사이버보안 전문가 양성을 위한 연구

김슬기* · 박대우*

*호서대학교 벤처대학원

The Research for cyber security experts

Seul-gi Kim* · Dea-woo Park*

*Hoseo Graduate School of Venture

E-mail : sgkim_18@naver.com, prof_pdw@naver.com

요 약

사이버세계는 국가와 국민의 인프라를 구성하고 통제한다. 사이버 공격과 개인정보유출로 국민경제 피해 및 국가 안보가 위협당하고있다. 2014년 12월 사이버 해킹공격으로 한국수력원자력의 원자력 냉각시스템 설계도면이 유출된적이 있으며, 청와대 홈페이지 해킹, KBS 방송국 해킹 등 사이버사고의 발생하였다. 이에 따라 정보통신기반보호법, 정보통신망이용촉진 및 정보보호등에 관한법률, 개인정보보호법이 시행되고있으며, 앞서가는 첨단 기술로 무장한 해커의 공격을 막기는 어려우나 인터넷 정보화 사회에서 형식적인 요건으로 개인정보보호법을 지켜야 하는 개인정보책임자 양성방안을 제안하고자 한다.

ABSTRACT

Cyber world constitute the infrastructure of the country and its people and control. Cyber attacks and leakage of personal information are being threatened damage to the national economy and national security. December 2014 had been cyber hacking attacks on Korea Hydro & Nuclear Power Nuclear cooling system design drawings of a spill, and Cheong Wa Dae website hacked, KBS stations occurred in cyber hacking accidents. As a result, ICT-based Protection Act, Promotion of Information and Communications Network Utilization and Information Act on Protection, etc., privacy laws are being enforced, personal information in the form of requirements from leading high-tech eoryeowoona is to prevent the attacks of armed hackers Internet information society It proposes positive measures to keep your personal information officer and laws.

키워드

사이버보안(Cyber Security), 자격증(certification), 지식(knowledge)

Ⅰ. 서 론

사이버세상이 도래하였다. 해외에서 미지를 찾아갈 때 스마트폰으로 현재 위치를 파악하고, 목적지를 검색하고, 교통통신을 선택하고 예약하고 결제할 수 있다. 이 정보는 스마트폰 사용자의 위치추적은 물론, 움직이면서 활동 내역을 알수 있는 근거가 된다. 사이버세상의 단점은 이러한 정보를 이용하여, 개인정보와 금융정보를 추적하고, 이러한 정보를 이용하여 경제적, 사회적 침해사고를 일으킬 수 있다는 점이다. 따라서 이러한 사이버 보안을 위한 전문가가 필요하고, 전문가를 양성하고 전문가를 측정하기 위한 전문기술과 소양을 갖춘 사이버보안전문가 양성이 필요하다. 본 논문에서는 사이버보안 전문가 양성을 위한 Web hacking, System hacking, Network hacking 등에 대한 보안 지식(Knowledge)를 DB에 축적하고, 학습 후에 자격증을 취득하고, 보수교육을 할수 있는 사이버보안전문가 양성을 위한 연구를 한다.

Ⅱ. 본 론

2.1 Web hacking

웹은 문자뿐만이 아닌 영상, 음성 등이 혼합된 멀티미디어 정보를 통신망으로 세계 각지에 연결시켜주는 서비

스다. 웹 사이트의 취약점을 공격하는 기술적 위협으로, 웹 페이지를 통하여 권한이 없는 시스템에 접근하거나 데이터 유출 및 파괴와 같은 행위를 뜻한다. OWASP Top 10 해킹방식으로는 인젝션, 인증 및 세션 관리 취약점, XSS, 취약점 직접 객체 참조, 보안 설정오류, 민감 데이터 노출, 기능 수준의 접근 통제누락, CSRF, 알려진 취약점이 있는 컴포넌트 사용, 검증되지 않은 리다이렉트 및 포워드가 선정되었다[1].

표1. 국정원 4대 취약점
Table 1. NIS vulnerabilities 4

	국정원 4대 취약점
SQL Injection 취약점	신뢰할 수 없는 데이터가 명령어나 질의어의 일부분으로써 인터프리터에 보내질 때 발생하며, 공격자의 악의적인 데이터는 예기치 않은 명령실행이나 권한없는 데이터에 접근하도록 인터프리터에 속일수 있다[2].
ZeroBoard 취약점	Zeroboard의 일부 php프로그램이 원격에 있는 php파일을 실행할 수 있는 결함이 있으며 컴퓨터 명령어를 실행하여 화면을 변조하거나 컴퓨터를 조작 할 수 있다.
Cross Site Script 취약점	적절한 확인이나 제한없이 애플리케이션이 신뢰할 수 없는 데이터를 갖고 웹브라우저로 보낼 때 발생되며 공격자가 피해자의 브라우저 내에서 스크립트의 실행을 허용함으로써, 사용자의 세션을 탈취하거나 웹사이트를 변조, 악의적인 사이트로 사용자를 리다이렉트 할 수 있다[3].
File Upload 취약점	첨부파일 업로드를 허용하는 홈페이지에서 .php .jsp등의 확장자 이름의 스크립트 파일의 업로드를 허용할 경우 원격으로 서버 컴퓨터의 시스템 운영 명령을 실행할 수 있다.

