기업 업종에 따른 정보보안컨설팅 방법 연구

이수연*

요 약

최근 기업의 해킹사고에 따라 보유하고 있는 개인정보의 노출은 심각한 수위에 이르게 되었다. 그리고 기업 업종에 따라 발생되는 보안위협요소도 달라지고 있다. 따라서 본 논문에서는 기업 업종에 따른 보안위협요소를 살펴보고 이에 적합한 정보보안컨설팅 방법을 제시하였다. 첫째, 금융·보험업은 내부 구성원의 인식 부족으로 인한 웜/바이러스 감염에 무방비 상태가 되지 말아야하며 조직의 내부 보안기준을 구성원에 동일하게 일괄 적용함으로써 고객정보 위험성이 높은 직군에 의해 보안사고가 발생하는 것을 사전에 대비해야한다. 그러므로 사람과 정보 중심의 정보보안컨설팅 방법이 적용되어야한다. 둘째, 개인기업의 경우 산업군의 속성에 따라 정보보안컨설팅이 이루어져야한다. 즉, 기업이나 기관에서 정보보안을 고려하게 되는 동기를 크게 Security Thread, Compliance, Biz-Requirement, Biz-Opportunities 로 나누어 각각의 동기에 따라 컨설팅이 이루어져야한다.

A Study on Information Security Consulting Method according to Type of Company

Su-youn Lee*

ABSTRACT

Exposure of personal information that is held by hacking accident near the company has led to severe water level. And, it has changed security threat elements generated according to businessenterprise. Therefore, in this paper, I looked at security threat elements and proposed the way of appropriate information security consulting according type of company. First, In the financial and insurance industries, and should not have been compromised by a worm virus infection due to lack of awareness inside of members, by collectively apply in the same way the internal security standards of the organization to members, the risk of customer information. It shall be provided in advance that the security accident occurs due to a higher job group. Therefore, information security consulting method based on people and information is applied. Secondly, in industry of company, to perform consulting information security based on the attributes of the case industry groups.

Key words : Information Security Consulting Method, Information and Personal-based Consulting, Attribute - based Consulting, Industry of Company

접수일(2015년 6월 15일), 수정일 (1차: 2015년 6월 30일)
게재확정일(2015년 6월 30일)

* 백석문화대학교 인터넷정보학부

1. 서 론

최근 기업의 해킹사고 비율이 41%로 높은 편임을 알 수 있다. 그러나 대규모 개인 정보 유출, 3.20 및 6.25 사이버테러 등 언론매체를 가득 채운 해킹, DDoS, 피싱 등 각종 보안사고 관련 소식에도 불구하고 효과적인 대응 방안을 제시한 개인 및 기업은 많지 않다. 아마도 보다 안전한 사업 환경을 구축하기 위해서는 좀 더 비싸고 좋은 솔루션을 구축하면 되는 것이 아니냐는 막연한 해결책을 제시할 수도 있다. [1]

2012년 조사에 따르면 기업 부문에서는 경기침체 등으로 인해 정보보호에 투자한 기업이 전반적으로 감소하였으며, 업종별·규모별 정보보호 수준 격차도 심화되고 있는 것으로 나타났다. 또한 개인 부문에서는 정보보호에 대한 인식은 높은 수준을 유지하고 있으나, 이용자단말의 비밀번호 설정, 무선랜 보안조치 등 실천은 상대적으로 저조한 것으로 조사되었다. 업종별로 정보보호 투자규모를 늘린 사업체는 정보서비스업 44.6%, 금융·보험업 65.5%로 각각 20.4%p, 25.6%p씩 증가하였다. 규모별로는종사자 수 5~9명 사업체의 26.9%, 종사자 수 250명 이상 사업체의 45.2% 가투자규모를 늘려 사업체의 규모가 클수록 투자에 적극적인 것으로 나타났다. 정보보호 조치가 강화된 정보서비스업 등 일부업종은 투자를 지속적으로 확대하고 있으나, 대부분의 기업에서는 경기침체 등으로 인해 투자에 소극적인 것으로 분석된다.

