https://doi.org/10.33778/kcsa.2020.20.4.187

봉쇄와 보안장비 수준평가를 통한 정보보호 위험평가 개선 연구

한 충 희*, 한 창 희**

요 약

정보보호 위험평가를 위해 다양한 정보보호 수준 평가와 정보보호 관리체계 인증이 그 어느때보다도 대규모로 이루어지고 있다. 그러나 정보보호 수준평가 우수기업과 정보보호 관리체계 인증 우수기업에 대한 정보보호 침해 사례가 지속적으로 발생하고 있는 실정이다. 기존의 정보보호 위험평가 방법론은 사이버 위협이 어디로부터 유입되는지에 대한 검토와 각 유입경로 구간에 대한 보안장비들의 적절한 운영여부에 대한 검토 없이 정보시스템 내부의 정보자산들을 식별하여 위험도를 정성적으로 판단하여 분석하고 있는 실정이다. 현재의 위험평가 방안을 개선하기 위해서는 사이버 위협이 어디로부터 유입되는지 살펴보고 각 유입구간별 봉쇄수준을 향상시켜 불필요하게 유입되는 사이버 위협을 절대적으로 감소시킬 필요가 있다. 이와 더불어 현재의 위험평가 방법론에서 간과되고 있는 보안장비의 적절한 구성과 운영수준에 대한 측정과 향상이 반드시 필요하다. 사이버 위협의 출입구를 최대한 봉쇄하고 어쩔 수 없이 열려 있는 틈새를 통과해서 내부로 유입되는 사이버 위협을 각 보안장비를 동원하여 탐지하고 대응하는 것이 필요한 것이다. 이에 본 논문에서는 ISMS-P 인증항목과 주요정보통신기반시설 취약점 분석평가 항목에 사이버 위협에 대한 봉쇄수준을 평가할 수 있는 심사항목과 각 유입경로 구간에 대한 보안장비 구성 수준을 측정하는 심사항목을 추가 제안하고자 한다. 이를 통해 사이버 위협의 유입 자체를 감소시키고 사이버 침해사고의 가능성을 원천적으로 차단하는데 기여하고자 한다.

A study for Information Security Risk Assessment Methodology Improvement by blockade and security system level assessment

Han Choong-Hee*, Han ChangHee**

ABSTRACT

In order to manage information security risk, various information security level evaluation and information security management system certification have been conducted on a larger scale than ever. However, there are continuous cases of infringement of information protection for companies with excellent information security evaluation and companies with excellent information security management system certification. The existing information security risk management methodology identifies and analyzes risks by identifying information assets inside the information system. Existing information security risk management methodology lacks a review of where cyber threats come from and whether security devices are properly operated for each route. In order to improve the current risk management plan, it is necessary to look at where cyber threats come from and improve the containment level for each inflow section to absolutely reduce unnecessary cyber threats. In addition, it is essential to measure and improve the appropriate configuration and operational level of security equipment that is currently overlooked in the risk management methodology. It is necessary to block and enter cyber threats as much as possible, and to detect and respond to cyber threats that inevitably pass through open niches and use security devices. Therefore, this paper proposes additional evaluation items for evaluating the containment level against cyber threats in the ISMS-P authentication items and vulnerability analysis and evaluation items for major information and communication infrastructures, and evaluates the level of security equipment configuration for each inflow.

Key words : Information Security Management, Risk Assessment, ISMS, ESC Model, foreign IP blocking

접수일(2020년 09월 28일), 수정일(1차: 2020년 10월 19일), 게재확정일(2020년 10월 27일)

* 전력거래소 안전보안실/정보보안팀(주저자)
** 육군사관학교 교수부/AI연구센터(교신저자)

1. 서 론

2001년 7월부터 정보보호관리체계(ISMS) 인증제도가 시행되었다. 2020년 5월 기준 ISMS-P(Personal Information & Information Security Management System) 234개, ISMS(Information Security Management System) 484개의 업체(기관)가 인증을 받아 종합적이고 체계적인 보안관리를 위해 지속적인 노력을 계속하고 있다.

그러나 ISMS 인증제도는 인증의 실수요자가 인식하는 인증의 효과성 등의 질적인 측면에서 미흡하다는 문제가 제기되고 있다. 2019년 11월 27일 업비트의 이더리움 핫월렛(인터넷이 연결된 암호화폐 지갑)에서 590억원 규모의 이더리움이 비정상적으로 출금되는 사고가 발생했다. 사고 이후 추가 피해를 막기 위해 핫월렛에 있던 모든 암호화폐를 콜드월렛(인터넷이 연결되지 않은 지갑)으로 이동시켜 더 이상의 비정상 출금사고가 생기지 않도록 조치하였다. 업비트의 운영회사 ㈜두나무는 암호화폐 거래소 운영(업비트)에 대하여 2018년 11월 이후 ISMS 인증을 암호화폐 거래소 최초로 획득한 기업이다. 업비트 해킹이후 암호화폐 업계 중심으로 ISMS 인증 무용론이 대두되었다. ISMS를 받아도 해킹을 당한다면 굳이 복잡한 과정을 거쳐 인증을 받을 필요가 있겠냐는 것이다. 현재의 ISMS 인증제도에서 간과하고 있는 것은 무엇일까에 대한 의문이 강해지고 있는 시점이다.

