사이버 보안 커리어 로드맵 - where & what

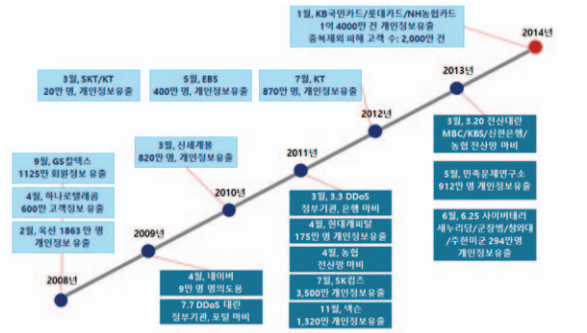
Ⅰ. 서 론

국내 해킹 분야는 1990년대 초 KAIST와 POSTECH 간의 해킹 전쟁으로 인해 해킹이라는 분야가 일반인에게 알려졌다[1]. 이후, KAIST와 POSTECH 출신들이 1990년 후반에 에이쓰리시큐리티컨설팅, 인젠, 해커스랩 등 보안전문회사를 만들면서 본격적인 해커들의 전성기가 이뤄졌다. 한편, 보안 분야에서는 수학과 암호학이 보안의 가장 선두적인 학문으로, 이 분야 전문가들이 보안 산업계에서 활동하기 시작했다. 당시만 해도 해킹과 보안이라는 분야는 일반인들이 쉽게 다가가기 어려운 분야였고, 이 분야에서 종사하는 전문가들도 매우 소수였다. 또한, 분야의 특이함으로 인해 해킹을 주로 하던 사람들은 정보보안전문 업체에서 모의해킹 업무를 하였고, 암호학을 주로 연구하는 사람들은 국가기관 또는 연구기관에서 보안솔루션을 개발하였다.

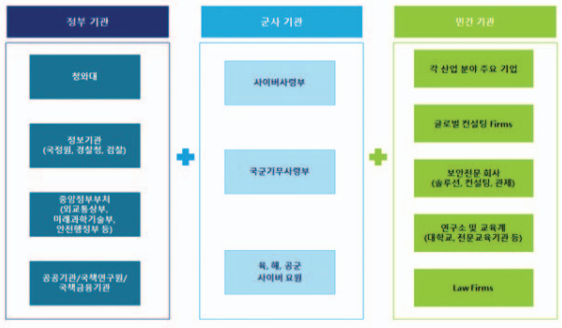
2000년 중반까지도 보안 전문가들은 학계나, 보안전문컨설팅 업체, 솔루션 업체 등 규모가 크지 않은 중소 업체에서 근무하는 경우가 많아

2003년 1월 25일 1.25 대란 발생 이후 정부에서는 보안을 총괄 책임 질 컨트롤 타워로 국가정보원을 정하였고, 이듬해 2004년 국가정보원 산하 국가사이버안전센터를 만들어서 운영하기 시작했다[2]. 그러나 이 때만해도 일반 기업들은 정보보안에 대해 전혀 무관심하여 전담 보안 팀이 없거나 심지어 정보보안전문가가 한 명도 없이 단지 IT 담당자가 보안을 겸임하는 경우가 많았다. 2000년 중반까지도 보안 전문가들은 학계나, 보안전문컨설팅 업체, 솔루션 업체 등 규모가 크지 않은 중소 업체에서 근무하는 경우가 많았고, 일부 게임회사

김 경 곤
딜로이트 안진회계법인
Manager



〈그림 1〉 2008년 이후 국내 주요 보안사고 이력



〈그림 2〉 사이버 보안 관련 근무 분야

나 증권회사에서 보안 전문가들을 영입하곤 했다.

2003년 이후 국내 그렇다 할 대형 보안사고가 생기지 않자 점차 기업에서는 보안에 대해 관심을 잃어가고 있었다. 그러다가, 2008년부터 매년 대형 보안사고가 터지자 기업에서는 저마다 보안전문가를 급히 채용하기 시작했다.

여기서는 일련의 보안 분야 채용 흐름을 분석하여 사이버 보안 분야에서 활동 할 수 있는 커리어 로드맵을 정리하였다. 사이버 보안 분야에서 활동하고 있는 현직이나, 이 분야에 들어오고자 하는 사람들이게 주로 활동할 수 있는 회사(Where)과 업무(What)가 무엇이 있는지 살펴보고자 한다.

Ⅱ. 사이버 보안 관련 근무 조직(Where)

1. 정부기관

사이버 시큐리티 분야에서 활동할 수 있는 곳은 크게 정부기관, 군사기관, 민간기업, Self-employed으로 구분 지을 수 있다. 정부기관으로는 청와대, 정보기관(국정원, 경찰청, 검찰 등), 중앙정부부처(외교통상부, 미래과학기술부, 안전행정부 등), 그리고 다수의 공공기관, 국책연구원, 국책금융기관 등이 있다. 군사기관으로는 사이버사령부, 국군기무사령부, 육·해·공군 등과 같은 조직이 있다.

