Analisis Risiko Manajemen Keamanan Layanan Internet of Things PT. XYZ Menggunakan Failure Mode and Effect Analysis Berdasarkan ISO 27002 dan COBIT 2019 = Risk Analysis Security Management of Internet of Things Services at XYZ Agency Using Failure Mode and Effect Analysis Based on ISO 27002 and COBIT 2019.

Jihar Mayangsari, author

Abstrak

ABSTRAK
PT. XYZ sebagai salah satu perusahaan telekomunikasi sedang mengembangkan model bisnis baru, yaitu Internet of Things (IoT). Koneksi perangkat IoT ke Internet dapat menjadi ancaman bagi pengguna dan penyedia layanan karena tantangan keamanan. Namun, ditengah potensi ancaman keamanan IoT, PT. XYZ sendiri belum fokus terhadap keamanan dan tidak adanya kerangka kerja tata kelola yang digunakan untuk layanan IoT mereka. Penelitian ini bertujuan untuk mengidentifikasi risiko yang terkait dengan manajemen keamanan layanan IoT di PT. XYZ. Penelitian ini menggunakan Failure Mode and Effect Analysis (FMEA) sebagai metode untuk mengidentifikasi risiko keamanan potensial pada layanan IoT dengan rekomendasi berdasarkan ISO 27002:2013 dan COBIT 2019. Data dikumpulkan dengan wawancara, observasi, studi literatur, dan kuesioner dengan total sembilan penilaian ahli. Dalam studi ini, layanan IoT dibagi menjadi tujuh domain: IoT Device dan Sensor, IoT Network, IoT Platform dan Aplikasi, People, Operations, Asset Management, dan Supplier Management. Kontribusi utama dari penelitian ini adalah untuk berkontribusi pada peningkatan kontrol keamanan dan manajemen risiko dalam layanan IoT. Hasil analisis risiko didapatkan kemungkinan 31 potensial risiko pada layanan IoT dengan 23 risiko yang membutuhkan tindakan korektif.
<hr>
ABSTRACT
XYZ agency as one of the telecommunications companies is developing a new business model, namely the Internet of Things (IoT). The connection of IoT devices to the Internet can be a threat to users and service providers due to security challenges. However, XYZ agency has not yet implemented a security framework for their IoT service. This study aims to identify the risks associated with IoT service security management at XYZ agency. This study uses Failure Mode and Effects Analysis (FMEA) as a method to identify potential security risks in IoT services with recommendations based on ISO 27002: 2013 and COBIT 2019. Data were collected by interview, observation, literature studies, and questionnaire with total 9 experts' judgement. In this study, IoT services are divided into seven domains: IoT Devices and Sensors, IoT Networks, Platforms and Applications, People, Operations, Asset Management, and Suppliers. The major contribution of this study is to contribute the improvement of security controls risk management in IoT services. The results of the risk analysis show that there are 31 potential risks in IoT services with 23 risks that require corrective action.