이에 본 논문에서는 주요정보통신기반시설에 대한 취약점 분석·평가제도와 ISMS 인증제도의 제도 전반에 대하여 살펴본다. 추가적으로 각각의 제도가 보완해야 할 사항들을 첫째, 사이버 위협 유입경로에 대한 봉쇄수준과 둘째, 사이버 위협 대응을 위한 보안장비 운영수준의 두 가지 측면에서 구체적으로 제시하여 정보보호 위험평가 제도의 발전에 기여하고자 한다.

2. 선행 연구

2.1 정보보호관리체계 인증제도

정보보호관리체계(ISMS) 인증제도는 [정보통신망 이용촉진 및 정보보호 등에 관한 법률] 제47조에 근거하여 기술적 물리적 보호조치 등 종합적인 관리체계가 인증심사 기준에 적합한지 여부를 한국인터넷진흥원으로부터 인증 받는 제도이다[1].

2012년 3월에는 그동안 실효성 문제로 논란이 많았던 정보보호 안전진단 제도를 폐지하고 ISMS로 의무화하는 법안을 개정하였다. 이와 함께 개인정보보호관리체계(PIMS, Personal Information Management System) 인증 제도, 정보보호 사전점검, 정보보호관리 등급제 등을 도입하는 근거를 마련하였다[2.3].

2018년 12월 기준으로 864건(누적)의 인증서가 발급되었으며, 601건의 인증서가 유지되고 있다[4]. 현재의 정보보호 관리체계 인증 추진체계는 정보보호 및 개인정보보호에 관한 관리체계 인증(ISMS-P)로 통합되어 정책기관으로 과학기술정보통신부, 인증기관으로 한국인터넷진흥원과 금융보안원, 심사기관으로 정보통신진흥협회 (KAIT), 정보통신기술협회(TTA), 개인정보보호협회(OPA)로 구성되어 시행중이다. 인증심사 기준은 관리체계 수립 및 운영(16개), 보호대책 요구사항(64개), 개인정보처리단계별 요구사항(22개) 총 102개 통제항목에 대한 적합성 평가를 진행한다[5].

2.2 주요정보통신기반시설 보호

정보통신 인프라의 발전으로 국가 기반시설의 정보통신기술에 대한 의존이 심화되면서 전자적 침해행위 예방 및 사후 대응체계를 구축하기 위해 2001년 [정보통신기반보호법]을 제정하였다. 2007년에는 ICT 환경 변화와 운영과정 상의 미비점을 반영하여 공공분야와 민간분야로 나누어 실무위원회를 구체화하였다. 국가정보원장과 과학기술정보통신부장관 등 대통령령이 정하는 국가기관의 장이 중앙행정기관에 주요정보통신기반시설의 지정을 권고하고 주요정보통신기반시설 보호대책 이행여부를 확인할 수 있도록 권한을 부여하였다[4].

2012년 개정된 시행령은 실무위원회의 변화에 맞는 구체적인 구성·운영방식을 명시하였다. 또한 취약점 분석평가 주기를 2년에서 1년으로 단축하였다. 주요정보통신기반시설의 지정 대상은 국가공공기관뿐 아니라 민간이 운영 관리하는 정보통신기반시설을 포함한다. 2018년 12월 기준으로 공공분야 기반시설은 140개 관리기관 262개 시설, 민간분야 기반시설은 91개 관리기관 149개 시설로 총 411개의 주요정보통신기반시설을 지정하여 관리중이다[4].

2.3 취약점 분석 평가 및 보호대책

주요정보통신기반시설이 신규 지정될 경우 6개월 이내에 취약점 분석 평가를 실시하여야 한다. 취약점 분석 평가는 453개의 관리적/물리적/기술적 점검항목에 대하여 2년 주기로 실시하였으나, 2012년 [정보통신기반보호법 시행령] 개정을 통해 매년 1회 실시로 강화되었다. 취약점 분석평가는 내부 전담반을 구성하여 수행하거나 한국인터넷진흥원, 국가보안기술연구소, 정보공유·분석센터, 정보보호 전문서비스 기업에 위탁할 수 있다. 주요정보통신기반시설에 대한 보호계획은 관리기관에서 제출한 보호대책을 종합·조정하여 매년 수립하고 시행한다. 국가정보원장과 과학기술정보통신부장관 등 대통령령으로 정하는 국가기관의 장은 보호대책의 이행여부를 확인하고 세부적인 내용을 점검하고 개선을 권고할 수 있다[4].

