https://doi.org/10.33778/kcsa.2020.20.4.197

국가·공공기관 전산망 특성에 따른 사이버 위협 분석 및 분류에 관한 연구

김 민 수*, 박 기 태**, 김 종 민**

요 약

지식정보사회에서 발전된 네트워크 인프라를 바탕으로 전산망의 구조는 보안성을 확보한 다양한 형태의 망 구성을 구축하여 운영하고 있다. 국가·공공기관 전산망의 경우 각 기관별 특성과 연계 기관까지 고려한 기술적, 관리적 보안환경 구축이 필요하며, 이를 위해 기관별 특성에 따른 사이버 위협을 분류 및 위협 지도를 바탕으로 기술적·관리적 취약점 및 사이버 위협을 분석 등을 통한 사이버 훈련을 위한 기본 연구의 중요성이 대두되고 있다. 따라서 본 연구에서는 인터넷망과 국가정보통신망의 이원적 인프라 망을 기반으로 구축되어진 국가·공공기관 전산망의 내·외부 사이버 위협에 따른 유형별 분석을 사례 기반의 시나리오를 통해, 실질적인 사이버 위협 요소를 도출 및 분석하여 사이버보안 훈련 요소 도출용 사이버 위협 MAP을 제시하고자 한다.

A Study on the Analysis and Classification of Cyber Threats According to the Characteristics of Computer Network of National·Public Organizations

Minsu Kim*, Ki Tae Park**, Jongmin Kim***

ABSTRACT

Based on the network infrastructure advanced in the information knowledge society, the structure of computer network is operated by establishing the composition of network in various forms that have secured the security. In case of computer network of national/public organizations, it is necessary to establish the technical and managerial security environment even considering the characteristics of each organization and connected organizations. For this, the importance of basic researches for cyber training by analyzing the technical/managerial vulnerability and cyber threats based on the classification and map of cyber threats according to the characteristics of each organization is rising. Thus, this study aims to analyze each type of external/internal cyber threats to computer network of national/public organizations established based on the dualistic infrastructure network of internet and national information network, and also to present the cyber threat framework for drawing the elements of cyber security training, by drawing and analyzing the actual elements of cyber threats through the case-based scenario.

Key words : Network Segmentation Environment, National Network, Public Institution Network, Cyber Threat Classification, Cyber Threat Map

접수일(2020년 10월 02일), 수정일(1차: 2020년 10월 26일), 게재확정일(2020년 10월 29일)

* 중부대학교 정보보호학과(주저자)
** ETRI부설연구소
*** 동신대학교 에너지응용학부 융합정보보안전공(교신저자)

1. 서 론

지식정보사회에서 발전된 네트워크 인프라를 바탕으로 전산망의 구조는 보안성을 확보한 다양한 형태의 망 구성을 구축하여 운영하고 있다.

국가 및 공공기관의 전산망 구성도 초연결 환경에서 폭발적으로 증가하는 사이버 위협[1]으로부터 효율적인 대응을 위하여 정보보호관리체계(Information Security Management System)를 기준으로 보안 인프라 구축을 진행하고 있다. 또한 다양한 형태의 망 구성 중 망 분리 구조를 바탕으로 사이버 위협으로부터 보안성을 확보하고 있지만, 내부 업무망에 영향을 미치는 사이버 위협의 경우 여러 경로를 통한 다양한 형태의 공격으로 진행될 가능성을 지니고 있다.

이에 따라 국가·공공기관 전산망의 보안성 확보를 위해 다양한 망 구성에 의한 사이버 위협의 특성을 파악하고 이를 바탕으로 국가·공공기관 전산망의 사이버 위협의 유형을 파악하고 공격의 연관성과 분석을 통해 사이버 공격에 대한 대응이 필요하다.

그리고 국가·공공기관 전산망의 경우 각 기관별 특성과 연계 기관까지 고려한 기술적, 관리적 보안환경 구축이 필요하며, 이를 위해 기관별 특성에 따른 사이버 위협을 분류 및 위협 지도를 바탕으로 기술적·관리적 취약점 및 사이버 위협을 분석 등을 통한 사이버 훈련을 위한 기본 연구의 중요성이 대두되고 있다[2][3][4][5].

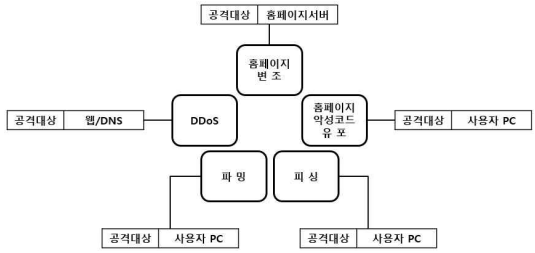
따라서 본 연구에서는 인터넷망과 국가정보통신망의 이원적 인프라 망을 기반으로 구축되어진 국가·공공기관 전산망의 내·외부 사이버 위협에 따른 유형별 분석을 사례 기반의 시나리오를 통해, 실질적인 사이버 위협 요소를 도출 및 분석하여 사이버보안 훈련 요소 도출용 사이버 위협 프레임워크를 제시하고자 한다.

2. 관련연구

2.1 사이버공격 유형

최근 해킹 수준의 발전과 사이버공격 도구의 성능 향상으로 국내에서 빈번하게 발생하고 있는 기존의 홈페이지 변조 및 악성코드 유포, 디도스 공격 유형과 더불어 피싱, 파밍, 스미싱 등의 공격 행위가 증가하고 있는 실정이다[6].

(그림 1)은 사이버공격 유형별 공격대상을 나타낸 것이다.