2.2 System hacking

운영체제 기반의 해킹 유형은 일반적으로 공격하고자 하는 시스템이 결정되면 먼저 운영체제 종류를 파악한 다음 그에 따른 취약점을 발견하고 다양한 공격방법을 시도한다[4]. 시스템의 프로그램 취약점을 이용한 해킹으로 버퍼오버플로우, 포맷 스트링과 같은 기법을 이용하여 취약한 시스템을 공격하여 해당 시스템에 접속하여 관리자 권한을 획득하는 행위를 뜻한다.

표2. 시스템 해킹 대표적인 3가지 기법
Table 2. Typical system hacked 3 techniques

	시스템 해킹
Back Door	시스템에 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고 응용프로그램이나 시스템에 접근이 가능해 시스템 재침임 또는 권한 취득이 가능하다.
Buffer overflow	C/C++ 컴파일러가 배열의 Boundary Check를 하지않아 선언된 크기보다 더 큰 데이터를 기록하고, Stack이나 Heap영역에 임의의 데이터 기록 및 실행을 허용한다.
Password Craking	사전에 나오는 단어나 키보다 자판 나열, 사용자 계정 정보에서 유추한 단어, 패스워드의 길이가 짧거나 설정되어있지 않은 경우가 취약한 패스워드의 분류로 나눠져 있다.

2.3 Network hacking

네트워크란 여러 가지 정보기기 사이에서 전송매체를 이용하여 데이터 통신을 제공하는 것을 뜻하며 현재의 시스템들은 대부분 네트워크에 연결되어 통신이 되고있는 상황이다[5]. 네트워크로 주고받는 모든 데이터들에 대한 가로채기 시도나 네트워크 통신을 방해해 네트워크상에 문제를 발생시키는 행위를 뜻한다.

표3. 네트워크해킹 대표적인 3가지 기법
Table 3. Typical network hacking 3 techniques

	네트워크 해킹
Spoofing	'속이다'라는 뜻으로 인터넷이나 로컬에서 존재하는 모든 연결에 스푸핑이 가능하며 서로 통신하고있는 상황을 속여 정보를 획득한다.
Sniffing	'코를 킁킁거리다'라는 뜻으로 데이터속에서 정보를 얻어내는 기법으로 랜카드로 들어오는 모든 전기 신호를 읽어들여 다른이의 패킷을 관찰하며 정보를 획득한다.
DDoS	DoS 경우 공격 대상이 수용할 수 있는 능력이상의 정보를 제공해 사용자 또는 N/W 용량을 초과시켜 정상적으로 작동하지 못하게하는 공격인데 이것을 분산으로 여러곳에서 한번에 진행하는 공격방식이다.

2.4 전문가 자격증

개인정보 보호법령 규정은 개인정보 처리단계별 규정을 두고 있으며, 개인정보보호 책임자를 임명해야 하나, 현실상황은 제대로 운영되지 않고 있다. 따라서 개인정보보호 책임자 자격증 과정을 만들어서 개인정보보호책임자 자격증을 발급해야 한다. 사이버보안전문가, 개인정보보호책임자 자격증이 필요하며, PC와 스마트폰에서 학습 실습을 위한 Knowldge DB 구축 및 온라인 프로그램 개발에 대한 내용을 바탕으로 자격증학습을 진행한다.

Ⅲ. 사이버보안 전문가양성 지식가평가

3.1 Web hacking Knowledge DB

웹의 구성요소 파악, 웹 공격기법 및 웹 관리에 대한 지식을 평가한다. 웹 해킹의 기본인 본인IP확인부터 웹 브라우저와 웹서버, 웹 애플리케이션, 데이터베이스 서버를 통해 인젝션, XSS, CSRF 등 웹 기반의 공격 기법 해킹지식을 이해해야한다. 웹 해킹 지식평가로는 취약한 인증 및 세션관리, 불안전한 직접 객체 참조, 잘못된 보안설정, URL 접속제한 실패, 불충분한 전송 계층 보호, 확인되지 않은 리다이렉션 및 전달상태[6]가 발생하지 않도록 웹 보안 평가를 진행할 것이다.

3.2 System hacking Knowledge DB

시스템 구성, 시스템을 기반으로 하는 공격방식에 대한 지식을 평가한다. 시스템 해킹 지식평가로는 패치, 방화벽, 계정관리, 패스워드 관리, 파일 및 폴더 관리, 보안 관련 정책, 로그 분석, 침입 추적에 관한 지식을 이해하고 이러한 공격에 대응하기 위한 관리 및 보안설정 방법을 학습하며 시스템 보안 평가를 진행할 것이다.

3.3 Network hacking Knowledge DB

네트워크의 구성 및 종류에 대한 개념, 네트워크 기반의 공격방식에 대한 지식을 평가한다. 네트워크 해킹 지식평가로는 방화벽, 침입탐지시스템, 가상사설망, 허니팟, 기타 보안 솔루션에 대한 지식을 이해하고 네트워크 기반의 공격기법인 Sniffing, Spoofing, DoS 공격에 대응하고 안전한 네트워크 관리를 위한 보안기술을 학습하며 네트워크 보안 평가를 진행 할 것이다.

