BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era saat ini teknologi informasi terus berkembang yang kini menjadi kebutuhan untuk dapat berkomunikasi dan memperoleh berbagai informasi di internet. Menurut Gemalto, pengguna teknologi menduduki peringkat keempat sejumlah 12 % yang memiliki jumlah kasus pelanggaran sebanyak 84.394.833 laporan. Data dari Indonesia Computer Emergency Response Team (IDCERT) , terhitung dari bulan januari hingga februari 2015 mendapat laporan sebanyak 30,99% kejahatan Spam, 15,67% tindakan hak kekayaan intelektual, 4,35% kejahatan spoofing/phising, 3,98 kejahatan network incident, dan 3,18% kejahatan malware [2].

Berdasarkan laporan Symantec[8] terdapat berbagai pelanggaran sejumlah 46% disebabkan oleh attacker/hacker. Jenis pelanggaran yang banyak ditemukan adalah malware yang ditemukan pada sistem operasi Android dan tingkat kejahatan yang disebabkan oleh malware terus bertambah dari tahun 2011 dengan jumlah 71 jenis malware menjadi 174 jenis malware pada tahun 2012, 231 jenis malware di tahun 2013, 277 jenis malware pada tahun 2014, hingga tahun 2015 menjadi 295 jenis malware dan tidak menutup kemungkinan jumlah pelanggaran malware akan terus

malware dan tidak menutup kemungkinan jumlah pelanggaran malware akan terus bertambah setiap tahunnya. Namun dari total 46% tersebut terdapat 22% lebih pelanggaran yang digolongkan sebagai "tindakan tidak sengaja" , 21% adalah tindakan pencurian atau kehilangan komputer atau perangkatnya, dan sisa 10% adalah karena adanya campur tangan orang dalam [3].

Pada sebuah perusahaan mengalami pelanggaran kejahatan bisa menjadi suatu bencana karena kejahatan tersebut terkait dengan data bisnis internal seperti daftar inventaris perusahaan dan riwayat transaksi. Menurut Whoa.com terdapat 5 penyebab pelanggaran keamanan yang sering terjadi pada perusahaan-perusahaan yang umum terjadi. Penyebab yang pertama adalah membiarkan kerentanan keamanan yang kurang diperhatikan atau diperbaiki sehingga dengan mudahnya attacker memiliki akses bebas ke dalam perusahaa. Contohnya menurut Verizon's 2015 Data Breach Investigations Report terdapat 99,9% dari kerentanan keamanan yang dapat dieksploitasi dan dipilih

suatu kerentanan tersebut untuk menjadi acuan attacker dimasa mendatang. Pelanggaran keamanan juga dapat disebabkan oleh kesalahan manusia (Human Error). Menurut data statistik dari studi Comp TIA yang dikutip oleh SHRM.org " Kesalahan

yang disebabkan oleh manusia berjumlah 52% dari total semua penyebab pelanggaran keamanan". Kesalahan manusia bisanya disebabkan oleh orang dalam itu sendiri yang disengaja oleh seseorang yang berwenang untuk mendapatkan keuntungan pribadi. Menurut DBIR 2015 Verizon 2015 [13] bahwa tujuan dari kejahatan yang dilakukan oleh orang dalam adalah untuk mendapatkan keuntungan pribadi berupa keuntungan finansial dan menjadi motivator utama. Namun banyak kesalahan manusia dapat dicegah dengan upaya memastikan karyawan tersebut mengetahui informasi-informasi dasar mengenai keamanan informasi dan dilakukanya pemeriksaan forensik perangkat pengguna setelah seseorang tersebut meninggalkan tempat kerjanya. Pada dasarnya untuk menghentikan atau mencegah penyalahgunaan oleh orang dalam hampir tidak mungkin namun suatu pelanggaran dapat dikurangi melalui pembagian informasi di jaringan atau cloud masing-masing. Semakin sedikit jumlah file dan sistem yang dapat diakses oleh seorang pengguna maka semakin sulit untuk menyalahgunakan akses. Penyebab keamanan lainnya disebabkan oleh aktivitas malware yang sangat mengkhawatirkan karena aktivitas malware dapat terjadi 5 aktivitas setiap detiknya dan telah berjumlah 70% hingga 90% menurut Verizon DBIR. Penyebab keamanan yang terakhir dan paling sering ditemukan adalah pencurian pada perangkat keras yang menyimpan informasi terkait perusahaan. Pencurian pada perangkat keras seperti laptop, monitor, smartphone, tablet, hard drive, thumb drive, CD & DVD, dan server tetapi pencurian tersebut sangat tergantung pada informasi yang disimpan pada perangkat kerasnya. Menurut laporan Verizon bahwa kebanyakan dari pencurian terjadi pada area ruang kerja korban sendiri dan kejadian tersebut berjumlah 55% . sebagian besar pencurian ini susah diprediksi dan kadang menjadi hal yang tidak terduga. Solusi terbaik adalah harus rutin mengurangi kesempatan untuk menghapus prangkat penyimpanan data dari situs kerja [6].

