국방 사이버 침해 대응을 위한 전산보안점검 프로그램 및 사용자 진단항목 개선 연구(육군 중심)

김 지 원* 정 의 섭** 정 찬 기***

요 약

최근 해킹, 바이러스 등 대한민국을 노린 공격이 증가하고 있다. 이와 마찬가지로 우리 군도 사이버 침해에 대한 노출이 심해지고 있으며 이를 대응하기 위해 국방부는 사이버 안보에 대한 기본절차를 규정하고 지침을 제공하고 있다. 그럼에도 불구하고 육군에서 발간하는 사이버방호작전 분석결과를 보면 침해건수는 점점 증가하고 있다. 이에 대한 문제점들을 개선하고자 사이버 침해 대응을 위해 가장 중요하면서 기본인 사용자 환경에서의 전산보안 점검항목을 재점검하여 안전하고 효율적인 전산보안 점검항목을 제시한다.

Improvement of Computer Security Check Program and User Inspection Items In Response To Military Cyber Security Breachment(For Army sector)

Kim Jee Won* Jung Ui Seob** Jung Chan Gi***

ABSTRACT

Recent cyber attacks on South Korea, including hacking and viruses, are increasing significantly. To deal with the cyber invasion of cyber aggression, the Ministry of National Defense defined the necessary procedures for cyber security with guidelines for cyber security. In spite of, based on the analyses the cyber defense operations published, the number of violations are increasing. To address issues stated above, the safety check items should be reviewed and revised. This paper will revisit current safety check items and provide new guidelines to prevent cyber security breaches, which will provide more safe and efficient cyber environment.

Key words : 육군, 사이버 보안, 침해 대응, 보안진단도구, 체크리스트

접수일(2017년 5월 26일), 수정일(1차: 2017년 6월 23일), 게재확정일(2017년 6월 30일)

* 아주대학교/NCW학과 사이버전전공 (주저자)
** 아주대학교/NCW학과 사이버전전공 (공동저자)
*** 아주대학교/NCW학과 (교신저자)

1. 서 론

보안업체인 카스퍼스키랩의 디도스 공격 보고서에 따르면 올해 1분기에 발생한 세계 72개국 상대 디도스 공격 중 우리나라를 노린 공격이 26.57%로 중국(47.78%)에 이어 두 번째로 많았다고 보고하였다. 이는 우리나라가 결코 사이버 안전지대가 아니라는 것을 확인할 수 있다.[1] 사이버 침해에 대비하여 국방부는 1965년 군사보안업무훈령을 시작으로 사이버 안보에 대한 기본절차를 규정하고 지침을 제공하고 있다. 하지만 이런 노력에도 불구하고 육군본부에서 발간하는 사이버방호작전 17년도 1/4분기의 결과를 보면 총 288건의 침해가 발생하였고[2] 2016년 국가정보보호백서의 통계자료에 의하면 소속 기관이 가장 취약한 정보보호 분야가 인적보안(58.7%)이라고 답하였다.[3] 이는 정보보호가 관리자측면에서만 강조될 사항이 아니라는 것을 알 수 있다. 그러므로 사용자 관점에서의 정보보호의 인식제고가 필요하고, 이를 위해서 먼저 선행되어야 할 사항이 바로 사용자의 보안점검항목들을 실효성 있게 구체화하는 것이다.

이를 위해 본 논문에서는 국방 정보보호 법규 및 규정에 대해 살펴보고 이를 토대로 기존의 사용자 보안점검항목 도출 배경을 살펴보고 분석한 뒤 개선된 전산보안프로그램과 자가진단항목을 제시하고자 한다.

