기업 보안 향상을 위한 RASS 보안 평가 모델 제안

김주원 · 김종민*

동신대학교

Proposed RASS Security Assessment Model to Improve Enterprise Security

Ju-won Kim · Jong-min Kim*

Dongshin University

E-mail : kim939598@naver.com / dyuo1004@dsu.ac.kr

요 약

사이버 보안성 평가란 위협 및 취약성 분석을 통해 시스템의 위험 수준을 평가하여 적절한 보안조치를 취하기 위한 과정이다. 최근 증가하고 있는 사이버 공격과 지속적으로 개발되는 지능형 보안 위협에 대비하기 위해 정확한 보안 평가 모델이 필요하다. 따라서 보안 장비와 구간, 취약점마다 가중치를 할당하여 점수화하는 매트릭 기반 보안 평가 모델 분석을 통해 위험도 평가 모델을 제시한다. 사이버 보안성 평가 시 필요한 요소들을 간략화하고 기업 환경에 맞춰 평가가 가능하다. 보안 장비별 평가를 통하여 기업 환경에 더 적합한 평가를 시행하여 추후 사이버 보안 평가 연구에 도움이 될 것으로 기대된다.

ABSTRACT

Cybersecurity assessment is the process of assessing the risk level of a system through threat and vulnerability analysis to take appropriate security measures. Accurate security evaluation models are needed to prepare for the recent increase in cyberattacks and the ever-developing intelligent security threats. Therefore, we present a risk assessment model through a matrix-based security assessment model analysis that scores by assigning weights across security equipment, intervals, and vulnerabilities. The factors necessary for cybersecurity evaluation can be simplified and evaluated according to the corporate environment. It is expected that the evaluation will be more appropriate for the enterprise environment through evaluation by security equipment, which will help the cyber security evaluation research in the future.

키워드

Cyber Security, Security Assessment, Risk Assessment, Security Scoring System

Ⅰ. 서 론

핵심 기반 시설은 폐쇄망의 네트워크에서 운영되었다. 그러나 상용 운영체제와 일부 개방된 네트워크 체계가 적용되고 있어, 사이버 보안 위험성이 증가하여 보안조치를 필요로 하고 있다[1]. 그렇게 보안 체계가 구축될수록 해당 체계의 보안성이 신뢰할 수 있는지 확인하고 대비하기 위해 보안 평가 모델이 필요하다. 보안 평가 모델은 구성요소별 취약성을 파악하고 취약성을 이용한 위협의 발생 가능성과 위협 발생 시 시스템에 미치는 영향의 정도를 결정하는 과정인 위험 분석을 통하여 해당 시스템을 평가하고 대상 시스템이 효과적으로 적용되고 있는지 파악하는 것이다[2]. 본 논문에서는 각 장비의 특성에 따라 대표적인 보안 취약성 평가 체계인 CWSS(Common Weakness Scoring System) 및 CVSS(Common Vulnerability Scoring System)와 비교한다. 가중치 기반 평가 모델, 메트릭 기반 평가 모델을 각 장비에 더 적절한 방식으로 보안 수준 평가하고 도출된 값을 통해 해당 인

* corresponding author

프라에 보안이 취약한 부분을 알 수 있어 보다 정확한 대비가 가능해질 것으로 보인다.

II. 사이버 보안 평가모델

1. CWSS(Common Weakness Scoring System)

CWSS는 소프트웨어 보안 취약점을 카테고리 형식으로 분류하고 소프트웨어 응용 프로그램 내에 존재하는 약점에 대한 정략적 측정을 시행 하여 취약점 우선 순위를 정하는 평가 모델이다[3].

2. CVSS(Common Vulnerability Scoring System)

CVSS는 소프트웨어 취약점의 특성과 심각도를 전달하는 개방형 프레임워크로 기준, 시간, 환경이라는 세 가지 메트릭 그룹으로 구성되어 있다. 매트릭은 0부터 10까지의 점수를 부여하여 해당 취약점의 심각도를 도출한다[4].

3. 기존 사이버보안 평가 모델의 문제점

CWSS는 소프트웨어의 보안 취약점을 위한 평가 방법으로 보안시스템에서의 위험평가를 하기 어려우며, 또한 CVSS 같은 경우 다면적인 변수들을 적용하여 평가를 하고 있으나, 위험도를 평가하는 것이 아닌 심각성을 평가하는 방법으로서 보안위협에 대해 위험도를 나타낼 수 없다는 단점을 가지고 있다. 또한 IT 시스템에 사용될 목적으로 개발되어 산업 시스템에 적용했을 경우 정확하지 않은 경우가 존재한다[5].

III. Risk Assessment Scoring System

보안 평가는 취약성을 파악하고 취약성을 이용한 위협의 발생 가능성과 위협 발생 시 시스템에 미치는 영향의 정도를 결정하는 과정인 위험 분석을 통하여 시스템을 평가하는 것이다. 본 논문에서는 네트워크 장비, 보안 장비의 위험 평가 모델을 제시하고 도출된 값을 통해 전체적인 위험도를 평가하는 모델을 제시한다.

