보시스템의 개발을 준비하는 단계로서 정보기술 체계의 분석과 사용자의 요구 사항 도출 및 예측되는 위험요소에 대한 평가도 함께 수행하였다. 정보보호의 요구사항은 도출은 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에서 하였다. 분석단계의 정보보호 활동 중 첫 번째인 프로젝트 수행 계획의 명시부터 마지막 정보보호 계획 수립까지를 다루었다. 그리고 S사의 분석단계의 보안 요구사항을 구현하여 전체적인 시스템의 분석과 매출의 향상도를 평가하였다.

References

[1] Yonghee Noh, Tae-Kyung Kim, “A Study on Developing Guidelines for Personal Information Protection in Library,” J. of Korea Society for Information Management, Vol. 32, No. 2, pp. 21-61, Jun. 2015

[2] Dal-mi Seo, Ki-Jong Cha, Yo-Soon Shin, Choong-Heui Jeong, Young-Mi Kim, “Assessment Method of Step-by-Step Cyber Security in the Software Development Life Cycle,“ Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 2, pp. 363-374, Apr. 2015

[3] Dae-Ha Park, Sang-Nyeong Yoo, Heung-Youl Youm, “Development of Information System Operational Audit Checklist for Personal Information Protection in Public Organizations,” Journal of Security Engineering, Vol. 12, No. 1, pp. 47-64, Feb. 2015