2. 이론적 배경

현재 우리 군의 전산보안 평가방법의 특징은 ISMS(정보보호관리체계)처럼 각종 위협으로부터 정보 자산을 보호하는 수준을 평가하는 것이 아니라 사용자가 준수해야할 보안사항을 점검하고 위반자를 조항에 따라 처벌하여 군사자료를 보호하는 것을 목적으로 하고 있다. 그러므로 먼저 국방 정보보호 법규 및 제도를 살펴보고 이를 토대로 현재 사용자 보안점검항목이 어떻게 도출되었는지를 알아야 한다.

2.1 국방 정보보호 규정

국방 정보보호 관련 규정은 크게 국방사이버안보훈령, 군사보안업무훈령, 정보작전방호태세 규정 등이 있으며 육군에는 군사보안 규정이 있다.

국방사이버안보훈령은 각 군의 사이버테러 및 사이버전 관련 역할 및 임무에 관해 규정하고 있으며, 군사보안업무 훈령은 군 보안의 핵심 훈련으로서 군사보안 및 정보통신 보안을 포함한 제반 군사보안업무에 대한 총제적인 원칙을 제공하고 있다.[4] 정보작전방호태세 규정은 사이버위협에 효과적으로 대비하기 위해 아군의 정보 및 체계에 대한 공격징후 또는 침해사고 발생 시 신속하게 대응하여 피해를 최소화하기 위한 사항을 명시하고 있으며[5] 육군의 군사보안 규정은 「군사보안업무훈령」에 의거 육군의 군사보안업무시행에 관하여 필요한 사항을 규정하고 있다.

2.2 사용자 점검항목 도출

국방사이버안보훈령은 별지에 정보보호시스템 보안기능 점검표를 두어 각 기능에 맞게 점검결과를 작성하도록 하고 있다. 여기서 사용자 보안점검 항목이 도출되었으며 네트워크 보호와 단말기 보호 항목이다. 네트워크 보호 항목에서는 인터넷과 인트라넷 망 분리, 단말기 보호 항목에서는 필수보안 SW설치 항목 등이 도출되었다. 군사보안업무훈령에서의 사용자 보안점검 도출항목은 정보시스템 보호기준 및 보호통제 항목이다. 보호통제 항목별로 보호요구사항을 명시하고 있으며 이를 토대로 사용자 보안점검항목이 도출되었으며 식별 및 인증, 안전한 세션관리, 최신버전 SW설치, 안전한 업데이트 적용 4가지 대분류 항목이다. 식별 및 인증 항목에서는 패스워드 보안성 기준, 안전한 세션관리에서는 세션 잠금 항목 등이 도출되었다. 육군 군사보안 규정에서는 정보통신보안을 근거하여 사용자 점검항목을 도출하였는데 개인소유 정보통신 장비 통제와 비밀번호 운용 두 가지 항목으로 도출되어 사용자 보안진단항목으로 사용되었다

3. 진단도구 현황 및 문제점

3.1 진단도구 현황

3.1.1 PC 보안진단 프로그램 내 PC 지키미

'내PC 지키미'는 사용자 PC의 필수 보안 프로그램의 설치 여부 등을 점검하여 확인하는 보안점검 프로그램으로 점검항목은 <표 3>과 같다.

<표 3> 내PC 지키미의 점검항목

구분	점검항목		내 용
1	PC 점검	보안 업데이트	바이러스 백신 설치 및 실행 여부 점검
			바이러스 백신의 최신 보안 패치 여부 점검
			한글프로그램의 최신 보안 패치 설치 여부 점검
		패스워드 안전성	로그인 패스워드 안정성여부 점검
			로그인 패스워드의 분기 1회 이상 변경여부 점검
		화면보호기 설정	화면보호기 설정 여부 점검
		공유폴더 설정	사용자공유 폴더 설정 여부 점검
		기타	USB 자동실행 허용 여부 점검
			미사용(3개월) ActiveX 프로그램 존재 여부 점검
2	패스워드 점검도구		
3	PC 정리 : 임시파일, 쿠키 등을 삭제		
4	보고서 보기 *: 운영체제 정보, 보안SW정보, 취약점 점검 내역 모니터링*		

저장매체통제체계

저장매체통제체계는 비인가된 저장매체의 사용을 통제하는 기능으로, 비인가된 저장매체(USB, 외장하드웨어, 스마트폰)를 연결 시 경고창과 함께 PC 접근을 통제하는 기능을 가진 필수 보안 소프트웨어이다.