민간기업은 더욱 세분화 할 수 있는데, 민간기업에는 각 산업 분야 주요 기업에서 정보보안 전문가를 채용하고 있다. 또한 글로벌 컨설팅 펌(경영컨설팅, IT컨설팅, 회계컨설팅 등), 보안전문회사(솔루션, 컨설팅, 관제), 연구소 및 교육계(대학교, 전문교육기관 등)이 있으며, 최근 개인정보유출 사고로 인한 소송 등 법적인 문제로 인해 법무법인(Law Firms)에서도 정보보안 전문가를 채용하고 있는 추세다.

조금 더 구체적으로 들어가면, 정부기관, 공공기관, 국책기관으로 청와대, 국가사이버안전센터, 안전행정부, 국가정보원, 경찰청 사이버테러대응센터, 미래창조과학부, 한국인터넷진흥원, 국가보안기술연구소, 금융보안연구원, 금융감독원, 금융결제원, 한국은행, 한국거래소, 한국증권전산(KOSCOM), 한국전력공사, 한국수자원공사, 한국도로공사, KDB금융그룹, IBK기업은행 등에서 정보보안 전문가를 채용하고 있다. 군사기관으로는 국군 사이버사령부와 기무사령부가 대표적이다.

2. 민간분야

민간 분야는 보다 더 다양하게 구분될 수 있다. 여기서는 글로벌 컨설팅 펌(Deloitte 등)에서 구분짓는 Industry 기준으로 분류한다. 세계적인 컨설팅 회사인 딜로이트는 민간산업을 다음과 같이 크게 구분하고 있다[3].

금융산업(FSI, Financial Services Industry)

- 은행업, 보험업, 금융투자업, 상호저축은행 & 여신전문금융업

생명과학 및 헬스케어(LSHC, Life Science & Health Care)

- 제약 및 바이오 제약산업, 의료기기산업, 병원 및 의료서비스, 중앙 및 지방정부 의료

소비재 및 물류산업(CB&T, Consumer Business & Transportation)

- 소비재산업, 여행 및 호텔&레저, 운송업, 유통업

에너지 및 자원 (E&R, Energy & Resources)

- 전력산업, 자원산업, 석유 및 가스산업, 수자원산업

제조업 (MFG, Manufacturing)

- 자동차 산업 분야, 철강 산업 분야, 화학 산업 분야, 기타 제조업 분야

첨단기술, 미디어, 통신 (TMT: Technology, Media & Telecommunications)

- 첨단기술산업, 미디어산업, 통신산업

〈그림 3〉 사이버 보안 관련 근무 분야

〈그림 4〉 민간 분야에서의 사이버 보안 근무 회사

3. 산업분야

각 산업 군별로 대표적으로 정보보안 전문가를 채용하고 있거나, 정보보안 팀을 운영하고 있는 조직은 다음과 같다.

금융산업 (FSI)

> 정부의 정책에 의해 의무적으로 정보보안 전문조직을 구성하고, 정보보안 전문가를 채용해야 하기 때문에 대부분의 금융기관에는 정보보안 전문가가 근무하고 있어

금융산업에 해당되는 금융 기관들은 정부의 정책(전자금융감독규정 및 모범규준 등)에 의해 의무적으로 정보보안 전문조직을 구성하고, 정보보안 전문가를 채용해야 하기 때문에 대부분의 금융기관에는 정보보안 전문가가 근무하고 있다. 금융산업에 대표적인 기업들은 다음과 같다.

- 시중은행 : KB국민은행, 우리은행, 신한은행, IBK기업은행, 하나은행, 외환은행, 스탠다드차타드은행, 씨티은행, HSBC
- 특수은행 : 농협, 수협, 한국산업은행, 기업은행, 수출입은행, 한국은행
- 증권 : 삼성증권, 미래에셋증권, 대신증권, KDB대우증권, 우리투자증권, 키움증권, 동양증권, 신한금융투자증권, 현대증권, 한국투자증권, 하나대투증권, 한화증권, HMC투자증권
- 신용카드 : 신한카드, KB국민카드, 현대카드, 삼성카드, 롯데카드, 하나SK카드, 우리카드, BC카드, NH농협, KEB외환은행카드, 기업은행카드

생명과학 및 헬스케어 (LSHC) 산업

생명과학 및 헬스케어 산업은 아직까지 금융권에 비해 정보보안 전문조직 구성 및 전문가 채용이 늦은 편이다. 하지만, 정부의 원격의료제도 시행 예정 및 생명과학 분야에서 다루는 개인정보의 민감성으로 인해 머지 않아 정보보안 전문조직을 운영할 가능성이 매우 높은 산업 분야다. 생명과학 및 헬스케어 산업에서의 대표적인 기업들은 다음과 같다.