그림 1은 시간당 총 이벤트와 위협 이벤트, 대응시간을 변수로 두어 네트워크 보안에 필요한 요소로 실시간으로 얻을 수 있는 정보를 기반으로 위험도를 평가함으로써 신속하게 평가를 진행할 수 있으며, 가중치 값을 포함 시켜 해당 이벤트의 위험성, 발현 구간, 목적에 따른 값을 부여해 값을 도출한다.

Risk Assessment Scoring System

m = Total Event
v = Risk Event
t = Response Time
i = Weight

$$\sum_{n=1}^{m} \frac{\left(v_m \cdot t_m \cdot i\right)}{m^2}$$

그림 1. RASS 위험 평가 모델

표 1. 위험 평가 매트릭

Level	Standard	Value
High	정보 누출이 중요한 시스템 또는 공격자가 모든 정보를 읽거나 수정, 삭제할 수 있으며 권한에 위협을 끼칠 수 있습니다.	5 이상
Medium	정보 누출이 중요한 기능에 직접적인 영향을 미치지는 않지만, 중요한 시스템을 지원하는 능력이나 중요 정보의 가독성 수준에 영향을 미칠 수 있습니다.	1.5 이상 ~ 5 미만
Low	정보 누출이 중요한 기능 및 지원 기능의 성능에 영향을 미치지 않는 수준입니다.	1.5 이하

RASS 위험평가모델에서 도출된 값은 표 1의 평가 매트릭을 통한 평가가 가능하다.

표 1의 매트릭은 Low 단계부터 High 단계까지 총 3가지 수준으로 위험도 평가가 가능한 매트릭이다. 그림 1의 RASS 위험 평가 모델을 적용했을 경우 1.5이하의 점수가 산출되면 Low 단계로 해당 수준에서는 정보 누출이 중요한 지원 기능의 성능에 영향을 미치지 않는 수준이라는 평가 결과를 도출하며, 1.5부터 5미만의 점수가 산출되면 Medium 단계로 해당 수준에서는 정보 누출이 중요한 기능에 직접적인 영향을 미치지는 않지만, 중요한 시스템을 지원하는 능력이나 중요 정보의 가독성 수준에 영향을 미칠 수 있다고 평가한다. 산출된 점수가 5 이상의 값일 경우 High 단계로 정보 누출이 중요한 시스템 또는 공격자가 모든 정보를 읽거나 수정, 삭제할 수 있으며 권한에 위협을 끼칠 수 있다는 결과가 산출된다. 위와 같이 산

출된 값을 통해 해당 시스템의 위험 수준을 파악이 가능하다.

표 2. 사이버 보안 평가 모델 비교 분석

항목		XorO
CVSS	점수 산출(Scoring)이 가능한가?	O
CWSS		O
RASS		O
CVSS	위험 수준 산출이 가능한가?	O
CWSS		O
RASS		O
CVSS	위험 측정이 가능한가?	X
CWSS		X
RASS		O
CVSS	가중치를 활용한 평가가 가능한가?	X
CWSS		O
RASS		O

III. 결론

보안 위협이 발전함에 따라 다양한 보안 모델이 구축되고 제시되면서, 보안성 평가 모델에 대한 관심도 높아지고 있다. 보안 평가 모델은 보안성 평가 결과를 통해 위험 우선순위에 따라 적절한 조치를 취하기 위해 필요한 사이버 보안 평가 방법이다. 매번 새로운 위협이 생겨나는 현재 새로운 보안 위협이 생겨날 때마다 해당 위협에 대한 더 적절한 대비가 필요 해졌다. 그러나 현재 보편화된 평가 모델인 CVSS와 CWSS는 기업 보안 평가에 적합하다고 보기 힘들다. 그렇기에 본 논문에서 기업을 대상으로 한 보안 평가에 더 유효한 RASS모델을 제시한다. 제시한 보안 평가 모델은 장비에 따른 보안 평가를 시행하고 장비의 특성에 맞는 변수와 평가 방식을 통해 기업 보안 평가에 적합한 평가가 가능하여 차후 보안 평가 모델 연구에 있어 도움이 될 것으로 보인다.

Acknowledgement

본 과제(결과물)는 2020년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.

References

[1] Ieck-Chae Euom, “A study on the cyber security assessment modeling of critical infrastructure” Journal of Digital Convergence Vol. 17. No. 8, pp. 105-113, 2019.

[2] Inkyung Kim, Namje Park, “Quantitative Cyber Security Scoring System Based on Risk Assessment Model” Journal of The Korea Institute of Information Security & Cryptology VOL.29, NO.5, Oct. 2019

[3] CWE, Common Weakness Scoring System (CWSS), http://cwe.mitre.org/cwss/

[4] Common Vulnerability Scoring System version 3.1: Specification Document [Internet]. Available : https://www.first.org/cvss

[5] CVSS score for vulnerability assessment, is this okay? [Internet]. Available : https://m.boannews.com/html/index.html