3.4 Hacking DB 평가 방법 기준

표4. Hacking DB 평가 지표
Table 4. Hacking DB Evaluation Indicators

주요 성능 지표 및 최종 개발 목표	가중치 (%)	객관적 측정 방법	
		시료수 (n≥5개)	시험 규격
1. PC 온라인에서 학습 작동	20	1	웹 접근성 품질 인증
2. 스마트폰에서 학습 작동	20	1	웹 접근성 품질 인증
3. 개인정보보호 책임자 - 사이버 보안전문가 서비스 2급, 3급	40	1	특허 출원
4. 2급, 3급 자격증 문제풀이	20	1	전문가 평가
시료 수 5개 미만 (n<5개)시 사유			
○(자격증)개인정보보호-(자격증)사이버보안전문가의 학습과 실습 및 평가를 위한 Knowledge Contents와 평가를 위한 문제풀이 플랫폼은 3W표준화 등으로 구성되어 시료가 1개면 호환 가능			

Ⅳ. 사이버보안 전문가 자격증

4.1 Knowledge 평가 측정

사이버보안전문가(2급,3급) 과정에서는 Web 해킹과 보안, 시스템 해킹과 보안, 네트워크 해킹과 보안 과정의 지식(knowledge) Data Base 구축과 특허 출원을 하며, 자격증 시험 평가 문제 100문제 이상 개발한다.

개인정보보호책임자(2급,3급) 과정에서는 수집처리유지파기, 보안관리 암호화, 법제도 처벌 과정의 지식(knowledge) Data Base 구축과 특허 출원을 하며, 자격증 시험 평가 문제 100문제 이상 개발한다.

위 내용을 자격증 과정의 지식(knowledge) Data Base 구축하고 온라인 Contents로 만들어 개인정보와 사이버보안을 위한 전문가 양성한다.

4.2 사이버보안 자격증 도입

정보보호책임자, 사이버보안전문가 민간자격증 취득 후 취업 알선 네트워크 확보한다. 또한 강의 요원을 선발하고 체계적으로 교육을 진행함으로써 해킹 보안교육 양성 우수강사 인력을 확보한다.

4.3 사이버보안 자격증 보수교육

해킹, 사이버보안은 경험적이고 비공개적인 기술로 학술적인 선행연구가 적으므로 중요정보, 개인정보, 금융정보에 대한 악성코드의 제작과 배포, 방어 시스템의 교육준비가 어렵다. 또한 정보보호, 사이버보안 교육 실습할 수 있는 사이트가 점차 없어지게되어 교육 및 실습할 수 있는 환경이 줄어들게된다. 따라서 정보보호, 사이버보안 학회 전문가와 유대관계로 전문가의 확보와 협조가 용이하도록 진행하며, 2015년 교육과정 개편된

2018년까지 SW교육(정보보호 포함) 필수화를 기반으로 정부의 사이버보안, 정보보호 인력 양성에 적극적으로 교육이 진행될예정이다.

Ⅴ. 결 론

사이버세계가 커질수록 사이버공격을 빈번하게 발생한다. 이러한 공격을 통해 개인정보유출이 발생되며 그에 따른 국민 경제 피해 및 국가안보가 위협당하고 있다. 사이버 공격에 대응하기 위해서는 정보보안에 관련된 인력양성이 필요한 시기이다. 이러한 취지에서 사이버공격에 대한 해킹개념과 자격증에 관련된 지식 및 교육과정, 개인정보보호법을 지켜야 하는 사이버보안 전문가 양성을 제안함으로써 자격증 과정을 통한 Knowledge DB를 통해 국가의 안정성을 강화하고 국력을 향상시킬 수 있다고 생각한다. 또한 전문가 자격증 과정을 개설하여, 자격증 학습-평가-인증 과정에서 수입발생-자격증 시스템, 교육기관, 평가기관-연계기관의 수입이 발생하여 기관들의 수입창출원과 종사자들의 일자리 창출이 가능할것이라 생각한다.

참고문헌

[1] 산산, OWASP TOP 10, 국정원 8대 취약점, Double MOUNTAIN, 2016.01.21., 네이버블로그, http://9chuck.blog.me/220604415715.
[2] 박대우,주덕규,손영현(2012), 「해킹보안전문가 3급」, 서울: 전자신문사, pp.295.
[3] 박대우,주덕규,손영현(2012), 「해킹보안전문가 3급」, 서울: 전자신문사, pp.296.
[4] 박대우,주덕규,손영현(2012), 「해킹보안전문가 3급」, 서울: 전자신문사, pp.254.
[5] 박대우,주덕규,손영현(2012), 「해킹보안전문가 3급」, 서울: 전자신문사, pp.208
[6] 박대우,주덕규,손영현(2012), 「해킹보안전문가 3급」, 서울: 전자신문사, pp.297