2012년부터 주요정보통신기반시설 관리기관 간 협력강화와 정보교류 확대를 위하여 기반보호포럼을 통해 우수기관 사례를 공유하고 발전방안을 논의한다. 또한 2012년부터 제어시스템 사이버보안 관련 업계, 학계, 연구기관 등 전문가 30명으로 구성된 '제어시스템 보안연구회'를 운영하고 있다. 최근에는 사이버위협헌팅, 제어시스템 보안관제방안, 국외동향 등을 논의하였다. 또한 2018년 3월과 5월 56개 관리기관의 120개 제어시스템을 대상으로 사이버공격 대응훈련을 실시하였다. 훈련은 내부자 위협 대응, 제어시스템 랜섬웨어 위협대응, 제어기기 및 네트워크 장비 보안점검 및 공급자망 위협 대응 등 4가지 주제로 실시되었다[4].

3. 사이버 위협의 유입경로 분석

2019년 1년 동안 전력분야 주요정보통신기반시설 중 한 곳의 사이버 위협 대응활동을 조사하여 통계적으로 분석하였다. 2019년 한해 동안의 통계를 살펴보면 총 7,537,830건의 사이버 위협을 탐지하여 대응활동을 수행하였다. 세부적으로 살펴보면 웹서비스 유입 6,191,000건(82.132%), 악성메일 926,928건(12.297%), 악성 웹사이트 419,831건(5.57%), 악성 매체 71건(0.0011%)의 순으로 <표 1과>과 같이 집계되었다. 이를 통해 80% 이상의 사이버 위협이 오픈된 웹서비스를 통해 유입되고 있으며 약 20% 정도를 악성메일 위협, 악성 웹사이트 위협, 악성 매체에 의한 위협이 유입되고 있음을 확인할 수 있다.

<표 1> 사이버 위협 유입경로별 유입 통계

No	Types of threats	Events	Ratios
1	Web service	6,191,000	82.1%
2	Bad e-mail	926,928	12.3%
3	Bad page	419,831	5.6%
4	Bad storage	71	0.001%
Total		7,537,830	100%

위의 통계를 바탕으로 사이버 위협을 유입경로 측면에서 정리하면 웹서비스 위협, 악성 전자메일 위협, 악성 웹페이지 위협, 악성 매체 위협의 4가지로 구분할 수 있다. 아래의 (그림 1)은 사이버 위협의 유입경로를 나타낸다.

(그림 1) Gates of Cyber Terror Threat

우선, 사이버 위협 유입경로에 대한 분석에서 사용되는 네트워크 또는 망의 구분을 3가지로 정의하기로 한다. 첫째, 제어망 또는 폐쇄망이다. 제어망 또는 폐쇄망은 인터넷과의 연결성이 존재하는 않는 상태에서 운영되는 네트워크 또는 망이라고 정의한다. 둘째, 회원망이다. 회원망은 ID와 패스워드, 공인인증서 등의 인증수단으로 허용된 회원들을 대상으로 운영되는 정보시스템 네트워크 또는 망이다. 셋째, 인터넷망이다. 인터넷망은 특별히 제한되지 않은 상태에서 인터넷과 연결된 네트워크 또는 망으로 정의한다. 그럼 지금부터 사이버 위협의 유입경로 측면에서의 위협의 4가지에 대해서 하나씩 살펴보도록 한다.

먼저, 오픈된 웹서비스로부터의 위협은 공인 IP를 이용하여 방화벽의 출발지 부분을 'Any'로 설정한 상태로 HTTP, HTTPS 등의 웹서비스를 제공하는 경우에 발생한다. 인터넷망처럼 누구나 접속하는 환경에서도 발생하지만 회원망처럼 ID와 비밀번호, 공인인증, OTP 등의 방법으로 제한된 회원들만 사용하는 인터넷 네트워크 환경에서도 오픈된 웹서비스 위협은 끊임없이 발생하고 있다. IP기반의 사이버 공격은 인터넷망과 회원망을 구분하지 않고 'Any'로 서비스 되는 공인 IP들을 목표로 24시간 쉬지 않고 사이버 위협을 시도하고 있다.

악성메일로부터의 위협은 전자메일서비스를 통해 유입된다. 지메일(gmail), 네이버(Naver)메일 등의 상용메일을 포함해서 회사에서 사용하는 회사메일에도 지속적으로 악성메일들은 유입되고 있다. 악성메일을 아무 의심 없이 클릭하여 APT 공격의 시작점이 되기도 한다. 사실 악성메일에 의한 위협을 방어할 수단이 완벽하지 않기 때문에 악성 메일들이 제대로 걸러지지 않고 사용자의 PC화면에 리스트업 되는 일들이 발생한다. 결국 최종적인 악성메일 대응은 사용자 스스로가 '이메일이 누구로부터 왔는지'에 대한 합리적인 의심을 통해서만 성공적인 방어를 할 수 있다. 이에 사용자들에게 악성메일에 대한 철저한 교육이 필요하다.