Penyebab terjadinya pelanggaran keamanan informasi adalah karena banyak dari pengguna teknologi informasi yang kurang memiliki kesadaran untuk menjaga keamanan informasi atau pun terdapat beberapa yang mengetahui cukup dalam

penggunaan smartphone namun jarang mereka untuk menerapkannya dengan baik. Salah satu usaha yang dapat dilakukan agar pengguna smartphone memiliki kesadaran adalah dengan memberikan pengetahuan berupa keamanan informasi sederhana. Salah satu pelatihan atau penyuluhan mengenai kesadaran keamanan informasi adalah dengan presentasi Pendidikan, pesan yang disebarkan melalui email secara acak, mengadakan grup dialog atau sharing dengan teman, keluarga, atau komunitas, lalu dapat juga melalui poster, berita di artikel, dan video [5].

Permasalahn dalam penelitian ini adalah mengenai tingkat kesadaran keamanan informasi bagi masyarakat namun pada penelitian ini hanya difokuskan kepada mahasiswa di Fakultas Teknologi Industri Universitas Trisakti. Penelitian tingkat kesadaran keamanan informasi menggunakan metode pengukuran hasil data yang terkumpul menggunakan level of awareness. Penulis melakukan penelitian tingkat

kesadaran keamanan informasi berdasarkan aspek Knowledge (Pengetahuan), Attitude (Sikap), Behaviour (Perilaku) yang diajukan dengan menggunakan kuesioner berupa pertanyaan berdasarkan 3 aspek tersebut. Maka dari itu diperlukan analisa knowledge, attitude, dan behaviour menggunakan pengukuran Level of awareness [3].

Berdasarkan latar belakang diatas, maka penulis melakukan penelitian yang berjudul "Faktor Penentu Tingkat Kesadaran Keamanan Informasi Mahasiswa Fakultas Teknologi Industri Universitas Trisakti"

1.2 Rumusan Masalah

Berdasarkan latar belakang yang saya sampaikan diatas, maka rumusan masalah dalam penelitian ini adalah bagaimana rangcangan peningkatan kesadaran keamanan informasi di Fakultas Teknologi Industri Universitas Trisakti.

1.3 Batasan Masalah

Agar tugas akhir ini dapat mencapai sasaran dan tujuan yang diharapkan, maka batasan masalah sebagai berikut :

1. Melakukan penelitian menggunakan kuesioner kepada mahasiswa di Fakultas Teknologi Informasi Universitas Trisakti.

2. Penelitian yang dilakukan penulis dinilai dari tigas apek yang terdapat dalam Information Security Awareness (ISA) yaitu Knowledge (Pengetahuan), Attitude (Sikap), Behaviour (Perilaku).
3. Teknik Sampling yang digunakan adalah simple random sampling.
4. Pengolahan data menggunakan program SPSS versi 25.0.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini, yaitu :

1. Menganalisa tingkat kesadaran seorang pengguna smartphone menggunakan pendekatan ISA dengan aspek Knowledge (Pengetahuan), Attitude (Sikap), Behaviour (Perilaku).
2. Mengetahui tingkat kesadaran seorang pengguna terhadap keamanan informasi.

1.5 Manfaat Penelitian

Manfaat dilakukanya penelitian ini, yaitu ;

1. Dapat mengetahui tingkat kesadaran pengguna smartphone dari segi aspek Knowledge (Pengetahuan), Attitude (Sikap), Behaviour (Perilaku).
2. Dilakukannya penelitian dapat digunakan sebagai dasar untuk menambah pengetahuan, mengembangkan kebijakan pada bidang keamanan informasi pada pemakaian smartphone.
3. Penelitian ini diterapkan pada mahasiswa aktif di Fakultas Teknologi Informasi Universitas Trisakti agar memberikan informasi mengenai tingkat keamanan

informasi sehingga mahasiswa dapat berkembang dan selalu menjaga keamanan informasi mengenai data-data pribadi.

4. Penulisan tugas akhir ini diharapkan dapat menjadi sarana dalam menerapkan kesadaran keamanan informasi penulis yang telah diterima selama perkuliahan dan menambah wawasan bagi penulis.

1.6 Sistematika Penyusunan

Dalam melaksanakan Tugas Akhir ini, tahap tahap yang dilakukan penulis adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penelitian yang digunakan dalam penelitian.

BAB 2 TEORI DASAR

BAB 2 TEORI DASAR

Bab ini berisi teori dasar yang sesuai dengan penelitian Tugas Akhir.

BAB 3 METODOLOGI PENELITIAN

Bab ini berisi metode yang digunakan dalam penelitian. Metode ini dimulai dari mendefisinikan masalah, rancangan instrument, teknik sampling, pengumpulan data, pengolahan data, analisis dan kesimpulan.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini berisi hasil pengujian, analisis data, dan rancangan pembinaan kesadaran keamanan informasi.

BAB 5 PENUTUP

Bab ini berisi kesimpulan dan saran dari hasil penelitian yang telah dilakukan.

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti
Devi Febrita Sari Hoesadha, 2021