생명과학(제약)회사(SK케미칼제약, 드림파머, 동아제

약, 녹십자, 유한양행, 한미약품, 대웅제약, JW중외제약 등), 의료서비스(서울대병원, 삼성서울병원, 삼성의료원, 세브란스병원, 현대아산병원)

소비재 및 물류산업 (CB&T)

소비재 및 물류산업도 굉장히 많은 개인정보를 취급하고 있기 때문에 관련 전문가들을 채용하거나 채용할 예정인 기업들이 많다. 소비재 및 물류산업에서의 대표적인 기업들은 다음과 같다.

-Consumer Product : 사무용품(한샘, 리바트, 퍼시스, 에이스침대, 에넥스, 보루네오가구), 생활용품(애경산업, 옥시, CJ라이온, 피죤, LG생활건강, 아모레퍼시픽), 음식료업(CJ제일제당, 오뚜기, 농심, 풀무원식품, 사조식품, 롯데칠성음료, 코카콜라음료, 한국야쿠르트, 해태제과, 빙그레), 의류/신발(제일모직, LG패션, 코오롱인터스트리, SK네트워크패션), 주류(하이트맥주, OB맥주, 진로, 배상면주가, 국순당), 화장품(아모레퍼시픽, 참존, LG생활건강, 코리아나 화장품, 코스맥스), 외국계 한국지사인 한국암웨이, 이베이코리아 등도 있다.

에너지 및 자원 (E&R)

에너지 및 자원 산업은 금융산업과 같이 쌍두마차를 이루는 중요한 산업 군이다. 금융산업과 같이 대량의 고객을 접하는 경우가 많지는 않으나, 한번 보안사고가 발생하면 피해 규모가 매우 크기 때문에 에너지 및 자원 산업 군에서도 정보보안 전문가를 채용하고 있거나 채용할 계획인 기업들이 많다. 에너지 및 자원산업에서의 대표적인 기업들은 다음과 같다.

자원개발.Mining(광물공사, LG상사), 에너지(STX에너지, GS에너지, SK가스, 서울도시가스, 대성에너지, E1), 정유(SK에너지, GS칼텍스, S-OIL, 현대오일뱅크, SK이노베이션), 전력(한국전력공사, 한국수자원공사, 한국남동발전, 한국중부발전, 한국서부발전, 한국남부발전, 한국동서발전), 수자원(한국수자원공사)

제조업(MFG)

제조업 분야는 한국 경제를 실제적으로 성장시키는 매우 중요한 산업 군이다. 삼성전자를 비롯하여 제조업 분야에서 제품을 만들어 해외로 수출하는 경우가 매우 많기 때문에 제조업 분야는 한국에서도 효도 산업 분야다. 제조업의 특성 상 정보에 대한 보안 보다는 물리적인 출입 보안이나 현물(제품) 보안이 중요하기 때문에 전통적으로 물리보안을 강화하였다. 하지만 물리보안뿐만 아니라, R&D, 지적재산권, 특허 등 전자적으로 보호해야 하는 데이터들이 많기 때문에 정보보안전문가를 채용하는 추세다. 제조업 분야에서의 대표적인 기업들은 다음과 같다.

자동차(현대.기아자동차, 르노삼성자동차, 쌍용자동차, 한국GM, 대우자동차), 자동차부품(현대모비스, 만도, 한라공조, 한국델파이, 두원공조, 현대오토넷, 현대케피코, 현대위아, 다이모스, 한국타이어, 넥센타이어, 금호타이어), 수입차(벤츠코리아, BMW코리아, 아우디, 폭스바겐, 토요타, 한국닛산, 혼다코리아, 한불모터시, 볼보코리아), 석유화학(호남석유화학, LG화학, SK케이칼, SKC, 한화케미칼, 대림산업유화, 금호석유화학, 삼성토탈, 삼성정밀화학, 삼성석유화학, OCI, 대한유화, KCC), 화학섬유(코오롱인더스트리, 태광산업, 휴비스, 웅진케이칼, 효성섬유), 소재부품(쌍용양회, 유진기업, 한일시멘트, 삼표, 아주산업, 동양시멘트, 한라시멘트, 아세아시멘트), 조선(현대중공업, 현대미포조선, 현대삼호중공업, 삼성중공업, 대우조선해양, STX조선해양, 한진중공업), 기계/중장비(두산중공업, 두산인프라코어, 두산엔진, 현대위아, S&T중공업), 전선(LS산전, 대한전선, LS전선), 철강(포스코, 현대제철, 동국제강, 현대하이스코, 동부제철, 포스코강판, 포스코P&S, 현대하이스코), 비철금속(고려아연, 풍산, 고려제강, 현대알루미늄, 롯데알미늄, 노벨리스코리아, 인터플렉스, 코리아써키트)

첨단기술, 미디어, 통신(TMT) 분야

첨단기술, 미디어, 통신 분야의 대표적인 기업으로는 다음과 같다.