공유폴더해제기

공유폴더해제기는 공유된 폴더를 식별하고 제거 하여 사용자가 미식별된 상태에서 자료유출을 방지하는 기능을 가진 필수 보안 소프트웨어이다.

PC전원차단 프로그램

PC전원차단 프로그램은 장시간 미사용 PC를 절전 모드로 전환시켜주는 기능을 제공한다. 이는 사용자 PC가 좀비PC가 되는 것을 방지해 준다.

전산보안진단체계

'전산보안진단체계'는 '내PC 지키미'와 같은 기능을 가진 PC 보안점검 프로그램으로 점검항목의 내용은 <표 4>와 같다.

<표 4> 전산보안진단체계의 점검항목

구분	점검항목	내 용
1	내컴퓨터 정보확인	
2	필수보안SW설치 여부	화면보호기
		공유폴더해제기
		저장매체통제체계
		내PC지키미
		바이로봇
		PC전원차단프로그램
		Eraser
3	PC비밀번호 변경	
4	보안바탕화면	
5	문서검색/삭제	
6	임시파일제거	
7	사이버보안진단 *: 비밀번호, 보안바탕화면, 필수S/W 설치여부 확인*	

<표 4>의 7번 항목은 매월 실시하는 사이버 보안진단의날 행사시 이 기능을 수행하지 않으면 PC를 사용할 수 없게 설정되어 사용자에게 보안점검의 강제성을 부여하는 특징을 가지고 있다.

3.1.2 수기용 사용자 체크리스트

사용자가 직접 작성하는 진단도구들로 PC로는 확인이 어려운 사용자의 보안의식 등도 포함하여 점검하기 위해 작성하는 보안점검 도구이다.

PC 사용자를 위한 체크리스트

PC 사용자의 행위로 인해 발생하는 취약점 위주의 점검항목으로 구성되어 있으며 <표 5>와 같다.

<표 5> 軍 사이버보안 체크리스트(PC사용자)

구분	점 검 항 목
1	PC부팅용, 로그인, 화면보호기, 비밀번호 설정 및 주기적 변경하기
2	필수보안SW 설치하고 바이러스 검사 및 자동업데이트 확인하기
3	PC운영체제 및 소프트웨어 최신 보안 업데이트 하기
4	인트라넷(국방망)과 인터넷 PC, 프린터 망혼용 금지하기
5	개인정보 포함된 파일은 암호화 또는 삭제하기
6	인터넷 메일을 통한 자료 송신 금지
7	출처가 불분명한 이메일은 열어보지 말고 삭제하기
8	비인가 SW 무단설치 및 사용 금지하기
9	휴대용 저장장치(USB)는 승인된 것만 사용하고, 외부반출 금지
10	공유폴더 사용 금지 및 불필요한 자료는 삭제하기

스마트폰 사용자를 위한 체크리스트

스마트폰 사용자 체크리스트도 사용자의 보안수준을 향상시켜 취약점에 노출되는 것을 방지하는 목적을 가진 점검항목이며 <표 6>과 같다.

