ANALISIS KEBIJAKAN KEAMANAN DATA PRIBADI DALAM MENYELARASKAN PERLINDUNGAN PRIVASI ADMINISTRASI PUBLIK

Oleh

Astrid Cahyani Fitri

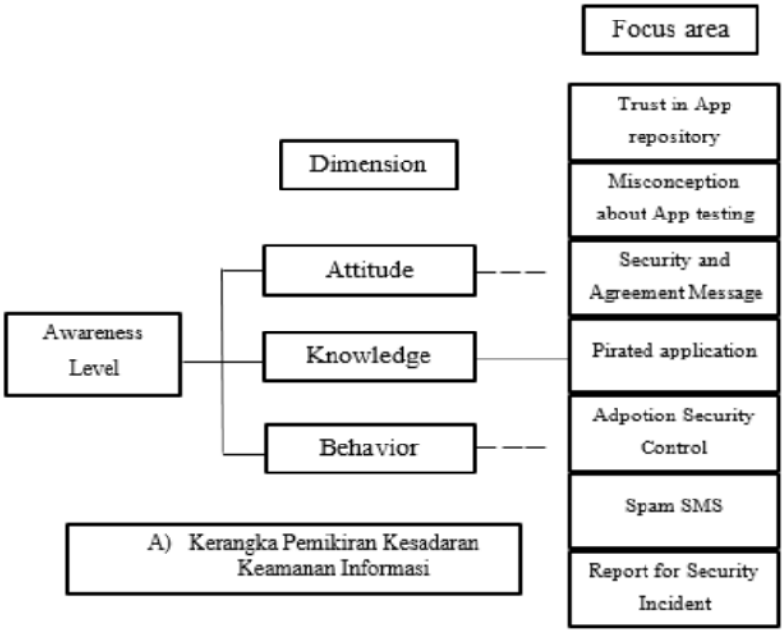
NPM : 2216041148

JURUSAN ILMU ADMINISTRASI NEGARA

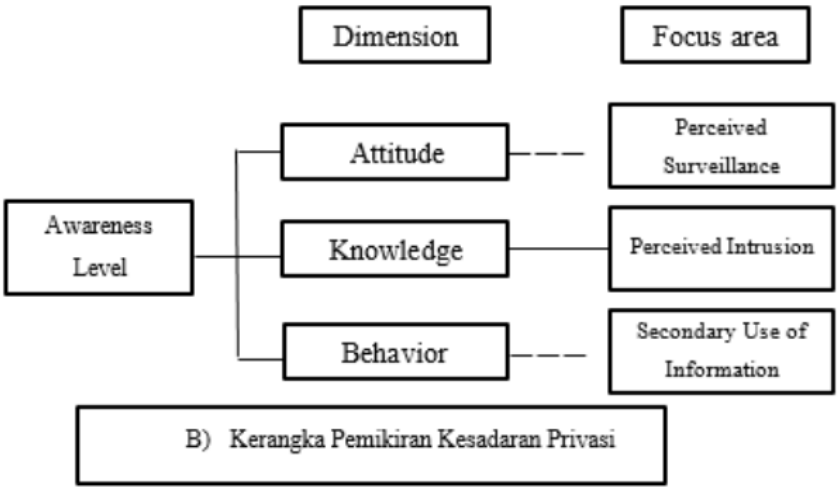
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS LAMPUNG

FISH BONE DIAGRAM



Gambar 1. Kerangka Pemikiran Kesadaran Keamanan Informasi



Gambar 2. Kerangka Pemikiran Kesadaran Privasi

BAB 3 METODE PENELITIAN

3.1 JENIS DAN PENDEKATAN PENELITIAN

Jenis penelitian yang digunakan adalah penelitian kuantitatif dimana data dikumpulkan dengan menggunakan kuesioner. Penelitian ini memiliki 42 pertanyaan dari kesadaran keamanan informasi dan 27 pertanyaan dari kesadaran privasi untuk menguji attitude, knowledge dan behavior dalam perspektif penggunaan smartphone Android. Beberapa pertanyaan dijawab dalam skala 3 poin yaitu setuju, tidak tahu dan tidak setuju (dimensi attitude dan knowledge), sementara yang lain hanya membutuhkan jawaban yang setuju atau tidak setuju (dimensi behavior).

3.2 VARIABEL PENELITIAN

Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu pengetahuan (apa yang mereka ketahui tentang keamanan dan privasi), Sikap (bagaimana perasaan mereka tentang keamanan dan privasi), Dan perilaku (apa yang mereka lakukan terhadap keamanan dan privasi) Masing-masimg dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi yaitu trust in application repository, misconception about app testing, Security and agreement message, pirated applicaion, adoption of security control spam sms dan report of security incidents dan tiga fokus area privasi yaitu perceived surveillance, perceived intrusion dan secondary use information. Untuk menguji validitas setiap item dalam kuesioner, penulis menggunakan korelasi Pearson Product Moment dimana setiap item yang memiliki koefisien korelasi sama atau lebih dari 0,3 adalah valid. Untuk pengujian reliabilitas penulis menggunakan metode Alpha Cronbach, dimana koefisiennya harus sama atau lebih dari 0,5. Sari et al. (2014) mengatakan bahwa pembobotan ditentukan dengan menggunakan analytical hierarchy process (AHP). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi subyektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen.

