Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.6, Dec. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.6.1261

봉쇄와 보안장비 수준 기반 정보보호 위험관리 수준 측정 연구

한 충 희,[1†] 한 창 희[2‡]
[1]한국전력거래소 (연구원), [2]육군사관학교 (교수)

A study for Cybersecurity Risk Management by Blockade and Defense Level Analysis

Choong-Hee Han,[1†] ChangHee Han[2‡]
[1]Korea Power Exchange (Researcher), [2]Korea Military Academy (Professor)

요 약

기존의 정보보호 위험평가 방법은 정보자산의 취약성을 평가하는데 중점을 둔다. 그러나 정보자산의 형태가 바뀌고 새로운 유형의 정보자산이 나오면 그에 대한 평가기준도 추가하거나 삭제하는 등의 보완을 거쳐야 하는 한계가 있다. 기존 방법들은 사이버 위협이 유입되는 경로에 연구가 미흡하다. 특히, 공인 IP를 가지고 있는 웹기반 정보시스템을 대상으로 유입되는 유입경로의 봉쇄를 위한 연구가 매우 부족한 상황이다. 이에 본 논문에서는 BDLA (Blockade and Defense Level Analysis) 기반 정보보호 위험평가 모델의 주요 연구내용을 소개 한다. 또한, BDLA기반 정보보호 위험평가 모델을 적용하여 17개 공공기관의 봉쇄수준과 보안장비 수준 측정을 통하여 정보보호 위험 수준을 연구하였다.

ABSTRACT

Existing information security risk assessment methods focus on evaluating the vulnerability of information assets. However, when the form of information assets changes and new types of information assets emerge, there is a limitation in that the evaluation standards for them are also added or deleted. Existing methods have insufficient research on the path through which cyber threats are introduced. In particular, there is very little research on blocking the inflow path for web-based information systems with public IPs. Therefore, this paper introduces the main research contents of the BDLA (Blockade and Defense Level Analysis)-based information security risk assessment model. In addition, by applying the BDLA-based information security risk assessment model, the information security risk level was studied by measuring the blockade level and security equipment level of 17 public institutions.

Keywords: BDLA, ESC Model, foreign IP band blocking

I. 서 론

2021년 클라우드, 이동통신 등 변화하는 ICT 환경 변화에 맞추어 주요정보통기반시설 취약점 분석평가 기준이 개정되었다. 기존의 위험평가 방법론은 정보자산에 초점을 맞추고 있어 정보자산의 형태가 변하면 각각의 형태에 따른 취약점 평가기준을 신설해야 하는 상황이다. 정보자산별 형태별로 다양한 평가기준을 제정하여 운영하고 있지만 기본적으로는 패치관리, 비밀번호 관리, 로그관리 등의 내용으로 요약할

Received(07. 28. 2021), Modified(1st: 10. 13. 2021, 2nd: 11. 11. 2021), Accepted(11. 11. 2021)
† 주저자, justicehan@kpx.or.kr
‡ 교신저자, chhan46@gmail.com(Corresponding author)

수 있으며 사이버 공격자들도 파악하고 있는 실정으로 사이버 위협을 완벽히 방어하기 어려운 상황이다.

이에 본 논문에서는 기존 위험평가 방법론들의 위험측정을 위한 연구 노력을 살펴본다. 또한, 기존 방법들의 한계점을 보완하기 위해 BDLA 기반 정보보호 위험평가 모델을 살펴본 후 17개 공공기관에 적용하여 정보보호 위험관리 수준을 분석한다.

II. 선행 연구

정보자산의 취약성을 측정하기 위해 공격 유형별 확률을 부여하거나 Attack Graph를 생성하여 위험을 측정하였다[1]. 사이버 공격에 의한 전력시장의 위험을 측정하기 위해 자산들의 중요도, 피해정도, 공격용이성 등을 기준으로 위험의 순위를 측정하였다 [2].

공격 경로를 생성하거나 Attack Graph와 MCDM을 이용하여 확률론적 관점에서 위험을 측정하였다[3]. Pravin은 전력 네트워크의 위험을 분석하는데 그래프 이론과 소셜 네트워크 이론을 활용하였다[4].