<표 6> 軍 사이버보안 체크리스트(스마트폰 사용자)[6]

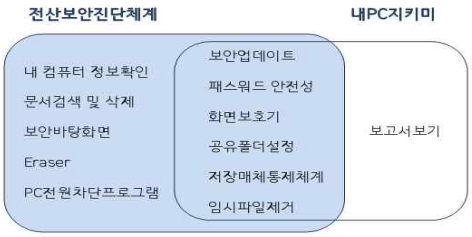
구분	점 검 항 목
1	단문문자(또는 SNS) 메시지에 포함된 URL 클릭하지 않기
2	스마트폰 최신 백신 설치 및 정기적 점검하기
3	공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)앱 미설치
4	스마트폰 운영체제를 항상 최신으로 업데이트 하기
5	루팅, 탈옥 등 스마트폰 구조를 임의로 변경하지 않기
6	스마트폰 앱 설치시 과도한 권한을 요구하는 앱은 설치하지 않기
7	스마트폰 또는 SNS에 중요정보 지우기
8	스마트폰 보안 잠금(비밀번호 또는 화면 패턴)설정하여 이용하기
9	스마트폰 Wi-Fi 연결시 제공자 불분명한 공유기 이용하지 않기
10	공인인증서는 USIM 등 안전한 저장장소에 보관하기

3.2 진단도구 문제점

지금까지의 육군을 중심으로 사용하는 사용자 점검 보안진단도구들을 보면 아래와 같은 문제점들을 도출할 수 있다.

3.2.1 과도한 중복

PC 보안진단 프로그램들이 그 기능이 서로 겹치는 부분이 상당히 존재한다. '전산보안진단체계'의 진단항목을 '내PC 지키미'와 비교해 보면 (그림 1)과 같이 '보고서 보기' 항목을 제외하고는 모두 '전산보안진단체계'의 진단항목들과 중복되어 있음을 알 수 있다.



(그림 1) 전산보안진단체계와 내PC지키미 관계

그리고 수기작성 체크리스트(PC 사용자)의 1번과 2번 항목의 필수보안 소프트웨어 설치는 PC 보안진단 프로그램과 중복되는 항목들이다.

3.2.2 시스템 환경 미고려

'내PC 지키미의' 패스워드 안전성 점검도구는 2008년 한국인터넷진흥원(KISA)에서 만든 진단도구로 현재 시스템 환경에 대해서는 패스워드의 안전성을 보장하기가 어렵다. 또한 기타 점검항목인 ActiveX 프로그램의 존재여부도 지금의 사용자 환경을 고려하면 불필요한 항목이다. 그리고 '전산보안진단체계'에서 Eraser라는 프로그램을 필수보안 소프트웨어로 설치하도록 하고 있는데 Eraser는 하드디스크(HDD)에만 환경에만 적용되는 파일소거프로그램으로 SSD환경에서는 필수 항목이 될 필요가 없다. 또한 수기작성 체크리스트들은 군만의 인트라넷 환경과 민감 데이터들의 보호 등 특수한 환경을 고려하는 부분이 부족하다.

4. 개선방향

앞에서 알 수 있듯이 현재의 PC 보안점검 프로그램들과 수기작성 체크리스트들은 불필요하게 중복되거나 시스템 환경을 고려하지 않은 점검항목이 상당수 존재한다. 이를 해결하기 위해 보안점검 프로그램들은 하나로 통합하고 수기작성 체크리스트들은 항목을 보강하는 방법으로 개선방향을 제시하고자 한다.

4.1 보안점검 프로그램 통합

중복되는 항목을 제거·통합하여 이른바 '新사이버보안 진단체계'를 제안하고자 한다. 新사이버보안 진단체계는 <표 7>와 같은 점검항목들로, 1번 항목인 Eraser 프로그램은 사용자의 시스템 환경을 고려함을 명시하였고, 4번 항목은 점검의 목적을 분명하게 내용을 수정하였다. 마지막으로 '내PC 지키미'와 '전산보안진단체계'와 중복되지 않는 보고서 보기 기능은 추가하였다.