3.3 TEKNIK PENGUMPULAN DATA

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah Kuisioner.

1. Kuisioner
Kuisioner dilakukan karena banyaknya data yang bocor dengan memberikan beberapa pertanyaan kepada informan.
2. Studi Pustaka
Studi Pustaka dilakukan karena banyaknya informasi dan data mengenai Strategi cyber security. Hal ini dapat ditelusuri melalui berbagai informasi dalam buku, jurnal ilmiah, koran, majalah, serta sumber informasi dari laman situs/website melalui internet. Studi pustaka menjadi penting dalam menganalisa konsep strategi cyber security di Indonesia.

3.4 KERANGKA PEMIKIRAN

Kerangka pemikiran dari penilitian ini menggunakan model Krueger dan Kerney (2006) yang mengadaptasi teori psikologi sosial yang mengusulkan tiga komponen untuk mengukur cara yang menguntungkan atau tidak menguntungkan terhadap objek tertentu. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai knowledge (pengetahuan seseorang), attitude (sikap seseorang) dan behaviour (perilaku seseorang. Dimensi knowledge digunakan untuk mengetahui bagaimana pengetahuan pengguna. Sedangkan Dimensi attitude digunakan untuk mengetahui bagaimana sikap pengguna dan dimensi behaviour untuk mengetahui hal-hal yang dapat dilakukan oleh pengguna. Masing-masing dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi dan tiga fokus area privasi. Metode yang diadopsi dari model Kruger dan Kearney.

Model Krueger dan Kerney (2006) untuk mengukur tingkat kesadaran dari tiap-tiap fokus area yang lima diantaranya diadaptasi dari Mylonas et al. (2013) yaitu trust in app repository, misconception about app testing, security and agreement message, prirated application, dan adoption of security control dimana trust in app repository bisa dilihat dari rasa percaya pengguna smartphone untuk mengunduh aplikasi di toko aplikasi atau repository aplikasi yang sudah disediakan oleh sistem operasi dari smartphone yang digunakan. Lalu misconception about app testing yang bisa dilihat dari kesadaran pengguna untuk menguji aplikasi pada repositorty aplikasi. Security and agreement message yang diketahui dari kesadaran pengguna tentang persetujuan keamanan aplikasi, persetujuan lisensi, dan konsekuensi penggunaan aplikasi. Selanjutnya prirated application berupa kekhawatiran pengguna untuk menginstal aplikasi bajakan dan banyaknya aplikasi bajakan yang mengandung malware. Kemudian adoption security control yang terlihat dari kontrol keamanan yang digunakan pengguna, anti virus smartphone pengguna, adanya kehadiran virus, dan lain sebagainya.

Kerangka pemikiran kesadaran privasi juga di adaptasi dari model Krueger dan Kerney (2006) dan fokus areaya diadaptasi dari Xu et al. (2012) yang menggunakan perceived surveillance, perceived intrusion, dan secondary use of information untuk mengukur kesadaran privasi pengguna smartphone. Fokus area perceived surveillance adalah untuk mengetahui apakah perangkat lokasi yang ada di smartphone memantau kegiatan pengguna, aplikasi mobile yang dapat mengumpulkan banyak informasi pengguna menimbulkan kekhawatiran pengguna, dan aplikasi mobile pada perangkat mobile yang dapat memantau kegiatan pengguna menimbulkan kekhawatiran pengguna. Sedangkan fokus area perceived intrusion adalah untuk mengetahui apakah penggunaan aplikasi mobile menimbulkan rasa tidak nyaman bagi penggunaya, informasi pribadi pengguna yang lebih mudah tersedia untuk orang lain, dan akibat dari penggunaan aplikasi mobile. Kemudiaan untuk fokus area secondary use of information adalah untuk mengetahui apakah Aplikasi mobile dapat menggunakan informasi pribadi pengguna untuk tujuan lain tanpa izin otoritas dari pengguna, aplikasi dapat menggunakan informasi pribadi pengguna untuk tujuan lain, dan aplikasi mobile dapat berbagi informasi pribadi pengguna dengan entitas lain tanpa otorisasi pengguna. Pengukuran kesadaran privasi ini perlu dilakukan untuk mengetahui sejauh mana pengguna dapat mengendalikan informasi pribadi pengguna terhadap hak akses yang diminta oleh aplikasi mobile dan kekhawatiran penyalahgunaan informasi oleh pengembang aplikasi dan pihak ketiga.