-첨단기술 대표기업

IT서비스 : 삼성SDS, LG CNS, SK C&C, 한국IBM, 포스코ICT, LG엔시스, 현대오토에버, 동부CNI, KTDS, 롯데정보통신, 한전 KDN, 신세계I&C, 코스콤, 우리FIS, 대우정보시스템, 동양시스템즈 등

TV/가전(삼성전자), 디스플레이(삼성디스플레이, LG디스플레이), 반도체(SK하이닉스), 반도체부품(삼성전기, LG이노텍, 삼성테크윈), 휴대폰(삼성전자, LG전자)

-Media 대표기업

게임(NC소프트, 넥슨, 네오위즈게임즈, NHN 엔터테이먼트), 광고(제일기획, 이노션, SK마케팅앤컴퍼니, 대홍기획, 한컴, 오리콤), 영화/엔터테인(CJ CGV, CJ E&M, SM엔터테인먼트, 로엔엔터테인먼트, JYP엔터테인먼트, HQ싸이더스), 포탈(NHN, 다음커뮤니케이션, SK커뮤니케이션)

-T(Telecommunication) 대표기업

유무선 통신서비스(KT, SK텔레콤, SK브로드밴드, LG U+, 삼성네트웍스)

여기서 각 산업분야를 구분하고 파악해야 하는 이유는 보안이라는 것은 조직의 교유한 비즈니스를 명확히 이해하고 있지 않으면, 혼자 외딴 섬에서 고기나 잡는 동떨어짐을 느끼게 될 뿐만 아니라, 본인이 속한 조직에서 인정을 받기가 더욱 어렵기 때문이다. 자신이 속해 있는 회사가 무엇으로 돈을 벌고 있는지에 대한 정확한 이해가 없으면, 회사에서 보호해야 하는 중요한 자산이 무엇인지도 알 수 없으며, 현업부서 사람들과 커뮤니케이션 할 때도 장애가 생길 수 있다. 무엇보다도 상층으로 올라가려면 반드시 회사의 핵심 비즈니스를 파악해야 C-Suite (CEO, CIO, CFO 등)에게 인정받으면서 일을 할 수 있기 때문이다.

글로벌 컨설팅 펌

민간 분야 중에서 산업 분야가 아닌 컨설팅 펌에서도 정보보안 전문가를 채용하고 있다. 여기서는 컨설팅 펌 중에서 사이버 보안 서비스를 수행하는 컨설팅 펌을 중점으로 설명한다. 컨설팅 펌은 글로벌 컨설팅 펌과 로컬 컨설팅 펌으로 구분할 수 있다. 세계적인 조사기관인 Gartner에서 글로벌 사이버 시큐리티 컨설팅 분야의 컨설팅 펌 중 상위 10개의 전세계 시장 순위를 조사한 결과를 보면 〈표 1〉과 같다.

또 다른 세계적인 리서치 기관인 Forrester 에서 2013년 1분기 Security와 Risk 분야 전문서비스 회사를 조사한 결과 다음과 같이 Deloitte, Accenture, IBM, E&Y, KPMG, PwC가 Leaders로 선정되었다.

〈표 1〉 상위 10개의 전세계 시장 순위

Top 10 Security Consulting Providers' Worldwide Market Share, 2011-2012 (Millions of Dollars)

2011 Rank	2012 Rank	Rank Change	Company	2011 Revenue	2012 Revenue	Annual Grawth Rate (%)	2012 Market Share (%)
1	1	-	Deloitte	878	1,001	14.0	9.3
2	2	-	Ernst & Young	826	966	16.9	8.9
4	3	+1	PwC	671	807	20.3	7.5
3	4	-1	IBM	721	710	-1.5	6.6
5	5	-	KPMG	478	514	7.5	4.8
6	6	-	Booz Allen Hamilton	430	454	5.6	4.2
7	7	-	Accenture	385	402	4.4	3.7
8	8	-	HP	336	347	3.4	3.2
9	9	-	SAIC	163	177	8.6	1.6
12	10	+2	EMC(RSA Security Division)	149	167	11.7	1.5

Sourec: Gartner (May 2013)

〈그림 5〉 정보보안 컨설팅 서비스 분야 전문 회사

〈그림 6〉 민간기관 중 글로벌 컨설팅 펌

이외에도 글로벌 컨설팅 펌 분야에서는 맥킨지, 보스턴컨설팅그룹, 베인&컴퍼니와 같은 전략 컨설팅 펌에서도 보안 전략 컨설팅 서비스를 제공하고 있다.

