Perancangan Kerangka Kerja Penilaian dan Mitigasi Risiko Keamanan Pada Sistem Diseminasi Terintegrasi Dengan Pendekatan STRIDE dan DREAD = Framework Design for Security Risk Assessment and Mitigation on Integrated Dissemination System Using the STRIDE and DREAD Approaches

Harry Kartono, author

Abstrak

Penerapan suatu integrasi sistem yang berisi informasi diseminasi suatu lembaga pemerintah ternyata membuka potensi ancaman yang mengganggu proses kerja sistem tersebut. Paparan risiko juga dapat mengakibatkan berhentinya sistem tersebut dalam melayani pengguna data sehingga menyebabkan kerugian baik pada lembaga yang membuat sistem tersebut maupun pengguna yang tidak bisa mengakses data yang ada dari sistem tersebut. Pengintegrasian sistem ini selain mempermudah pengguna dalam mengakses sebuah informasi juga mempercepat proses informasi tersebut diolah dan disajikan ke pengguna. Banyaknya sistem yang terintegrasi merupakan tantangan tersendiri dalam membuat saling keterhubungan dalam sistem dan juga pengamanan dari integrasi sistem tersebut. Penilaian Risiko Keamanan sangat diperlukan pada integrasi sistem ini. Pada sistem terintegrasi, metodologi untuk melakukan penilaian risiko keamanan terdiri dari 5 tahap, mulai dari dekomposisi sistem yang terdapat pada Sistem Diseminasi Terintegrasi(SDT), mengintegrasi satu komponen dengan komponen pada sistem lain, identifikasi klasifikasi ancaman menggunakan klasifikasi STRIDE, penilaian risiko dari setiap ancaman menggunakan DREAD, dan perencanaan tindakan mitigasi dari risiko tersebut tersebut. Pada penilaian risiko didapatkan risiko paling tinggi terpapar ancaman adalah komponen webserver. Pada mitigasi ancaman disarankan rutin melakukan pembaharuan perangkat lunak yang dipakai oleh tiap komponen.

.....The application of an integrated system that contains information for the dissemination of a government agency turns out to open potential threats that disrupt the work process of the system. Exposure to risk can also result in the cessation of the system in serving data users, causing losses to both the institutions that make the system and users who cannot access existing data from the system. In addition to make it easier for users to access information, the integration of this system also speeds up the process of processing and presenting this information to users. The number of integrated systems is a challenge to create interconnectedness in the system and to secure the integration of these systems. Security Risk Assessment is very necessary in the integration of this system. In an integrated system, the methodology for conducting a security risk assessment consists of 5 stages, starting from the decomposition of the system contained in the Integrated Dissemination System (IDS), integrating one component with components in other systems, identification of threat classification using the STRIDE classification, risk assessment of each threat using DREAD, and planning mitigation actions for each of these risks. In the risk assessment, it was found that the highest risk of exposure to threats was the webserver component. In threat mitigation, it is recommended to routinely update the software used by each component.