Pengembangan Model Cyberdisaster Situation Awareness dan Konsep Pengujian Pengendalian Risiko untuk Meningkatkan Ketahanan dan Keamanan Siber = Evelopment of Cyberdisaster Situation Awareness Model and Risk Control Testing Concept to Increase Resilience and Cyber Security

Nungky Awang Chandra, author

Abstrak

Serangan siber yang meningkat dan bervariasi membutuhkan sebuah model yang mampu meningkatkan ketahanan dan kesadaran akan ancaman serangan bencana siber. Penelitian ini mengembangkan model cyberdisaster situation awareness yang mampu menggambarkan dua tahap proses yaitu penilaian tingkat risiko ancaman bencana siber dan kerangka pengujian kerentanan keamanan siber melalui metode audit, tabletop exercise dan penetration testing. Penelitian ini menggunakan metode risiko formal fuzzy FMEA dan temporal risk. Hasil penelitian pertama menunjukan bahwa model cyberdisaster situation awareness mampu meningkatkan ketahanan keamanan siber. Model ini menggambarkan bahwa dengan metode fuzzy FMEA didapatkan nilai tingkat risiko bencana tertinggi yaitu ancaman serangan ransomware dan gempa bumi. Dari dua nilai risiko yang tertinggi tersebut dilakukan validasi faktor-faktor yang mempengaruhi tingkat kesadaran dalam menghadapi ancaman ransomware dan gempa bumi melalui survey 152 responden. Hasil survey menunjukan bahwa keputusan respon bencana siber dipengaruhi oleh faktor kapabilitas sistem ($p < 0,05$), faktor pengetahuan ($p < 0,05$), dan faktor kesadaran akan situasi bencana ($p < 0,05$). Pada penelitian kedua menunjukan bahwa kerangka pengujian kerentanan keamanan siber dengan pendekatan temporal risk dapat membantu meningkatkan ketahanan dan keamanan siber. Metode pengujian audit, tabletop exercise dan penetration testing akan menghasilkan dua klasifikasi risiko yaitu risiko yang dapat diterima (tolerable risk) dan risiko yang tidak dapat diterima (intolerable risk). Penelitian ini juga menggunakan aplikasi untuk membantu mengukur tingkat risiko keamanan siber berdasarkan Annex ISO 27001:2013. Hasil pengujian penilaian risiko dengan metode audit berdasarkan annex ISO 27001:2013 ditemukan bahwa tingkat risiko yang dapat diterima adalah akuisisi, pengembangan dan pemeliharaan sistem, dengan nilai indeks kinerja pengamanan sebesar 38.29%. Untuk hasil pengujian metode tabletop exercise dihasilkan bahwa tidak ditemukan tingkat risiko tinggi atau yang tidak dapat diterima, dengan nilai indeks kinerja pengamanan sebesar 75%. Hasil pengujian dengan metode penetration testing menunjukan bahwa risiko yang tidak dapat diterima adalah pengendalian akses dan pengamanan komunikasi, dengan nilai indeks pengendalian pengamanan sebesar 16.66%. Dari temuan kerentanan ini dilakukan tindakan perbaikan melalui aplikasi untuk meningkatkan ketahanan dan keamanan siber. Tindakan perbaikan ini menghasilkan kinerja pengamanan 100% memenuhi annex ISO 2700:2013. Kebaruan dari penelitian ini adalah konsep model kerangka cybersituation awareness yang mampu menilai risiko ancaman keamanan siber dan pengujian kerentanan pengendalian keamanan siber.

.....Cyber attacks that are increasing and varied require a model that is able to increase resilience and awareness of the threat of cyber-disaster attacks. This study develops a cyberdisaster situation awareness model that is able to describe two stages of the process, namely the assessment of the level of cyber disaster threat risk and a cybersecurity vulnerability testing framework through audit methods, tabletop exercise and

penetration testing. This study uses a formal risk method fuzzy FMEA and temporal risk. The results of the first study showed that the cyberdisaster situation awareness model was able to increase cyber security resilience. This model illustrates that with the fuzzy FMEA method, the highest level score of disaster risk is the threat of ransomware attacks and earthquakes. From the two highest risk values, validation of the factors that affect the level of awareness in dealing with the threat of ransomware and earthquakes was carried out through a survey of 152 respondents. The survey results show that cyber disaster response decisions are influenced by factors such as system capability ($p < 0.05$), knowledge factor ($p < 0.05$), and awareness of disaster situations ($p < 0.05$). The second research shows that a cybersecurity vulnerability testing framework with a temporal risk approach can help improve cyber resilience and security. The audit testing method, tabletop exercise and penetration testing will produce two risk classifications, namely tolerable risk and intolerable risk. This study also uses an application to help measure the level of cybersecurity risk based on Annex ISO 27001: 2013. The results of risk assessment with testing the audit method based on annex ISO 27001:2013 found that the acceptable level of risk is the acquisition, development and maintenance of the system, with a security performance index value of 38.29%. For the results of the tabletop exercise test method, it was found that there was no high or unacceptable risk level, with a security performance index value of 75%. And for the test results using the penetration testing method, it shows that the unacceptable risk is access control and communication security, with a security control index value of 16.66%. From the findings of these vulnerabilities, corrective actions are taken through applications to increase cyber resilience and security. These corrective actions result in 100% security performance meeting the annex ISO 27001:2013. The novelty of this research is the concept of a cybersituation awareness framework model that is able to assess cybersecurity threat risks and test cybersecurity control vulnerabilities.