<표 7> 新사이버 보안진단체계

구 분	점검항목	내 용
1	필수보안 S/W설치 여부	화면보호기
		공유폴더해제기
		저장매체통제체계
		바이로봇
		PC전원차단프로그램
		Eraser(노트북제외)
2	PC비밀번호 변경	
3	보안바탕화면 변경	
4	문서검색/ 불필요한 자료 삭제	
5	임시파일제거	
6	사이버보안진단	
7	보고서보기	

4.2 수기 체크리스트 통합 및 추가

수기로 점검하는 체크리스트들은 사용자들의 보안인식 수준을 향상시키는데 목적이 있다고 판단하여 점검항목의 내용을 명확히 하였고 사용자의 편의성을 고려하여 필수 항목만으로 점검하도록 하였다.

4.2.1 軍 사이버보안 체크리스트(PC 사용자)

기존의 PC사용자의 점검항목을 보면 1, 2번 항목이 '新사이버 보안진단체계'의 1번 항목과 중복되므로 점검항목의 내용을 수정하였다. 또한, 기존의 10번 항목인 '공유폴더 사용 금지 및 불필요한 자료는 삭제하기'도 新사이버보안 체크리스트의 4번 항목과 중복되므로 삭제하였다. 그러므로 기존 항목에 비해 점검항목이 줄어들어 사용자의 편의성을 증진시켰다.

<표 8> 新사이버보안 체크리스트(PC사용자)

구분	점 검 항 목
1	사이버 보안진단체계 실시하기
2	바이러스 검사 및 자동업데이트 확인하기
3	PC운영체제 및 소프트웨어 최신 보안업데이트 하기
4	인트라넷(국방망)과 인터넷 PC, 프린터 망혼용 금지하기
5	개인정보 포함된 파일은 암호화 또는 삭제하기
6	인터넷 메일을 통한 자료 송신 금지
7	출처가 불분명한 이메일은 열어보지 말고 삭제하기
8	비인가 SW 무단설치 및 사용 금지하기
9	휴대용 저장장치(USB)는 승인된 것만 사용하고, 외부반출 금지

4.2.2 軍 사이버보안 체크리스트(스마트폰 사용자)

기존의 '軍 사이버보안 체크리스트(스마트폰 사용자)'는 군만의 특수한 환경과 최근 사이버 공격기법 적용이 다소 미흡하여 아래와 같은 내용을 추가할 필요가 있다고 판단하였다.

첫 번째, 악성코드 감염에 유의하기

APT공격기법에서 개인을 노리는 감염방법의 90%가 악성코드를 통한 감염이다.[7] APT 공격을 막는 가장 효율적인 방법은 단축 URL 등 악성 링크 판단이 직관적으로 어려운 사이트를 열 때 신중을 기하는

것이다. 특히, 개인정보가 중요하고 민감한 군인들은 첨부파일을 여는데 더욱 신중을 기할 필요가 있다고 판단되어 구체적인 내용으로 추가하였다.

두 번째, 블루투스로 출처가 불분명한 기기 연결하지 않기

출처가 불분명한 기기와 블루투스를 연결하면 악성코드로 감염, 정보 유출 등 여러 침해행위에 노출될 수 있으므로 평상시 블루투스를 항상 꺼두고 필요할 때만 출처가 확인된 기기에 한해서 연결해야 할 것이다.

세 번째, 군용 PC와 연결하지 않기

스마트폰을 PC에 연결하면 상호간의 바이러스 감염이 이루어질 수 있다. 저장매체인 스마트폰은 군 보안 규정상 PC에 연결해서는 안 된다는 것을 보안교육의 목적으로 재차 강조하고 있어 체크리스트 항목에 추가할 필요가 있다고 판단하여 항목을 추가하였다.

위 3가지 항목을 추가하여 작성한 '新 軍 사이버보안 체크리스트(스마트폰 사용자)'는 <표 9>과 같다.

