전자상거래 개인정보보호를 위한 IT보안감사체계 연구

이은경[O], 박병우[*], 장석은[*], 이상준[**]
[O*]전남대학교 정보보안협동과정
[**]전남대학교 경영학부
e-mail: diva0123@hanmail.net[O], nowzic@daum.net[*], seokeunjang@gmail.com[*], s-lee@chonnam.ac.kr[**]

Study on IT security audit system for e-commerce private information protection

Eun-kyoung Lee[O], Byoung-woo Park[*], Seok-eun Jang[*], Sang-joon Lee[**]
[O*]Dept. Information security course, Chonnam National University
[**]School of Business Administration, Chonnam National University

● 요 약 ●

최근 여기어때, 인터파크 등 전자상거래 기업을 대상으로 발생한 개인정보 해킹사고 사례를 보면, 사람의 취약점을 노리는 지능화지속위협(APT) 공격과 알려진 해킹 기술이 복합적으로 이루어지고 있다. 해킹사고가 발생한 기관은 한국인터넷진흥원(KISA) 정보보호관리체계(ISMS) 의무대상 기관으로써 정보보호관리체계를 유지·관리하고 있었다. 그럼에도 불구하고 대형의 개인정보 유출사고가 발생한 주요 원인은 정보보호관리체계가 적용되지 않았던 정보시스템과 인력을 대상으로 해킹이 이루어졌기 때문이다. 해킹 위협의 변화에 따라 전자상거래 보안 수준도 변화해야 하는데, 개인정보보호 관련 규제 준수도 전자상거래 기업에서는 힘든 상황이다. 고객의 개인정보 유출 사고는 일반인을 매출 기반으로 서비스하고 있는 전자상거래 기업에서는 치명적이다. 안전한 전자상거래 플랫폼 기반에서 고객에게 서비스를 제공하기 위해서는 무엇보다도 중요 자산인 고객의 개인정보보호를 위해 역량을 집중해야 한다. 한정된 예산과 자원으로 안전한 서비스를 제공하기 위해서는 기존에 구축된 정보보호관리체계를 기반으로 IT보안감사체계를 전사적으로 확대하여 지속적으로 모니터링 할 필요가 있다. 이에 본 연구에서는 최신 사이버 보안 위협 동향과 전자상거래 기업 대상으로 발생한 최근 개인정보유출사고 사례를 분석을 통해 시사점을 도출하여 전자상거래 개인정보보호를 위한 IT보안감사체계를 제시하였다.

키워드: 전자상거래(E-commerce), 정보보호관리체계(ISMS), IT보안감사(IT Security Audit), 지능화지속위협(APT), 개인정보보호(Privacy)

I. Introduction

최근 국내에서 발생하는 개인정보 해킹사고 대부분은 조직 내 특정 개인을 표적 삼아 내부 시스템을 장악하는 형태로 이루어지고 있다. 정부와 기업에서는 정보보호관리체계 의무 제도를 통해 보안강화를 위해 애쓰고 있지만 여전히 개인정보유출사고는 끊임없이 발생하고 있다.

특히 최근 개인정보유출사고는 고객의 개인정보를 대량으로 보유하면서 상대적으로 취약한 전자상거래 기업을 대상으로 발생하고 있는 경향이 있다. 해킹사고 사례가 있었던 전자상거래 기업은 정보보호관리체계를 구축하여 각종 보안 솔루션을 도입하고 내부 보안관리체계를 유지하고 있었다. 그러나 해킹으로 이용됐던 정보시스템은 정보보호관리체계 범위에 해당하지 않은 내부 정보시스템이 주로 악용되었다.

따라서 규제에 적용되지 않은 내부 정보시스템 및 인력을 통한 사이버 보안 위협을 예방하고 대고객 개인정보보호 강화를 위한 전사적이고 지속적인 IT보안감사체계 도입이 필요한 시점이다. 이에 본 연구에서는 최신 사이버 보안 위협 동향과 전자상거래 기업 대상으로 발생한 최근 개인정보유출사고 사례를 분석을 통해 시사점을 도출하여 전자상거래 개인정보보호를 위한 IT보안감사체계를 제시하고자 한다.

II. Related works

1. Cyber Security Threat Trend

한국인터넷진흥원에서 2017년 12월에 발표한 '2018년 7대 사이버 공격 전망'에 따르면, 공격수법은 더욱 교묘하게 진화하고 확대될 것으로 예상된다.