Deepa Kundur 등은 전력분야에 대한 사이버 공격 위험을 측정하였다[5]. Jin Wei 등은 사이버-물리 계층 구조를 적용하고, 영역별로 분할하여 위험을 측정하였다[6].

Irving Lachow는 '단순, 발전된, 복합적 위협'으로 위험을 구분하였다[7]. Reith는 성가신(N : Nuisance) 위협에서 중요한(S : Significant) 위협으로 나누어 측정하였다[8].

한충희는 2019년 한해 동안의 전체 사이버 위협을 유입경로별로 분석하였다. 이를 바탕으로 사이버 위협의 유입경로를 웹서비스 위협, 악성 전자메일 위협, 악성 웹페이지 위협, 악성 매체 위협으로 구분하고 BDLA기반 정보보호 위험평가 모델을 정립하였다[9].

MITRE에서는 ATT&CK을 제안하였다[10]. ATT@CK는 공격 진행 단계 및 적용 망에 따라 위협을 구분하였다[11]. ISMS-P는 기밀성, 무결성, 가용성을 목표로 한다[12]. 기반시설 취약점 분석평가는 관리적·물리적·기술적 점검 항목에 대한 개선 과정이다[13].

III. BDLA 기반 정보보호 위험평가 모델

BDLA(Blockade & Defense Level Analysis)기반 정보보호 위험평가 모델은 사이버 위협이 유입되는 구간들을 크게 웹서비스 위협, 악성 이메일 위협, 악성 페이지 위협, 악성 저장매체 위협과 같이 크게 4가지로 구분하였다. BDLA 기반 정보보호 위험평가 모델은 위에 구분한 4개의 사이버 위협 유입 구간에 대한 봉쇄 수준과 보안장비 수준을 측정하여 위험을 평가하는 방법이다. 기존 방법들과의 차이점은 정보자산들의 중요도에 대한 평가를 진행하지 않는다는 것이다.

BDLA 기반 정보보호 위험평가 모델은 그림 1과 같이 유입경로별 봉쇄수준 측정과 방어역량 수준측정으로 구성된다.

Fig. 1. BDLA based Risk Assessment

BDLA 기반 정보보호 위험평가 모델의 유입경로별 봉쇄수준은 그림 2와 같이 4개의 유입경로별 봉쇄수준의 합이다. 웹서비스 위협의 봉쇄 수준을 16점으로 구성하고 다른 유입경로에 대한 봉쇄수준은 8점씩 부여하여 총 40점으로 구성한다. 정보보호의 현장의 관점에서 웹기반 정보시스템들을 대상으로 유입되는 웹서비스 위협 봉쇄 강화가 가장 시급하기 때문이다.

Fig. 2. Blockade Level (BL) Assessment

방어체계수준(Defense System Level, DSL)은 유입경로별 방어체계수준의 합이다. 유입경로별 방어체계수준은 15점씩 부여한다. 전체 정보시스템의 사이버 안전성은 균형적으로 구성되어야 하기 때문이다. 상대적으로 취약한 유입경로에 대한 방어장비 수준을 개선하는 활동이 반드시 필요하다. 방어체계수준은 그림 3과 같이 봉쇄장비수준과 진압장비수준으로 구성한다[14].

Fig. 3. Defense System Level (DSL)

IV. BDLA기반 위험관리 수준 측정

33개 기관의 정보보안 담당자들에게 (부록)의 BDLA 기반 위험평가 체크리스트에 따라 체크한 후 이메일로 회신하도록 요청하였다. 회신된 17개 기관의 봉쇄수준과 방어체계 수준에 대해 각 기관별 위험관리 수준을 분석하였다.

첫째, 웹서비스 위협 유입구간 봉쇄는 거의 이루어지지 않고 있었다. 웹서비스에 대한 미봉쇄 수준은 98%, 나머지 악성메일, 악성페이지, 악성매체에 대한 미봉쇄 수준은 각각 7%, 2%, 14%로 측정되었다.

