Evaluasi dan strategi perbaikan kualitas keamanan infrastruktur teknologi informasi PT XYZ berbasis perluasan kerangka kerja cybersecurity capability maturity model (C2M2) = Evaluation and strategy to improve the security quality of PT XYZ's information technology infrastructure based on the framework’s expansion of the cybersecurity capability maturity M\model (C2M2)

Cyril Nugrahutama Kurnaman, author

Abstrak

Indonesia merupakan negara dengan jumlah penduduk dan pengguna internet terbesar keempat di dunia membuat kemungkinan serangan siber semakin besar. Oleh karena itu, dalam mempertimbangkan banyak potensi serangan siber yang dapat terjadi, perusahaan harus memiliki pemahaman yang mendalam tentang kualitas keamanan infrastruktur teknologi informasi (TI) yang dimilikinya. Penelitian ini mengevaluasi kualitas keamanan infrastruktur TI yang dimiliki PT XYZ saat ini dan membandingkannya dengan kualitas keamanan infrastruktur TI yang diharapkan PT XYZ menggunakan perluasan model kematangan keamanan siber yaitu Cybersecurity Capability Maturity Model (C2M2). Peneliti mengadopsi 10 (sepuluh) domain C2M2 dan 2 (dua) domain lain yang bersumber dari Center for Internet Security (CIS) Controls sehingga jumlah domain yang diuji pada model konseptual adalah 12 domain. Perluasan model ini menyesuaikan dengan kondisi dalam masa pandemi COVID-19. Metode yang digunakan dalam penelitian ini adalah in-depth interview dan kuesioner self-evaluation assessment. Data kemudian diolah dan dianalisis menggunakan gap analysis dan importance-performance analysis. Berdasarkan hasil penelitian, 10 domain C2M2 dan 2 domain CIS yang diujikan terhadap PT XYZ memiliki gaps pada Maturity Indicator Level (MIL) di masing-masing domain. Hampir seluruh domain yang diujikan berada di kuadran A pada matriks importance-performance analysis dimana tingkat kinerja rendah namun tingkat kepentingan tinggi. Skala prioritas dibuat agar PT XYZ dapat fokus memperbaiki domain yang memiliki selisih gaps besar dan tingkat kepentingan tinggi. Prioritas I atau prioritas utama domain yang harus segera dibenahi oleh PT XYZ adalah asset, change, and configuration management (ACM); identity and access management (IAM); dan event and incident response, continuity of operations (IR). Kemudian, prioritas II yaitu domain threat and vulnerability management (TVM). Lalu, prioritas III yaitu domain risk management (RM) dan situational awareness (SA). Kemudian, prioritas IV yaitu domain workforce management (WM) dan data protection (PR). Lalu, prioritas V yaitu domain information sharing and communications (ISC) dan cybersecurity program management (CPM). Terakhir, prioritas VI yaitu domain supply chain and dependencies management (EDM). Hal ini menunjukkan bahwa secara keseluruhan kualitas keamanan infrastruktur TI di PT XYZ belum mampu mengatasi risiko keamanan yang ada sehingga membutuhkan banyak perbaikan dan perlu dievaluasi secara menyeluruh.

.....Indonesia is a country with the fourth largest population and internet users in the world, making the possibility of cyberattacks even greater. Therefore, in considering the many potential cyberattacks that can occur, companies must have a deep understanding of the security quality of their information technology (IT) infrastructure. This research evaluates the security quality of PT XYZ's current IT infrastructure and compares it with the quality of IT infrastructure security expected by PT XYZ using a framework’s

expansion of Cybersecurity Capability Maturity Model (C2M2). The researcher adopted 10 (ten) C2M2 domains and 2 (two) other domains sourced from the Center for Internet Security (CIS) Controls so that the number of domains tested in the conceptual model is 12 domains. The expansion of this model adapts to conditions during the COVID-19 pandemic. The methods used in this research are in-depth interviews and self-evaluation assessment questionnaires. The data is then processed and analyzed using gap analysis and importance-performance analysis. Based on the research results, 10 C2M2 domains and 2 CIS domains tested against PT XYZ have gaps in the Maturity Indicator Level (MIL) in each domain. Almost all of the tested domains are in quadrant A in the importance-performance analysis matrix where the level of performance is low but the level of importance is high. The priority scale is made so that PT XYZ can focus on improving domains that have large gaps and high levels of importance. Priority I or the main priority domains that must be addressed by PT XYZ are asset, change, and configuration management (ACM); identity and access management (IAM); and event and incident response, continuity of operations (IR). Then, priority II is the threat and vulnerability management (TVM) domain. Then, priority III is the domain of risk management (RM) and situational awareness (SA). Then, priority IV is the domain of workforce management (WM) and data protection (PR). Then, priority V is the domain of information sharing and communications (ISC) and cybersecurity program management (CPM). Finally, priority VI is the supply chain and dependencies management (EDM) domain. This shows that the overall security quality of PT XYZ's IT infrastructure has not been able to overcome the existing security risks so that it requires a lot of improvements and needs to be evaluated thoroughly.