

عنوان مقاله:

A Model to Measure Effectiveness in Cyber Security Situational Awareness

محل انتشار:

مجله مهندسی کامپیوتر و دانش، دوره 7، شماره 1 (سال: 1403)

تعداد صفحات اصل مقاله: 10

نویسندگان:

.Motahareh Dehghan - Department of Industrial and Systems Engineering, Tarbiat Modares University

.AmirAbbas Mahdi Zadeh - Department of Computer Engineering, Amirkabir University of Technology

.Babak Sadeghian - Department of Computer Engineering, Amirkabir University of Technology

خلاصه مقاله:

Nowadays, the number of cyberattacks and, consequently, the risk of them is increasing significantly. So, it is vital to be aware of the cybersecurity situation. This paper provides a model to measure the success or effectiveness of the organization's security missions, that is, to determine whether security events such as the occurrence of an attack or the selection of countermeasures have been effective on the success of organizational missions. Two components are considered as inputs for this purpose. The first one is the network dependency graph which demonstrates how different assets in the network are dependent on each other and with what intensity or weight they affect each other. Another component is the mission dependency graph which specifies the relation between organizational assets, tasks, functions, and mission objectives. It also specifies the impact of the assets on the organizational tasks, functions, and mission objectives. Previous researches focused more on determining the impact of attacks on different assets. However, this paper aims to assess this impact by considering the organizational mission. This model is proposed in such a way that its components are separable. It helps different organizations with specific goals and different requirements to use this model so that they can personalize and customize its different components. This model can be employed for critical asset recognition. Moreover, it enables us to know which countermeasures are more effective in terms of the organizational mission.

کلمات کلیدی:

Measure of Effectiveness, cyberattacks, situational awareness, Impact assessment, mission, mission dependency graph, network dependency graph

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/2001141>

