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

2023

BAB II

1. Penelitian Terdahulu

Di era teknologi informasi ini smartphone menjadi kebutuhan untuk bisa berkomunikasi dan berbagi informasi seperti mengirim SMS atau email, entertainment, media sosial tanpa mengkhawatirkan jarak dan waktu. Menurut data yang dilansir website Statista, di awal tahun 2016, Android merupakan smartphone terpopuler dengan jumlah pengguna terbanyak di dunia, yaitu sekitar 1,8 miliar. Dilansir oleh laporan Symantec (2015), 46%, mayoritas pelanggaran yang disebabkan oleh attacker/hacker. Namun, 22% lebih dari pelanggaran diklasifikasikan sebagai "tidak sengaja dibuat publik," dan 21% adalah karena pencurian atau kehilangan komputer atau perangkatnya dan 10% adalah karena adanya keterlibatan orang dalam. Semua jenis pelanggaran data dapat dicegah jika data dienkripsi, secara efektif dapat menghilangkan dampak dari data ini jatuh ke tangan yang salah. Menurut Al-Sehri (2012), salah satu faktor yang menjadi pemicu terjadinya pelanggaran keamanan informasi dan privasi adalah karena pengguna smartphone memiliki kesadaran yang tidak memadai dalam menggunakan smartphone dengan aman, beberapa dari mereka memiliki pengetahuan yang cukup memadai dalam penggunaan smartphone tetapi mereka tidak menerapkannya dengan baik.

Menurut World Bank dalam infokomputer oleh cakrawala, berdasarkan data ITU (International Telecommunication Union), misalnya porsi pengguna internet di dunia adalah sekitar 49% populasi pada tahun 2017. Porsi tersebut meningkat pesat dibandingkan tahun 2000 yang hanya sekitar 6,7%. Serupa halnya menurut Internet World Stats yang memperkirakan porsi pengguna internet di dunia adalah sebesar 64,2% populasi pada kuartal pertama tahun 2021. Adapun jumlah pengguna internet yang diperkirakan itu adalah sebanyak lebih dari 5 miliar. Jumlah tersebut meningkat sekitar 1.300% dibandingkan tahun 2000.Tak hanya itu, jumlah serangan juga meningkat. Menurut Deep Instinct misalnya, jumlah cyber attack atau serangan siber menggunakan malware mengalami peningkatan sebesar 358% pada tahun 2020 dibandingkan tahun 2019. Sementara, khusus ransomware, peningkatannya sebanyak 435% pada tahun 2020 dibandingkan tahun sebelumnya. Adapun besarnya peningkatan yang disebutkan Deep Instinct tersebut berdasarkan basis data Deep Instinct yang menerima data dari berbagai sumber, termasuk pihak ketiga dan yang didapatkan dari konsumen Deep Instinct. Data yang dikumpulkan pun diklaim merefleksikan ratusan juta kejadian pada tahun 2020.

Secara nasional, menurut Hasyim Gautama terdapat sejumlah permasalahan terkait dengan strategi penguatan cyber security di antaranya: 1) Lemahnya pemahaman penyelenggara negara atas security terkait dengan dunia cyber yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya penggunaan secured system, 2) Legalitas penanganan penyerangan di dunia siber, 3) Pola kejadian cyber crime sangat cepat sehingga sulit ditangani, 4) Tata kelola kelembagaan cyber security nasional masih terbatas, 5) Rendahnya awareness atau kesadaran akan adanya ancaman cyber attack internasional yang dapat melumpuhkan infrastruktur vital suatu negara dan 6) Masih lemahnya industri dalamnegeri untuk memproduksi dan mengembangkan perangkat keras

atau hardware terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah keamanan dalam dunia siber [4]. Untuk di Indonesia, menurut BSSN (Badan Siber dan Sandi Negara) menyatakan sepanjang bulan Januari sampai Agustus tahun lalu, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibandingkan periode yang sama pada tahun 2019 yang sekitar 39 juta. Pada tahun 2021 ini sejumlah pihak menilai pula serangan siber belum akan mereda. Kaspersky misalnya menyebutkan bahwa pandemi COVID-19 bisa membuat munculnya berbagai gelombang kemiskinan yang kemungkinan meningkatkan kejahatan, termasuk melakukan cyber attack.Indonesia sangat membutuhkan strategi keamanan siber nasional era society 5.0 saat ini. Jika suatu keamanan sebagai kebebasan dari ancaman atau bahaya, salah satu pendorong yang terpenting dalam mengelola cyber security adalah bagaimana ancaman dipahami dalam ruang siber kemudian dicari solusinya. Tanpa upaya cyber security yang tepat, kemungkinan ancaman akan meningkat.

