Analisis risiko keamanan informasi kementerian ESDM = Analysis of information security risk at ministry of energy and mineral resources.

Arief Anthadi Putera, author

Abstrak

Kementerian Energi dan Sumber Daya Mineral (ESDM) melaksanakan kegiatan pembinaan dan pengawasan minyak dan gas bumi, mineral dan batubara, energi baru terbarukan, ketenagalistrikan dan geologi. Pusat Data dan Teknologi Informasi merupakan unit organisasi pengelola sistem informasi terpusat untuk mendukung kementerian ESDM menyelenggarakan fungsi bisnis utama maupun pendukung. Hal ini mendorong Kementerian ESDM dalam memberikan keamanan dan kenyamanan pada layanan sistem elektronik untuk menjaga reputasi pelayanan publik. Saat ini terdapat beberapa sistem informasi yang tergolong kritikal mengalami kegagalan fungsi layanan sehingga menurunkan reputasi sebagai penyelenggara sistem elektronik. Peraturan menteri komunikasi dan Informatika mewajibkan penerapan manajemen keamanan informasi pada layanan sistem informasi pemerintah. Hal tersebut mendorong kementerian ESDM untuk meningkatkan pengamanan informasi karena saat ini terdapat kelemahan pengamanan informasi pada area pengelolaan risiko di kementerian ESDM. Saat ini belum ada aktivitas manajemen risiko menyeluruh di kementerian ESDM. Tujuan penelitian ini untuk melakukan analisis risiko keamanan informasi kemudian memberikan rekomendasi penanganan risiko di kementerian ESDM. Penelitian yang dilakukan adalah penelitian kualitatif dengan menggunakan studi kasus di kementerian ESDM dengan menggunakan kerangka kerja sistem manajemen keamanan informasi SNI ISO/IEC 27005:2018. Penelitian ini menghasilkan 14 risiko dengan tingkat risiko tinggi, 29 risiko dengan tingkat risiko sedang dan tujuh risiko dengan tingkat risiko rendah. Hasil analisis risiko menemukan penggunaan aplikasi perizinan tanpa otorisasi yang berdampak pada penyalahgunaan wewenang dalam penerbitan izin. Selain itu, hasil analisis risiko menemukan penurunan kemampuan perangkat lunak yang disebabkan aktivitas serangan dari eksternal karena celah kerentanan pada perangkat sistem. Penelitian ini memberikan rekomendasi rencana penanganan risiko untuk mengurangi dampak terhadap layanan maupun reputasi di Kementerian ESDM. Rekomendasi penanganan risiko diantaranya memberikan pelatihan mengenai kesadaran keamanan informasi dan rekomendasi penerapan prosedur pengujian keamanan sistem. Rekomendasi penanganan risiko keamanan informasi ini dapat digunakan untuk meningkatkan keamanan informasi di Kementerian ESDM dan memenuhi syarat dalam penerapan sistem manajemen pengamanan informasi.

The Ministry of Energy and Mineral Resources (EMR) conducts development, control and supervision activities in the fields of oil and gas, minerals and coal, renewable energy, electricity, and geology. Center for Data and Information Technology is a unit of centralized information system to support the Ministry of EMR to perform the main business and support functions. This encourages the Ministry of EMR in ensuring security in electronic system services to maintain a reputation in serving the public. Currenty, there are several information sistems that are classified as critical experiencing services malfunctions, thus lowering the reputation as an electronic system provider. Regulation of the Minister of Communication and Information that requires the implementation of information security management system in electronic

system services,therefore the Ministry of EMR needs to improve information security. Based on this, there are weaknesses on information security in the risk management area. There is currently no comprehensive risk management activity in the ministry of EMR. Therefore, this study aims to conduct an analysis of information security risks at the ministry of EMR. This research conducted was qualitative research using case studies in the ministry of EMR. This research uses an information security management system framework SNI ISO / IEC 27005. This study reveals 14 risks with high-risk levels, 29 risks with medium-risk levels and seven risks with low-risk levels. The results of the risk analysis found the use of unauthorized login applications that resulted in abuse of authority in the permits. In addition, the results of risk analysis found a decrease in software capabilities caused by external attack activity due to vulnerability in system devices. This research provides recommendations for risk management plans to reduce the impact on services and reputation in the Ministry of EMR. Risk management recommendations include providing training on information security awareness and recommendations for the implementation of system security testing procedures. These information security risk management recommendations can be used to improve information security at the Ministry of EMR and meet the requirements to the implementation of information security management.