국내 보안 회사

국내에는 정보보안서비스를 하는 회사들은 어디가 있는지 알아보자. 미래창조과학부에서는 주요정보통신기반시설의 취약점 분석·평가 업무 및 보호대책을 수립하기 위한 지식정보보안컨설팅 전문업체를 선정했다. 기존 지식정보보안컨설팅 전문업체로는 인포섹, 안랩, 롯데정보통신, STG시큐리티, 에이쓰리시큐리티, 시큐아이, 싸이버원 7곳이다.

〈그림 7〉 민간기관 중 보안전문회사, 연구소 및 교육계, Law Firms

연구소 및 교육계

국내 연구소와 교육계에서도 정보보안전문가가 활약을 하고 있다. 2010년 고려대학교 정보보호대학원에서는 KAIST 해커출신인 김휘강 엔씨소프트 보안실장을 고려대 교수로 임명하였다. 그 이후로도 다수의 해커 및 보안전문가들이 정보보호전문대학교에서 교수 및 연구원으로 활동하고 있다.

Law Firms

전통적으로 변호사의 영역이었던 로펌에서도 정보보안전문가의 수요는 꾸준히 늘고 있다. 특히 보안사고 및 개인정보관련 소송으로 인해 변호사들은 정보보안전문가의 도움이 절대적으로 필요하여 김&장, 태평양, 율촌 등 주요 법무법인에서는 정보보안전문가를 전문위원으로 채용하고 있다.

Ⅲ. 사이버 보안 관련 직업 (What)

사이버보안 분야의 가장 첫 직업 군은 해커와 암호전문가로 구분할수 있을 것이다. 해커는 컴퓨터가 탄생한 후 컴퓨터를 많은 사람들이 쓸 수 있도록 하기 위해 1980년대 미국 MIT 학생들에 의해 처음 탄생 된 후, 지금까지도 제한된 자원에 접근하는 공격 기술을 가진 사람들로 일컬어지며, 공격성향에 따라 Black Hacker, White Hacker, Gray Hacker 등으로 불려지기도 한다. 해커들이 언더 그라운드에서 제도권으로 들어오면서 침투 테스터(Penetration Tester)로 전환하는 경우가 많다.

암호전문가는 주로 수학적 배경지식을 가진 사람들로써, 군대에서 많은 필요에 의해 교육되고 훈련된 사람들이 처음에 주를 이루었다. 세계대전을 겪으면서 적국의 암호 시스템을 해독하고, 자국의 암호 시스템을 강화하기 위해 많은 암호학자들이 배출되었다. 이후 암호분야 전문가들이 정보를 보호하기 위해 암호뿐만 아니

라 접근 제어, 인증 등 다양한 보안 솔루션들을 개발하면서 자연스럽게 공격자로부터 중요정보를 보호하는 입장에 서게 되었다.

국내에서는 1990년 초반에 해커라는 용어가 사람들에게 알려지기 시작했고, 이후 1990년 후반에 초기 해커들이 보안컨설팅 회사를 창립하면서 국내에서는 모의해커라는 특이한 직업 군이 생겨났다.

그리고 2000년 초반에 당시 정보통신부에서 정보보안전문업체로 지정된 회사에서 국가 인프라 기관에 대해 합법적으로 해킹을 시도해서 취약점을 찾고, 권고안을 제시하기 시작했다. 2000년 초반부터 중 후반까지 폭발적으로 해커가 취약점을 찾고 공격하는 환경이 발전하였고, 그러면서 기술적으로는 시스템 해킹, 네트워크 해킹, 웹 해킹을 넘어, 애플리케이션을 공격하는 리버스 엔지니어링 기법들도 발전하기 시작했다.

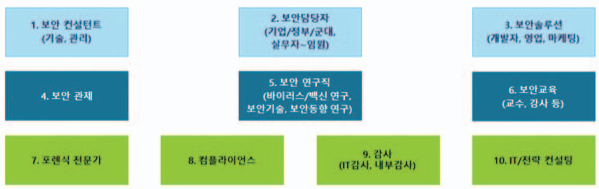
2000년 초반부터 중 후반까지 폭발적으로 해커가 취약점을 찾고 공격하는 환경이 발전하였고, 기술적으로는 시스템 해킹, 네트워크 해킹, 웹 해킹을 넘어, 애플리케이션을 공격하는 리버스 엔지니어링 기법들도 발전하기 시작

기술적인 측면과 더불어 관리적인 측면의 보안도 점차 중요해짐에 따라, 정보보안의 선두 국가인 영국에서 BS7799라는 정보보안관리체계를 만들기 시작했다. 그리고 이것이 2001년도에 ISO 조직에서 국제표준으로 등록되면서 ISO27001 정보보호관리체계가 만들어졌고, 이를 준수하는지 인터뷰와 실사, 점검을 수행하는 보안관리 컨설턴트들도 활약하기 시작했다.