Fig. 1. KISA 2018 Cyber Security Threat Trend [1]

Fig. 1에 언급된 7대 사이버 공격 전망에서 언급한 사이버 보안 위협의 특징을 살펴보면 크게 3가지 유형으로 분류할 수 있다.

첫째, 사람의 취약점을 노리는 지능형 지속 공격이다. 주요 공격 형태는 지능형 공격과 결합한 랜섬웨어 공격, 악성코드 감염 및 유포 방법의 다양화이다.

둘째, 신기술 보안 취약점과 금전이익을 노리는 공격 형태이다. 주요 공격 형태는 가상화폐 관련 서비스와 금전이익을 노리는 공격, 취약한 IoT(Internet of Things) 기기의 오프라인 범죄 악용 사례가 있다.

셋째, S/W 취약점을 노리는 고도화된 해킹 공격이다. S/W 개발체계 해킹을 통한 대규모 악성코드 감염, 사회적 이슈 관련 대규모 공격 위협, 중앙관리 S/W 취약점 및 관리 미흡을 통한 표적공격 등이 대표적인 사례이다.

2. Personal information leakage case analysis

최근 발생한 전자상거래 기업 대상 개인정보유출사고 사례 분석을 통해 주요 취약점을 도출하고자 한다.

2.1 Interpark Personal Information Leakage Case

2016년에 발생한 인터넷 쇼핑몰 '인터파크' 개인정보유출사고는 내부 직원의 지인을 사칭한 스피어피싱 해킹으로 2,200만 건의 회원정보가 유출되었다[2]. 스피어피싱은 조직 내에 신뢰할 만한 발신인으로 위장해 ID 및 패스워드 정보를 요구하는 일종의 피싱 공격. 메일을 보내 가짜 사이트로 유도하여 악성 코드를 설치하게 하거나 ID와 패스워드를 입력하게 하여 네트워크에 침입할 수도 있다[3]

해킹 공격은 다음 4단계를 거쳐서 수행되었다. 1단계 : 메일을 통한 내부망(직원PC) 최초 감염, 2단계 : 내부망(파일공유서버) 감염 확산 및 정보수집, 3단계 : 개인정보취급자 PC·DB서버 점거, 4단계 : 개인정보 탈취 및 유출이다.

이와 같은 해킹 공격 과정에서 발견된 주요 취약점은 5가지이다. 첫째, 해킹을 당한 직원PC가 정보보호관리체계 인증 범위 대상이 아니었고, 둘째, 지능화지속위협(APT)에 대한 보안대책이 적용되지 않았다는 문제가 있었다. 셋째, 개인정보취급자 PC에 대한 인터넷 차단(망분리)이 제대로 적용되지 않았다. 파일공유서버가 내·외부 네트워크를 연결되는 접점이 된 것이다. 넷째, 주요 시스템에 대한 패스워드 관리 및 개인정보처리시스템에 대한 세션타임아웃 설정이 미흡 했다. 다섯째, 해당 직원이 업무 종료 후 PC 전원을 종료하지 않아 해커가 악성코드가 감염된 해당 PC를 통해 야간에 자유롭게 해킹을 할 수 있어서 피해가 확산되었다.

2.2 'Goodchoice' Personal information leakage case

2017년에 발생한 위드이노베이션 숙박 어플 '여기어때(Goodchoice)' 해킹사고는 97만 명의 개인정보가 유출된 사건이다. 내부 관리시스템에 대한 기본적인 웹 취약점 보완조치가 이루어지지 않아 SQL Injection, Session Hijacking 등의 알려진 웹 공격으로 쉽게 내부 개인정보가 외부로 유출되었다.

Sql Injection은 데이터베이스(DB)에 접근하는 페이지의 취약점을 이용한 공격이다. Session Hijacking은 정당한 사용자가 인증을 거친 후 받은 권한 정보를 몰래 가로채는 공격이다.

'여기어때'도 2017년 정보보호관리체계 의무대상으로 지정되어 인증준비를 하고 있었으나, 해당 시스템은 인증범위에서 제외되어 있어 기본적인 웹 취약점 진단을 수행하지 않았다.

방송통신위원회 조사 결과에 따르면 기본적인 개인정보보호조치가 이루어지고 있지 않았으며, 정보통신망법상 위반 사항으로 침입탐지 시스템 미준수, 개인정보 보호기간 6개월 보관 시 월 1회 정기점검 미이행, 개인정보 암호화 미조치, 관리자 페이지 접근 변경 권한 미조치, 1년간 서비스 미이용자 개인정보 미처리 등이 발견되었다[4].