악성 웹페이지로부터의 위협은 악성 웹페이지를 탐색하는 경우에 발생하는 위협이다. 실제 통계를 살펴보면 악성 메일에 의한 위협보다 더 많은 악성코드 감염 사례가 나타나고 있는 상황이다. 우리는 효율적인 업무수행을 위해 인터넷 웹페이지를 탐색하고 파일을 다운 받는 일들을 종종 수행하게 되는데 이러한 과정들을 통해 유입되는 사이버 위협 감염 사례들이 증가하고 있는 것이다. 유해사이트차단 솔루션 등으로 악성 웹사이트들을 차단하는 활동들을 수행하지만 사이버 공격자들은 끊임없이 위치를 바꿔 가면서 악성 웹사이트들을 생성하고 있는 실정이다.

악성 매체로부터의 위협은 오염된 저장장치를 사용하는 과정에서 바이러스, 웜, 트로이목마, 인터넷 악성코드, 스파이웨어 등의 악성코드를 침투시키면서 발생하는 위협이다. 최근 사이버 위협에 대한 대응의 일환으로 상용 USB의 사용이 금지되고 정보시스템에 대한 외부 저장매체의 반입을 원칙적으로 금지하고 있다. 그러나 업무상의 이유로 종종 외부저장매체의 반입이 이루어지는 경우가 있는데 백신 소프트웨어의 탐지 기능의 한계로 반입하는 순간 탐지되지 못한 상태로 유입되거나 백신 소프트웨어의 탐지 룰이 업데이트 된 후에 사이버 위협으로 탐지되어 치료 또는 삭제되는 경우들이 발생하고 있다.

4. 사이버 위협 봉쇄수준 평가 방안 제안

사이버 위협에 대한 봉쇄수준과 각 위협구간별 보안장비의 적정한 보유수준에 대한 평가 방안을 제시한다. 각 사이버 위협의 구간에 대한 봉쇄수준의 배점은 웹서비스를 통해 유입되는 구간에 대해서는 16점, 나머지 3개 구간에 대해서는 8점씩을 부여하여 총 40점을 부여한다. 각 사이버 위협의 구간에 대한 보안장비의 평가는 봉쇄장비와 진압장비로 구분하여 평가하며 각각에 대해서 8점, 7점을 동일하게 부여한다. 웹서비스 구간 봉쇄수준에 더 많은 점수를 부여하는 이유는 웹서비스 구간에 대한 봉쇄강화가 절실하기 때문이다.

4.1 사이버 위협 봉쇄수준 평가

정보보호 인증 및 평가제도의 실질적 개선을 통해 기업들의 사이버 안전성이 실제적으로 개선되도록 보완해야 한다. 이를 위해서는 사이버 위협의 유입경로에 대한 봉쇄수준과 보안장비 수준 측정을 위한 신규 평가항목의 추가가 필요하다.

2017년 12월 발간된 과학기술정보통신부의 '주요정보통신기반시설 취약점 분석·평가 방법 상세가이드'는 453개의 관리적/물리적/기술적 점검항목으로 이루어져 있다. 관리적 분야 114개, 물리적 분야 26개, 제어시스템 22개, 네트워크 38개, 보안시스템 26개, DBMS서버 24개, Unix서버 73개, Windows서버 82개, PC 20개, 웹취약점 28개로 구분된다.

2018년 11월 7일 시행된 과학기술정보통신부의 '정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시'는 9장 39조로 이루어져 있다. 또한 동 고시는 8개의 별표와 15개의 서식을 별도로 제시하고 있는데 [별표 7] '인증기준'에서 인증항목과 상세 내용을 기술하고 있다.

'주요정보통신기반시설 취약점 분석·평가 방법 상세가이드' 관리적 분야에 115번째 신규 점검항목으로 'A-115 [유입경로별 봉쇄] HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로에 대한 봉쇄수준을 개선하는가' 라는 점검항목을 추가하는 것이 필요하다. <표 2>는 세부적인 내용을 제시한다.

<표 2> Details of a new audit item

No	Item	Details
A-115	유입경로별 봉쇄	HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로에 대한 봉쇄수준을 개선하는가

'정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시'의 [별표 7]은 '관리체계 수립 및 운영'과 '보호대책 요구사항' 그리고 '개인정보처리 단계별 요구사항' 3개 분야로 구성되어 있다. '관리체계 수립 및 운영'의 '1.2 위험관리' 분야에 1.2.5 [유입경로별 봉쇄] '최고경영자는 HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로에 대한 봉쇄수준을 개선하는 활동을 수행하여야 한다' 는 인증항목을 추가하는 것이 필요하다. 다음 <표 3>은 세부적인 상세내용을 제시하였다.