다만, 개인정보관리책임자 임명(58.1%, 9.9%p 증가), 개인정보보호 전담조직 운영(45.0%, 10.9%p 증가), 정보보호 교육 실시(19.8%,1.2%p 증가) 등개인정보보호 분야의 활동은 개선된 것으로 조사되었다. 이는 정보통신망법, 개인정보보호법 등 관련 법·제도를 개선한 결과가 영향을 미친 것으로 분석된다. 개인부문 실태조사 결과에서는 인터넷 이용자의 정보보호 인식은 98.7%로 매우 높은 수준을 유지하고 있으나, 정보보호 실천 활동은 전년보다 감소한 것으로 파악되었다. 정보보호 제품·서비스 이용률은 88.2%로 높은 편이나, 윈도우 로그인 암호설정(26.1%), PC부팅암호설정(27.2%), 무선공유기 암호설정(51.2%) 등 기본적인 정보보호 조치는 여전히 낮게 나타났다. 따라서 본 논문에서 기업의 업종별에 따른 보안위협요소를 살펴보고 이에 적합한 정보보안컨설팅 방법을 제시하고자 한다.

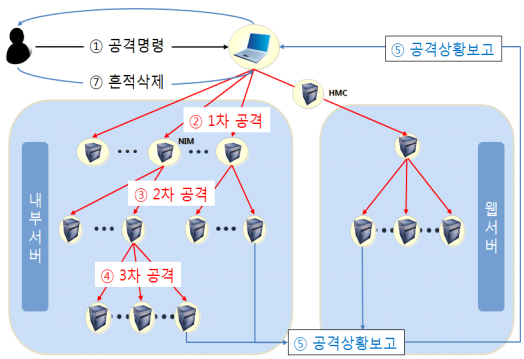
본 논문의 구성은 다음과 같다. 먼저 2장에서는 업종별로 개인정보 유출침해 사례를 조사해보았다 3장에서는 기업 보안정책 수립 시 점검해야할 항목을 살펴보았다. 그리고 업종별 정보보안컨설팅 방법을 살펴보고 방향을 제시하였다. 4장에서는 결론과 향후 연구계획에 대해서 설명하였다.

2. 개인정보 유출침해 사례

2.1 금융·보험업

금융기관들은 이중 삼중의 보안시스템이 구축되어 공공기관이나 다른 민간 기업들에 상대적으로 안전한 것으로 인식되고 있다. 공인인증서, 보안카드, 키보드 프로그램, 1회용 비밀번호 생성기, OTP 등을 사용해 해킹이나 정보침해에 대응하고 있다. 그러나 해킹이나 사이버테러, 그리고 내부자에 의한 고의적인 개인정보 유출과 훼손이 빈번하게 발생 중이다. 예를 들어, 농협의 전산망 마비로 인한 금융대란, SC 제일은행과 현대 캐피털의 개인정보 유출 사례가 대표적이다. 또한, 2007년 국민은행처럼 동의를 구하지 않고 개인정보를 임의로 사용하여 사회적 물의를 야기했다.

반면 정부기관과 함께 금융기관은 해킹이나 사이버테러의 주요한 목표가 되고 있고 다양한 방법에 의해 개인정보 유출과 시스템 파괴가 발생하고 있다. 2011년 4월 발생한 사상 최악의 농협 전산망 파괴는 사고나 과실이 아닌 고의적인 범행으로 특히, 이동식 저장장치(USB)를 통한 새로운 수법이다.[2] [그림 1]은 농협전산망 공격시나리오를 보여준다.



(그림 1) 농협전산망 공격 시나리오

또한, 2011년 4월 현대캐피털은 해커의 침입으로 인해 175만명의 개인정보가 유출되었는데 해킹사고의 원인은 현대캐피탈이 전자금융거래법 등 관련 법규에서 정한 사고예방대책을 소홀히 했기 때문이다. 즉, 서버에 접근할 수 있는 계정과 비밀번호 관리에 허술했고 광고메일 서버에 접속할 수 있는 계정과 비밀번호 5개를 외부인에게 부여하고 퇴직 직원이 재직시절 계정과 비밀번호를 이용해 정비내역 조회 서버에 7차례나 무단 접속하는 것을 방치했다. 그리고 2011년 2월 15일부터 4월 7일까지 해킹사건의 주범이 이용한 것과 같은 인터넷프로토콜(IP)주소에서 해킹시도가 이뤄진 것을 포착하고서도 예방조치를 하지 않았다.

다양한 개인정보를 유출시켜 피해를 주기고 했는데 2007년 3월 국민은행은 자사 인터넷복권 통장 가입고객 중 접속 빈도가 낮은 32,277명에게 인터넷복권 구매 안내메일을 발송하였다. 그러나 발송 대상인 고객들의 명단을 파일로 첨부해 개인정보인 고객 이름과 주민등록번호, 이메일 주소 등이 노출되었다.