Tantangan terbesar saat ini adalah penguatan kelembagaan cyber security, ketidakadaan hukum untuk keamanan siber dan kurangnya tenaga professional serta kerjasama di dalam negeri maupun dengan dunia internasional. Sehingga, menjadi penting bagi pemerintah untuk penguatan cyber security dan mempersiapkan orang-orang yang dibutuhkan di dunia yang semakin digital. UU Keamanan Siber juga harus disahkan secepat mungkin untuk memulai upaya keamanan nasional Indonesia terhadap peningkatan serangan siber di era society 5.0 sekarang ini.

Berbeda dengan internet konvensional, platform mobile memungkinkan untuk real-time dan komunikasi data dan transmisi yang selalu menyala, yang menimbulkan ancaman privasi. Informasi Privasi menjadi kekhawatiran pengguna tentang kemungkinan kehilangan privasi sebagai akibat dari pengungkapan informasi kepada pihak ketiga seperti pengembang aplikasi. Teori ini memaparkan bahwa smartphone yang sangat dikenal khususnya Android merupakan sistem operasi mobile phone yang memiliki resiko yang besar, masih banyak pengguna smartphone yang belum menyadari aturan keamanan dan privasi yang harus diperhatikan dalam menggunakan smartphone. Padahal, banyak kasus-kasus terjadi seputar dampak negatif karena kurangnya kesadaran kemanan dan privasi dalam menggunakan smartphone, termasuk di Indonesia, diakibatkan oleh faktor ketidakpahaman akan keamanan informasi dan privasi ketika mendapatkan SMS/email dari orang tidak dikenal yang menyertakan link palsu yang merupakan website buatan penyerang untuk membuat smartphoneterkena serangan malware yang mengakibatkan pengambilan data secara illegal sampai rusaknya internal dari perangkat (smartphone) yang digunakan.

2. Kerangka Teori

Menurut Whitman dan Mattord (2011), keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. Menurut McLeod dan Schell (2008) keamanan informasi ditujukan untuk mencapai tiga tujuan utama, yaitu kerahasiaan ketersediaan, dan integritas . Dalam penelitian ini, keamanan informasi dibagi menajadi 7 indikator 5 diantaranya trust in application repository,

misconception about app testing, security and agreement message, pirated applicaion, dan adoption of security control (Mylonas, 2013) ditambah 2 indikator seperti spam sms dan report of security incidents (Sari et al., 2014).

Menurut Smith et al. (2011), terdapat empat definisi privasi informasi yaitu privasi sebagai hak asasi manusia, privasi sebagai komoditas, privasi sebagai keadaan akses terbatas, dan privasi sebagai kemampuan untuk mengendalikan informasi tentang diri sendiri.

Menurut Xu et al. (2012), persepsi pengguna smartphone dari sudut pandang pengawasan terhadap pengguna bisa sangat menonjol karena kegiatan pengumpulan data yang agresif oleh aplikasi mobile.

Kedua, persepsi intrusi dapat dipicu ketika aturan kepemilikan dilanggar, yaitu, ketika aplikasi mobilemampu membuat keputusan independen tentang memiliki atau meminta informasi pribadi pengguna. Dalam penelitian ini dan berdasarkan penelitian sebelumnya privasi terdiri dari tiga indikator yaitu perceived surveillance, perceived intrusion, secondary use information (Xu et al., 2012).

3. Landasan Teori

A. Teori Strategi Keamanan

Kajian keamanan telah mengalami perkembangan yang signifikan. Pemahaman konsep keamanan pasca perang dingin tidak lagi sempit sebagai hubungan konflik atau kerjasama antar negara, tetapi juga berpusat pada keamanan untuk masyarakat, kemudian Arnold Wolfers dalam Perwita & Yani mendefinisikan keamanan adalah, “security, in any objective sense, measures the absence of threats to acquired values and in a subjective sense, the absence of fear that such values will be at tacked” [5]. Sementara itu, strategi menurut John P. Lovell diartikan sebagai serangkaian langkah-langkah atau keputusan-keputusan yang dirancang sebelumnya dalam situasi kompetititf dimana hasil akhirnya tidak semata-mata bersifat untung-untungan. Strategi adalah cara yang digunakan untuk mencapai suatu tujuan atau kepentingan dengan menggunakan power yang tersedia, termasuk juga kekuatan militer [6]. Global cyber securitymenurut Arnold harus dibangun di atas lima bidang kerja: Kepastian Hukum (undang-undang cyber crime); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); capacity building dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman cyber crime terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman cyber).