<표 3> Details of a new audit item

No	Item	Details
1.2.5	유입경로별 봉쇄	최고경영자는 HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로에 대한 봉쇄수준을 개선하는 활동을 수행하여야 한다

오픈된 웹서비스에 의한 위협으로 발생하는 위험을 봉쇄하는 수준의 평가 척도는 기관의 웹서비스 중 해외로부터의 접근을 허용하고 있는 웹서비스의 비율이 어느 정도인가로 결정할 수 있다. 평가점수는 총 16점을 부여하며, 100~91% 2점, 90~81% 4점, 80~61% 6점, 60~51% 8점, 50~41% 10점, 40~31% 12점, 30~21% 14점, 20~0% 16점으로 평가한다.

악성메일에 의한 위협으로 발생하는 위험을 봉쇄하는 수준의 평가 척도는 기관의 악성 메일 모의훈련 중 모의 악성메일 열람자의 비율이 어느 정도인가로 결정할 수 있다. 평가점수는 총 8점을 부여하며, 100~21% 1점, 20~18% 2점, 17~14% 3점, 13~10% 4점, 9~7% 5점, 6~4% 6점, 3~2% 7점, 1~0% 8점으로 평가한다.

악성 웹페이지에 의한 위협으로 발생하는 위험을 봉쇄하는 수준의 평가척도는 기관의 악성 웹페이지에 의해 발생된 악성코드 감염자의 비율이 어느 정도인가로 결정할 수 있다. 전체 직원 중 악성 웹페이지를 이용하다가 악성코드에 감염된 직원의 비율에 따라 평가점수는 총 8점을 부여하며, 100~21% 1점, 20~18% 2점, 17~14% 3점, 13~10% 4점, 9~7% 5점, 6~4% 6점, 3~2% 7점, 1~0% 8점으로 평가한다.

악성 저장매체에 의한 위협으로 발생하는 위험을 봉쇄하는 수준의 평가척도는 기관의 외부저장

매체 허용 비율이 어느 정도인가로 결정할 수 있다. 전체 직원 중 외부저장매체를 반입 신청하는 직원의 비율에 따라 평가점수는 총 8점을 부여하며, 100~81% 1점, 80~61% 2점, 60~51% 3점, 50~41% 4점, 40~31% 5점, 30~21% 6점, 20~11% 7점, 10~0% 8점으로 평가한다.

아래의 <표 4>는 사이버 위협 봉쇄수준에 대한 평가척도를 세부적으로 나타낸다. 봉쇄수준과 보안장비수준을 이용한 위험평가 총 점수는 100점으로 봉쇄수준에 40점을 부여하고 보안장비수준에 60점을 부여하였다. 봉쇄수준 40점 중 웹서비스 위협 봉쇄수준에 16점을 부여하고 나머지 3개 유입경로에 대한 봉쇄수준에는 각각 8점씩 부여하여 총 40점 만점이 되도록 구성하였다. 웹서비스 위협 봉쇄수준에 대한 배점을 다른 유입경로보다 2배를 부여한 이유는 다른 위협에 대해서는 현재의 체계하에서 어느 정도 관리를 하고 있는 실정이나 웹서비스를 통한 위협 유입에 대해서는 아무런 관리가 이루어지고 있지 않은 상황이라는 점을 감안하여 2배의 가중치를 부여하였다.

<표 4> Details of risk assessment scale

Category	Blockade Level		
	Guidelines	Scale	P
Open Web Threat	Not Blocked Webs per Total Webs * Total Webs = every web which has public IP for servicing HTTP * Not blocked Webs for oversea IP ranges	20~0%	16
		30~21%	14
		40~31%	12
		50~41%	10
		60~51%	8
		80~61%	6
		90~81%	4
		100~91%	2
Bad Email Threat	Bad Email Opened User ratios in Bad Email Test * 기관의 악성메일모의훈련 열람율 평균값 적용 * 비 시행시 0점	1~0%	8
		3~2%	7
		6~4%	6
		9~7%	5
		13~10%	4
		17~14%	3
		20~18%	2
		100~21%	1
Bad Page Threat	Contaminated users Ratios per total users * 전체 직원 수 대비 실제 악성페이지 감염건수 비율	1~0%	8
		3~2%	7
		6~4%	6
		9~7%	5
		13~10%	4
		17~14%	3
		20~18%	2
		100~21%	1
Bad Storage Threat	Media Control Exception Ratio * 전체 직원 수 대비 인터넷망 외부저장매체 사용신청건수 비율	10~0%	8
		20~11%	7
		30~21%	6
		40~31%	5
		50~41%	4
		60~51%	3
		80~61%	2
		100~81%	1

4.2 사이버 위협 보안장비 수준 평가

'주요정보통신기반시설 취약점 분석·평가 방법 상세가이드' 기술적 분야 중 보안시스템 분야에 S-27 [유입경로별 보안장비 운영] 'HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로별 최적의 보안장비 운영'이라는 27번째 신규 점검항목을 추가하는 것이 필요하다. <표 5>는 세부적인 내용을 제시한다.