(그림 2) 사이버공격 유형별 공격대상

2.2 망분리 기술

인터넷에 대한 의존도가 높아지면서 사이버 공격은 해킹, 악성프로그램 유포 등 다양한 유형으로 나타나고 있으며, 사이버 공격은 정보유출, 시스템 다운, 사이트 및 망 마비 등으로 개인뿐만 아니라 국가적으로도 많은 피해를 주고 있다.

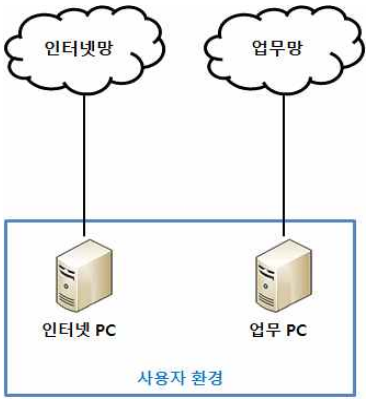
증가하고 있는 사이버 공격을 차단하여 국가 및 산업의 중요 정보를 보호하기 위한 방안으로 망분리 기술이 요구되었으며, 2008년부터 국가기관의 망분리 사업이 진행되어 왔다.

국가·공공기관 전산망 또한 망분리를 도입하여 인터넷 망과 업무망으로 구분하여 운영함으로써 보안 인프라로서 인터넷으로부터의 보안 위협을 차단하고 있다.

2.2.1 물리적 망분리

대표적인 물리적 망분리는 2대의 시스템을 사용하는 방식으로 하나의 시스템은 내부망에만 접속할 수 있고, 나머지 시스템으로는 인터넷망에만 접속할 수 있도록 함으로써 외부에서의 보안 위협 요소가 내부망에 영향을 미치는 것을 원천적으로 차단하는 방법이다[7][8][9].

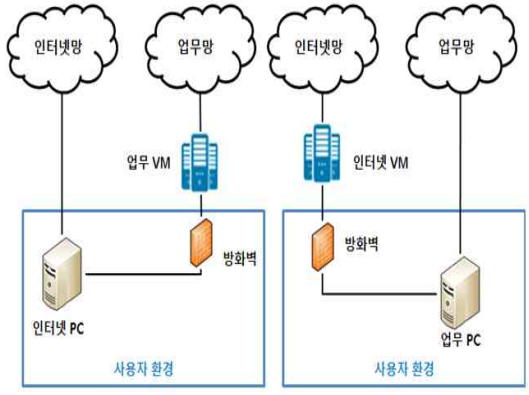
2대의 시스템을 사용하는 직관적인 방식인 만큼 가장 보안성이 높고, 도입 문턱도 낮지만 시스템 구입비용이 기존 대비 2배로 늘어나는 단점이 있다. (그림 2)는 물리적 망분리를 나타낸 것이다.



(그림 2) 물리적 망분리

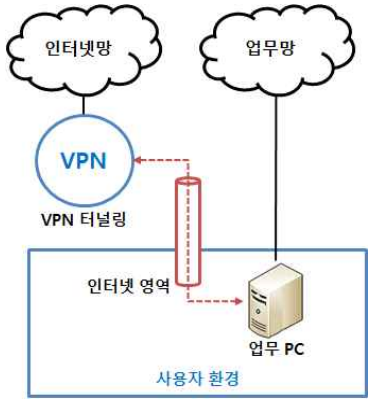
2.2.2 논리적 망분리

논리적 망분리는 일반적으로 가상화 기술을 기반으로 시스템 또는 네트워크를 구분하는 방식으로 [10][11], 시스템을 가상화하는 클라이언트 기반 컴퓨팅(CBC) 방식은 한 대의 시스템만을 필요로 하기 때문에 초기 도입 비용이 가장 저렴하나 고장 발생 시 복구가 어려워 신속한 장애 대처가 쉽지 않다. (그림 3)은 논리적 망분리(VDI-업무 망분리)와 논리적 망분리(VDI-인터넷 망분리)를 나타낸 것이다.



(그림3) 논리적 망분리(VDI-업무 망분리)와 논리적 망분리(VDI-인터넷 망분리)

또한, 서버기반컴퓨팅(CBC) 방식은 사용자가 단말기로 중앙 서버에 접속해 가상 시스템을 할당받아 사용하는 방식으로 강력한 중앙 집중 관리가 가능하지만, 서버와 스토리지 등 대규모 인프라 구축으로 초기 도입비용이 높다. (그림 4)는 논리적 망분리(CBC-인터넷 망분리)를 나타낸 것이다.



(그림 4) 논리적 망분리(CBC-인터넷 망분리)

3. 사이버 보안 훈련 시나리오 수립 및 분석

3.1 시나리오 범위 및 수립 절차

3.1.1 분석 범위

사이버 보안 훈련 시나리오 수립 범위는 <표 1>과 같이 외부 접점과 물리보안 영역, 메일시스템, 홈페이지, 백업 시스템, VPN(Virtual Private Network), IP 기반 센서 및 무선 단말 등이 있다.

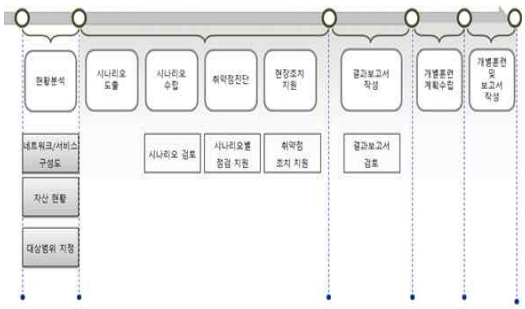
<표 1> 사이버 보안 훈련 시나리오 수립 범위

분석 범위
- 외부 접점 - 전광판, CCTV, 출입통제 시스템 - 메일시스템, 홈페이지 - 백업 시스템 - VPN - -전력 관련 시스템 - IP 기반 센서 및 무선 단말

3.1.2 수립 절차

3.1.2.1 사전 준비 사항

사전 준비 사항은 현황 분석 단계로 네트워크 및 서비스 구성도, 자산 현황, 대상범위 지정을 수행해야 하며, AP 무선 중계기, 악성코드 배포(제한적으로 배포), 화상회의, 프린터 네트워크, 전광판(IP 기반), CCTV(IP기반), 외부 VPN 접속 등 점검 항목에 대해 관련 담당자 또는 유지보수 업체 지원이 필요하다. (그림 5)는 사이버보안 훈련 시나리오 수립 및 분석의 사전준비 사항을 나타낸 것이다.



