Perancangan Kerangka Kerja Penanganan Insiden Berbasis Teknik Forensik Digital pada Perangkat BYOD (Bring Your Own Device): Studi Kasus Pemerintah Kota Depok = Incident Handling Framework Design Using Digital Forensic Techniques on BYOD (Bring Your Own Device): Case Study of Depok City Government

Linda Rosselina, author

Abstrak

Perkembangan teknologi informasi yang semakin meningkat menyebabkan perubahan pola kehidupan masyarakat. Di lingkungan pemerintahan, pemerintah dituntut untuk dapat memberikan pelayanan terbaik dengan berbasis teknologi informasi. Interaksi yang lebih besar dengan dunia siber, tentunya akan meningkatkan potensi terjadinya insiden. Terlebih lagi pada masa pandemi ini sebagian aktivitas kerja dilakukan di rumah (Work From Home) dengan menggunakan perangkat pribadi (Bring Your Own Device). Hal ini berpotensi meningkatkan kerentanan terhadap keamanan siber. Manajemen keamanan siber yang handal sangat diperlukan agar apabila terjadi insiden siber dapat dilakukan penanganan yang tepat untuk menghindari kerugian baik material maupun non material. Salah satu kebutuhan penting dalam manajemen keamanan siber adalah kerangka kerja yang akan menjadi panduan dalam proses penanganan insiden keamanan siber yang tepat. Pada penelitian ini dilakukan perancangan kerangka kerja penanganan insiden siber dengan integrasi teknik forensik dan dibatasi pada perangkat BYOD. Forensik digital digunakan untuk melakukan investigasi sistematis dan mendokumentasikan rangkaian bukti ketika terjadi insiden. Proses investigasi yang tepat akan memberikan pemahaman insiden siber secara menyeluruh dan memberikan wawasan yang dapat dimasukkan dalam strategi keamanan siber jangka panjang. Perancangan dilakukan dengan mengacu pada standar NIST SP 800-86, NIST SP 800-61, dan ISO/ IEC 27035-1: 2016, ISO/IEC 27037: 2012, ENISA, dan SWGDE. Penelitian ini menghasilkan rancangan Kerangka Kerja Penanganan Insiden Keamanan Siber dengan menggunakan teknik forensik yang terbagi dalam tahap pre-insiden, pre-analisis, analisis, dan post-analisis. Untuk memvalidasi hasil perancangan dilakukan studi penerapan awal pada Pemerintah Kota Depok. Hasil validasi menyatakan bahwa kerangka kerja penanganan insiden dapat digunakan sebagai dasar acuan dalam penanganan insiden siber dan pembuatan petunjuk operasional selanjutnya.

.....The increasing development of information technology causes changes in the pattern of people's lives. In the government environment, the government is required to provide the best service based on information technology. More significant interaction with the cyber world, of course, will increase the potential for incidents to occur. Moreover, during this pandemic, some work activities are carried out at home (Work From Home) using personal devices (Bring Your Own Device). Using personal devices has the potential to increase vulnerabilities to cybersecurity. Reliable cybersecurity management is necessary so that proper handling can be done to avoid material and non-material losses if a cyber incident occurs. One of the critical requirements in cybersecurity management is a framework that will be a guide in the process of handling cybersecurity incidents appropriately. In this study, a cyber incident handling framework was designed to integrate forensic techniques and was limited to the BYOD device. Digital forensics is used to carry out systematic investigations and document the series of evidence when incidents occur. A proper investigation

process will provide a thorough understanding of cyber incidents and provide insights that can be incorporated into a long-term cybersecurity strategy. The design is carried out by referring to the standards of NIST SP 800-86, NIST SP 800-61, and ISO/ IEC 27035-1: 2016, ISO/IEC 27037: 2012, ENISA, and SWGDE. This study resulted in the design of a Cyber ââSecurity Incident Handling Framework using Forensic Techniques divided into pre-incident, pre-analytical, analysis, and post-analytical stages. An initial application study is needed to validate the design results conducted on the Depok City Government. The validation results state that the incident handling framework can be used to handle cyber incidents and make further operational instructions.