<표 5> Details of a new audit item

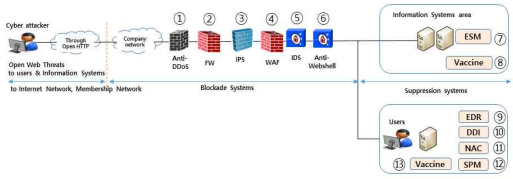
No	Item	Details
S-27	유입경로별 보안장비 운영	HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로별 최적의 보안장비 운영

사이버 위협에 대한 보안장비의 적절한 구성과 운영을 측정하기 위한 인증기준은 '보호대책 요구사항'의 '2.10 시스템 및 서비스 운영관리' 분야에 2.10.10 [유입경로별 보안장비 운영] '사이버 위협에 효과적으로 대응하기 위해 HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로에 대한 봉쇄장비와 진압장비를 적절하게 구성하고 운영하여야 한다' 는 인증항목을 추가하는 것이 필요하다. 다음 <표 6>은 세부적인 상세내용을 제시하였다.

<표 6> Details of a new audit item

No	Item	Details
2.10.10	유입경로별 보안장비 운영	사이버 위협에 효과적으로 대응하기 위해 HTTP 웹서비스, 웹메일, 웹페이지, 저장매체 4가지의 사이버 위협 유입경로에 대한 봉쇄장비와 진압장비를 적절하게 구성하고 운영하여야 한다

오픈된 웹서비스 위협으로 내부에 유입된 사이버 위협을 방어하는 방어체계 수준의 평가는 봉쇄장비수준과 진압장비수준의 합이며 총 15점으로 구성한다. 봉쇄장비수준은 봉쇄장비로 (그림 2)에 나열된 6개 장비, 즉, Anti-DDoS, 방화벽, IPS, WAF, IDS, Ant-Webshell 보안장비가 모두 적정한 수준으로 운영하고 있다면 8점을 부여한다.

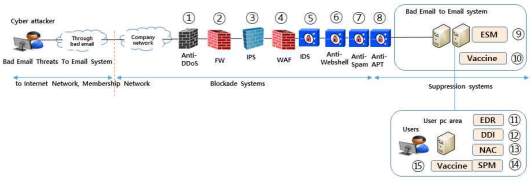


(그림 2) Web threat path & security systems

여기에서 1개의 장비가 부족한 경우에는 6.5점, 2개의 장비가 부족한 경우에는 5점, 3개의 장비가 부족한 경우에는 3.5점, 4개의 장비가 부족한 경우에는 2점, 5개의 장비가 부족한 경우에는 1점을 부여하고 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다.

진압장비수준은 그림 2와 같이 백신(Virus Vaccine), NAC(Network Access Control), DDI(Deep Discovery Inspector), EDR(Endpoint Detection Response), SPM(Security Policy Management)의 사용자 측 진압장비와 서버제품에 대한 백신(Virus Vaccine for Severs)과 ESM와 같은 진압장비 7개 제품을 모두 준비하여 운영하고 있는 경우에는 7점을 부여한다. 여기에서 1개의 장비가 부족한 경우에는 6점, 2개의 장비가 부족한 경우에는 5점, 3개 또는 4개의 장비가 부족한 경우에는 3.5점, 5개의 장비가 부족한 경우에는 2점, 6개의 장비가 부족한 경우에는 1점을 부여하고 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다.

악성메일 위협으로 내부에 유입된 사이버 위협을 방어하는 방어체계 수준의 평가는 봉쇄장비수준과 진압장비수준의 합이며 총 15점으로 구성한다. 봉쇄장비수준은 봉쇄장비로 (그림 3)에 나열된 8개 장비, 즉, Anti-DDoS, 방화벽, IPS, WAF, IDS, Anti-Webshell, Anti-Spam, Anti-APT 보안장비가 모두 적정한 수준으로 운영하고 있다면 8점을 부여한다.

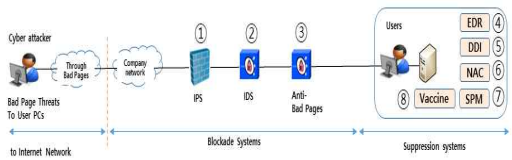


(그림 3) Bad email threat path & security systems

여기에서 1개의 장비가 부족한 경우에는 6.5점, 2개의 장비가 부족한 경우에는 5점, 3개의 장비가 부족한 경우에는 3.5점, 4개의 장비가 부족한 경우에는 2점, 5개의 장비가 부족한 경우에는 1점을 부여하고 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다.