(그림 5) 사전준비 사항

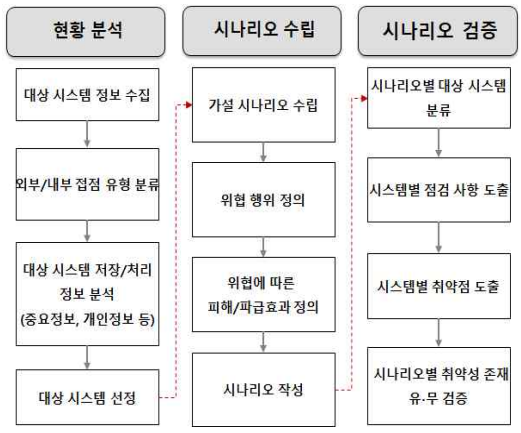
<표 2>는 점검항목 별 점검사항 및 지원 필요사항에 대한 내용이다.

<표 2> 사전점검 사항

점검 항목	점검사항	지원필요사항
AP 중계기	·인터넷 접속 가능 여부 ·AP 중계기 관리 페이지 ·암호화 알고리즘 설정 및 키관리	·AP 중계기 관리자 페이지 ·AP 접속 정보
원격 접속	·내부 시스템으로 직접 접속 가능 여부	·방화벽 정책 ·VPN 접속 정책
악성 코드 배포	·악성코드 유입으로 인한 내부 전파 가능성	·악성코드 배포 대상 ·악성코드 배포 방법 (메일/내부 업무시스템 등)
화상 회의	·내부 화상회의 노트북/PC에서 내부 시스템으로 접속 여부	·화상회의 접속 네트워크 정보
프린터	·네트워크 프린터 관리 포트 및 UI 접근 여부	·네트워크 프린터 정보
전광판	·내/외부 전광판 접속 가능 여부 ·중앙서버에서 전광판으로 원격 접속 및 전광판에서 업무시스템으로 접속 가능 여부 ·LED 전광판을 통한 내부 업무 시스템 접속 가능 여부	·전광판 접속 정보 (IP, 접속ID/Password 등) ·전광판 네트워크 정보
CCTV	·내/외부 CCTV 접속 가능 여부 ·CCTV 통신 회선으로 업무시스템 접속 가능 여부	·CCTV 네트워크 정보
외부 기관 접속	·외부 기관에서 내부 업무시스템으로 직접 접속 가능 여부	·방화벽/VPN 정책 ·금융결재원 접속 정보
내부 VPN 접속	·내부 VPN 접속 시 접속 정보 노출(하드코딩된 접속 정보) ·외부에서 관리자 페이지 노출	·VPN 접속 정보 ·VPN 접속을 위한 인증 정보(필요 시 인증서 제공)

3.1.2.2 수립 절차

사이버 위협 시나리오 수립 절차는 (그림 6)과 같이 현황 분석, 시나리오 수립, 시나리오 검증 순으로 진행되며, 분석 범위에 관련된 시스템을 기준으로 기존의 사이버 위협 사례를 바탕으로 시나리오를 수립 및 검증을 수행하게 된다.

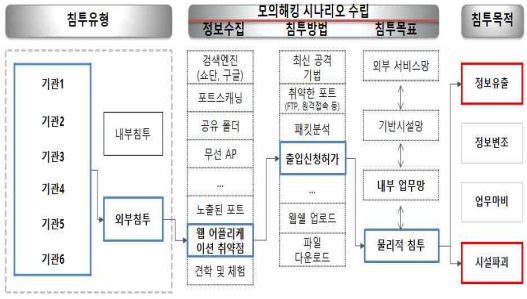


(그림 6) 시나리오 수립 절차

3.2 시나리오 수립 방법

모의해킹 시나리오에 대한 가설을 기반으로 실제 침투 경로를 유형별로 분류하여 시나리오의 적합성을 검토하여 실제 수행 시나리오를 도출하게 된다.

예를 들어, 웹 어플리케이션의 취약점을 통해 외부 해커의 임의적인 출입신청허가로 물리적 침투를 허용하여 정보유출 및 시설파괴 등의 목적을 달성한다. (그림 7)은 시나리오 수립 방법을 나타낸 것이다.



(그림 7) 시나리오 수립 방법

시나리오는 각 기관별로 수립을 진행하고 되며, 내·외부에서 침입 시 실제 시스템에 접근 가능성과 그에 따른 피해여파를 토대로 위험도를 산정하게 된다. <표 3>은 외부 침투 시나리오 별 위험도를 책정한 것이다.