3. Status and implication of related works

최근 사이버 보안 위협 및 개인정보유출사고 사례를 분석한 결과를 토대로 다음과 같이 시사점을 도출하였다.

3.1 Strengthen education and training on information protection for all employees

사람의 취약점을 노리는 사이버 보안 위협이 증가함에 따라 무엇보다도 임직원의 철저한 보안관리가 필요한 시점이다.

특정인을 노리는 표적 공격 형태의 악성코드 배포에 대응하기 위해서는 기술적인 대책으로는 한계가 있기 때문이다. 임직원이 지인이나 알려진 기관을 사칭한 이메일에 속지 않기 위해서는 정기적인 보안 공지 및 '악성코드 이메일 대응 훈련'과 같은 훈련이 필요하다.

또한 개인정보취급자 뿐만 아니라 모든 직원이 기본적인 PC 보안관

리 수칙(보안패치, 퇴근시 전원 끄기 등)을 포함한 기업 보안 정책을 인지하고 준수할 수 있도록 인식제고 활동도 꾸준히 이루어져야 한다.

3.2 Regular Vulnerability Assessment for all web sites

해킹 사례를 보면, 대고객 서비스가 아닌 외부에 노출된 내부 관리 시스템을 통해 고객의 개인정보보호가 유출되었다. 사내 시스템이라 하더라도 대고객 서비스와 같은 네트워크에 있다면, 취약한 사내 시스템을 통해 내부 정보가 유출될 위험이 항상 존재한다. 이에 외부 인터넷 접속이 불필요한 홈페이지의 경우 외부 접속을 차단하고 사내에서만 사용할 수 있도록 조치하여야 하며, 기본적인 웹 취약점에 대해서는 조치를 할 수 있도록 관리하여야 한다.

3.3 Restrictions on user access and special permissions

직원 PC, 파일서버, 개인정보처리시스템, 웹어플리케이션 등 사내 정보시스템에 대한 철저한 ID 및 패스워드 관리가 필요하다. 또한 직원의 직무변경, 퇴사 등에 따른 권한 관리도 철저하게 이루어져야 하며, 정기적인 접근 권한에 검토에 따른 불필요한 권한 삭제가 이루어져야 한다.

3.4 Regular monitoring activities on compliance with laws and regulations

전자상거래 정보보호 관련 법·규제(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법 등)에 관련 준수 여부를 자체적으로 점검하는 활동이 필요하다. 정보보호관리체계 인증 범위를 포함하여 고객 개인정보에 대한 접근이 가능한 조직, 시스템 및 어플리케이션, 데이터베이스를 전수 식별하여 이에 대한 개인정보 보호조치를 적용해야 한다.

III. IT보안감사체계

2장 관련 연구를 통해 분석한 결과를 통해 개인정보 유출 사고를 예방하기 위해서는 전사적인 정보보호관리체계가 지속적으로 운영되는 것이 필요함을 알 수 있었다. 그러나 현실적으로 전사 조직과 정보시스템을 범위로 정보보호관리체계를 운영하기 위해서는 전담 정보보호 조직과 예산 확충이 필요하다. 이에 본 논문에서는 전자상거래 개인정보보호 강화를 위해 기존에 많은 전자상거래 기업에서 구축한 KISA 정보보호관리체계를 모델로 조직, 정보시스템에 대한 전사적인 모니터링 활동을 강화할 수 있는 IT보안감사체계를 제시한다. IT보안감사체계는 감사 수행 절차, 조직, 대상, 기준, 주기, 방법으로 구분하여 다음과 같이 정의하였다.

1. Procedure for performing audit

정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는 지를 점검하기 위하여 연 1회 이상 IT 보안 감사를 수행하여야 한다. 이를 위해 감사 기준, 범위, 주기, 방법 등을 구체적으로 정한 감사 계획을 수립하여 실시한다. 감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다[5].

2. Audit performance organization

감사팀 구성은 기 수립된 정보보호관리체계의 감사팀 구성 요건에 따라 독립성 및 전문성을 확보할 수 있도록 구성하여야 하며, 감사 인력은 사전에 정의된 자격요건을 충족한 자여야 한다. 조직 내에 전담 IT 보안 감사 조직이 없을 경우, 일반적으로 정보보호 전담조직 인력과 외부 정보보호 전문가를 포함하여 감사팀을 구성하며, 감사 계획 수립 시 포함하여 경영진 검토 및 승인을 득한다.