진압장비수준은 그림 3과 같이 백신, NAC, DDI, EDR, SPM의 사용자 측 진압장비와 서버제품에 대한 백신과 ESM와 같은 진압장비 7개 제품을 모두 준비하여 운영하고 있는 경우에는 7점을 부여한다. 여기에서 1개의 장비가 부족한 경우에는 6점, 2개의 장비가 부족한 경우에는 5점, 3개 또는 4개의 장비가 부족한 경우에는 3.5점, 5개의 장비가 부족한 경우에는 2점, 6개의 장비가 부족한 경우에는 1점을 부여하고 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다.

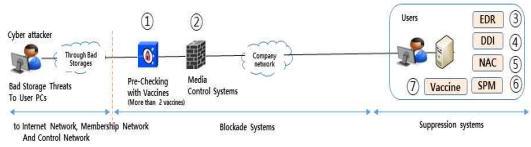
악성 웹페이지 위협으로 내부에 유입된 사이버 위협을 방어하는 방어체계 수준의 평가는 봉쇄장비수준과 진압장비수준의 합이며 총 15점으로 구성한다. 봉쇄장비수준은 봉쇄장비로 (그림 4)에 나열된 3개 장비, 즉, IPS, IDS, Anti bad page 보안장비가 모두 적정한 수준으로 운영하고 있다면 8점을 부여한다.



(그림 4) Bad page threat path & security systems

여기에서 1개의 장비가 부족한 경우에는 5점, 2개의 장비가 부족한 경우에는 3점, 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다. 진압장비수준은 그림 4와 같이 백신, NAC, DDI, EDR, SPM의 사용자 측 진압장비 5개 제품을 모두 준비하여 운영하고 있는 경우에는 7점을 부여한다. 여기에서 1개의 장비가 부족한 경우에는 5점, 2개의 장비가 부족한 경우에는 3점, 3개 또는 4개의 장비가 부족한 경우에는 1점, 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다.

악성 저장매체 위협으로 내부에 유입된 사이버 위협을 방어하는 방어체계 수준의 평가는 봉쇄장비수준과 진압장비수준의 합이며 총 15점으로 구성한다. 봉쇄장비수준은 봉쇄장비로 (그림 5)에 나열된 2개 장비, 즉, Pre-VirusVaccine, Media Control 보안장비가 모두 적정한 수준으로 운영하고 있다면 8점을 부여한다.



(그림 5) Bad storage threat path & security systems

여기에서 1개의 장비가 부족한 경우에는 3점, 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다. 진압장비수준은 그림 5와 같이 백신, NAC, DDI, EDR, SPM의 사용자 측 진압장비 5개 제품을 모두 준비하여 운영하고 있는 경우에는 7점을 부여한다. 여기에서 1개의 장비가 부족한 경우에는 5점, 2개의 장비가 부족한 경우에는 3점, 3개 또는 4개의 장비가 부족한 경우에는 1점, 모든 장비가 준비되어 있지 않을 경우에는 0점을 부여한다.

아래의 <표 7>은 사이버 위협 유입경로에 대한 적절한 보안장비 구성여부에 대한 평가척도를 세부적으로 나타낸다. 봉쇄수준과 보안장비수준을 이용한 위험평가 총 점수는 100점으로 봉쇄수준에 40점을 부여하고 보안장비수준에 60점을 부여하였다. 보안장비 수준은 60점 만점으로 이루어지며 각 유입경로별로 가이드라인과 비교하여 보안장비가 어느 정도 부족한지를 검토하여 점수를 부여하도록 하였다. 4개 유입경로에 대한 배점은 어느 한 경로에 대한 보안장비 수준의 부족은 전체 위협대응활동에 영향을 준다는 점에서 각각 15점으로 동일하게 부여 하였다

<표 7> Details of risk assessment scale

Defense System Level				
Category		Guidelines	Scale	P
Open Web Threat	Blockade System Level	①Anti-DDoS ②FW ③IPS ④WAF ⑤IDS ⑥Anti-WebShell	if all blockades are ready	8
			if one blockade is missing	6.5
			if two blockades are missing	5
			if three blockades are missing	3.5
			if four blockades are missing	2
			if five blockades are missing	1
			if nothing is ready	0
	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤Vaccine for Servers ⑥ESM ⑦SPM	if all suppressions are ready	7
			if one suppression is missing	6
			if two suppressions are missing	5
			if three-four suppresions are missing	3.5
			if five suppressions are missing	2
			if six suppressions are missing	1
			if nothing is ready	0
Bad Email Threat	Blockade System Level	①Anti-DDoS ②FW ③IPS ④WAF ⑤IDS ⑥Anti-WebShell ⑦Anti-Spam ⑧Anti-APT	if all blockades are ready	8
			if one~two blockades are missing	6.5
			if three blockades are missing	5
			if four blockades are missing	3.5
			if five~six blockades are missing	2
			if seven blockades are missing	1
			if nothing is ready	0
	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤Vaccine for Servers ⑥ESM ⑦SPM	if all suppressions are ready	7
			if one suppression is missing	6
			if two suppressions are missing	5
			if three-four suppresions are missing	3.5
			if five suppressions are missing	2
			if six suppressions are missing	1
			if nothing is ready	0