<표 3> 외부 침투 시나리오 별 위험도

구분	세부 시나리오	중요도·위험도
외부침투	·대표 홈페이지 취약점 (파일 업로드, SQL Injection) 등을 통한 웹서버, DB 서버의 시스템 권한 획득	최상
	·외부 업무 수행을 위해 서비스 중인 VPN에 대해 관리자 페이지 및 관리 콘솔 노출 취약성을 이용한 내부망 접속	최상
	·외부 노출 VPN의 Client에 남아있는 인증 정보 및 추측하기 쉬운 계정/패스워드 사용을 통한 내부 업무시스템 접속	최상
	·금융결재원, 은행, 기상청 등 외부 서비스망과 연계된 서버의 VPN을 통해 서비스 연계 포트외 SSH, RDP 통신을 이용한 내부 업무 시스템으로 접속	상
	·기반시설 내 무선중계기(AP)를 로비, 옥상, 비업무시설에서 취약한 패스워드 및 암호알고리즘 설정 취약성을 이용하여 내부 업무시스템으로 접속	상
	·Shodan, Censys 등 검색 서비스에 노출된 열려 있는 유지보수용 포트를 이용한 내부 업무시스템 직접 접속	상
	·외부 기반시설 통제 구역 범위 외의 장소에 설치된 IP 기반의 CCTV 및 전광판 등의 통신회선 또는 관리 PC를 이용하여 내부 시스템 접속	상
	·관리기관 건물 내의 로비, 접견실, 대기실 등에서 바닥 또는 벽면에 존재하는 통신 포트를 접속하여 내부 업무 시스템 접속	상

<표 4>는 내부 침투 시나리오 별 위험도를 책정한 것이다.

<표 4> 내부 침투 시나리오 별 위험도

구분	세부 시나리오	중요도·위험도
내부침투	·기관의 PC 또는 서버에서 VPN을 통해 기반시설 내부 업무 시스템으로 직접 접속	최상
	·기반시설 운영자 또는 보안 담당자의 업무 PC에서 외부 인터넷을 통해 악성코드 유입 및 내부 업무시스템으로 침투	최상
	·고객센터내 민원 신청 업무를 위한 PC 또는 현장 사무실 (설비, 지역사무소)에서 비인가 USB 및 CD/DVD 등을 이용한 악성코드 감염, 중요정보 누출	상

	·현장 사무실 (설비, 지역 사무소 등) 내 비인가 노트북 반입을 통해 악성코드 유입 및 내부 업무시스템으로 직접 접속	상
	·내부 시설의 IP 기반의 CCTV, 출입통제 단말, 전광판의 통신 회선을 사용하여 관리 PC 또는 서버에 원격 접속 후 기반시설의 중요 시스템에 우회 접속	상
	·기반시설내 사무실, 회의실 등에서 내부 무선중계기의 취약한 비밀번호 및 암호알고리즘을 이용한 내부 업무망 접속 후 기반시설로 우회 접속	상
	·내부 네트워크 프린터에 접속하여 관리자 화면을 통해 악성프로그램이 포함된 펌웨어로 업데이트 후 접속 가능한 PC에 원격접속 및 악성코드 배포	상
	·내부 PC 및 윈도우 서버의 C$, D$ 등 공유되어 있는 폴더를 검색하여 중요 정보 유출	상

4. 사이버 위협 Map 도출 및 보안성 강화 방안

4.1 사이버 공격 기법

4.1.1 시스템 및 서비스 설정 취약점을 이용한 공격

시스템 및 서비스 설정 취약점을 이용한 공격은 시스템과 시스템에서 제공하는 각종서비스 설정과 관련된 취약점을 이용하는 것으로 그 수준은 그리 높지 않는 경우가 대부분이다. 시스템에 존재하는 취약점은 일반 시스템 분석 도구를 이용하여 찾을 수 있으며, 해킹 하는데 특별한 소스코딩 작업 등 고난이도의 기술이 필요하지 않기 때문에 비교적 쉽게 공격할 수 있으며, 시스템 명령어를 알고 이를 이용하여 시스템 설정을 확인할 수 있는 경우에는 좀 더 쉽게 공격할 수 있다.

공격기법을 세부적으로 분류하면 파일 시스템의 쓰기 권한 취약점을 이용하는 경우와 SUID프로그램 관리상의 문제점을 이용하는 경우, 환경변수를 이용하는 경우가 포함된다.

이는 시스템 명령어들을 사용할 수 있고, 이를 이용하여 시스템 설정들을 확인할 수 있는 경우 공격에 쉽게 적용시킬 수 있는 방법으로 대개 유닉스 시스템에서 사용되는 파일 권한(rwxs-rwx-rwx)등을 악용하는 사례로 그 내용은 다음과 같다.

(1) 쓰기권한 취약점을 이용한 공격

멀티유저 운영체제는 보안상의 이유로 다른 사용자가 자신의 파일을 읽거나 파일에 다른 내용을 기록하는 것을 금지하고 있다. 이런 역할을 하는 것을 퍼미션(Permission) 이라고 하며 다른 사용자의 파일을 마음대로 접근하지 못하도록 하기 위해 사용된다. 퍼미션은 읽기, 쓰기, 실행 등 3가지 권한으로 이루어진다.

즉 파일이나 디렉토리에 각각의 접근권한을 부여하여 허가받은 사용자(그룹)만 파일에 접근, 실행할 수 있도록 하는 것으로 파일이나 디렉토리를 다른 사람들과 안전하게 공유하거나 개인적인 목적으로만 사용할 수 있다.

퍼미션은 소유자가 속한 그룹과 그와 유저(그룹)로 나누어지며 만일 관리자가 파일이나 디렉토리의 권한을 잘못 부여하면 비 인가자가 특정 파일을 실행하여 악의적인 행위를 수행할 수 있게 된다.

(2) Suid 프로그램 관리상의 문제를 이용하는 공격

일반적으로 파일의 권한은 실행한 사용자의 권한을 따르지만 Suid가 설정되어 있을 경우에는 소유자의 권한을 따른다.