2.2 개인기업 부문

개인기업의 경우 필요 이상으로 광범위하게 개인정보를 보유하고 있지만 개인정보보호에 대한 의식과 예산 그리고 기술 확보는 낮아 개인정보 유출과 침해사고가 빈번하게 발생하고 있다. 주요한 사고현황을 보면 2008년 옥션 개인정보 유출 사건(1,863만 명), GS칼텍스 개인정보 유출(1,125만 명), 2010년 중국해커 관여 개인정보매매(2,000만 명), 2011년 네이트 개인정보 유출(3,500만 명)과 가비아&한국엡손 개인정보유출 등 매년 발생하고 있다. 개인 기업에서의 개인정보 유출·침해는 외부에서의 해킹이나 내부인사의 저장창치나 서류를 통한 유출 등 다양한 방법으로 이루어질 정도로 철저한 보안의식 및 기술적 대안이 미흡한 현실이다.

2011년 7월 26일 국내 대형 포털 사이트인 네이트온 - 싸이월드가 소위 '맞춤형 악성코드'에 의해 해킹을 당했는데 약 3,500만 명에 달하는 회원의 이름, 아이디, e-mail, 비밀번호, 주민등록번호 등이 모두 유출되어 상당한 충격이었다. 한국의 인터넷 활용인구가 약 3,700만 명 정도라는 사실을 감안할 때 우리나라 인터넷 사용인구 대부분의 개인정보가 유출된 것으로 국내 해킹 사고 중 사상 최대 규모이다. 이러한 개인정보 유출사고가 더욱 문제인 것은 비교적 정보보호에 만전을 기하고 있을 것으로 기대되었던 대형 포털 사이트의 개인정보들이 유출되었다는 점이다. 가장 유력한 해킹경로로는 무료 백신 업데이트 과정에서 악성코드에 감염된 개발자의 컴퓨터인 것으로 추정되고 있고 최근에 발생한 농협 및 현대캐피털의 개인정보 유출 사례와 유사한 양상을 보인다.

[표 1] 개인정보 및 사이버테러 유형 분류

수 준	피해유형	대표피해 사례
개인 수준	이메일 해킹	- 경찰청장 메일 초기화면을 외부에 공개
	시스템 파괴	- 해킹을 통해 웜 바이러스, 좀비화 등을 통한 시스템 마비
기업 수준	개인정보 유출	- SK 커뮤니케이션스(해킹) - GS 칼택스(내부직원의 유출)
	시스템 파괴	- 2009년 7.7 DDoS 사례 - 에스토니아에 대한 러시아 해커의 공격 등

3. 기업의 보안정책

본 장에서는 기업의 정보보안을 위해 수립되어지는 정책에 어떠한 항목들이 필요하고 현재 기업에서 이루어지고 있는 보안컨설팅 방법을 살펴보았다.

3.1 기업 보안정책 수립 시 필요 항목

기업의 보안정책을 수립하기 위해서는 다음과 같은 항목들을 점검해 보아야한다.[3]

■ 정보보호 정책서 작성 및 보유
정보보호 정책을 구현하기 위한 지침, 표준, 절차 등이 구현되어 있어야한다.

■ 정보보호 정책 배포 및 교육
승인된 정책 및 지침이 모든 임직원에게 적절히 공표되고 교육되어 있어야한다.

■ 정보보호 정책 검토
정보보호 정책은 정기적으로(혹은 중대한 변화가 발생할 경우) 검토하고 업데이트 되어야한다.

■ 정보보호담당자
정보보호 활동을 계획, 실행, 검토하는 정보보호 담

당부서 또는 담당자가 별도로 존재해야한다.

- 정보보호담당자 자격
  정보보호관리자 또는 담당자는 충분한 보안기술을 보유하거나 보안관련 전문자격증(CISA, CISSP 등)을 보유하고 있어야한다.
- 외부 전문가의 활동
  주기적으로 외부 보안전문가에 의한 정보시스템 보안 취약점 진단 및 이에 대한 평가를 받고 있어야한다.
- 정보보호에 관한 독립적 검토
  정보보호의 통제목적/통제방안/정책/절차/처리 등 정보보호 관리와 이행에 대한 조직은 정기적으로 혹은 정보보호 구현에 중대한 변화가 발생할 경우 독립적(외부전문가 또는 내부 통제부서 등)으로 검토해야한다.
- 외부위탁 계약 시 보안 요구사항
  외부위탁 계약시 정보시스템/네트워크/인력/사무환경 등을 관리통제하기 위한 보안 요구사항을 계약서상에 명시해야한다.
- 외부자 보안관리
  정보시스템 및 관련 시설에 대한 제 3자 또는 외부인의 접근을 통제해야한다.

