

Pengembangan Metode Penilaian Risiko Keamanan Informasi Menggunakan Model Bayesian Attack Graphs (Studi Kasus: Infrastruktur Integrated Collection System Badan XYZ) = Development of Information Security Risk Assessment Method Using Bayesian Attack Graphs Model (Case Study: XYZ Agency Integrated Collection System Infrastructure)

Sulistiadi, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920525241&lokasi=lokal>

Abstrak

Integrated Collection System (ICS) merupakan sebuah sistem pengumpulan data kegiatan survei atau sensus yang dikelola oleh Badan XYZ. Melalui ICS, Badan XYZ dapat mempercepat proses kegiatan statistik tanpa mengurangi kualitas data yang dihasilkan. Akan tetapi, ICS juga mempunyai isu dalam hal keamanan informasi yaitu terdapat celah-celah kerentanan yang dapat dieksploitasi oleh suatu serangan siber. Untuk menangani permasalahan tersebut, penelitian ini bertujuan untuk mengusulkan pengembangan metode penilaian risiko keamanan informasi dengan menggunakan model Bayesian Attack Graphs (BAG). Penilaian risiko dengan menggunakan model BAG dinilai cocok untuk menilai paparan risiko pada serangan siber yang menargetkan celah kerentanan. Sebagai kontribusi keilmuan, penelitian ini mengusulkan formulasi penilaian risiko menggunakan dua faktor risiko, faktor likelihood dan faktor impact. Metrik likelihood memakai EPSS, sedangkan metrik impact memakai sub skor impact CVSS. Melalui pengembangan metode penilaian yang diusulkan, diperoleh nilai rata-rata nilai paparan risiko pada infrastruktur ICS sebesar 0.365. Dengan demikian, paparan risiko pada infrastruktur ICS berkategori Low, sehingga paparan risiko serangan berantai melalui celah-celah kerentanan pada infrastruktur ICS dapat dikatakan rendah. Dengan adanya output dari penelitian ini, model penilaian risiko melalui pengembangan model BAG dapat menilai lebih akurat suatu paparan risiko serangan siber melalui celah-celah kerentanan di suatu sistem.

.....The Integrated Collection System (ICS) is a statistics data collection system managed by XYZ Agency. Through ICS, the organization can speed up the process of statistical activities without reducing the quality of the data it produces. However, ICS also has issues in terms of information security, namely that there are vulnerabilities that can be exploited by cyberattacks. To address these problems, this study aims to propose the development of an information security risk assessment method using the Bayesian Attack Graphs (BAG) model. Risk assessment using the BAG model is considered suitable for assessing risk exposure to cyberattacks that target device vulnerabilities. As a contribution, this research proposes the formulation of a risk assessment using two risk factors, the likelihood factor and the impact factor. The likelihood metric uses EPSS, while the impact metric uses the CVSS impact sub-score. Through the development of the proposed valuation method, the average risk exposure value for the ICS infrastructure is 0.365. Thus, the risk exposure to the ICS infrastructure is in the Low category, so that the risk exposure to chain attacks through vulnerabilities in the ICS infrastructure can be said to be low. With the output of this study, the risk assessment model through the development of the BAG model can more accurately assess an exposure to the risk of cyberattacks through vulnerabilities in a system.