예를 들면 패스워드 파일은 관리자 권한이 있어야 한다. 이 경우 Suid를 이용하여 사용자도 임시로 관리자 권한을 획득하여 패스워드를 수정할 수 있다. 따라서 파일을 생성할 경우 Suid 권한을 잘못 부여하게 되면 공격자는 아무런 제약 없이 관리자권한으로 프로그램을 실행, 사이버 공격을 수행할 수 있다.

4.1.2 프로그램 취약점을 이용한 공격

프로그램 취약점을 이용하는 공격기법은 프로그래밍 상의 보안 오류와 프로그램 동작상의 보안 오류로 인하여 발생하는 취약점이 있을 수 있다. 후자의 경우에는 프로그램 단독으로 문제가 일어나는 경우도 있지만 여러 프로그램이 동시에 수행될 경우에 문제가 발생하는 경우도 있다. 프로그램 동작상의 오류로 인한 문제는 특정 프로그램에 대한 문제로 권고문의 형태로 알려지고 패치가 가능하게 된다.

프로그램 오류를 이용한 기법은 해킹의 핵심이라고 할 수 있는데, 공격 종류에는 CGI/JAVA 스크립트 취약점, ASP, PHP 스크립트 취약점을 이용한 공격, 버퍼 오버플로 공격, 힙 오버플로 공격, 레이스 컨디셔닝 공격, 포맷 스트링 공격 등이 있는데 각종 스크립트 언어의 취약점은 기본적으로 각종 소스 파일들을 읽을 수 있는 능력이 있어야 하기 때문이다. 일반적으로 각종 스크립트의 취약점들은 스크립트 자체의 문제만으로 해킹에 이용되는 경우 보다는 다른 해킹 기법과 연관되어 이용되는 경우가 대부분이다.

(1) 버퍼오버플로우 공격

버퍼오버플로우는 배열로 할당한 메모리 공간에 데이터(주로 문자열)를 저장하는 과정에서 할당된 배열 공각영역을 넘어서 다른 저장 공간을 침범하는 현상을 말한다. 프로그램 언어에 따라 런 타임에 배열경계 침범하는 현상을 말한다.

프로그램 언어에 따라 런 타임에 배열경계 침범을 허용하거나 불허할 수가 있는데, C/C++ 프로그램 언어는 경계 침범을 허용하는 대표적인 언어 중의 하나이다. 버퍼오버플로우가 보안침해를 위한 공격 수단이 될 수 있는 이유는 대부분의 버퍼(배열공간)가 스택영역에 할당될 수 있고, 그 주변에는 프로그램 흐름을 결정하는 복귀주소 등의 제어정보가 존재하기 때문이다. 즉 버퍼를 벗어나 일부 데이터가 제어정보를 덮어쓰고, 악성코드가 존재하는 곳에 데이터에 대한 주소를 가지고 있다면 해당 프로그램은 원래의 목적대로 실행되지 못하고, 공격자의 의도된 침해 기능을 수행하게 되는 것이다.

Buffer란 일종의 임시 기억장소로 데이터를 임시로 저장하는 공간을 말하며 버퍼의 종류는 Stack, Heap 2가지로 구분된다. 그렇기 때문에 버퍼 오버플로우 공격 또한 Stack-Based Buffer Overflow, Heap-Based Buffer Overflow로 구분된다.

(2) 포맷스트링 공격

포맷스트링(Format String)이란 C언어에서 일반적으로 Data 변수를 입출력문에서 일정한 형태로 받아들이거나 출력하기 위해서 사용하는 기호로 공격자가 출력문에서 올바르지 못한 방법을 악용하여 실제 메모리 번지를 공격하여 원하는 값으로 변경하거나 시스템 관리자 권한을 절취하는 공격기법을 의미한다.

4.1.3 프로토콜 취약점을 이용한 공격

프로토콜의 취약점을 이용한 공격기법의 경우 해커는 각종 프로토콜 자체를 이해하고 있어야 한다. 따라서 다른 해킹 기법보다 높은 수준이 된다. 일반적으로 프로토콜 취약점을 이용한 해킹은 기 작성된 해킹 프로그램을 이용하는 경우가 대부분이다.

대표적인 인터넷 프로토콜인 TCP/IP 프로토콜은 1960년대 미국 DoD(Department of Defense)에 의해 통신기술 사업으로 시작되었고 1975년 ARPANET IFIP(International Federation of Information Processing Work Group 6.1)에 의해 개발이 완료 되었다. TCP/IP 프로토콜은 데이터 통신을 위해 다수의 층(Layer)으로 구성되어 있다.

TCP 프로토콜은 데이터를 주고받는 것에 대한 규약으로 프로토콜 개발초기에는 보안측면 보다는 활용성에 중점을 두었기 때문에 사이버 공격에 매우 취약하다. 현재 인터넷은 TCP/IP기반으로 운영되고 있으며 아직까지 해커는 TCP/IP 프로토콜 취약점을 이용한 사이버 공격을 지속적으로 수행하고 있다.

프로토콜의 취약점이란 TCP/IP뿐만 아니라 각종 인터넷 프로토콜(ICMP, ARP,RARP, UDP등)의 설계상의 취약점을 포함한다.

(1) DoS 계열 공격

네트워크에 분산되어 있는 다수의 컴퓨터가 일시에 특정 전산장비(서버 등)에 패킷(Packet)을 송출, 네트워크를 넘쳐나게 하거나 전산장비(서버 등)의 가용성을 소진시켜 정상 서비스를 제공하지 못하도록 하는

공격을 말한다. 컴퓨터 이용자는 공격의도가 없으나, 자신의 컴퓨터를 해커에게 조종당해 자신도 모르게 공격을 수행하게 된다. 해커는 공격 대상과는 무관하게 다수의 컴퓨터를 해킹하여 공격용 프로그램(트로이의 목마)을 설치한 후 좀비 PC에게 공격지령을 내린다. 표적이 된 서버는 트로이 목마가 설치된 컴퓨터로부터 공격을 받기 때문에 실제 공격자를 찾아내는 것은 어렵다.