3.2 정보보안컨설팅

기업 보안정책 중에서 외부 전문가 활동 즉, 주기적으로 외부 보안 전문가에 의한 정보시스템의 보안 취약점 진단 및 이에 대한 평가를 해주는 보안컨설팅이 매우 중요한 역할을 한다. 본 절에서는 전통적인 정보보안컨설팅에 대해 살펴보고자한다.

(그림 2) 전통적인 보안 컨설팅 방법

(그림 2)는 국제노동기구(ILO)에서 제시한 밀란 모형(Milan Model, 1996)을 중심으로 제시되었다.[4]

정보보안 컨설팅은 '체계 수립 컨설팅'과 '개인정보보호 컨설팅'으로 구분할 수 있다. 일반적으로 보안체계를 만드는 것이 '체계 수립 컨설팅'이다.

체계 수립 컨설팅은 정보 자산을 구분하는 것부터 시작된다. 기업 내부의 정보는 어떤 것들인지, 문서는 어떤 것들이 있는지, PC 내의 파일뿐만 아니라 DB 내의 정보를 파악한다. 특히 기업 평판을 기반으로 중요한 정보를 구분하고 있는지도 점검한다. 정보에 대한 파악이 완료되면 취약점 판단을 진행한다. 서버에 취약점이 있는지, 내부 직원의 부주의로 인한 보안 위협 여부와 외부 위협, 즉 해킹 등 공격이나 물리적인 침입에 의한 위험도를 산정한다. 가장 심각한 위협부터 비교적 위험도가 낮은 위협까지 구분한다. 이렇게 산정한 위험도를 토대로 고객사의 보안 책임자와 논의를 통해 어느 정도의 위험 수준까지 수용할 것인지를 결정한다. 덜 중요한 자산에 대해서는 어느 정도 위험을 감수하고, 위험이 심각하게 우려되는 부분에 대해서는 위험 해결을 결정하는 등의 내용을 포함한 보호 대책서를 작성한다. 이때 솔루션 구축을 위한 지침서와 직원 교육 방안까지 마련한다. 고객의 조직을 기반으로 누가, 무엇을, 어떻게 해야 하는지를 구체적으로 정리하여 제시한다.

'개인정보보호 컨설팅'은 다르다. 개인정보 보호와 관련된 법적 요구 사항은 일반적인 법적 요구 사항과는 다르기 때문이다. 개인정보 보호를 위해서는 개인정보의 흐름, 즉 개인정보의 라이프사이클(Lifecycle)에 대한 분석이 핵심이다. 개인정보가 온/오프라인에서 어떻게 수집됐는지, 수집 과정에서 동의 및 목적에 대한 정리가 적절했는지, 개인정보가 어떻게 저장되고 누가 사용하고 있는지, 위탁 업체 등 어떻게 외부로 나가고 어떻게 폐기되기까지 개인정보의 흐름 과정에서의 위험도를 평가한다. 그렇기 때문에 개인정보 보호 컨설팅은 여러 가지 요소를 고려해야 하고, 좀 더 많은 시간이 소요된다.

3.3 기업 업종에 따른 정보보안컨설팅 방법론

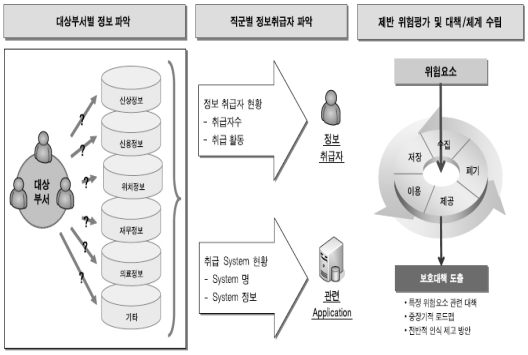
기업의 피해유형을 보면 개인정보유출과 시스템파괴로 나눌 수 있으며 이에 따른 정보보안컨설팅 방법

이 달라야한다.