B. Cyber Security Concept dalam Keamanan Nasional

Ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep “cyber security”. Karena cyber space merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi [7]. Maka konsep cyber security tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadiancaman terhadap keamanan nasional. Perkembangan teknologi informasi juga telah

memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik tapi juga meluas ke dunia maya. Konsekuensinya, negara harus beradaptasi dengan perkembangan ini, konsep keamanan dunia maya sudah saatnya ditetapkan sebagai salah satu "wilayah" negara yang menjaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan cyber tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah. Cyber security ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan urusan individual yang dihubungkan dengan teknologi, dan secara khusus dengan teknologi internet.

Terminologi "keamanan informasi (information security)" dan cyber security adalah dua konsep berbeda. Dalam konteks tertentu ada kesamaan pemahaman jika dikaitkan dengan proteksi aset atau perlawanan terhadap spionase industri dan ekonomi, perlawanan terhadap terorisme atau kejahatan ekonomi, perlawanan terhadap konten-konten terlarang. Dalam konteks lain, dua konsep tadi memiliki perbedaan. Cyber security mencakup segalasesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental. Sedangkan keamanan informasi berhubungan dengan isu-isu yang lebih luas, seperti kedaulatan negara, keamanan nasional, proteksi atas infrastruktur penting, keamanan aset-aset yang terlihat maupun yang tidak terlihat, dan proteksi data personal dan sebagainya.

C. Teori Manajemen Teknologi Informasi

Ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu: perkembangan perangkat lunak (software) seperti sistem dan aplikasi dan perkembangan alat keras (hardware) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (content management), telecommunication and networking, perkembangan internet serta perdagangan online atau melalui internet. Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: pertama, sistem informasi (information systems) dan kedua, kompetisi organisasi (organizational competition); ketiga, information systems (sistem informasi) dan organizational decision making (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan system informasi (organizational use of information systems).

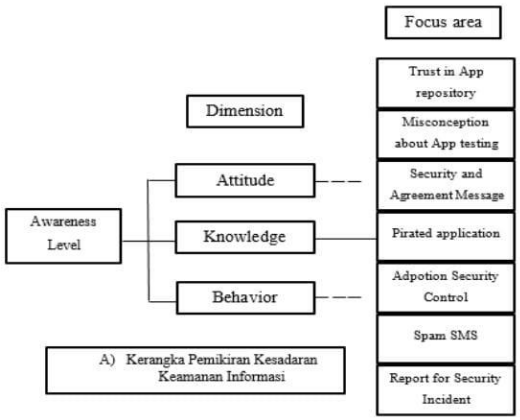
D. Teori Cyber Attack

Malware adalah setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses, serta menimbulkan bahaya terhadap atau merusak system. Dalam cyber attack, selain virus, terdapat beberapa jenis serangan malware antara lain: (1) Spyware yang melacak aktivitas, pengumpul penekanan tombol, dan pengambilan data, (2) Adware dirancang untuk menampilkan iklan namun juga ditemukan membawa spyware, (3) Bot yang dirancang otomatis melakukan tindakan tertentu secara online, (4) Ransomware yang mengenkripsi data di komputer dengan kunci yang tidak diketahui oleh pengguna [9]. Jenis-jenis malware inilah yang dimanfaatkan sehingga mempengaruhi karakteristik di ruang siber. Menurut Undang-Undang[10], karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti

Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar beberapa hal yakni kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau

permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja.

4. Kerangka Berpikir



Gambar Kerangka Pemikiran Kesadaran Keamanan Informasi

Kerangka pemikiran kesadaran keamanan informasi pada Gambar dengan menggunakan 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 kontrol keamanan yang digunakan pengguna, anti virus smartphone pengguna, adanya kehadiran virus, dan lain sebagainya. Adapun dua fokus area lainya dari kerangka pemikiran kesadaran keamanan informasi pada Gambar yang diadaptasi dari Sari et al. (2014) yaitu spam sms dan report for security incident. Ketujuh fokus area yang telah disebutkan di atas, digabungkan bertujuan agar penelitian lebih konprehensif untuk mengukur kesadaran kaamanan informasi.

Referensi :

Al-Sehri, 2012. Information security awareness and culture, British Journal of Arts and Social Sciences; 6(1): 61-69.

Gemalto, 2015. Information Security Threat Annual Reports. Gemalto Corporation. 2015; 43.

IDCERT, 2015. Laporan Dwi Bulan I 2015. Indonesia Computer Emergency Response.

McLeod, Raymond & Schell, George P. 2008. Sistem Informasi Manajemen, Edisi 10. Jakarta: Salemba Empat.

Kruger, H.A., & Kearney W., D., 2006. A prototype for assessing information security Awareness. Computer & Security Volume 25 : 289-29.

Mylonas, A., Kastania, A., Gritzalis, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. Computer & Security Volume 34 : 47-66.

Sari, Kencana, P., Candiwan, 2014. Measuring Information Security Awareness of Indonesian Smartphone.Users.TELKOMNIKA..Vol.12,No.2,June 2014,pp.493-500.