여기서 KISA에서 발간한 2012 국내 지식정보보안 산업 실태조사 연구보고서를 참고하여, 다시 사이버보안에 대한 직업 카테고리를 정리해 보면, "정보보안 연구 및 개발직, 정보보안 관리직, 정보보안 영업직, 기타 정보보안 관련직"으로 구분하고 있다.

실제 해커로써 활동하고 있는 사람들도 정보보안 컨설턴트로 불리는 경우도 있지만, Security Researcher라고 불리는 경우도 있다. 조금 더 구체적으로 정보보안 직업 군을 정리하면 직접적인 분야 6개와 확장분야 4개, 총 10개 분야로 구분할 수 있다.

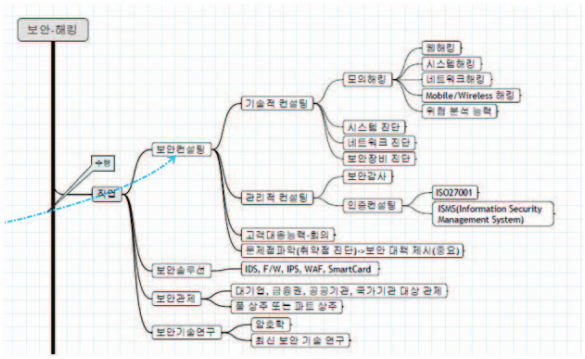
"1) 보안컨설턴트(기술, 관리), 2) 보안담당자(기업/정부/군대 실무자, 임원), 3) 보안솔루션(개발자, 영업, 마케팅), 4) 보안관제, 5) 보안연구직(바이러스/백



〈그림 8〉 사이버보안에 대한 직업 카테고리

〈표 2〉 사이버보안에 대한 직업 카테고리, KISA

구분	세부분류	세부 직종 예시	인원(명)	인원(명)	인원(명)	인원(명)
종보보안 연구 및 개발직	암호 및 인증 기술	관련 연구소 및 산업체의 연구원	284	339	549	680
	시스템 및 네트워크 기술	컴퓨터시스템 분석 및 설계 전문가, 네트워크 분석 및 설계 전문가	246	393	559	484
	응용기술 및 서비스	컴퓨터 바이러스 치료사	167	344	441	503
정보보안 관리직	정보시스템 관리	데이터베이스 관리자 (DB운영)/OS 운영자/리눅스 전문가 전산관리 전문가/시스템 엔지니어/CIO/CSO/CISO	148	400	497	779
	정보보안 컨설팅	정보보안 컨설턴트	105	238	233	236
정보보안 영업직	정보보안 마케팅	정보보안제품 마케팅, 국내외 판로확보	176	312	403	244
기타 정보보안 관련직	정보시스템 감리 및 인증	정보시스템 감시사	12	23	41	42
	정보보안 교육	관련 학과를 개설한 대학의 교수/관련 시설교육기관의 강사	11	23	11	6
	기타	물리적인 보안 종사자(경비인력, 보안업체인력 등) 및 내부 관리인력 등	53	71	17	184
전체 합계(총 보안 인력)			1,202	2,133	2,751	3,158



〈그림 9〉 정보보안관련 직업 군 (2007년 파도콘 발표자료)

신 연구, 보안기술 연구, 보안동향 연구), 6) 보안교육(교수, 강사)"으로 구분할 수 있다. 정보보안 분야를 좀 더 확장하여, 정보보안을 공부하거나 종사하고 있는 사람이 갈 수 있는 분야로 "7) 포렌식, 8) 컴플라이언스, 9) 감사(IT감사, 내부감사), 10) IT컨설팅" 분야로도 진출할 수 있다.

〈그림 9〉는 2007년 파도콘 컨퍼런스에서 발표했던 내용 중 해킹/보안 직업에 대한 부분이다.

2007년에 발표할 당시보다 지금은 사이버 보안 분야가 더 각광받고 있는 추세이다. 그렇지만 직업군이 매우 다르게 변화한 것은 아니며, 큰 틀에서는 2007년과 크게 다르지 않았다. 다만 보안 전문가를 필요로 하는 조직들이 확실히 급격하게 증가한 것은 사실이다. 또한, 보안전문가가 갈 수 있는 직업의 스펙트럼도 넓어졌을 뿐아니라, 정부에서 최고정보보호책임자(CISO)를 의무화 하는 등 스펙트럼의 높이도 높아졌다.

다음으로 보안 컨설턴트에 대해 조금 더 구체적으로 살펴보자.