DDoS 공격은 Flooding 공격, Connection 공격, Application 공격으로 나누어지며 최근에는 공격 수행 후 증거 인멸을 위해 디스크(HDD)를 파괴하는 등 수법이 점점 교묘해 지고 있다. DDoS 공격은 피해 시스템을 공격하기 전 좀비PC를 확보하여야 하며 공격명령을 하달하여 일시에 공격을 수행한다. DDoS 공격은 국가적인 혼란을 야기하거나 게임업체·금융기관 등을 공격하여 기업의 이미지를 저하 시키는 등 주로 전문 해킹조직에 의해 수행된다.

(2) 스니핑(Sniffing) 공격

스니핑(Sniffing)은 '코를 킁킁거리다, 냄새를 맡다' 등의 의미를 가지며 이 공격은 사전적 의미와 같이 네트워크상에서 자신이 아닌 다른 상대방의 인터넷 통신을 엿듣는 행위를 말한다. 간단히 말하면 네트워크 트래픽을 도청하는 과정을 '스니핑'이라고 할 수 있으며 스니핑 공격은 공격시 막는 것도 어려우며, 탐지 역시 쉽지가 않다. 스니핑을 할 수 있도록 하는 프로그램을 '스니퍼'라고 하며 스니퍼를 설치하는 과정은 전화기에 도청장치를 설치하는 과정과 유사하다.

스니핑은 보안의 기본요소 중 기밀성(Confidentiality)을 해치는 공격방법으로 인터넷을 통해 이루어지는 통신내용을 절취할 수 있다. 이러한 공격에 대응하기 위해서는 데이터 암호화 통신을 수행하여야 한다.

랜(LAN)에서의 스니핑은 Promiscuous 모드에서 작동한다. 랜 카드는 설정된 IP 주소와 고유한 MAC(Media Access Control) 정보를 가지고 있으며 자신의 랜 카드에 들어오는 프로토콜 형식에 따라 IP 주소 및 MAC 정보를 인식하고 자신의 버퍼에 저장 유무를 결정한다. 그러나 스니핑은 자신이 받지 말아야 할 다른 네트워크 정보까지 모두 받아들이는 것이다. 이렇듯 자신의 네트워크 정보(IP, MAC)를 무시하고 모든 패킷을 받아들이는 상태를 Promiscuous 모드라고 한다. 대표적인 공격기법에는 Switch Jamming, ARP Redirect 공격, ARP spoofing 공격, ICMP Redirect 공격 등이 있다.

4.1.4 사회공학을 이용한 공격

(1) 피싱(Phishing)

피싱(Phishing)은 전자우편 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여 비밀번호, 신용카드 번호 등 비밀정보를 부정하게 얻으려는 Social Engineering의 한 종류이다. '피싱'이란 용어는 점점 더 복잡한 미끼들을 이용해서 사용자의 금융정보와 패스워드를 '낚는'다는 데서 유래 되었다.

인터넷 사기꾼(피셔)들은 일반 해커와 달리 사용자의 하드웨어와 소프트웨어 손상이나 자신의 이름을 알리는 것에는 관심이 없으며 오직 금융사기를 통해 금전적인 이득을 취하는 데 목적이 있다.

피싱 공격자들은 익명으로 보다 효과적인 방법을 통해 금전적으로 가치 있는 정보를 빼낼 수 있는 기술을 끊임없이 개발하고 향상시키고 있다.

피싱의 종유에는 도메인 사기(Domain Spoofing), 신뢰할만한 공식기관 사칭, 특정 사회적 뉴스 가장, 가짜 사이트 등이 있다.

(2) 메일공격

인터넷상에서 수신자의 의사와 관계없이 불특정 다수에게 특정 목적의 이메일 또는 뉴스그룹 기사를 발송하는 것을 의미한다. 스팸메일은 대부분 수신자가 원하지도 않고, 관심도 없는 메시지이거나 각 뉴스그룹의 토론 주제와도 상관없는 기사로 다수의 사람들에게 상품을 광고하거나 특정 상품 또는 기업을 비방할 목적으로 전자메일을 이용하여 발송하는 행위를 말한다.

4.1.5 악성코드(Malware)에 의한 공격

악성코드는 바이러스, 트로이안, 백도어 웜 등을 이

용한 공격이다. 특히 백도어 웜은 시스템을 해킹하고 자기를 복제하는 공격으로 최근에 가장 많이 사용되고 있다.

트로이안이나 백도어 웜은 매우 다양한 형태로 나타나고 있으며, 최근에는 전문가가 아니어도 사용할 수 있도록 쉬운 인터페이스를 사용한 프로그램도 나왔다. 백도어 웜을 이용한 공격을 하려면 운영체제나 응용프로그램의 취약점에 대한 이해와 프로그램 제작 능력을 갖추고 있어야 한다. 다음은 악성코드의 종류에 대한 내용은 다음과 같다.

(1) virus

virus는 컴퓨터 시스템에 몰래 침투해 숙주 프로그램이나 실행 가능한 파일에 자기자신이나 변형된 자신을 감염시키고 또 다른 대상을 감염시킴으로써 컴퓨터 시스템과 파일을 파괴하는 코드 혹은 프로그램이다. Virus는 컴퓨터 비정상적인 동작 유발, 데이터 삭제, 컴퓨터 성능 저하, 인터넷 속도 저하 등의 악성행위를 수행한다.