둘째, 방어체계 수준은 기반시설 보유기관 5곳의 방어체계 수준이 비 기반시설 기관 12곳의 방어체계 수준보다 다소 양호한 수준이었다. 부족한 봉쇄장비로는 Anti-Webshell이 거의 모든 기관에서 보유하지 않고 있었다. 그 다음으로 IDS, Anti-Badpage, WAF, Anti-APT, Anti-Spam, Pre-Vac 등으로 분석되었다. 부족한 진압장비로는 EDR을 대부분 보유하지 않고 있었다. 그 다음으로 DDI , SPM의 순으로 분석되었다.

사이버 위협이 내부 사용자 PC 또는 서버에 유입되기 전에 탐지하고 대응하기 위한 봉쇄장비는 적정 봉쇄장비 대비 평균 1.0대 부족하였다. 웹서비스 위협 봉쇄장비는 1.1대, 악성메일 봉쇄장비는 1.4대, 악성페이지 봉쇄장비는 0.8대, 악성매체 봉쇄장비는 0.7대가 부족한 것으로 분석되었다.

유입구간별로 사이버 위협을 실질적으로 탐지하고 대응할 수 있는 진압장비는 적정 진압장비 대비 평균 1.9대 부족하였다. 웹서비스 위협 진압장비는 1.9대, 악성메일 진압장비는 1.9대, 악성페이지 진압장비는 1.9대, 악성매체 진압장비 1.9대가 부족한 것으로 분석되었다.

17개 조사 대상기관의 BDLA 위험관리 수준은 64.1점으로 분석되었다. 세부적으로는 주요정보통신기반시설 보유 5개 기관은 68.8점, 나머지 12개 기관은 60.7점으로 전반적으로 주요정보통신기반시설 보유기관의 정보보안 위험관리 수준이 양호한 것으로 분석되었다. 이러한 결과는 전반적으로 주요정보통신기반시설 보유기관의 보안장비 보유 수준이 상대적으로 양호하였기 때문으로 분석되었다. 그림 4는 각 기관별 상세 측정 결과이다.

Category	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	Average
Blockade level of Open Web Threat	2	2	2	2	2	4	2	2	2	2	2	2	2	2	2	2	2	2.1
Blockade level of Bad Email Threat	6	8	8	8	4	4	4	4	4	4	5	1	8	8	8	6	4	5.5
Blockade level of Bad Page Threat	6	8	8	8	8	8	6	8	8	8	7	8	8	8	8	7	8	7.6
Blockade level of Bad Storage Threat	8	8	8	8	7	8	8	8	8	6	6	8	8	8	8	4	8	7.5
Blockade Level total	22.0	26.0	26.0	26.0	21.0	24.0	20.0	22.0	22.0	20.0	20.0	19.0	26.0	26.0	26.0	19.0	22.0	22.8
Defense system level of Open Web Threat	7.0	11.5	13.5	10.0	8.5	10.0	11.5	12.5	12.5	12.5	8.5	13.0	14.0	14.0	13.0	10.0	14.0	11.5
Defense system level Bad Email Threat	8.5	11.5	13.5	10.0	10.0	10.0	10.0	12.5	12.5	12.5	7.0	13.0	12.5	14.0	13.0	10.0	14.0	11.4
Defense system level Bad Page Threat	6.0	11.0	15.0	11.0	6.0	4.0	10.0	13.0	13.0	10.0	4.0	11.0	10.0	13.0	11.0	6.0	10.0	9.6
Defense system level Bad Storage Threat	9.0	11.0	15.0	11.0	3.0	4.0	6.0	13.0	13.0	8.0	4.0	6.0	13.0	13.0	6.0	9.0	5.0	8.8
Defense level total	30.5	45	57	42	27.5	28	37.5	51	51	43	23.5	43	49.5	54	43	35	43	41.4
Blockade & defense level analysis	52.5	71.0	83.0	68.0	48.5	52.0	57.5	73.0	73.0	63.0	43.5	62.0	75.5	80.0	69.0	54.0	65.0	64.1

Fig. 4. Blockade & defense level of 17 organizations

V. 결 론

기존의 정보보호 위험관리 방법들은 보이지 않는 사이버 위협을 측정하기 위해 수학적 지식을 통해 위험을 측정하고자 하였으나 보완이 필요한 실정이다.