3. Audit Object and Criteria

피 감사 대상은 전사 조직 및 정보시스템을 전제로 한다. 감사 점검 기준은 최근 사이버 보안 위협 및 개인정보유출사고 사례 분석 결과를 바탕으로 Tabl 1.과 같이 전자상거래 기업을 위한 주요 점검 기준을 선정하였다. 주요 점검 기준은 PC 및 사무실 보안관리, 기술적 취약성 진단 수행 및 조치 여부, 정보시스템 접근권한 관리, 정보보호 관련 법·규제 준수로 분류하였다.

Table 1. System Environment

Item	Contents
PC and office security management	Change of password 90 days, security patch, vaccine installation, power off at work, whether to block personal information from PC
Performing technical vulnerability diagnostics	Servers, networks, databases, security systems, web applications, etc.
Management of information system access control	Regular review and action on applicants, job changers, retirees, long-term unused accounts, abnormal access and records of personal information
Compliance with laws and regulations related to information protection	Check compliance : Intrusion detection system installation, 6 months of personal information protection period and once a month periodic inspection, personal information encryption, administrator page access restriction, Separate user's personal information for 1 year and keep user's notice, etc.

4. Audit performance cycle and method

KISA 정보보호관리체계 기준에 따라 연 1회 이상 감사를 실시하는 것을 기본 원칙으로 한다. 본 논문에서는 전사 조직 및 정보시스템을 대상으로 함에 따라 효율적인 점검을 위해 Table2.와 같이 문서 감사와 현장 감사를 실시하며, 현장 감사는 샘플링 감사 방법을 적용한

다. 문서 감사는 사전에 정의한 감사 기준에 따라 부서별로 자체 점검을 하고, 점검한 내역을 감사팀에 제출한다. 문서 감사 결과가 미흡한 부서를 대상으로 현장 감사를 샘플링 하여 실시하며, 현장 감사를 연 2회 이상 실시할 경우, 감사의 효율성을 위해 기 점검한 대상은 제외한다. 단, 조치가 미흡하여 재점검이 필요하다 판단될 경우에는 현장 감사 계획 수립 시 포함하여 경영진 승인을 득한 후 실시할 수 있다. 문서 감사 시 허위 내용을 제출한 경우에는 사규에 따라 인사 평가 반영, 경영진 보고 등의 제재를 가할 수 있다.

Table 2. Annual audit performance cycle and method

Item	1Q	2Q	3Q	4Q
Document audit	O		O	
Field audit		O		O

IV. Conclusions

정부와 많은 전자상거래 기업에서는 개인정보보호 강화를 위해 KISA 정보보호관리체계 인증 의무화 제도를 도입하여 운영하고 있지만, 인증 범위를 대외 서비스로 한정하여 관리·운영함에 따라 관리되지 않는 부분을 통한 개인정보유출사고가 끊임없이 발생하고 있다. 이에 형식적인 정보보호관리체계 운영에서 벗어나 실효성 있는 관리가 필요하다. 이에 본 연구에서는 최신 사이버 보안 위협 동향과 전자상거래 기업 대상으로 발생한 최근 개인정보유출사고 사례를 분석을 통해 시사점을 도출하여 전자상거래 개인정보보호를 위한 IT보안감사체계를 감사 수행 절차, 조직, 대상, 기준, 주기, 방법 구분하여 제시하였다. 이 방안은 기존에 KISA 정보보호관리체계를 수립한 전자상거래 기업을 대상으로 한다는 제약점을 갖고 있다. 비즈니스 환경이 급변하고 있어 향후 KISA 정보보호관리체계 인증 의무대상이 아닌 스타트 업 전자상거래 기업에서도 확대 적용 가능한 IT보안감사체계 연구가 추가로 필요하다.

REFERENCES

[1] KISA, "2018 Cyber Security Threat Trend", Dec. 2017.
[2] Boannews, Press Releases, "Interpark Hacking, Three Implications of 'Past Grade' Fraud in 4.4 Billion" Dec. 7. 2016.
[3] TTA, Information and communication terminology dictio nary, *http://terms.tta.or.kr*
[4] KOREA COMMUNICATIONS COMMISSION, "WITH INOVATION Hacking accident investigation result", Apr. 17. 2017.
[5] KISA, "Detailed check items of ISMS certification stand ard", May. 15. 2013.