(2) Worm

Worm은 자기복제성을 가지고, 숙주 프로그램이나 파일이 없이 독자적으로 실행되어 프로그램 내에서 스스로 자신을 복제하거나 프로그램과 프로그램 사이 또는 컴퓨터와 컴퓨터 사이를 이동하여 전파시키며, 기억장소에 코드 형태 혹은 실행파일로 존재하는 프로그램 조각이다.

Worm은 자기 자신을 복제하는 행위, 사용자가 인지하지 못한 방법으로 이메일을 전송하는 행위, 해당 프로그램 혹은 개발사에서 배포하지 않은 정상적인 파일에 새로운 코드를 삽입하는 등의 악성행위를 수행한다.Virus와 Worm은 모두 자기복제가 가능하다는 점에서 공통점을 가지지만, 전파 방법에 대한 차이점이 존재한다. Virus는 파일 등에 삽입되어 전파되지만, Worm은 파일과는 독립적으로 그 자체만으로도 네트워크를 통해 전파된다.

(3) Trojan Horse

Trojan Horse는 정상적인 단일 프로그램으로 위장하고 있으나 악성 루틴을 포함하고 있는 프로그램이다. Trojan Horse는 다른 프로그램 내에 사용자가 알 수 없도록 포함되며, 스스로 복제하지 못한다. 공격자가 고의로 삽입시키기 때문에 프로그램의 버그와는 다르며 스스로 복제를 못하기 때문에 Worm이나 Virus와 다른 특징을 지닌다. Trojan Horse의 주요 악성행위로는 Backdoor설치, DDoS 공격, Key Logging을 통한 ID 및 Password 수집 등이 포함된다. Trojan Horse와 자기 복제가 불가능하고 다른 파일을 감염시키지 못하며, 사용자가 실행시키도록 하여 스스로 피해를 유발한다. Virus가 정상적인 Boot 영역 및 파일 등을 감염시키면서 전파된다는 점에서 차이가 있다.

(4) Bot

Bot은 사용자의 컴퓨터를 공격자가 제어할 수 있도록 만들어 주는 프로그램으로, 다양한 경로로 사용자의 컴퓨터에 침입하여 Bot Master의 명령에 따라 활동한다. Bot Master는 Bot에 감염된 컴퓨터를 자유롭게 제어할 수 있을 뿐만 아니라 컴퓨터에 저장된 정보를 수집할 수 있어 각종 정보 유출이 가능하고, 다른 시스템을 공격하는 데 사용된다. 이러한 Bot들이 네트워크를 형성한 경우를 Botnet이라 부른다.

(5) Key-logger

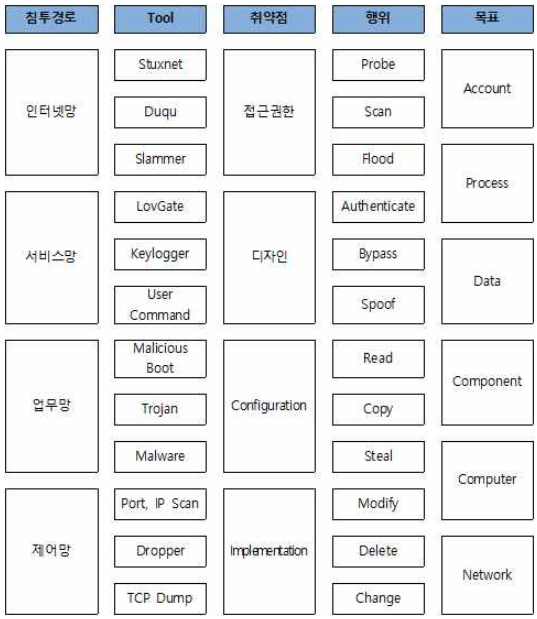
Key-logger는 키보드로부터의 입력을 감시하고 기록하여 공격자에게 전송하는 악성코드이다. Key-logger는 감염된 컴퓨터의 사용자가 키보드를 통해 입력한는 ID, Password, 주민등록번호, 계좌번호, 신용카드번호 등의 모든 데이터를 훔쳐볼 수 있는 악성행위를 수행한다.

4.2 사이버 위협 분류

사이버 위협 시나리오 도출을 위해 (그림 7)과 같이 침투경로 ▶ Tool ▶ 취약점 ▶ 행위 ▶ 목표 순으로 결과를 나타낸다.

취약점을 기준으로 국가·공공기관 전산망 구조에서의 사이버 위협 시나리오를 도출하기 위해 침투경로,

Tool, 취약점, 공격 행위, 최종 목표로 구분하여 세부 공격을 정리하였다. 세부 공격의 경우 시스템 및 서비스 설정 취약점을 이용한 공격으로 쓰기권한 취약점을 이용한 공격과 Suid 프로그램 관리상의 문제를 이용하는 공격으로 구분하였고, 프로그램 취약점을 이용한 공격으로 버퍼오버플로우 공격, 포맷스트링 공격으로 구분하였다. 또한 프로토콜 취약점을 이용한 공격으로 DoS 계열 공격, 스니핑(Sniffing) 공격으로 구분하였고, 사회공학을 이용한 공격으로 피싱, 메일공격으로 구분하였다. 그리고 악성코드에 의한 공격으로 Virus, Worm, Trojan Horse, Bot, Key-logger의 악성행위로 구분하였다.



(그림 7) 사이버 위협의 분류

4.3 사이버 위협 대응 프레임워크

사이버위협에 시나리오에서 볼 수 있듯이 공격자는 정보자산, 인적자산의 취약점을 노리고 있으며, 공격자의 사이버위협으로부터 자산을 보호하기 위해서는 상시적인 보안 대응과 관리가 필요하다.