이에 본 논문에서는 BDLA기반 정보보호 위험평가 모델을 적용하여 기존 정보보호 위험평가에서 간과하고 있었던 사이버 위협의 유입경로별 봉쇄수준과 보안장비 수준을 측정하였다. 이번 연구를 통해 웹서비스 위협에 대한 봉쇄가 거의 이루어지지 않고 있음을 확인하였다. 또한 보안장비가 적정한 수준으로 구성되지 않고 있는 상황을 계량적으로 분석하였다.

기존 정보보호 위험평가 방법의 한계를 보완할 수 있도록 BDLA기반 정보보호 위험평가 모델을 활용하는 것이 필요하다. BDLA기반 정보보호 위험평가를 통해 사이버 안전성이 획기적으로 강화되기를 기대한다.

References

[1] Dong-Joo Kang, Huy-kang Kim, ‘Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry” Journal of The Korea Institute of Information Security and Cryptology , vol.23, no.3, pp. 445-457, 2013.

[2] Matias Negrete-Pincetic, Felipe Yoshida, George Gross, “Towards Quantifying the Impacts of Cyber Attacks in the

Competitive Electricity Market Environment," IEEE Bucharest PowerTech, Oct. 2009,

〔3〕 Nian Liu, Jianhua Zhang, and Wenxia Liu, "Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM," IEEE Transactions on Power Delivery, Vol.25 , no.3, pp. 1492-1500, Jun. 2010.

〔4〕 Pravin Chopade and Dr. Marwan Bikdash, "Modeling for Survivability of Smart Power Grid when subject to severe emergencies and vulnerability," Proceedings of IEEE Southeastcon, Mar. 2012.

〔5〕 Deepa Kundar, Xianyong Feng, Shan Liu, Takis Zourntos, Karen L., Burtler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," First IEEE International Conference on Smart Grid Communications, Oct. 2010.

〔6〕 Jin Wei, Deepa Kundur, Takis Zourntos, "On the Use of Cyber-Physical Hierarchy for Smart Grid Security and Efficient Control," 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), May. 2012.

〔7〕 Irving Lachow, FranklinD.Krame "Cyberpower and National Security", Potomac Books Inc, April. 2009.

〔8〕 Enter Greg Reith, "Prioritizing Cyber Threats With Real-Time Threat Intelligence," RFSID, 2018.

〔9〕 Han Choong-Hee, 'A study for Information Security Risk Assessment Methodology Improvement by blockade and security system level assessment' Korea Information Assurance Society, vol.20, no.4, pp. 187- 196, Oct, 2020.

〔10〕 B. E. Strom et al, "MITRE ATT&CKTM: Design and Philosophy," MITRE White paper, Jul. 2018.

〔11〕 Lee Hyunjin, "A study for configuration about cyber attack scenario using MITRE ATT&CKTM", Annual Conference of IEIE 2020, Vol 42, pp. 1103-1104, Korea, Jun. 2019.

〔12〕 Dong Hyun Kim, "A Study on the ISMS-P Accreditation Effect Using the Seven Threats of Security - Focused on Enterprise Size and Career", The Journal of Korean Institute of Information Technology - vol.18, no.4, pp.109-119, Apr. 2020.

〔13〕 Jaehyun Choi, "Security Vulnerability Management Measures for Major Information and Communication Infrastructure using VMS", Journal of The Institute of Electronics and Information Engineers vol.57, no.6, pp.37 - 43, June 2020

〔14〕 Han Choong-Hee, "Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis", Process Safety and Environmental Protection, Elsevier, vol.155, pp.306-316, Nov. 2021.