3.3.1 금융·보험업 컨설팅 방법

금융·보험업은 보안사고가 결국 고객의 금전적 손실을 초래하기 때문에 전통적인 정보보안컨설팅만으로는 대응하기가 어렵게 된다. 따라서 보다 효율적이고 현실적인 위험분석 및 평가를 통해 대응책을 마련해야한다. 즉, 내부 구성원의 인식 부족으로 인한 웜/바이러스 감염에 무방비 상태가 되지 말아야하며 조직의 내부 보안기준을 구성원에 동일하게 일괄 적용함으로써 고객정보 위험성이 높은 직군에 의해 보안사고가 발생하는 것을 사전에 대비해야한다. 또한 인력 채용 시 신원 검증을 거치고 접근통제, 모니터링이 강하게 이루어져야한다. 이와 같이 사람과 정보에 대한 위험분석이 별도로 이루어져야만 보안 사고를 막을 수 있다.[5]

특히, 정보 및 사람 중신의 위험분석 기법은 보호대상 핵심 업무 프로세스상의 핵심 정보와 사람에 내재한 위험을 파악하고 특히, 상관관계에 대한 교차분석을 통해 간과할 수 있는 위험을 분석하는 데 있다.



(그림 3) 정보 중심, 사람 중심의 위험분석 개념도

3.3.2 개인 기업 컨설팅 방법

일반 개인 기업인 경우 정보보안에 대한 특별한 법/제도가 존재하지 않기 때문에 별도의 예산을 확보해가면서 정보보안을 고려하기는 힘든 상황이지만 엄청난 고가의 장비를 이용하는 기업에서는 고객의 다양한 정보를 악용하는 사고사례가 발생하므로 이에 대한 정보보안 컨설팅이 필요한 시점이다. 금융·보험업에서 이루어지는 정보 중심, 사람 중심 정보보안컨설팅보다는 산업군의 속성에 따라서 정보보안컨설팅이 이루어져야한다. 예를 들어, 게임 산업의 활성화로 인해 개인정보 유출 관련 소송 사례와 게임프로그램 소스가 국외로 유출되는 사고 등은 개인 기업이 단독으로 정보보안 컨설팅을 받는 것보다는 Security Drivers 관점에서 정보보안 컨설팅이 이루어져야한다. 즉, 기업이나 기관에서 정보보안을 고려하게 되는 동기를 크게 Security Thread, Compliance, Biz-Requirement, Biz-Opportunities 로 나누어 각각의 동기에 따라 컨설팅이 이루어지게 된다.[6]

4. 결 론

기업의 해킹사고에 따라 보유하고 있는 개인정보의 노출은 심각한 상황까지 이르렀다. 그리고 기업 업종에 따라 발생되는 보안위협요소도 다르다. 따라서 본 논문에서는 기업 업종에 따른 보안위협요소를 살펴보고 이에 적합한 정보보안컨설팅 방법을 제시하였다.

첫째, 금융·보험업은 내부 구성원의 인식 부족으로 인한 웜/바이러스 감염에 무방비 상태가 되지 말아야하며 조직의 내부 보안기준을 구성원에 동일하게 일괄 적용함으로써 고객정보 위험성이 높은 직군에 의해 보안사고가 발생하는 것을 사전에 대비해야한다. 그러므로 사람과 정보 중심의 정보보안컨설팅 방법이 적용되어야한다. 둘째, 개인기업의 경우 산업군의 속성에 따라 정보보안컨설팅이 이루어져야한다.

향후에는 제시된 두 가지 정보보안컨설팅 방법에 대해 실제적인 적용 사례를 연구하므로 기존의 보안컨설팅 시장에서 적용되고 있는 법/제도적 방법론과 비교하고자 한다.

참고문헌

[1] 이수그룹, “http://www.isu.co.kr/”

[2] 신원부, 김태훈, 김종엽, “개인정보보호의 현황과 개선 방안”, 한국위기관리논집 제9권 제6호, 2013.06

[3] 김민수, “기업 보안정책 수립 시 체크리스트”, ㈜인젠
[4] 한국산업기술진흥협회, “보안컨설팅용 실무가이드”, 2007.12.
[5] 이수영, “위험분석 기법과 보안컨설팅 동향”, 2008.8
[6] 홍진기, “국내 정보보보안컨설팅의 종류와 사례 소개”, 인포섹(주)

[저 자 소 개]

이 수 연 (Su-youn Lee)

1990년 단국대학교 전자계산학과 (이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)
1997년 3월 ~ 현재 백석문화대학교 인터넷정보학부 교수