<표 9> 新사이버보안 체크리스트(스마트폰 사용자)

구분	점 검 항 목
1	단문문자(또는 SNS) 메시지, ***이메일에 포함된*** URL 클릭하지 않기
2	***운영체제 최신유지,*** 백신 설치 및 업데이트 하기
3	공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)앱 미설치
4	스마트폰 구조를 임의로 변경하지 않기***(루팅, 탈옥 등)***
5	스마트폰 앱 설치시 과도한 권한을 요구하는 앱은 설치하지 않기
6	스마트폰 또는 SNS에 ***군사관련 정보*** 지우기
7	스마트폰 보안 잠금(비밀번호 또는 화면 패턴)설정하여 이용하기
8	기기들과의 Wi-Fi, ***블루투스*** 연결시 제공자 불분명한곳은 이용하지 않기
9	공인인증서는 USIM 등 안전한 저장장소에 보관하기
10	***군용 PC와 연결하지 않기***

5. 결 론

사이버 공간은 계속 발전하고 있으며, 우리 생활의 중심은 점점 사이버 공간으로 옮겨가고 있다.[8] 이러한 흐름에 맞춰 국방부도 국방체계를 IT중심으로 전환하고 있는 중이다.[9] 그럼에도 불구하고 현재 육군의 사용자 보안진단도구는 과거의 시스템 환경에 머물러 있거나 불필요하게 중복된 항목들로 구성되어 사용자에게 신뢰도가 떨어질 우려가 있다.

본 연구에서 제시한 보안진단 항목으로 사이버 침해 대응을 진단한다면 사용자의 편의성을 증진시킴과 동시에 보안성 측면에서 기존의 보안진단 항목보다 향상된 개선된 진단도구가 될 것이라 기대한다.

참고문헌

[1] 연합뉴스, "한국 겨냥 디도스 공격 급증, 1분기 세계 2번째 많아", 2017. 5. 17

[2] 육군본부, "사이버방호작전 분석결과", 2017.

[3] 국가정보원, 미래창조과학부, 방송통신위원회, 행정자치부, "2016 국가정보보호백서", 2016.

[4] 국방부, "군사보안업무훈령", 2016. 07

[5] 최광복, " 사이버전 대응을 위한 국방 정보보호환경 분석과 보안관리모델 연구방향 고찰", 정보보호학회지, 2011.

[6] 국방부, "PC 및 스마트폰 사이버 보안 체크리스트", 2017. 4.

[7] 조호대, 신동일, "공공 및 민간부문의 사이버침해사고 현황분석에 따른 대응방안", 한국콘텐츠학회논문지, 9(1), 331-338, 2009.

[8] 최광복, "국가사이버위협에 따른 국방사이버대응실태", 정보보호학회지, 22(8), 36-40, 2012.

[9] 권오훈, 이명훈, 이재우, 임채호, "국방망의 지속적인 실시간 보안관리체계", 정보보호학회지, 23(6), 54-66, 2013.

[10] 김점구, 노시춘, 이도현 "Injection Flaws를 중심

으로 한 웹 애플리케이션 취약점 진단시스템 개발", 융합보안논문지, 2012 06.
[11] 윤재석, "국가 사이버보안 전략 수립과 개선을 위한 참조 모델 개발", 융합보안논문지, 2016. 06.

[저 자 소 개]

김 지 원 (Jee-Won Kim)
2002년 2월 동국대학교 학사
2016년 8월 연세대학교 석사
2016년 7월 ~ 현재
육군사관학교 컴퓨터과학과 강사
2017년 3월 ~ 현재
아주대학교 박사과정

email : jeewonkim@ajou.ac.kr

정 의 섭 (Ui-Seob Jung)
2016년 2월 아주대학교 석사
2002년 4월 ~ 현재
공군 정보체계관리단 정보보호팀 근무
2017년 3월 ~ 현재
아주대학교 박사과정

email : heaven22@hanmail.net

정 찬 기 (Chan-Gi Jung)

1986년 공군사관학교 전자공학 학사
1994년 플로리다공대 전산공학 석사
2001년 플로리다공대 전산공학 박사
2017년 3월 ~ 현재
아주대학교 NCW학과 교수

email : ckjung34@gmail.com