또한 각 단계별로 필요 기술과 정책의 마련이 필요하며 모든 기술적·정책적 보호조치를 마련하는 것은 현실적으로 어렵지만 각 자산 별 특성과 이에 따른 위협 현황에 따라 우선순위를 설정해 단계적으로 마련할 필요성이 존재한다. (그림 8)은 사이버위협 대응 프레임워크를 나타낸 것이다.

(그림 8) 사이버위협 대응 프레임워크

5. 결론

국가·공공기관의 전산망은 인터넷망과 국가정보통신망의 이원적 인프라 망을 기반으로 기관별로 인터넷망, 서비스망, 업무망, 제어망으로 구성되어지며, 사이버 위협의 분석 및 분류를 위해 시나리오 범위를 한정하여 외부접점, 시스템(DMZ 구간 시스템, 백업 시스템, 제어 시스템, 출입통제 시스템), VPN(Virtual Private Network), 각종 IoT 시스템으로 구분하였다. 또한 사이버공격의 유형은 홈페이지 변조 및 악성코드 유포, 디도스 공격 유형과 더불어 피싱, 파밍 등의 공격 행위를 적용하였다.

사이버공격 유형별 매트릭스를 통해 공격자의 인터넷 연결환경, 취약점 악용, 침투해위, 내부행위, 피해내용, 공격의도를 기준으로 종합해보면 유선환경을 통해 프로토콜, 운영체제, 응용프로그램의 취약점을 이용하여 정보유출, 정보변조/파괴, 서비스 불가 등의 피해가 발생하며 주로 웹과 메일을 통해 악성코드의

종류에 따른 공격 형태를 이루고 있다.

이와 같은 사이버공격의 유형을 바탕으로 이메일을 통해 악성코드 감염, 서비스망에 대한 DDoS공격, 홈페이지 변조, 랜섬웨어, 업무망 및 제어망에 대한 비인가 저장장치나 시스템 연결 및 원격 접속으로 인한 시스템 마비, 정보유출 등의 공격 더 나아가 IoT 장비를 악용한 DDoS 공격이나 모바일 게임 인기에 편승한 사이버 위협에 노출될 수 있다.

따라서, 사이버위협에 시나리오를 바탕으로 공격자는 정보자산, 인적자산의 취약점을 노리고 있으며, 공격자의 사이버위협으로부터 자산을 보호하기 위해서는 상시적인 보안 대응과 관리가 필요하다.

또한 각 단계별로 필요 기술과 정책의 마련이 필요하다. 모든 기술적·정책적 보호조치를 마련하는 것은 현실적으로 어렵지만 각 자산 별 특성과 이에 따른 위협 현황에 따라 우선순위를 설정해 단계적으로 마련할 필요성이 존재한다.

참고문헌

[1] 한국인터넷진흥원, “2019년도 7대 사이버 공격 전망 발표”, https://www.kisa.or.kr/notice/press_View.jsp? mode=view&p_No=8&b_No=8&d_No=1739&ST=total&SV=, 2018.

[2] 이선재, 이일구, 안예린, 박소영, 윤지희, 정유진, 최유림, 윤선우, 정다은, “사이버보안 위협 분석 및 개선 방안에 대한 연구”, 한국산업보안연구, Vol.9, No.1, pp.69-97, 2019.

[3] 김완주, 박창욱, 이수진, 임재성, “사이버 방어작전 프레임워크 기반의 공격그룹 분류 및 공격예측 기법”, 정보과학회논문지, Vol.20, No.6, pp.317-328, 2014.

[4] 전상준, 김정호, “고도화된 사이버위협에 효과적으로 대응하기 위한 지능형사이버위협 대응시스템(CTI) 연구”, 한국통신학회 학술대회논문집, pp.584-585, 2018.

[5] 이경률, 이선영, 임강빈, “기반시설 보안위협 분류 및 분석”, 한국통신학회논문지, Vol.43, No.3, pp.572-579, 2018.

[6] 한국인터넷진흥원, “사이버공격 대응 기본 매트릭스”, https://www.kisa.or.kr/public/library/IS_View.jsp?mode=view&p_No=158&b_No=158&d_No=171, 2014.

[7] 김선욱, 김성운, 김학영, 정성권, 이숙영, “IOV 기반 가상 데스크탑 서비스를 이용한 물리적 네트워크 망분리 시스템 설계 및 구현”, 한국정보과학회 학술발표논문집, pp.1210-1212. 2014.

[8] 박성완, 김지희, 김진철, 송주영, 이승원, “물리적 망분리 자요연계시스템 개발 및 실증”, 대한전기학회 학술대회 논문집, pp.39-42, 2015.

[9] 이용희, 유승재, “가상화를 이용한 논리적, 물리적 망분리 구축”, 융합보안논문지, Vol.14, No.2, pp.25-33, 2014.

[10] 조성호, 최진탁, “NFS를 이용한 효율적인 논리적 망분리 시스템 구현”, 한국정보기술학회논문지, Vol.16, No.6, pp.101-112, 2018.

[11] 김민수, 신상일, 안정준, 김귀남, “FTS를 이용한 논리적 망 분리와 행위기반 탐지 시스템에 관한 연구” 융합보안논문지, Vol.13, No.4, pp.109-115, 2013.

〔저자소개〕

김 민 수 (Minsu Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2015년 산업보안학박사
2019년~현 재 중부대학교 정보보호학과 조교수

email : mskim@joongbu.ac.kr

박 기 태 (Ki Tae Park)

2000년 컴퓨터공학사
2002년 컴퓨터공학석사
2007년 컴퓨터공학박사
2014년~현 재 ETRI부설연구소

email : tgkim@nsr.re.kr

김 종 민 (Jongmin Kim)
2010년 체육학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 동신대학교 에너지융합대학 에너지응용학부 융합정보보안전공 교수

email : dyuo1004@dsu.ac.kr