부록. BDLA based Cybersecurity Risk Assessment Checklist

구분	Blockade Level			Defense System Level			
	criteria	Scale	P	criteria	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	Blockade System Level	①Anti-DDoS ②FW ③IPS ④WAF ⑤IDS ⑥Anti-WebShell	if all blockades are ready	8
		30~21%	14			if one blockade is missing	6.5
		40~31%	12			if two blockades are missing	5
		50~41%	10			if three blockades are missing	3.5
						if four blockades are missing	2
						if five blockades are missing	1
						if nothing is ready	0
		60~51%	8	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤Vaccine for Servers ⑥ESM ⑦SPM	if all suppressions are ready	7
		80~61%	6			if one suppression is missing	6
		90~81%	4			if two suppressions are missing	5
						if three-four suppressions are missing	3.5
						if five suppressions are missing	2
		100~91%	2			if six suppressions are missing	1
						if nothing is ready	0
Bad Email Threat	Bad Email Opened User ratios in Bad Email Test * 기관의 악성메일모의훈련 열람율 평균값 적용 * 비 시행시 0점	1~0%	8	Blockade System Level	①Anti-DDoS ②FW ③IPS ④WAF ⑤IDS ⑥Anti-WebShell ⑦Anti-Spam ⑧Anti-APT	if all blockades are ready	8
		3~2%	7			if one~two blockades are missing	6.5
		6~4%	6			if three blockades are missing	5
		9~7%	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
		13~10%	4	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤Vaccine for Servers ⑥ESM ⑦SPM	if all suppressions are ready	7
		17~14%	3			if one suppression is missing	6
		20~18%	2			if two suppressions are missing	5
						if three-four suppressions are missing	3.5
						if five suppressions are missing	2
		100~21%	1			if six suppressions are missing	1
						if nothing is ready	0
Bad Page Threat	Contaminated users Ratios per total users * 전체 직원 수 대비 실제 악성페이지 감염건수 비율	1~0%	8	Blockade System Level	①IPS ②IDS ③Anti-Badpage	if all blockades are ready	8
		3~2%	7			if one blockade is missing	5
		6~4%	6			if two blockades are missing	3
		9~7%	5			if nothing is ready	0
		13~10%	4	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤SPM	if all suppressions are ready	7
		17~14%	3			if one suppression is missing	5
		20~18%	2			if two suppressions are missing	3
						if three-four suppressions are missing	1
		100~21%	1			if nothing is ready	0
Bad Storage Threat	Media Control Exception Ratio * 전체 직원 수 대비 인터넷망 외부저장매체 사용신청건수 비율	10~0%	8	Blockade System Level	①Pre-Vaccine ②Media Control	if all blockades are ready	8
		20~11%	7			if one blockade is missing	3
		30~21%	6			if nothing is ready	0
		40~31%	5	Suppression System Level	①Vaccine ②NAC ③DDI ④EDR ⑤SPM	if all suppressions are ready	7
		50~41%	4			if one suppression is missing	5
		60~51%	3			if two suppressions are missing	3
		80~61%	2			if three-four suppressions are missing	1
		100~81%	1			if nothing is ready	0
CTTBL (봉쇄수준)				CTTDSL (방어수준)			
CTTRML(사이버 테러위협 위험관리 수준) :							

〈저자소개〉

한 충 희 (Choong-Hee Han) 정회원
1996년: 동국대학교 컴퓨터공학 (학사)
2002년: 동국대학교 정보보호학과 (이학석사)
2019년: 전남대학교 정보보호협동과정 (이학박사)
2002년 3월~현재: 한국전력거래소 정보보안팀 차장
2021년 3월~현재: 전남대학교 대학원 정보보안협동과정 겸임강사
〈관심분야〉 보안관제, 침해대응, 주요정보통신기반시설 보호대책, 개인정보보호 등

한 창 희(ChangHee Han) 정회원
1990년: 육군사관학교 물리 이학사
1994년: 美 Syracuse 대학교 전산학 석사
2004년: 美 Univ. of Southern California 전산학 박사
1994년~현재: 육사 컴퓨터과학과 교수
〈관심분야〉 정보보호, 정보보호 인력 양성, 정보통신 기반보호, 정보보호 R&D