Bad Page Threat	Blockade System Level	①IPS ②IDS ③Anti-Badpage	if all blockades are ready	8
			if one blockade is missing	5
			if two blockades are missing	3
			if nothing is ready	0
	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤SPM	if all suppressions are ready	7
			if one suppression is missing	5
			if two suppressions are missing	3
			if three-four suppressions are missing	1
			if nothing is ready	0
Bad Storage Threat	Blockade System Level	①Pre-Vaccine ②Media Control	if all blockades are ready	8
			if one blockade is missing	3
			if nothing is ready	0
	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤SPM	if all suppressions are ready	7
			if one suppression is missing	5
			if two suppressions are missing	3
			if three-four suppressions are missing	1
			if nothing is ready	0

5. 결 론

기존의 위험평가 방법은 웹서비스로 유입되는 사이버 위협에 대한 봉쇄와 전체적인 방어체계 수준 대한 측정항목이 결여된 상황이다. 이를 개선하기 위해 사이버 위협을 유입경로별로 구분하고 그에 대한 봉쇄 수준과 방어체계 수준을 점검하고 보완대책을 수립하는 것이 반드시 필요할 것이다.

이에 본 논문에서는 일반 기업 및 공공 분야의 정보통신시설에 대한 사이버 위협 위험평가를 실시하는 경우에 명확하고 체계적으로 확인할 수 있는 위험평가 척도를 사이버 위협의 유입경로별 봉쇄수준과 보안장비 수준평가 방법을 통해 제시하였다.

유입경로별로 사이버 위협은 첫째, 웹서비스 위협, 둘째, 악성 전자메일 위협, 셋째, 악성 페이지 위협, 넷째, 악성 매체 위협으로 구분할 수 있다. 웹서비스 위협은 인터넷망과 회원망에서 나타나며, 전체 웹서비스 중 해외로부터의 접근을 허용하는 비율에 따라 봉쇄수준을 평가할 수 있다. 악성 전자메일 위협도 인터넷망과 회원망에서 나타나며, 악성메일훈련에서의 열람율에 따라 봉쇄수준을 평가한다. 악성웹페이지 위협은 인터넷망에서만 나타나며 전체 직원 중 악성웹페이지 감염자 비율로 봉쇄수준을 평가할 수 있다. 악성매체 위협은 인터넷망, 회원망, 제어망 모든 망에서 나타나며 인터넷망에서 USB, CD, 하드디스크 등의 외부저장매체의 읽기 허용과 관련된 매체제어 예외처리율로 봉쇄수준을 평가할 수 있을 것이다.

사이버 위협은 100% 완벽하게 봉쇄될 수 없을 것이다. 최대한 봉쇄하고 나머지 사이버 위협은 진압해야 할 것이다. 따라서 각 유입경로별 사이버 위협 방어체계 수준을 정확히 평가하고 보완하는 것이 매우 중요하다.

유입경로별 봉쇄수준에 대한 심도 있는 검토와 내부에 유입되는 사이버 위협들에 대한 봉쇄장비와 진압장비들의 적절한 구성과 운영에 대한 평가항목을 새롭게 추가하고 매년 정기적으로 평가되고 보완된다면 사이버 안전성이 획기적으로 강화될 수 있을 것으로 기대한다.

참고문헌

[1] Jang Sang Soo, 'Information Security Management System Authorized Judgement Defected Matter Analysis Study', Journal of The Korea Institute of Information Security & Cryptology, Vol. 20(1), pp. 31~38, Feb. 2010.

[2] Legal Knowledge Information System, Act for Information and Communication Network Usage Promotion, Information Security, etc,. 2011

[3] KISA, 'Study of Enhancement of Information Security Safety Diagnosis System Operation', 2009.

[4] KISA, 'National Information Protection White Paper', May. 2019.

[5] KISA, 'Notification on Information Security and Personal Information Security Management', Jan. 2019.

〔저자소개〕

한 충 희 (Han Choong-Hee)
1996년 2월 동국대 컴퓨터공학 학사
2002년 2월 동국대 정보보호학 석사
2019년 8월 전남대 정보보호학 박사
email : justicehan@kpx.or.kr

한 창 희 (Han ChangHee)
1990년 육군사관학교 물리 이학사
1994년 美 Syracuse 대학교 전산학 석사
2004년 美 Univ. of Southern California 전산학 박사
1994년~현재 육사 컴퓨터과학과 교수
email : chhan46@gmail.com