1) 보안컨설턴트(기술, 관리)

보안 컨설턴트는 병원의 의사가 환자의 건강상태를 정기적으로 검사하는 일을 하는 것처럼 조직(기업, 정부기관 등)의 전산시스템에 있을 수 있는 취약점을 검사하는 일을 한다. 컨설턴트는 자신의 지식과 경험을 바탕으로, 기업의 보안담당자에게 자문을 제공하는데, 자문의 유형에 따라 기술적 측면과 관리적 측면으로 크게 구분을 할 수 있다. 통상적으로 구분하는 기준이 기술적, 관리적인 것이지 실제 업무를 하다 보면 혼합되는 경우도 많다. 기술 기반의 보안 컨설턴트는 주로 정보시스템에 대한 취약점 진단, 침투 테스트 등을 수행하여 조직의 정보시스템에 있는 취약점을 발견하고 공격하여 실질적으로 얼마나 해킹으로부터 피해가 심각한지를 증명해주는 역할을 한다.

반면 관리 기반의 보안 컨설턴트는 주로 정보보호관리체계(ISO/IEC 27001, ISMS), 개인정보보호관리체계(PIMS, PIPL 등)와 같이 정부나 국제단체에서 권고하는 프레임워크, 체크리스트를 기반으로 조직의 보안 수준이 어느 정도 인지를 측정하고, 부족한 부분을 식별해서 개선할 점, 그리고 향후 보완해야 할 점을 마스터 플랜에 담아 담당자에게 전달한다. 한국에서는 관리 기반의 보안 컨설팅 시장이 ISMS, ISO/IEC 27001, PIMS와 같은 Compliance 기반의 컨설팅이 주를 이루고 있지만, 외국에서는 보안 전략 수립, 보안 조직 설계, 사이버 인텔리전스 체계 수립 등과 같이 실질적으로 조직의 보안을 향상 시키기 위한 다양한 종류의 컨설팅 서비스를 제공하고 있다.

보안 컨설턴트는 항상 고객 사 보안 담당자들에게 보안 자문을 제공해 줘야 하기 때문에 항상 새로운 보안 동향(기술적 측면, 관리적 측면)을 숙지해서 정보를 제공해줘야 한다. 또한, 끊임 없는 자기 계발을 통해 자신의 브랜드를 높여서 고객이 서로 찾도록 하는 컨설턴트가 되어야지 보안 컨설턴트로써는 성공한 것이 아닌가 싶다.

2) 보안담당자(기업/정부/군대 실무자, 임원)

기업의 보안 담당자는 자신이 속한 기업의 정보 자산을 내/외부의 악의적인 사용자로부터 침해 되거나, 유출되는 것을 막는 역할을 수행하는 사람들이다. 많은 기업 보안담당자들은 보안 측면에서는 해박한 지식과 경험을 가지고 있으나, 본인이 속해 있는 조직이 무엇으로 성장하고 있는지를 간과하고 있는 경우가 많다. 따라서 기업의 보안담당자가 반드시 알아야 하는 것은 기술적인 측면도 있지만, 본인이 속해있는 조직의 업을 정확히 이해해야 하며, 우리 조직은 무엇으로 성장하고

〈그림 10〉 실무진부터 CISO까지 갖추어야 하는 역량

있는지를 알아둬야지 지켜야 할 대상을 명확히 알 수가 있는 것이다.

자신이 속해 있는 조직의 핵심 자산이 무엇인지 알기 위한 방법 중 하나는, 만일 상장회사라면 dart.fss.or.kr 과 같은 공시 사이트에서 자신이 일하고 있는 회사의 사업계획서와 재무제표를 반드시 꼼꼼히 살펴보는 것도 매우 좋은 방법이다. 회사의 사업계획서를 보면 우리회사가 무엇으로 성장하고 있는지, 어떤 분야가 핵심 업무인지를 알 수 있으며, 재무제표가 있는 감사보고서를 보면 구체적으로 어떤 부분이 회사의 주요 매출이 되어 회사의 성장에 견인차가 되고 있는지, 회사의 내부통제시스템은 어떤지를 보다 정확히 이해할 수 있게 된다.

회사가 무엇으로 먹고 사는지, 회사의 최고 경영진(CEO)가 어떤 분야를 중시하고 있는지를 정확이 알고 있는 보안담당자와 그렇지 않고 보안만 알고 있는 기업의 보안담당자의 성장 잠재력은 하늘과 땅 차이다. 회사의 주요 서비스와 주요 매출을 알고 있는 기업의 보안담당자는 속해 있는 팀장에게도 다르게 보일 것이며, 현업과 커뮤니케이션 할 때나, 특히 향후 진급하여 경영층과 커뮤니케이션 할 일이 생길 때도 보다 더 경영진의 마음에 드는 관점으로 보안을 이야기 할 수 있을 것이다. 기업의 보안담당자는 경력에 따라 신입부터, 팀장, 최고정보보호책임자(CISO)까지 나눠질 수 있으며, 각각에서 중요하게 고려해야 할 부분은 〈그림 10〉과 같다.

자신이 하고 있는 사이버 보안 분야의 일이 어떠한 의미를 지니고 있는지를 생각해야

Ⅳ. 결 론

2013년 12월 24일 매일경제 신문에 'Why'가 주는 긍정의 힘 이라는 사설이 실렸다. '와이(Why)로 시작하라'라는 세계적 베스트셀러를 쓴 사이먼 사이넥, 그는 TED 강의에서 '위대한 리더들이 어떻게 행동을 이끌어냈나'를 주제로 강의를 했다. TED 강의 조회수는 무려 1370만회다. 그는 잘 나가는 컨설턴트였으며, 마케팅 회사를 창업해 큰 성공을 거뒀다. 하지만 그는 깊은 어둠 속에 있는 것 같았다고 한다. "고객들은 훌륭했고 나는 좋은 삶을 살고 있었죠. 어떤 잣대로든 행복해야 했어요. 그러나 전혀 그러지 않았어요." 그는 "더 이상 일에서 성취감을 느낄 수 없었다"며 "내 열정에 불을 붙일 무언가가 필요했다"고 회생했다. 고민 끝에 그는 자신의 존재이유를 찾는 데서 인생을 시작했다. 기자의 지인도 좋은 부서에서 승승장구 하면서 성공하고 있었는데 깊은 회의에 빠져서 내가 왜 이 일을 해야 하는지 모른다고 했다. 그는 한직인 소비자 제품, 서비스 부서에서 일하기를 지원했는데, 소비자들을 돕는 데에서 자신의 '와이'를 찾았기 때문이라고 한다.

사설에서는, 사람은 두 부류의 종류가 있다고 한다. 한 부류는 승리(Winning)을 쫓고, 한 분류는 의미(Meaning)을 좇는다. 전자는 권력, 높은 자리, 돈이 중요하다. 그러나 후자에게는 자신이 왜 존재하는지 삶의 이유가 중요하다. 기자의 지인과 사이먼은 한때 전자의 삶을 추구하다가 깊은 회의감을 느끼고 후자로 넘어왔다. 사설에서는 승리로 얻은 권력과 자리를 결국은 사라지지만, 의미를 추구한 삶의 흔적은 아름다운 추억으로 남는다고 이야기를 하고 있다.

하지만, 회의감이라는 것은 승리와 성취한 경험이 있는 사람들에게만 찾아오는 것이라고 생각한다. 최선의 노력을 다해 자신이 추구하는 성공의 경험을 해본 사람만이 자신의 삶의 의미를 생각해볼 여유가 생긴다. 지극히 현실적으로, 경제적으로 궁핍하고 외로운 상태에

서 자신의 존재의미나 회의감을 느낄 여유를 가지기는 힘들다. 그렇지만 자신의 성공적인 커리어를 쌓는 과정에서 Why가 빠져있는 것은 잘 나가다가도 한 순간에 한 없이 회의감에 빠질 때가 있다. 따라서 자신이 추구하는 성공적인 모습을 그려보면서 Why의 의미를 늘 마음속에 가지는 것이 중요하다.

사이버 보안 분야를 준비하는 학생이나, 갓 기업에 입사한 사회 초년생이나, 10년 이상의 경력을 가지고 있는 중간 간부, 그리고 기업의 최고정보보안책임자(CISO) 모두 본인이 맡고 있는 위치에서 최선을 다하는 것뿐만 아니라, 자신이 하고 있는 사이버 보안 분야의 일이 어떠한 의미를 지니고 있는지를 생각해야 하며, 지속적으로 행복과 성공을 성취할 수 있는 far-off goals을 가져야 한다. 그래야 열심히 노력한 이후에 다가오는 회의감을 피할 수 있다. 유명한 컨설턴트에서 교육자로 전향한 Angela Lee Duckworth는 성공에 대한 열쇠는 "기개(Grit)"이라고 했는데, 기개를 만들어가는 원천으로써 자신이 왜 일하는지 에 대한 의미를 갖는 것이 중요하다는 것이다.

참 고 문 헌

[1] "해커의 전설, 벤처의 신화 되다." "http://www.sisapress.com/news/articleView.html?idxno=61327" 2011. 8.

[2] "국정원, 20일 '국가사이버안전센터' 개소식" "http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=047&aid=0000042869"

[3] Deloitte 산업별 서비스 "http://www.deloitte.com/view/ko_KR/kr/industries/index.htm"

김 경 곤

2013년 2월 고려대학교 정보보호대학원 석사 수료
2008년 2월 숭실대학교 컴퓨터학부 졸업
2011년 12월~현재 딜로이트 안진회계법인
2008년 1월~2011년 12월 삼일회계법인(PwC)
2006년 2월~2007년 12월 SK 인포섹
2003년 8월~2006년 2월 에이쓰리시큐리티컨설팅
2013년 Harvard Career Management Certification 과정 수료

〈관심분야〉
사이버보안 커리어, 모바일 보안, 사이버 리스크